Geometry of Banach Spaces: A New Route Towards Position Based Cryptography

Marius Junge[1]**, Aleksander M. Kubicki**[2] **, Carlos Palazuelos**[2,3]**,
David Pérez-García**[2,3]

[1] Department of Mathematics, University of Illinois, Urbana, IL 61801, USA. E-mail: mjunge@illinois.edu
[2] Departamento de Análisis Matemático y Matemática Aplicada, Universidad Complutense de Madrid, 28040 Madrid, Spain. E-mail: amkubickif@gmail.com
[3] Instituto de Ciencias Matemáticas, 28049 Madrid, Spain. E-mail: cpalazue@ucm.es; dperezga@ucm.es

Abstract: In this work we initiate the study of position based quantum cryptography (PBQC) from the perspective of geometric functional analysis and its connections with quantum games. The main question we are interested in asks for the optimal amount of entanglement that a coalition of attackers have to share in order to compromise the security of any PBQC protocol. Known upper bounds for that quantity are exponential in the size of the quantum systems manipulated in the honest implementation of the protocol. However, known lower bounds are only linear. In order to deepen the understanding of this question, here we propose a position verification (PV) protocol and find lower bounds on the resources needed to break it. The main idea behind the proof of these bounds is the understanding of cheating strategies as vector valued assignments on the Boolean hypercube. Then, the bounds follow from the understanding of some geometric properties of particular Banach spaces, their type constants. Under some regularity assumptions on the former assignment, these bounds lead to exponential lower bounds on the quantum resources employed, clarifying the question in this restricted case. Known attacks indeed satisfy the assumption we make, although we do not know how universal this feature is. Furthermore, we show that the understanding of the type properties of some more involved Banach spaces would allow to drop out the assumptions and lead to unconditional lower bounds on the resources used to attack our protocol. Unfortunately, we were not able to estimate the relevant type constant. Despite that, we conjecture an upper bound for this quantity and show some evidence supporting it. A positive solution of the conjecture would lead to stronger security guarantees for the proposed PV protocol providing a better understanding of the question asked above.

Contents

1. Introduction

In the field of position based cryptography (PBC) one aims to develop cryptographic tasks using the geographical position of a third party as its only credential. Once the party proves to the verifier that it is in fact located at the claimed position, they interact considering the identity of the third party as granted. Basing cryptographic security on the position of the communicating parties might be very appealing in practical contexts such as the use of autonomous cars (see [1] for an interesting digression on this topic), or the secure communication between public services or banks. Besides that, at a more fundamental level, secure PBC could also serve as a way to circumvent insecurity under man-in-the middle attacks, a security leak suffered by standard cryptographic primitives. This vulnerability still prevails even in presence of information-theoretical security, as, for example, in the celebrated case of Quantum Key Distribution. In these settings, the security guarantees always come after the assumption that the identity of the trusted agents is granted. In PBC this assumption can be, at least, relaxed. Moreover, PBC proved to be a rich field of research emanating deep questions and connections from its study. To mention a few, attacks for PBC has been related with quantum teleportation [2], circuit complexity [3], classical complexity theory [4] and, very recently, with properties of the boundary description of some processes in the context of the holographic duality AdS/CFT [5,6]. In this work, we add to this list a connection with deep questions on the geometry of Banach spaces.

The main task in PBC is the one of *Position Verification* (PV). In PV a prover has to convince a verifier (usually composed by several agents spatially distributed) that it is located at a claimed position. This setting has been studied since the 90's in the context of classical cryptography. Nonetheless, in purely classical scenarios, PV is easily proven to be insecure against a team of colluding adversaries surrounding the honest location [7]. This motivates the study of *quantum* PV protocols, in which the communication between prover and verifier is in general quantum. This idea was initially developed by Kent [8] and made rigorous only later on in [9]. In this last paper, the authors construct

a generic attack for any quantum PV protocol. To construct the general attack of [9], the authors built on the work of Vaidman [10], realizing that the cheating action in the setting of PV consists in performing what they called *instantaneous non-local computation*. In this last task, two (or more) distant agents have to implement a quantum operation on a distributed input when subjected to non-signalling constraints—see [9] or Sect. 2.2 below for more details. At a first sight, the existence of general attacks to quantum PV renders the development of secure PBQC a hopeless program. However, their attack did not come for free for the adversaries, as in the case of classical PV. On the contrary, in order to cheat, the dishonest agents have to use a huge amount of entanglement—a delicate and expensive resource in quantum information processing. Even when in [2] another generic attack to PV was proposed exponentially reducing the entanglement consumption, the amount of entanglement required is still far from what is realizable in any practical situation. This leads naturally to the following question, which is the one motivating this work:

Question 1. How much entanglement is necessary to break *any* PV protocol?

Answering this question with a large enough lower bound would lead to the existence of PV protocols which are *secure for all practical purposes*, term coined in [4]. More concretely, we say that a PV protocol is secure for all practical purposes if the resources needed to break it are significantly larger in order of magnitude than the resources manipulated by the honest parties. For us, the size of the resources in place is quantified by the dimension of the systems that are manipulated in the execution of the protocol. In a hypothetical future in which we have at our disposal large scale quantum computers, there is no clear reason to distinguish between classical and quantum resources and solving Question 1 in this sceptical setting is the final goal in the study of PBC. However, as an intermediate step towards this aim, we focus here in the study of quantum resources disregarding classical communication and computation as free resources (for both, honest and dishonest agents). We hope that the study of this scenario will contribute to the ultimate understanding of Question 1. Indeed, some of the results presented here can be translated to the sceptical framework described above. Although we will say a few words about how this is achieved in Sect. 1.1, a full study of this more ambitious setting is out of the scope of the present manuscript.

We comment now on the progress in the field that is already available. In [9], the authors provide the first PV protocol secure against cheaters with *no* entanglement. This was improved in [2] and later in [11] providing PV protocols requiring a linear amount of entanglement (linear in the size of the system manipulated in the honest protocol). In terms of this figure of merit, the entanglement consumption in the generic attack of [2] is exponentially large, hence leaving an exponential gap between lower and upper bounds for the amount of entanglement necessary to break PV protocols. After almost 10 years since [9] this is still essentially all it is known about Question 1 in its original formulation. Other works have studied attacks with some specific structure [4], have designed attacks that are efficient at emulating the computation of unitaries with low complexity [3] or have studied security under additional cryptographic assumptions [12].

After the completion of this manuscript we learnt about the concurrent work [13] which studies a similar setting as the one considered in this work, focusing on the trade-off between the *quantum* resources used by the honest party in comparison with the *quantum* resources of the attackers. In that work, the authors show the existence of qubit routing protocols in which the honest prover is required to manipulate a single qubit and a $2n$-bits classical string and are secure against adversaries sharing an entangled state of dimension linear in the dimension of the classical message. In the intermediate setting

commented on before, when the focus is put on the study of quantum resources, the results reported in [13] are incomparably stronger than the results we obtain here. However, in order to contrast both works, we mention that while in [13] the classical part of the challenge is required to be distributed symmetrically from both sides of the prover— considering PV in a one-dimensional line—, in our setting the classical information is distributed asymmetrically only from one of the verifiers surrounding the honest location. This can be understood as a further step in-between the intermediate setting in which classical resources are completely disregarded and the final goal of finding *secure for all practical purposes* PV protocols. Stressing this point, we emphasize that the techniques and ideas we introduce here might serve as groundwork for a deeper study of the problem. In fact, as we said before, it is possible to extend some of our results to protocols in which the interaction between verifiers and prover is purely quantum and, in overall, of much lower dimension(with no distinction between classical and quantum systems). We leave for the future the study of such ramifications of our work. For completeness, we also mention that another possibility to achieve the goal of *security for all practical purposes* in PV would be improving the bounds obtained in [13]. Known attacks to the protocols proposed there consume exponentially more resources than the lower bounds of [13], a fact that invites to explore the pointed direction. Nevertheless, it seems that new techniques have to come into play for pursuing that aim.

1.1. Summary of results. Here we aim to go back to Question 1 in its simplest form: the one-dimensional case without any further assumptions. Unfortunately, we were not able to find a definite answer to the question but we report here some progress that opens an avenue for a deeper understanding of the problem.

From now on, we focus on the study of *quantum* resources required to attack PV, considering classical communication as a free resource and unlimited computational power for all the agents involved. In this work,

- we connect the study of Question 1 with powerful techniques coming from Banach space theory,
- consequently providing new lower bounds on the amount of entanglement necessary to break a specific PV protocol presented in Sect. 3. However, these bounds are not completely general but depend on some properties of the strategies considered. Intuitively, *smooth* strategies, i.e., strategies with a smooth dependence in the unitary to be implemented, lead to exponential lower bounds.
- Finally, we consider the possibility of turning the previous bounds unconditional. We relate the validity of this with a collection of open problems in local Banach space theory. In particular, we relate the bounds on resources to break our PV protocol with estimates for type constants of tensor norms of ℓ_2 spaces. In this direction, we put forward a conjecture that would imply the desired unconditional exponential lower bounds and then provide some evidence supporting it.

The protocol G_{Rad}. To formalize this discussion, we propose a PV protocol that we denote G_{Rad}. This makes reference to a family $\{G_{\mathrm{Rad}}^{(n)}\}_{n \in \mathbb{N}}$ rather than to a single task. The index n represents a security parameter that determines the size of the quantum systems manipulated in the honest implementation of the protocol. From now on, this parameter will be implicitly referred to, allowing us to drop the superindex in $G_{\mathrm{Rad}}^{(n)}$ and refer to it simply as G_{Rad}.

The general structure of a PV protocol in the studied setting—one-dimensional PV— proceeds in four basic steps (see Fig. 1, left panel, for a graphical description):
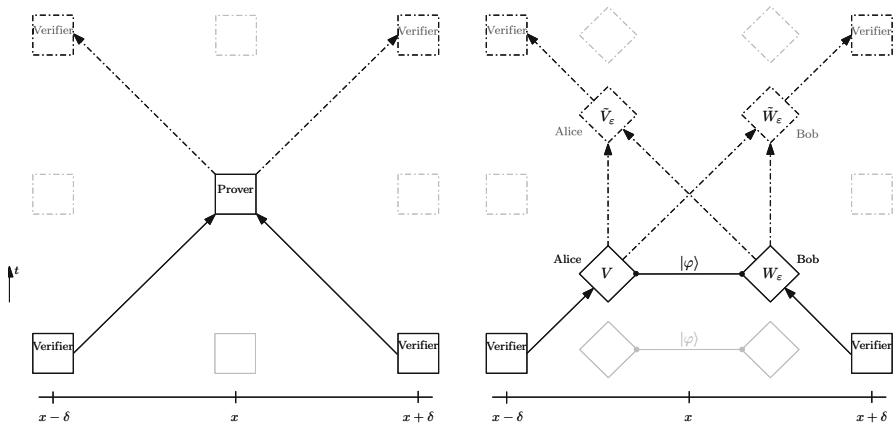
Fig. 1. Causal structure of one-dimensional PV protocols. Honest implementation (left) versus adversarial scenario (right)

1. The verifier prepares a bipartite system and distributes it to two verifying agents that surround the location to be verified, x. For the sake of concreteness, we locate these agents at points $x \pm \delta$ for some positive δ.
2. Agents at $x \pm \delta$, when synchronized, communicate the registers they hold to x.
3. An honest prover located at x, upon receiving both registers, immediately applies a required computation resulting in another bipartite system. The latter has to be returned to locations $x \pm \delta$. One register should be sent to the agent at the left of x ($x - \delta$), and the other, to its right ($x + \delta$).
4. Finally, the verifiers check whether the prover's answer arrives on time and whether the computation was performed correctly. Based on this information they declare the verification successful or not.

In the dishonest scenario, two cheaters surrounding the location x intercept the communication with the honest prover and try to emulate the ideal action in the honest protocol. In order to succeed, they have to prevent any delay in their response. This restricts cheaters' action to consist of two rounds of local operations mediated by a step of *simultaneous two-way communication*—see Sect. 2.2 for a detailed discussion of this model.

Once we have fixed this basic setting, let us describe the protocol G_{Rad} involved in our main results. Roughly speaking, the challenge posed to the prover in our protocol is solved by the implementation of the set of diagonal unitaries determined by sign vectors $\varepsilon \in \{\pm 1\}^{n^2}$. The intuition behind the choice of this set of unitaries can be supported by the fact that it contains instances with exponential circuit complexity, as a simple counting argument shows. Furthermore, in [14] we noticed that this set of unitaries is almost as hard as possible in terms of the memory required by a Programmable Quantum Processor that implements it. Since Programmable Quantum Processors seem to be closely related with the existing teleportation based attacks to PV [2,9], we found the previously noted fact an indication that the referred set of unitaries might be a good choice for the study of PV. More formally, the honest implementation of G_{Rad} is as follows:

1. the verifiers start uniformly sampling $\varepsilon = (\varepsilon_{ij})_{i,j=1}^n \in \{\pm 1\}^{n^2}$ and preparing the state $|\psi\rangle := \frac{1}{n} \sum_{i,j=1}^n |i\rangle_A \otimes |j\rangle_B \otimes |ij\rangle_C$ in a tripartite Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C$.

The verifying agent at $x - \delta$ receives registers $\mathcal{H}_A \otimes \mathcal{H}_B$ while the one at $x + \delta$ is informed (classically) of the choice of ε. Register $\mathcal{H}_C$ is kept as private during the execution of the protocol.

2. Then, registers $\mathcal{H}_A \otimes \mathcal{H}_B$ are forwarded to the verifying location x from its left. From the right, the classical information about the choice of ε is communicated.

3. An honest prover located at x, upon receiving both pieces of information, has to apply the diagonal unitary on $\mathcal{H}_A \otimes \mathcal{H}_B$ determined by ε. Immediately, registers $\mathcal{H}_A \otimes \mathcal{H}_B$ must be returned, but this time only $\mathcal{H}_A$ should travel to the verifier at $x - \delta$. Register $\mathcal{H}_B$ should be sent to the verifier at $x + \delta$.

4. After receiving those registers, the verifiers check the answer's timing and, at some later time, they perform the measurement $\{|\psi_\varepsilon\rangle\langle\psi_\varepsilon|, \mathrm{Id} - |\psi_\varepsilon\rangle\langle\psi_\varepsilon|\}$ on system $\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C$, where $|\psi_\varepsilon\rangle := \frac{1}{n} \sum_{i,j} \varepsilon_{ij} |i\rangle_A \otimes |j\rangle_B \otimes |ij\rangle_C$. They accept the verification only if the arriving time was correct and the outcome of the measurement was the one associated to $|\psi_\varepsilon\rangle\langle\psi_\varepsilon|$.

Next, let us specify the implementation of G_{Rad} in an adversarial scenario. In this situation, we consider that two cheaters located between the honest location x and the verifying agents at $x \pm \delta$, intercept the communication in the honest protocol. In this work, we refer to these cheaters as Alice, at position $x - \delta'$, and Bob, at position $x + \delta'$, for some $0 < \delta' < \delta$. Their general action proceeds as follows[1] (see again Fig. 1 for clarification): in advance, the cheaters share a state $|\varphi\rangle$ in which Bob, after receiving the information about ε, applies an isometry W_ε and sends part of the resulting system to Alice together with the classical information determining ε. On her part, when Alice receives registers $\mathcal{H}_A \otimes \mathcal{H}_B$ of $|\psi\rangle$, she applies another isometry V (independent of ε) on these registers and her part of the shared state $|\varphi\rangle$. Part of her resulting system is communicated to Bob. After this step of simultaneous two-way communication Alice and Bob are allowed to apply another pair of local isometries $\tilde{V}_\varepsilon \otimes \tilde{W}_\varepsilon$ on the systems they hold. Then, they have to forward an answer to agents at $x \pm \delta$.

Main results. The structure of G_{Rad} allows us to understand cheating strategies as vector valued assignments on the n^2-dimensional boolean hypercube, $\mathcal{Q}_{n^2} = \{\pm 1\}^{n^2}$. In our main result, we find lower bounds for the resources consumed in such an attack depending on the *regularity* of the former assignment. Very informally, we can state:

Cheating strategies depending on the value of $\varepsilon \in \{\pm 1\}^{n^2}$ in a sufficiently regular way require an amount of entanglement exponential in n in order to pass G_{Rad}.

To quantify the regularity of a strategy we introduce a parameter σ that can be regarded as a measure of the *total influence* of the associated function on the Boolean hypercube. We give a precise definition for this parameter in Sect. 4. Here, we restrict ourselves to give an intuitive idea behind this definition presenting some approximate expressions below. Based on two complementary ideas, given a strategy we construct two different assignments leading to two parameters σ^i and σ^{ii}. Given a cheating strategy $\mathcal{S}$, characterized by a sequence of elements $\{\tilde{V}_\varepsilon, \tilde{W}_\varepsilon, V, W_\varepsilon, |\varphi\rangle\}_{\varepsilon \in \mathcal{Q}_{n^2}}$, we can bound, up to logarithmic factors:

---

[1] For simplicity, we state here the case in which Alice and Bob use what we call *pure* strategies. The most general case can be reduced to this one by purification. See Sect. 3 for a detailed discussion.

$$\sigma^i \lesssim_{\log} \mathbb{E}_\varepsilon \left(\sum_{i,j} \frac{1}{2} \left\| \tilde{V}_\varepsilon \otimes \tilde{W}_\varepsilon - \tilde{V}_{\bar{\varepsilon}^{ij}} \otimes \tilde{W}_{\bar{\varepsilon}^{ij}} \right\|^2 \right)^{1/2} + O\left(\frac{1}{n} \right), \qquad (1)$$

$$\sigma^{ii} \lesssim_{\log} \mathbb{E}_\varepsilon \left(\sum_{i,j} \frac{1}{2} \left\| \left(V \otimes (W_\varepsilon - W_{\bar{\varepsilon}^{ij}}) \right) |\varphi\rangle \right\|_{\ell_2}^2 \right)^{1/2} + O\left(\frac{1}{n} \right), \qquad (2)$$

where $\| \cdot \|$ and $\| \cdot \|_{\ell_2}$ are the operator and euclidean norms respectively. Here, $\bar{\varepsilon}^{ij}$ denotes the sign vector $(\varepsilon_{11}, \ldots, -\varepsilon_{ij}, \ldots, \varepsilon_{nn})$. The first of these parameters is therefore related with how strongly the *second round of local operations* in the strategy depends on ε. In the other hand, σ^{ii} is similarly concerned with the dependence on ε of the *first round of local operations*. With this at hand, we can state—yet informally—our main result. Denoting the success probability attained by a strategy $\mathcal{S}$ in G_{Rad} as $\omega(G_{\mathrm{Rad}}; \mathcal{S})$, we can say that:

Theorem 1.1 (Informal). *Given a cheating strategy for G_{Rad}, $\mathcal{S}$, in which the local dimension of the quantum systems manipulated by the cheaters during its execution is at most k,*

I.

$$\omega(G_{\mathrm{Rad}}; \mathcal{S}) \leq C_1 + C_2 \, \sigma^i \, \log^{1/2}(k) + O\left(\frac{1}{n^{1/2}} \right);$$

II.

$$\omega(G_{\mathrm{Rad}}; \mathcal{S})$$
$$\leq \tilde{C}_1 + C_3 \, \sigma^{ii} \, n^{3/4} \log^{3/2}(nk) + O\left(\frac{1}{n^{1/2}} + \frac{\log^{3/2}(nk)}{n} \right);$$

where C_1, $\tilde{C}_1 < 1$, C_2, C_3 are positive constants.

What this theorem tells us is that cheating strategies for G_{Rad} for which σ^i or σ^{ii} are small enough necessarily need to make use of quantum resources of size exponential in a power of n, (loosely) matching the exponential entanglement consumption of known attacks[2]. We give a more concrete statement in the form of a corollary:

Corollary 1.2 (Informal). *Consider a cheating strategy for G_{Rad}, $\mathcal{S}$, attaining value $\omega(G_{\mathrm{Rad}}; \mathcal{S}) \geq 1 - \epsilon$ for some $0 \leq \epsilon \leq \frac{1}{8}$. Denote by k the local dimension of the quantum resources used in $\mathcal{S}$.*
If $\sigma^i = O(\mathrm{polylog}(n)/n^\alpha)$ or $\sigma^{ii} = O(\mathrm{polylog}(n)/n^{3/4+\alpha})$ for some $\alpha > 0$, then:

$$k = \Omega\left(\exp\left(n^{\alpha'} \right) \right) \quad \text{for some } \alpha' > 0.$$

---

[2]   The attack from [2] requires an entangled system of dimension $O(\exp(n^4))$, that is still much larger than our bounds for smooth strategies. Nonetheless, we consider that any separation on resources that is exponential in a power of n is enough to discriminate between the relative power among different agents. This is our main motivation in this work.

As we see, the regularity parameters $\sigma^{i(ii)}$ play a key role in these results. We notice that known attacks in [2,9] in fact fulfil the hypothesis of the previous corollary: the second round of local operations in these attacks is ε-independent, hence[3] $\sigma^i \sim \log(n)/n$. However, we do not know how generic this behaviour is. More generally, it turns out that from any Programmable Quantum Processor [15]—as the already considered protocol of Port Based Teleportation, for example—with the capability of implementing the diagonal unitaries required in G_{Rad}, we can construct an assignment Φ fulfilling Theorem 1.1 with regularity parameter again of order $\sigma^i \sim \log(n)/n$. Therefore, Corollary 1.2 also applies to this broader case allowing to recover some of the results obtained in [14]. This is not a coincidence, our approach here builds on ideas introduced in this previous work.

Turning our attention towards σ^{ii}, a trivial example of a family of *smooth* attacks for which $\sigma^{ii} \sim \log(n)/n$ is given by cheaters sharing no entanglement in advance – even when entanglement can be created in the first round of local operations and distributed for the second round. By contrast, we can also easily compute σ^{ii} for the attack in [2] obtaining $\sigma^{ii} = O(1)$. Therefore, our second item in Theorem 1.1 is not able to predict good lower bounds for this case. Still, we think that this second item might be useful for restricting the structure of possible attacks to PV, especially in conjunction with the first part of the theorem.

More importantly, the second part of Theorem 1.1 leads us to put forward the possibility of an unconditional lower bound for k, i.e., a bound in the spirit of Corollary 1.2 but dropping out the assumptions regarding $\sigma^{i(ii)}$. Even when we were not able to prove such a bound, we relate its validity with a conjecture about the geometry of some Banach spaces. More concretely, our conjecture has to do with estimates of type constants of tensor norms on finite dimensional Hilbert spaces. Even when these properties for the case of a single Hilbert space are very well understood—in fact, in this case the study of type and cotype reduces to an elementary generalization of the parallelogram law—, the situation changes dramatically when tensor products of several such spaces are considered. For the latter, long-standing questions remain open as, for example, whether the simple space $\ell_2 \otimes_\pi \ell_2 \otimes_\pi \ell_2$ has finite cotype (see Sects. 2.3.1, 2.3.3 for the definition of the objects mentioned here). This is a famous question asked by Pisier decades ago—see, for instance, [16]—and about which still very little is known.

Once we formally state the conjecture in Sect. 5, we provide some computation supporting it. We analyze the most direct approaches to disprove the conjectured statement providing an estimate of the volume ratio of some relevant spaces. This might have interesting ramifications on the still not completely understood relation between volume ratio and cotype of Banach spaces.

Further extensions of this work. To conclude this introductory summary, we highlight that there is a natural way to remove the classical part of the input in G_{Rad}, obtaining protocols in which the overall dimension (classical and quantum) of the systems the honest agents are required to manipulate is polynomial in n. Taking inspiration from the definition of G_{Rad}, we now fix $\varepsilon \in \mathcal{Q}_{n^2}$ as publicly known and define a PV protocol G_ε that proceeds as follows:

1. the verifier starts uniformly preparing the state $|\psi\rangle := \frac{1}{n} \sum_{i,j} |i\rangle_A \otimes |j\rangle_B \otimes |ij\rangle_C$ in a tripartite Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C$. The agent at $x - \delta$ receives register $\mathcal{H}_A$ while the one at $x + \delta$ receives $\mathcal{H}_B$. Register $\mathcal{H}_C$ is kept as private during the execution of the protocol.

---

[3]   Notice that in this case the first summand in the RHS of (1) vanishes. This leads to the estimate $\sigma^i \lesssim_{\log} 1/n$. A look into the proof of the upper bound (1), Proposition A.1, i., reveals that the logarithmic term hidden in $\lesssim_{\log}$ is indeed proportional to $\log(n)$.

2. Then, registers $\mathcal{H}_A \otimes \mathcal{H}_B$ are forwarded to the verifying location x, $\mathcal{H}_A$ from its left and $\mathcal{H}_B$ from its right.

3. An honest prover located at x, upon receiving both pieces of information, has to apply the diagonal unitary on $\mathcal{H}_A \otimes \mathcal{H}_B$ determined by ε. Immediately, registers $\mathcal{H}_A \otimes \mathcal{H}_B$ must be returned. $\mathcal{H}_A$ should travel to the verifier at $x - \delta$ and $\mathcal{H}_B$, to the verifier at $x + \delta$.

4. The verification is now carried out in the same way as in G_{Rad}.

Considering the *family* of protocols $\{G_\varepsilon\}_{\varepsilon \in \mathcal{Q}_n^2}$ as a whole, it is possible to recover a notion of smooth strategies with some associated regularity parameter σ. Such notion of regularity allows us to obtain an equivalent result to Theorem 1.1—and, therefore, to Corollary 1.2—for this case. A criticism that might be made at this point is that it is less clear than before why one should expect any regularity among strategies that applies to different games. A possible line of argumentation against this criticism could be stated in terms of protocols for instantaneous non-local quantum computation: if one aims to construct protocols that are universal, in the sense they are able to non-locally implement any unitary, it seems rather difficult to come with something that depends on the unitary to be implemented in a very non-regular way. The authors of [2] seem to go along with that idea when stating the notion of *"protocols which only make black-box use of the unitary"*.

Leaving aside the concerns triggered by the appearance of regularity assumptions, one could also pursue unconditional bounds for $\{G_\varepsilon\}_{\varepsilon \in \mathcal{Q}_{n^2}}$ following a similar route as the one drawn in Sect. 5. This time the Banach spaces that appear are even more convoluted and, at the moment of writing this manuscript, we do not have any serious evidence to guess the behaviour of their type properties. The study of the issues arising from the previous considerations is postponed for future research.

Finally, as a general comment, we note that the study of PV protocols can be phrased in terms of *quantum games*, a framework that might provide the right level of abstraction for further generalizations of the present work. The interested reader can find a detailed account of such rephrasing in [17, Chapter 4].

1.2. Proof sketch. Here we sketch the main ideas behind the proof of Theorem 1.1. These ideas are also at the bottom of the constructions that allow us to establish the more general connection between Question 1 and type constants that leads to the conjecture indicated above.

As we have already mentioned, the starting point of our study is the identification of each cheating strategy, $\mathcal{S}$, with a vector-valued function $\Phi : \mathcal{Q}_{n^2} \to X$, being $\mathcal{Q}_{n^2} = \{\pm 1\}^{n^2}$ and X, a well-suited Banach space. With an appropriate definition of Φ—which also includes the choice of X—we can obtain a bound on the success probability $\omega(G_{\text{Rad}}, \mathcal{S})$ in terms of the average norm of the image of that function. We obtain bounds of the following kind:

$$\omega(G_{\text{Rad}}; \mathcal{S}) \leq \mathbb{E}_\varepsilon \|\Phi(\varepsilon)\|_X,$$

where ε is taken uniformly distributed in $\mathcal{Q}_{n^2}$. Therefore, the key quantity we study is precisely $\mathbb{E}_\varepsilon \|\Phi(\varepsilon)\|_X$. For that, we bring together two main ingredients. On one hand, a Sobolev-type inequality of Pisier for vector-valued function on the Boolean cube and, on the other, the type-2 constant of the Banach space X, $\text{T}_2(X)$. The combination of these two tools provides us with an inequality:

$$\mathbb{E}_\varepsilon \|\Phi(\varepsilon)\|_X \leq \|\mathbb{E}_\varepsilon \Phi(\varepsilon)\|_X + C \, \sigma_\Phi \, \text{T}_2(X), \tag{3}$$

where C is an independent constant and σ_Φ is a regularity measure for Φ[4]. Specific choices for Φ and X leads to parameters $\sigma^{i(ii)}$ appearing in Theorem 1.1.

Now, depending on how Φ is constructed, $\left\| \mathbb{E}_\varepsilon \Phi(\varepsilon) \right\|_X$ can be upper bounded by a quantity strictly smaller than 1– see, for instance, Proposition 4.6 . Once such a bound is obtained, the focus can be put on the second term in the RHS of (3).

To obtain Theorem 1.1 we propose in Sect. 4 two possible choices for Φ and study the type constants of their image spaces. Furthermore, in order to remove the dependence on σ in the bounds obtained in that way, we propose in Sect. 5 yet another choice for Φ. This third function is regular enough by construction allowing to obtain bounds depending only on the dimension of the system used by the cheaters. The downside of this latter approach is that the space X in this last case becomes more involved and its type properties cannot be estimated with the techniques at our disposal.

To finish this introduction we sum up the structure of the paper: we start introducing in Sect. 2 preliminary material needed to develop this work. Then, in Sect. 3 we study general aspects of cheating strategies for G_{Rad} paving the ground for our main results. The analysis of strategies leading to Theorem 1.1 is presented in Sect. 4. In Sect. 5 we discuss the possibility of pushing forward the techniques presented in this work to obtain unconditional lower bounds on the resources required by the cheaters, only dependent on the dimension of the quantum system they manipulate. We connect this question with the problem in local Banach space theory of obtaining precise estimates for the *type constants* of particular Banach spaces. After establishing that connection in a precise and rigorous way, we provide some calculations supporting a positive resolution of a conjecture that would lead us to strengthening the security of G_{Rad}. The paper ends with a discussion of the results presented and possible directions for future work. This corresponds to Sect. 6.

2. Preliminaries

2.1. Notation. In order to simplify the presentation, we use symbols $\approx$ and $\lesssim$ to denote equality and inequality up to multiplicative dimension independent constants and $\approx_{\mathrm{log}}$ and $\lesssim_{\mathrm{log}}$, equality and inequality up to multiplicative logarithmic factors on the dimensions involved.

The quantum mechanical description of a system is based on an underlying complex Hilbert space, that we denote $\mathcal{H}$, $\mathcal{H}'$, $\mathcal{H}_A$, $\mathcal{H}_B$, $\mathcal{K}$, …. When the dimension is known to be a specific natural number, say n, we use the notation ℓ_2^n. Given that, a density matrix is a trace one, positive operator $\rho : \mathcal{H} \to \mathcal{H}$. We denote the set of density matrices as $\mathcal{D}(\mathcal{H})$. Quantum operations are completely positive trace preserving linear maps $\mathcal{D}(\mathcal{H}) \to \mathcal{D}(\mathcal{H}')$. The set of these maps is denoted here as $\mathrm{CPTP}(\mathcal{H}, \mathcal{H}')$ or simply $\mathrm{CPTP}(\mathcal{H})$ when the input and output spaces are the same. The operation of discarding a subsystem is implemented by the partial trace. We specify the subsystem discarded by its underlying Hilbert space, e.g., in a composed system with underlying Hilbert space $\mathcal{H} \otimes \mathcal{H}'$ the operation of discarding $\mathcal{H}'$ is denoted $\mathrm{Tr}_{\mathcal{H}'} \in \mathrm{CPTP}(\mathcal{H} \otimes \mathcal{H}', \mathcal{H})$. To describe the evolution of a quantum system after a measurement, we make use of *instruments*, that are collections of completely positive trace non-increasing maps summing up to a trace preserving map. To denote a completely positive (maybe non trace-preserving) map we

---

[4]   See Sect. 2.3.4 for a detailed discussion. There, the more refined type-2 constant with m vectors is considered, see Corollary 2.17. For the sake of simplicity, we consider the plain type-2 constant in this introductory section.

use the symbol CP instead of the previous CPTP. The set of instruments composed by finite collections of maps in $CP(\mathcal{H}, \mathcal{H}')$ are denoted $\text{Ins}(\mathcal{H}, \mathcal{H}')$.

To denote Banach spaces we usually use letters X, Y, ... and X^*, Y^*, ... for the corresponding Banach duals. B_X denotes the unit ball of a Banach space X. $\mathcal{B}(X, Y)$ is the space of bounded linear operators between arbitrary Banach spaces X and Y, while $\ell_p(X)$ and $L_p(X)$, with $p \in (0, \infty]$, are the classical (vector valued) spaces of $p-$summable sequences and $p-$integrable functions on the unit interval. More specifically, we also fix now the notation for two Banach spaces that will appear repeatedly. Given two Hilbert spaces $\mathcal{H}, \mathcal{H}'$, we denote as $\mathcal{B}(\mathcal{H}, \mathcal{H}')$ and $\mathcal{S}_1(\mathcal{H}, \mathcal{H}')$ the space of bounded and trace class operators from $\mathcal{H}$ into $\mathcal{H}'$, respectively. In the finite dimensional case, $\mathcal{H} = \ell_2^m$, $\mathcal{H}' = \ell_2^n$, we simplify this notation to $M_{n,m}$ and $\mathcal{S}_1^{n,m}$ (M_n, $\mathcal{S}_1^n$ when $n = m$). To denote elements of the computational basis we use the quantum information oriented convention of using the symbols $|i\rangle$, $\langle i|$, $|j\rangle$, ... When working with elements in the complex vector space composed by $n \times m$ matrices—as is the case of elements in $M_{n,m}$ or $\mathcal{S}_1^{n,m}$, case we consider repeatedly below—the usual basis of matrices with only one non-zero entry is denoted here as $\{|i\rangle\langle j|\}_{\substack{i=1,...,n \\ j=1,...,m}}$. Observing the range of each subindex, the convention chosen here matches the standard agreement on regarding *kets* $|i\rangle$ as column vectors and *bras* $\langle i|$ as rows.

2.2. *Position based cryptography in 1-D.*

The major aim of this work is to make progress towards Question 1. For that, we restrict ourselves to the simplest scenario: position verification in 1-D. In this situation, we restrict the world to a line in which we consider a preferred location x—the position to be verified. The verifier, composed by two agents, V_L and V_R, is located around this honest position. Let us consider V_L in position $x - \delta$ and V_R in position $x + \delta$. Then, V_L and V_R perform an interactive protocol sending (possibly quantum) messages in the direction of x. These messages arrive to x at the same time, so that a honest prover located at x could receive them and, accordingly, generate answers for V_L and V_R. The verifier accept the verification if and only if:

- (correctness) the answers are correct with respect to verifier's messages (according to some public rule);
- (timeliness) the answers arrive on time to the locations of V_L and V_R. Assuming that the signals between verifiers and prover travel at some known velocity c, the answers should arrive to V_L and V_R at time $2\delta/c$ after the start of the protocol.

Before continuing, let us set a generic structure for such a protocol. To prepare the messages V_L and V_R must forward, the verifier prepares a (publicly known) state in a composite system with some underlying Hilbert space $\mathcal{H}_L \otimes \mathcal{H}_R \otimes \mathcal{H}_C$. That is, he prepares a density matrix ρ_0 on that state space and sends the register $\mathcal{H}_L$ to V_L and $\mathcal{H}_R$ to V_R. $\mathcal{H}_C$ is considered to take into account the possibility that the verifier keeps some part of the initial system as private during the protocol. Then, V_L and V_R send their systems in the direction of x. Now, the agent(s) interacting in the middle with V_L and V_R apply some quantum operation on the communicated system $\mathcal{H}_L \otimes \mathcal{H}_R$ obtaining as output another state $\rho_{ans} \in \mathcal{D}(\mathcal{H}'_L \otimes \mathcal{H}'_R)$. The subsystems $\mathcal{H}'_L$, $\mathcal{H}'_R$ are forwarded to V_L, V_R, respectively. To decide whether the verification is correct or not, the verifiers first check the *timeliness* condition is fulfilled and then perform a (publicly known) dichotomic measurement on the system $\mathcal{H}'_L \otimes \mathcal{H}'_R \otimes \mathcal{H}_C$.

Remark 2.1. Above, ρ_0 and ρ_{ans} are in general quantum states but they could perfectly describe also classical messages as well as quantum-classical messages. This will be indeed the case in the concrete scheme analized in this work.

Remark 2.2. Note that a honest prover, that is, an agent at position x, shouldn't have any problem to pass the test: at time δ/c he would receive the whole system $\mathcal{H}_L \otimes \mathcal{H}_R$ from the verifiers, having the capability to perform any global operation on it to prepare his answer. This answer can still arrive on time to V_L and V_R. The action described in the previous lines is the most general operation that can be performed on verifier's messages, which are the only information transmitted in the protocol. Therefore, if the challenge is well designed (it can be passed), the honest prover must be able to succeed at it[5].

Next, let us focus on how the general protocol described above can be cheated. In order to impersonate the identity of a honest prover at position x, a couple of adversaries, Alice and Bob, at positions $x \pm \delta'$, $0 < \delta' < \delta$, can intercept the message systems $\mathcal{H}_L$, $\mathcal{H}_R$, interact between themselves to generate answers for the verifier and forward those answers in correct timing. In order to respect the timeliness of the protocol, the most general action of the cheaters proceeds as follows:

1. Before the start of the protocol, Alice and Bob prepare some shared entangled state in a private register $\mathcal{H}_{E_a} \otimes \mathcal{H}_{E_b}$;
2. Alice receives question register $\mathcal{H}_L$ and applies a quantum channel $\mathcal{A} \in$ CPTP$(\mathcal{H}_L \otimes \mathcal{H}_{E_a}, \mathcal{H}_{A \to B} \otimes \mathcal{H}_{A \to A})$. Similarly, Bob receives $\mathcal{H}_R$ and applies $\mathcal{B} \in$ CPTP$(\mathcal{H}_R \otimes \mathcal{H}_{E_b}, \mathcal{H}_{B \to A} \otimes \mathcal{H}_{B \to B})$;
3. the cheaters interchange registers $\mathcal{H}_{A \to B}$ and $\mathcal{H}_{B \to A}$, keeping $\mathcal{H}_{A \to A}$, $\mathcal{H}_{B \to B}$;
4. after this last step, Alice holds system $\mathcal{H}_{A \to A} \otimes \mathcal{H}_{B \to A}$, on which she applies another channel $\tilde{\mathcal{A}} \in$ CPTP$(\mathcal{H}_{A \to A} \otimes \mathcal{H}_{B \to A}, \mathcal{H}'_L)$. Similarly, Bob applies $\tilde{\mathcal{B}} \in$ CPTP$(\mathcal{H}_{B \to B} \otimes \mathcal{H}_{A \to B}, \mathcal{H}'_R)$;
5. finally, Alice sends $\mathcal{H}'_L$ to V_L and Bob $\mathcal{H}'_R$ to V_R.

Fig. 2. Structure of adversarial action attacking 1-D PV protocols. In step 3, we model any kind of communication between Alice and Bob, classical or quantum. However, in the particular setting studied later on in Sect. 3, we will see that the dimension of $\mathcal{H}_{A \to B}$ and $\mathcal{H}_{B \to A}$ is essentially determined by the quantum resources the cheaters share, allowing us to disregard the classical communication that they might additionally use. See Sect. 3, Lemma 3.1, for a precise statement

We call in this work *simultaneous two-way communication scenario*, *s2w*, the set of actions—strategies from now on—with this structure. This scenario is central for us and will appear repeatedly in the rest of this manuscript.

2.3. Banach spaces, operator ideals and type constants. At a technical level, the results of this work follow from the study of Banach spaces formed by tensor products of Hilbert spaces. The spaces $M_{n,m}$ and its dual, $\mathcal{S}_1^{n,m}$, play a prominent role in the rest of

---

[5] We don't take into account here the computational limitations at which the agents might be subjected.

the manuscript. Properties of these spaces in conjunction with a classical Sobolev-type inequality of Pisier allow us to obtain our main result, Theorem 1.1.

The key property we study of these spaces are type constants, that we introduce in Sect. 2.3.3. Before that, we need to introduce some objects we work with in the following sections.

2.3.1. Operator ideals A deeper understanding of the constructions appearing in this work is provided by the perspective of the theory of operator ideals. For the reader's convenience, we first sum up the contents of this section: given two finite-dimensional[6] Banach spaces X and Y we consider the space of bounded linear operators from X into Y, $\mathcal{B}(X, Y)$. An operator ideal is essentially an assignment of any pair of Banach spaces X and Y with a subset of $\mathcal{B}(X, Y)$ that has the *ideal* property of being closed under composition with bounded linear maps. We provide [18,19] as standard references on this matter for the interested reader. In this section:

1. The first examples of operator ideals we introduce are *tensor norms* on pairs of Banach spaces. This includes the space of bounded operators, $\mathcal{B}(X, Y)$, or $X^* \otimes_\varepsilon Y$ in tensor norm notation, 2-summing operators $\pi_2(X^*, Y)$, or $X \otimes_{\pi_2} Y$, and the ideal of nuclear operators, denoted as $\mathcal{N}(X, Y)$, or $X^* \otimes_\pi Y$[7].
2. When X and Y are Hilbert spaces, another prominent family of operator ideals are the well-known Schatten classes $\mathcal{S}_p$, for $p \in [1, \infty]$. It turns out that these classes can be generalized to operators between arbitrary Banach spaces, leading to the definition of weak Schatten von-Neumann operators of type $p \in [1, \infty]$, denoted here as $\mathfrak{S}_p^w(X, Y)$ or $X^* \otimes_{\mathfrak{S}_p^w} Y$.
3. Finally, here we also define a variant of the space $\mathfrak{S}_p^w(X, Y)$ that appears naturally in our study and that seems to be new in the literature. We denote this space $\mathfrak{S}_p^{w-cb}(X, Y)$ or $X^* \otimes_{\mathfrak{S}_p^{w-cb}} Y$ and call it the space of *weak-cb* Schatten von-Neumman operators of type $p \in [1, \infty]$. The appellative cb is reminiscent of the fact that this new structure makes use of constructions coming from operator space theory. Indeed, $\mathfrak{S}_p^{w-cb}$ is an operator ideal but in the operator space sense, therefore belonging more naturally to that category than to the one of Banach spaces. In any case, we state this as a matter of curiosity and completeness, and these fine-grained details are irrelevant for the scope of the present work. Nonetheless, it is possible that a further exploration of these structures could lead to the clarification of some of the problems we leave open.

After this brief summary, we provide now the details of the contents cited above. We follow part of the exposition [18, Chapter 2] with suitable simplifications adapted to the scope of this work.

For finite dimensional Banach spaces X and Y, the space of linear maps $X \to Y$ can be identified in a simple way with the tensor product $X^* \otimes Y$, as was implicitly assumed above. The identification consists in associating to any element in $X^* \otimes Y$, $\hat{f} = \sum_i x_i^* \otimes y_i$, the linear map $f : X \ni x \mapsto f(x) := \sum_i x_i^*(x) y_i \in Y$. Conversely, to any linear map $f : X \to Y$ we associate the tensor $\hat{f} = \sum_i x_i^* \otimes f(x_i)$, where

---

[6] Even though in most cases the following material also applies in the infinite-dimensional case, for simplicity, we restrict to finite dimension that is all we will use here. This allows us to use the equivalence between operators and tensor products in a comfortable way ignoring the subtleties that appear at this point for infinite dimension.

[7] Recall that here we restrict X and Y to be finite dimensional.

$\{x_i\}_i$, $\{x_i^*\}_i$ are dual bases of X and X^*, respectively. Based on that, we will tend to present our results making explicit the tensor product structure but sometimes, especially in this introductory part of the paper, it will be more natural to talk about mappings, so we will use both conventions interchangeably.

The first operator ideal we encounter is the one of bounded operators from X into Y, that we denote $\mathcal{B}(X, Y)$ and that is the Banach space of linear operators $f : X \to Y$ endowed with the operator norm, $\|f\| := \sup_{x \in B_X} \|f(x)\|_Y < \infty$. Using the equivalence stated before, understanding this space as a tensor product is precisely how the injective tensor product is defined: $X^* \otimes_\varepsilon Y \simeq \mathcal{B}(X, Y)$. If X and Y are finite dimensional spaces, the dual of $X^* \otimes_\varepsilon Y$ coincides with the projective tensor product, $X \otimes_\pi Y^* \simeq (\mathcal{B}(X, Y))^*$. It is enough for the scope of this manuscript to take this equivalence as the definition of $X \otimes_\pi Y^*$. These norms satisfy the desirable *metric mapping property*: for any Banach spaces X_0, X_1, Y_0, Y_1, and any operators $f \in \mathcal{B}(X_0, X_1)$, $g \in \mathcal{B}(Y_0, Y_1)$,

$$\|f \otimes g : X_0 \otimes Y_0 \to X_1 \otimes Y_1\| \le \|f : X_0 \to X_1\| \, \|g : Y_0 \to Y_1\|. \tag{4}$$

Furthermore, we call *tensor norm* to any α that associates to any pair of Banach spaces X, Y, a norm $\| \cdot \|_{X \otimes_\alpha Y}$ such that:

- α is *in between* of the tensor norms ε and π. That is,

$$\text{for any } x \in X \otimes_\alpha Y, \quad \|x\|_{X \otimes_\varepsilon Y} \le \|x\|_{X \otimes_\alpha Y} \le \|x\|_{X \otimes_\pi Y};$$

- α satisfies the metric mapping property.

Later on, in Sect. 5 we will more generally refer as tensor norms to the *tensorization* of different tensor norms. For example, if α, α' are tensor norms, the assignment on any three Banach spaces X, Y, Z of the norm $(X \otimes_\alpha Y) \otimes_{\alpha'} Z$ will also be referred as tensor norm.

The last tensor norm that we need is the 2-summing norm: for an operator $f \in \mathcal{B}(X, Y)$,

$$\|f\|_{\pi_2(X,Y)} := \left\| \mathrm{Id} \otimes f : \ell_2 \otimes_\varepsilon X \to \ell_2(Y) \right\|, \tag{5}$$

where the norm in $\ell_2(Y)$ is defined by $\|(y_i)_{i \in \mathbb{N}}\|_{\ell_2(Y)} = (\sum_{i \in \mathbb{N}} \|y_i\|_Y^2)^{1/2}$ for any sequence of elements $y_i \in Y$.

Next we introduce Schatten classes of compact operators between Hilbert spaces, that are the model to define the generalizations in the theory of operator ideals that we use later on. To define the p-th Schatten class $\mathcal{S}_p(\mathcal{H})$, for $1 \le p \le \infty$, we associate to any compact operator on a Hilbert space, $f : \mathcal{H} \to \mathcal{H}$, its sequence of singular values $(s_i(f))_{i \in \mathbb{N}}$, where $s_1(f) \le s_2(f) \le \ldots$. With this sequence, we define the norm $\|f\|_{\mathcal{S}_p(\mathcal{H})} := \left\|(s_i(f))_i\right\|_{\ell_p}$, which provides the normed structure on $\mathcal{S}_p(\mathcal{H})$. We use the simpler notation $\mathcal{S}_p$ to denote the p-th Schatten class of operators on the separable Hilbert space ℓ_2. In the finite dimensional case we use the notation $\mathcal{S}_p^{n,m}$ to refer to the pth Schatten class of operators from ℓ_2^m into ℓ_2^n. Notice that the case $p = \infty$ coincides with the operator ideal we denoted before as $M_{n,m}$, while for $p = 1$ we obtain $\mathcal{S}_1^{n,m}$.

Now, moving into operators between arbitrary Banach spaces we define:

Definition 2.3. Given an operator $f : X \to Y$ and $1 \le p \le \infty$ we say that f is of weak Schatten-von Neumann type ℓ_p if

$$\|f\|_{\mathfrak{S}_p^w(X,Y)} := \sup \left\{ \left\| \left(s_i(g \circ f \circ h) \right)_i \right\|_{\ell_p} : \begin{array}{l} \|g : Y \to \ell_2\| \le 1 \\ \|h : \ell_2 \to X\| \le 1 \end{array} \right\} < \infty,$$

where $(s_i(g \circ f \circ h))_i$ is the sequence of singular values of the operator $g \circ f \circ h :$ $\ell_2 \longrightarrow \ell_2$.

We denote by $\mathfrak{S}_p^w(X, Y)$ the space of operators $f : X \longrightarrow Y$ of weak Schatten-von Neumann type ℓ_p. Alternatively, in the tensor product notation, we refer to this space by $X^* \otimes_{\mathfrak{S}_p^w} Y$.

To finish this section we introduce the space $\mathfrak{S}_p^{w-cb}(X, Y)$ announced at the beginning of this section. Its definition is based on Definition 2.3 and it incorporates elements of the theory of operators spaces. This forces us to endow X and Y with operator space structures (o.s.s), that is, norms on the *matrix levels* of these spaces, $M_n(X) \equiv M_n \otimes X$, $M_n(Y) \equiv M_n \otimes Y$ for any $n \in \mathbb{N}$—see [20] or [21] for a detailed exposition on operator spaces. With that, the natural notion for maps between operator spaces is the notion of *completely bounded* operators, that is, linear operators $f : X \to Y$ such that

$$\| f : X \to Y \|_{cb} := \sup_{n \in \mathbb{N}} \| \mathrm{Id} \otimes f : M_n(X) \to M_n(Y) \| < \infty.$$

The Banach space of completely bounded operators between X and Y is denoted by $\mathcal{CB}(X, Y)$. Identifying again linear maps with elements of the tensor product $X^* \otimes Y$, in the finite dimensional case we denote $\mathcal{CB}(X, Y) =: X^* \otimes_{\min} Y$.

A Banach space can be endowed in general with several o.s.s. In the case of the space $\mathcal{B}(\mathcal{H}, \mathcal{K})$, with $\mathcal{H}$ and $\mathcal{K}$, Hilbert spaces, there is a natural o.s.s. determined by promoting the isomorphism $M_n(\mathcal{B}(\mathcal{H}, \mathcal{K})) \simeq \mathcal{B}(\mathcal{H}^{\otimes n}, \mathcal{K}^{\otimes n})$ to an isometry (fixing that way the norm in the *matrix levels* of the space)[8]. For a Hilbert space $\mathcal{H}$, we introduce here the so-called *row* and *column* o.s.s., denoting the corresponding operator spaces R and C, respectively. R is defined via the *row* embedding:

$$\mathcal{H} \simeq \mathcal{B}(\ell_2, \mathbb{C}),$$

from which we define a norm on $M_n(\mathcal{H})$ considering the following isomorphism to be an isometry: $M_n(\mathcal{H}) \simeq M_n(\mathcal{B}(\mathcal{H}, \mathbb{C})) \simeq \mathcal{B}(\mathcal{H}^{\otimes n}, \ell_2^n)$.

Similarly, C is defined substituting the previous *row* embedding by it *column* version

$$\mathcal{H} \simeq \mathcal{B}(\mathbb{C}, \ell_2).$$

These last two operator spaces turn out to be non-isomorphic, on the contrary to what happens at the Banach level, where they are simply Hilbert spaces. They are still dual between themselves, that is, $C^* \simeq R$ and $C \simeq R^*$ completely isometrically[9]. However, to properly state those identifications we need a notion of duality for operator spaces. This notion is induced by that of completely bounded maps introduced before. We say that, for an operator space X, X^* is its dual if

$$M_n(X^*) = \mathcal{CB}(X, M_n) \quad \text{for any } n \in \mathbb{N}.$$

Notice that for $n = 1$ the previous characterization of X^* coincides with the dual as Banach spaces[10]. As a last comment on operator spaces, we note that this duality allows to endow $\mathcal{S}_1(\mathcal{H})$ with a natural o.s.s. as the dual of $\mathcal{B}(\mathcal{H})$. Now we finally have all the ingredients to define:

---

[8]   Here we considered hilbertian tensor products in such a way that $\mathcal{H}^{\otimes n}$ and $\mathcal{K}^{\otimes n}$ are again Hilbert spaces.

[9]   Meaning that not only $C^* \simeq R$ and $C \simeq R^*$ stand isometrically but also $M_n(C^*) \simeq M_n(R)$ and $M_n(C) \simeq M_n(R^*)$ for any $n \in \mathbb{N}$.

[10]   For that it is necessary to consider the fact that $\mathcal{CB}(X, \mathbb{C}) \simeq \mathcal{B}(X, \mathbb{C})$.

Definition 2.4. Given an operator between operator spaces $f : X \to Y$ and $1 \leq p \leq \infty$ we say that f is of weak-cb Schatten-von Neumann type ℓ_p if

$$\|f\|_{\mathfrak{S}_p^{w-cb}(X,Y)} := \sup \left\{ \left\| (s_i (g \circ f \circ h))_i \right\|_{\ell_p} : \begin{array}{l} \left\| g : Y \longrightarrow C \right\|_{cb} \leq 1 \\ \left\| h : R \longrightarrow X \right\|_{cb} \leq 1 \end{array} \right\} < \infty,$$

where $(s_i (g \circ f \circ h))_i$ is the sequence of singular values of the operator $g \circ f \circ h : \ell_2 \longrightarrow \ell_2$.

We denote by $\mathfrak{S}_p^{w-cb}(X, Y)$ the space of operators $f : X \longrightarrow Y$ of weak-cb Schatten-von Neumann type ℓ_p. Alternatively, in the tensor product notation, we refer to this space by $X^* \otimes_{\mathfrak{S}_p^{w-cb}} Y$.

Remark 2.5. Since $B_{\mathcal{CB}(X,Y)} \subseteq B_{\mathcal{B}(X,Y)}$ for any operator spaces X, Y, it follows that

$$\|f\|_{\mathfrak{S}_p^{w-cb}(X,Y)} \leq \|f\|_{\mathfrak{S}_p^{w}(X,Y)}, \tag{6}$$

for any $1 \leq p \leq \infty$ and any $f \in \mathfrak{S}_p^{w-cb}(X, Y)$.

Before ending this section, we provide an alternative characterization of the norm introduced above when $X = M_{n,m}$, $Y = \mathcal{S}_1^{n,m}$ and $p = 2$. That is the case appearing in our study of cheating strategies for PV in Sect. 4. For that, we understand $\mathfrak{S}_2^{w-cb}(M_{n,m}, \mathcal{S}_1^{n,m})$ as the tensor product $\mathcal{S}_1^{n,m} \otimes_{\mathfrak{S}_2^{w-cb}} \mathcal{S}_1^{n,m}$. Then,

Lemma 2.6. *Given a tensor $f \in \mathcal{S}_1^{n,m} \otimes \mathcal{S}_1^{n,m}$, where $\mathcal{S}_1^{n,m}$ is endowed with its natural o.s.s. (as the dual of $M_{n,m}$), we have that:*

$$\|f\|_{\mathcal{S}_1^{n,m} \otimes_{\mathfrak{S}_2^{w-cb}} \mathcal{S}_1^{n,m}} = \sup_{\substack{r \in \mathbb{N} \\ g,h \in B_{M_{nr,m}}}} \left\| (h \otimes g)(f) \right\|_{\ell_2^{r^2}}.$$

Above, the action of $h = \sum_{i=1}^n \sum_{j=1}^r \sum_{l=1}^m h_{ijl}|ij\rangle\langle l| \in M_{nr,m}$ on a tensor $t = \sum_{i=1}^n \sum_{l=1}^m t_{il}|i\rangle\langle l| \in \mathcal{S}_1^{n,m}$ is defined by

$$h(t) := \sum_{j=1}^r \left(\sum_{i=1}^n \sum_{l=1}^m h_{ijl} t_{il} \right) |j\rangle \in \ell_2^r.$$

Proof. The claim follows from the following observations:

- a standard argument shows that the supremum in Definition 2.4 can be taken over finite dimensional C_r and R_r, where $r \in \mathbb{N}$ is arbitrarily large;
- for an operator between Hilbert spaces, as $g \circ f \circ h$ in Definition 2.4, the ℓ_2-sum of the singular values coincide with the Hilbert–Schmidt norm of the operator, which is the same as the Euclidean norm of the tensor associated. In our case, with a slight abuse of notation, the relevant tensor is $(h \otimes g)(f)$;
- finally, when we set $X = M_{n,m}$, $Y = \mathcal{S}_1^{n,m}$ in Definition 2.4, the optimization is carried over elements $g \in B_{\mathcal{CB}(\mathcal{S}_1^{n,m}, C_r)}$ and $h \in B_{M_{n,m}}$. But now, it is again a standard result that the following are complete isometries [20, Section 9.3]: $\mathcal{CB}(\mathcal{S}_1^{n,m}, C_r) \simeq M_{nr,m} \simeq \mathcal{CB}(R_r, M_{n,m})$. The claim of the lemma is obtained acting with g, h viewed as elements in $B_{M_{nr,m}}$, as defined in the statement. □

2.3.2. Interpolation of Banach spaces Properties of interpolation spaces allow us to obtain estimates for the type constants of certain spaces that are useful for our purposes in this work. Here we restrict ourselves to the study of the complex interpolation space $(X_0, X_1)_\theta$ for $0 < \theta < 1$ and finite dimensional Banach spaces X_0, X_1. We decided to avoid here a full treatment of the rather cumbersome definition of these spaces and focus on stating some natural properties they display. That is enough for the scope of our work. We redirect the interested reader to the classical references [22,23].

In our case, in which X_0, X_1 are finite dimensional, the space $(X_0, X_1)_\theta$ can always be constructed. In the general case, for arbitrary Banach spaces, if we still can define $(X_0, X_1)_\theta$ we say that the couple (X_0, X_1) is compatible[11], so we fix this terminology from now on. For the sake of concreteness, here we will consider the case in which X_0, X_1 and $(X_0, X_1)_\theta$ are algebraically the same space but endowed with different norms. The complex interpolation method, that assigns to any compatible couple (X_0, X_1) the space $(X_0, X_1)_\theta$, is an *exact interpolation functor of exponent* θ. This means that it satisfies the following:

Theorem 2.7 ([22], Thm. 4.1.2.). *For any compatible couples* (X_0, X_1), (Y_0, Y_1), *and any linear map* $f : (X_0, X_1)_\theta \to (Y_0, Y_1)_\theta$:

$$\left\| f : (X_0, X_1)_\theta \to (Y_0, Y_1)_\theta \right\| \leq \left\| f : X_0 \to Y_0 \right\|^{1-\theta} \left\| f : X_1 \to Y_1 \right\|^\theta,$$

where $\| \cdot \|$ *above denotes the usual operator norm.*

Now we turn our attention to the classical sequence ℓ_p spaces. Interpolation in this case becomes remarkably natural. We have the isometric identification $\ell_p = (\ell_\infty, \ell_1)_{1/p}$ for any $1 \leq p \leq \infty$. Indeed, such an identification follows in a much more general setting. For a Banach space X and $p \in (0, \infty]$, let us denote $L_p(X)$ the space of p-integrable X valued functions on the unit interval. That is, measurable functions $f : [0, 1] \to X$ such that

$$\|f\|_{L_p(X)} := \left(\int_0^1 \|f(t)\|_X^p \mathrm{d}\mu(t) \right)^{\frac{1}{p}},$$

for an (implicitly) given measure μ. With that we can state:

Theorem 2.8 ([22], Thm. 5.6.1.). *For any compatible couple* (X_0, X_1), $p_0, p_1 \in [1, \infty]$ *and* $\theta \in (0, 1)$ *the following follows with equal norms:*

$$\left(L_{p_0}(X_0), L_{p_1}(X_1) \right)_\theta = L_p\left((X_0, X_1)_\theta \right),$$

where $\frac{1}{p} = \frac{1-\theta}{p_0} + \frac{\theta}{p_1}$.

Notice that $\ell_p(X)$ spaces can be regarded as particular instances of $L_p(X)$ where the natural numbers are identified with a subset of the interval $[0, 1]$ and μ is fixed as the discrete measure with unit weights on that subset. This allows us to translate the previous statement also to this case:

$$\left(\ell_{p_0}(X_0), \ell_{p_1}(X_1) \right)_\theta = \ell_p\left((X_0, X_1)_\theta \right), \tag{7}$$

where $\frac{1}{p} = \frac{1-\theta}{p_0} + \frac{\theta}{p_1}$.

Pleasantly, an analogue result for Schatten classes is also true.

---

[11] Technically, this condition is usually stated as the requirement that X_0 and X_1 embed continuously in a common Hausdorff topological vector space.

Theorem 2.9 ([24], Cor. 1.4.). *For a p_0, $p_1 \in [1, \infty]$ and $\theta \in (0, 1)$ the following follows with equal norms:*

$$(\mathcal{S}_{p_0}, \mathcal{S}_{p_1})_\theta = \mathcal{S}_p,$$

where $\frac{1}{p} = \frac{1-\theta}{p_0} + \frac{\theta}{p_1}$. When it applies, $\mathcal{S}_\infty$ must be understood as the Banach space (with the operator norm) of compact operators in a separable Hilbert space.

These are all the basic results we need regarding complex interpolation. To finish this section, we now relate some of the norms introduced in Sect. 2.3.1 with the space $(X^* \otimes_\varepsilon Y, X^* \otimes_\pi Y)_{\frac{1}{2}}$.

Proposition 2.10. *Given finite dimensional Banach spaces X, Y, for any $f \in X \otimes Y$),*

$$\left\| f \right\|_{X \otimes_{\mathfrak{S}_2^{w-cb}} Y} \leq \left\| f \right\|_{X \otimes_{\mathfrak{S}_2^w} Y} \leq \left\| f \right\|_{(X^* \otimes_\varepsilon Y, X^* \otimes_\pi Y)_{\frac{1}{2}}}.$$

Proof. Recalling that we have already established the first inequality in Remark 2.5. Therefore we focus on the second inequality.

According to the definition of $\mathfrak{S}_2^w(X, Y)$, Definition 2.3, we can directly write:

$$\left\| f \right\|_{\mathfrak{S}_2^w(X,Y)} = \sup_{\substack{g \in B_{\mathcal{B}(Y,\ell_2)} \\ h \in B_{\mathcal{B}(\ell_2,X)}}} \| g \circ f \circ h \|_{\mathcal{S}_2} = \sup_{\substack{g \in B_{\mathcal{B}(Y,\ell_2)} \\ h \in B_{\mathcal{B}(\ell_2,X)}}} \| g \circ f \circ h \|_{(\mathcal{S}_\infty, \mathcal{S}_1)_{1/2}},$$

where we have used Theorem 2.9 to state the last equality.

The map $g \circ f \circ h : \ell_2 \to \ell_2$ can be interpreted, as a tensor, as the image of the mapping $h^* \otimes g : X^* \otimes Y \to \ell_2 \otimes \ell_2$ acting on f. With this, the previous expression can be rewritten as:

$$\left\| f \right\|_{\mathfrak{S}_2^w(X,Y)} = \sup_{\substack{g \in B_{\mathcal{B}(Y,\ell_2)} \\ h \in B_{\mathcal{B}(\ell_2,X)}}} \| (h^* \otimes g)(f) \|_{(\mathcal{S}_\infty, \mathcal{S}_1)_{\frac{1}{2}}}$$

$$\leq \| f \|_{(X^* \otimes_\varepsilon Y, X^* \otimes_\pi Y)_{\frac{1}{2}}} \sup_{\substack{g \in B_{\mathcal{B}(Y,\ell_2)} \\ h \in B_{\mathcal{B}(\ell_2,X)}}} \| h^* \otimes g : (X^* \otimes_\varepsilon Y, X^* \otimes_\pi Y)_{\frac{1}{2}}$$

$$\to (\mathcal{S}_\infty, \mathcal{S}_1)_{\frac{1}{2}} \|.$$

Now, it only remains to show that for any contractions $h^* : X^* \to \ell_2$, $g : Y \to \ell_2$

$$\| h^* \otimes g : (X^* \otimes_\varepsilon Y, X^* \otimes_\pi Y)_{\frac{1}{2}} \to (\mathcal{S}_\infty, \mathcal{S}_1)_{\frac{1}{2}} \| \leq 1.$$

This follows from the interpolation property, Theorem 2.7:

$$\| h^* \otimes g : (X^* \otimes_\varepsilon Y, X^* \otimes_\pi Y)_{\frac{1}{2}} \to (\mathcal{S}_\infty, \mathcal{S}_1)_{\frac{1}{2}} \|$$

$$\leq \| h^* \otimes g : X^* \otimes_\varepsilon Y \to \mathcal{S}_\infty \|^{\frac{1}{2}} \| h^* \otimes g : X^* \otimes_\pi Y \to \mathcal{S}_1 \|^{\frac{1}{2}},$$

together with the understanding of $\mathcal{S}_\infty$ and $\mathcal{S}_1$ as the tensor products $\ell_2 \otimes_\varepsilon \ell_2$ and $\ell_2 \otimes_\pi \ell_2$, respectively. This allows us to bound

$$\| h^* \otimes g : X^* \otimes_\varepsilon Y \to \mathcal{S}_\infty \| = \| h^* : X^* \to \ell_2 \| \| g : Y \to \ell_2 \| \leq 1,$$

thanks to the metric mapping property displayed by the injective tensor norm, ε (4). Analogously

$$\| h^* \otimes g : X^* \otimes_\pi Y \to \mathcal{S}_1 \| = \| h^* : X^* \to \ell_2 \| \| g : Y \to \ell_2 \| \leq 1.$$

Hence, the claim in the statement follows. □

Being more specific, when $X^* = Y = \mathcal{S}_1^{n,m}$, Proposition 2.10 reads

$$\|f\|_{\mathcal{S}_1^{n,m} \otimes_{\mathfrak{S}_2^{w-cb}} \mathcal{S}_1^{n,m}} \leq \|f\|_{\mathcal{S}_1^{n,m} \otimes_{\mathfrak{S}_2^w} \mathcal{S}_1^{n,m}} \leq \|f\|_{(\mathcal{S}_1^{n,m} \otimes_\varepsilon \mathcal{S}_1^{n,m}, \, \mathcal{S}_1^{n,m} \otimes_\pi \mathcal{S}_1^{n,m})_{\frac{1}{2}}}. \tag{8}$$

2.3.3. Type/cotype of a Banach space The key properties of a Banach space we study are its *type* and *cotype*. These are probabilistic notions in the local theory of Banach spaces that build on *Rademacher* random variables[12]. We call a random variable ε Rademacher if it takes values -1 and 1 with probability $1/2$ each. We refer by $\{\varepsilon_i\}_{i=1}^n$ to a family of n i.i.d. such random variables. Then, $\mathbb{E}_\varepsilon \, \phi(\varepsilon)$ denotes the expected value of a function ϕ over any combination of signs $\{\varepsilon_i\}_{i=1}^n$ with uniform weight $1/2^n$.

Definition 2.11. Let X be a Banach space and $1 \leq p \leq 2$. We say that X is of (Rademacher) type p if there exists a positive constant T such that for every natural number n and every sequence $\{x_i\}_{i=1}^n \subset X$ we have

$$\left(\mathbb{E}_\varepsilon \left[\| \sum_{i=1}^n \varepsilon_i x_i \|_X^2 \right] \right)^{1/2} \leq \mathrm{T} \left(\sum_{i=1}^n \|x_i\|_X^p \right)^{1/p},$$

Moreover, we define the Rademacher type p constant $\mathrm{T}_p(X)$ as the infimum of the constants T fulfilling the previous inequality.

The notion of type of a normed space finds a dual notion in the one of cotype:

For $2 \leq q < \infty$, the Rademacher cotype q constant of X, $\mathrm{C}_q(X)$, is the infimum over the constants C (in case they exist) such that the following inequality holds for every natural number n and every sequence $\{x_i\}_{i=1}^n \subset X$,

$$\mathrm{C}^{-1} \left(\sum_{i=1}^n \|x_i\|_X^q \right)^{1/q} \leq \left(\mathbb{E}_\varepsilon \left[\| \sum_{i=1}^n \varepsilon_i x_i \|_X^2 \right] \right)^{1/2}.$$

In parallel with the previous definition, we also say that X is of cotype q if $\mathrm{C}_q(X) < \infty$.

Comment 2.12. The above definitions can be found elsewhere in an alternative form in which the term $\left(\mathbb{E}_\varepsilon \| \sum_{i=1}^n \varepsilon_i x_i \|_X^2 \right)^{1/2}$ above is replaced by $\mathbb{E}_\varepsilon \| \sum_{i=1}^n \varepsilon_i x_i \|_X$ or, in other cases, by $\left(\mathbb{E}_\varepsilon \| \sum_{i=1}^n \varepsilon_i x_i \|_X^p \right)^{1/p}$. Due to Kahane inequality [26] (see also [25, Section 4] for the specific application of Kahane inequality to the present context) both expressions are equivalent up to a universal constant and there is no essential difference between definitions.

If the number of elements x_i in the definitions above is restricted to be at most some natural number m, we obtain the related notion of *type/cotype constants of X with m vectors*, denoted here as $\mathrm{T}_p^{(m)}(X)$ and $\mathrm{C}_q^{(m)}(X)$. This is the precise notion we will use later on. Although it will be frequently enough to work with the notion of type constants, sometimes we will need to make this distinction.

Coming back to the better studied context of type and cotype (without any restriction on the number of elements), it is well known that X being of type p implies cotype q

---

[12] There also exists in the literature a *gaussian* notion of type/cotype. See, e.g., [25]. Both notions are in fact intimately related, but here we only consider the *Rademacher* version of the story.

for the dual, X^*, where q is the conjugate exponent such that $1/p + 1/q = 1$. This can be summarized in the inequality—see, e.g., [27]:

$$C_q(X^*) \leq T_p(X), \qquad \text{for } 1 < p \leq 2,\ 2 \leq q < \infty\ :\ \frac{1}{p} + \frac{1}{q} = 1. \tag{9}$$

The reverse inequality fails in general—and, in fact, the pair of spaces considered in this work, $(M_n, \mathcal{S}_1^n)$, is an instance of that phenomenon. However, it turns out that the reverse inequality can be made true *up to logarithmic* factors [27,28]:

$$T_p(X) \lesssim \log(\dim(X))\, C_q(X^*), \qquad \text{for } 1 < p \leq 2,\ 2 \leq q < \infty\ :\ \frac{1}{p} + \frac{1}{q} = 1. \tag{10}$$

Our interest now turns into the interaction between type and interpolation. In fact, type constants behave well w.r.t. interpolation methods, a fact that will be extremely useful in next section. We state the following general known result:

Proposition 2.13. *Let X_0, X_1 be an interpolation couple, where X_i has type p_i for some $1 \leq p_i \leq 2$, $i = 0,\ 1$. Let $0 < \theta < 1$ and $1 < p < 2$ such that $\frac{1}{p} = \frac{1-\theta}{p_0} + \frac{\theta}{p_1}$. Then,*

$$T_p\big((X_0, X_1)_\theta\big) \leq \big(T_{p_0}(X_0)\big)^{1-\theta} \big(T_{p_1}(X_1)\big)^\theta.$$

The proof follows easily from the interpolation properties of vector valued ℓ_p and L_p spaces. We decided to include a simple proof next without any claim of originality.

Proof. An alternative characterization of the type-p constant of a Banach space X is given by the norm of the mapping:

$$\begin{aligned} \text{Rad} : \ell_p(X) &\longrightarrow L_2(X) \\ (x_i)_i &\longmapsto \sum_i \varepsilon_i\, x_i \end{aligned},$$

where $\{\varepsilon_i\}_i$ are i.i.d. Rademacher random variables and[13]

$$\Big\| \sum_i \varepsilon_i\, x_i \Big\|_{L_2(X)} := \left(\mathbb{E}_\varepsilon \Big\| \sum_i \varepsilon_i x_i \Big\|_X^2 \right)^{\frac{1}{2}}.$$

Then, we write

$$T_p\left((X_0, X_1)_\theta\right) = \big\| \text{Rad} : \ell_p\left((X_0, X_1)_\theta\right) \longrightarrow L_2\left((X_0, X_1)_\theta\right) \big\|.$$

Taking into account the equivalences (Theorem 2.8):

$$\ell_p\left((X_0, X_1)_\theta\right) = \big(\ell_{p_0}(X_0), \ell_{p_1}(X_1)\big)_\theta, \qquad L_2\left((X_0, X_1)_\theta\right) = (L_2(X_0), L_2(X_1))_\theta,$$

we can bound:

$$\begin{aligned} \big\| \text{Rad} : \ell_p &\left((X_0, X_1)_\theta\right) \longrightarrow L_2\left((X_0, X_1)_\theta\right) \big\| \\ &\leq \big\| \text{Rad} : \ell_{p_0}(X_0) \longrightarrow L_2(X_0) \big\|^{1-\theta}\ \big\| \text{Rad} : \ell_{p_1}(X_1) \longrightarrow L_2(X_1) \big\|^\theta \\ &= \big(T_{p_0}(X_0)\big)^{1-\theta} \big(T_{p_1}(X_1)\big)^\theta. \end{aligned}$$

$\square$

---

[13] Formally, to establish this identification we consider a realization of the random variables ε_i as real valued functions on the interval $[0, 1]$. A standard choice is setting $\varepsilon_i(t) = \text{sign}\left(\sin(2^i \pi t)\right)$. In that way, for a function ϕ of the random variable ε, $\mathbb{E}_\varepsilon \phi(\varepsilon) = \int_0^1 \phi(\varepsilon(t)) dt$, which makes the connection with L_p spaces.

2.3.4. Vector valued maps on the Boolean hypercube The main idea in this work is based in the study of strategies to break a particular family of PV protocols—referred to as G_{Rad}—as assignments on the boolean hypercube $\mathcal{Q}_m = \{-1, 1\}^m$. We will associate to any cheating strategy a vector valued mapping $\Phi : \mathcal{Q}_m \to X$, for some Banach space X. Regular enough Φ's will lead to good lower bounds on resources required by the cheaters, contributing to the understanding of Question 1. To quantify the regularity of such maps we introduce the following parameter (depending also on the choice of the space X):

Definition 2.14. To any Banach-space valued map $\Phi : \mathcal{Q}_m \to X$ we associate the parameter:

$$\sigma_\Phi := \log(m) \, \mathbb{E}_{\varepsilon \in \mathcal{Q}_m} \left(\sum_{i=1}^{m} \| \partial_i \Phi_S(\varepsilon) \|_X^2 \right)^{1/2},$$

where $\partial_i \Phi(\varepsilon) := \frac{\Phi(\varepsilon_1,...,\varepsilon_i,...,\varepsilon_m) - \Phi(\varepsilon_1,...,-\varepsilon_i,...,\varepsilon_m)}{2}$ is the discrete derivative on the boolean hypercube in the i-th direction.

Intuitively, σ is an average on both the point ε and the direction i (unnormalized in this last case) of the magnitude of the derivative of the map Φ. The prefactor $\log(m)$ is of minor importance for our purposes and we added it to the definition of σ_Φ to obtain more compact expressions later on.

Example 2.15. In order to gain some familiarity, let us compute the parameter σ of a linear map

$$\begin{aligned} \Phi : \mathcal{Q}_m &\longrightarrow & X \\ \varepsilon &\mapsto & \Phi(\varepsilon) := \tfrac{1}{m} \sum_j \varepsilon_j x_j \end{aligned},$$

where $x_j \in B_X$ for $j = 1, \ldots m$

First, for any point $\varepsilon \in \mathcal{Q}_m$, and a direction $i \in [m]$:

$$\partial_i \Phi(\varepsilon) = \frac{1}{2m} \left(\sum_j \varepsilon_j x_j - \varepsilon_j (-1)^{\delta_{i,j}} x_j \right) = \frac{1}{m} \varepsilon_i x_i.$$

Therefore,

$$\sigma_\Phi = \frac{\log(m)}{m} \left(\sum_i \| x_i \|_X^2 \right)^{\frac{1}{2}} \leq \frac{\log(m)}{m^{\frac{1}{2}}}.$$

This is the ideal case in which our results lead directly to powerful lower bounds on the resources required to break our PV protocols.

Ultimately, the motivation for the definition of σ_Φ is the bound in Corollary 2.17 below. This is a consequence of the following Sobolev-type inequality due to Pisier for vector-valued functions on the hypercube:

Lemma 2.16 ([29], Lemma 7.3). *In a Banach space X, let $p \geq 1$, $\Phi : \mathcal{Q}_m \to X$ and ε, $\tilde{\varepsilon}$ be independent random vectors uniformly distributed on $\mathcal{Q}_m$. Then,*

$$\mathbb{E}_\varepsilon \left\| \Phi(\varepsilon) - \mathbb{E}_\varepsilon \Phi(\varepsilon) \right\|_X^p \leq (C \log m)^p \, \mathbb{E}_{\varepsilon,\tilde{\varepsilon}} \left\| \sum_i \tilde{\varepsilon}_i \, \partial_i \Phi(\varepsilon) \right\|_X^p,$$

where $\partial_i \Phi(\varepsilon) := \frac{\Phi(\varepsilon_1,...,\varepsilon_i,...,\varepsilon_n) - \Phi(\varepsilon_1,...,-\varepsilon_i,...,\varepsilon_n)}{2}$.

It is now very easy to combine this result with the type properties of X in order to obtain:

Corollary 2.17 (of Lemma 2.16). *Consider a function $\Phi : \mathcal{Q}_m \longrightarrow X$, where X is a Banach space. Then*

$$\mathbb{E}_\varepsilon \left\| \Phi(\varepsilon) \right\|_X \leq \left\| \mathbb{E}_\varepsilon \Phi(\varepsilon) \right\|_X + C \, \sigma_\Phi \, \mathrm{T}_2^{(m)}(X),$$

where C is an independent constant.

This is the cornerstone of the building leading to Theorem 1.1.

Proof of Corollary 2.17. Fix $p = 1$ in Lemma 2.16. Therefore, we have that :

$$\mathbb{E}_\varepsilon \left\| \Phi(\varepsilon) - \mathbb{E}_\varepsilon \Phi(\varepsilon) \right\|_X \leq (C \log m) \, \mathbb{E}_{\varepsilon,\tilde{\varepsilon}} \left\| \sum_i \tilde{\varepsilon}_i \, \partial_i \Phi(\varepsilon) \right\|_X.$$

Additionally, we can trivially bound:

$$\mathbb{E}_\varepsilon \left\| \Phi(\varepsilon) - \mathbb{E}_\varepsilon \Phi(\varepsilon) \right\|_X \geq \mathbb{E}_\varepsilon \left\| \Phi(\varepsilon) \right\|_X - \left\| \mathbb{E}_\varepsilon \Phi(\varepsilon) \right\|_X.$$

On the other hand, according to the definition of the type-2 constant (with m vectors) of X—recall also Comment 2.12—we can say:

$$\mathbb{E}_{\varepsilon,\tilde{\varepsilon}} \left\| \sum_i \tilde{\varepsilon}_i \, \partial_i \Phi(\varepsilon) \right\|_X \lesssim \mathrm{T}_2^{(m)}(X) \, \mathbb{E}_\varepsilon \left(\sum_i \| \partial_i \Phi_S(\varepsilon) \|_X^2 \right)^{1/2}.$$

That's enough to obtain the statement. □

2.3.5. Some key estimates of type constants Corollary 2.17 provides us with a tool to upper bound the expected norm of the image of a map $\Phi : \mathcal{Q}_m \to X$, provided that we have some control over the RHS of the inequality in the statement. The only piece there that is independent of the map Φ is the type-2 constant (with m vectors) $\mathrm{T}_2^{(m)}(X)$, to which the rest of this section is devoted.

Later on, the normed spaces $M_{n,m}$ and $\mathcal{S}_1^{n,m} \otimes_{\mathfrak{S}_2^{cb-w}} \mathcal{S}_1^{n,m}$ will play a prominent role. The type and cotype properties of $M_{n,m}$ as well as $\mathcal{S}_1^{n,m}$ are well known. In particular the following estimates hold:

$$\mathrm{C}_2(M_{n,m}) \approx \min(n^{1/2}, m^{1/2}), \qquad \mathrm{T}_2(M_{n,m}) \approx \log^{1/2}(\min(n,m)), \qquad (11)$$

$$\mathrm{C}_2(\mathcal{S}_1^{n,m}) \approx 1, \qquad \mathrm{T}_2(\mathcal{S}_1^{n,m}) \approx (\min(n,m))^{1/2}. \qquad (12)$$

For $\mathcal{S}_1^{n,m} \otimes_{\mathfrak{S}_2^{cb-w}} \mathcal{S}_1^{n,m}$ the situation is not that well understood at all. In fact, we were not able to obtain any non-trivial estimate for its type properties so far. Then,

instead of dealing directly with this space, we will consider the interpolation space $(\mathcal{S}_1^{n,m} \otimes_\varepsilon \mathcal{S}_1^{n,m}, \mathcal{S}_1^{n,m} \otimes_\pi \mathcal{S}_1^{n,m})_{\frac{1}{2}}$. The norm in this latter space turns out to be an upper bound to the norm in $\mathcal{S}_1^{n,m} \otimes_{\mathfrak{S}_2^{cb-w}} \mathcal{S}_1^{n,m}$, recall Proposition 2.10. From now on we use the following notational short-cut: $(\mathcal{S}_1^{n,m} \otimes_\varepsilon \mathcal{S}_1^{n,m}, \mathcal{S}_1^{n,m} \otimes_\pi \mathcal{S}_1^{n,m})_\theta = \mathcal{S}_1^{n,m} \otimes_{(\varepsilon,\pi)_\theta} \mathcal{S}_1^{n,m}$. Thanks to the extra structure in $\mathcal{S}_1^{n,m} \otimes_{(\varepsilon,\pi)_{1/2}} \mathcal{S}_1^{n,m}$ provided by interpolation, we are able to obtain a bound for its type constants. To simplify the presentation, we consider in the following that $\min(n,m) = n$. We can state:

Proposition 2.18. *Given $0 < \theta < 1$, and natural numbers $n \leq m$:*

$$\mathrm{T}_{\frac{2}{1+\theta}} \left(\mathcal{S}_1^{n,m} \otimes_{(\varepsilon,\pi)_\theta} \mathcal{S}_1^{n,m} \right) \lesssim_{\log} n^{\frac{1-\theta}{2}}.$$

An immediate consequence of the previous proposition is a bound for the type-2 constant with n^2 vectors:

$$\mathrm{T}_2^{(n^2)} \left(\mathcal{S}_1^{n,m} \otimes_{(\varepsilon,\pi)_\theta} \mathcal{S}_1^{n,m} \right) \leq n^\theta \, \mathrm{T}_{\frac{2}{1+\theta}} \left(\mathcal{S}_1^{n,m} \otimes_{(\varepsilon,\pi)_\theta} \mathcal{S}_1^{n,m} \right) \lesssim_{\log} n^{\frac{1+\theta}{2}},$$

where the first inequality follows as an application of Hölder inequality in the definition of $\mathrm{T}_2^{(n^2)}(X)$ (recall Definition 2.11 and comments afterwards).

Particularizing for $\theta = \frac{1}{2}$:

$$\mathrm{T}_2^{(n^2)} \left(\mathcal{S}_1^{n,m} \otimes_{(\varepsilon,\pi)_{\frac{1}{2}}} \mathcal{S}_1^{n,m} \right) \lesssim_{\log} n^{\frac{3}{4}}. \tag{13}$$

This is the key type-estimate to obtain part II. of the main Theorem 1.1.

For the sake of concreteness, we explicit here the logarithmic corrections in (13):

$$\mathrm{T}_2^{(n^2)} \left(\mathcal{S}_1^{n,m} \otimes_{(\varepsilon,\pi)_{\frac{1}{2}}} \mathcal{S}_1^{n,m} \right) \lesssim n^{3/4} \log^{1/2}(nm) \log(n).$$

Proof of Proposition 2.18. The proof proceeds in two steps. First, using techniques from [16,30], we obtain the estimate

$$\mathrm{T}_2(\mathcal{S}_1^{n,m} \otimes_\varepsilon \mathcal{S}_1^{n,m}) \lesssim_{\log} n^{1/2}. \tag{14}$$

With this at hand, Proposition 2.18 follows from how type constants interact with the complex interpolation method, Proposition 2.13. In particular, it is enough to fix $p_0 = 2$, $p_1 = 1$ in that result and consider the trivial bound $\mathrm{T}_1(\mathcal{S}_1^{n,m} \otimes_\pi \mathcal{S}_1^{n,m}) = 1$.

Therefore, there remains to provide a proof for (14). To prove the stated estimate we bound the cotype-2 constant of the dual, $M_{n,m} \otimes_\pi M_{n,m}$. Therefore, from the duality between type and cotype, Eq. (10), we obtain:

$$\mathrm{T}_2(\mathcal{S}_1^{n,m} \otimes_\varepsilon \mathcal{S}_1^{n,m}) \lesssim \log(nm) \, \mathrm{C}_2(M_{n,m} \otimes_\pi M_{n,m}).$$

To estimate $\mathrm{C}_2(M_{n,m} \otimes_\pi M_{n,m})$ we use the following bound on the cotype of the projective tensor product, implicit in [16][14]

$$\mathrm{C}_2(M_{n,m} \otimes_\pi M_{n,m}) \lesssim \mathrm{C}_2(M_{n,m}) \, \mathrm{UMD}(M_{n,m}) \, \mathrm{T}_2^2(M_{n,m}),$$

---

[14] The key result here is Theorem 5.1 in [16]. The bound we use is obtained keeping track of the constants appearing in the isomorphic statement of that theorem. We are indebted to Jop Briët for kindly sharing with us some very useful private notes on Pisier's method.

where UMD(X) is the analytic UMD (unconditional martingale difference) parameter of the Banach space X. We now bound each of the quantities in the RHS of the last inequality:

- recalling (11) we have that $C_2(M_{n,m}) \lesssim n^{1/2}$ and $T_2(M_{n,m}) \lesssim \log^{1/2}(n)$;
- we estimate UMD($M_{n,m}$) from known bounds for the UMD constant of the p-Schatten class $\mathcal{S}_p$, for $1 < p < \infty$. It is known that these spaces are UMD and the following estimate for UMD($\mathcal{S}_p$) is available [31]:

$$\text{UMD}(\mathcal{S}_p) \lesssim p.$$

This also translates to the same bound for the subspace $\mathcal{S}_p^{n,m}$. Now, we take into account the following relation between the UMD constants of arbitrary spaces X and Y at Banach-Mazur distance $d(X, Y)$. This is a direct consequence of the geometric characterization of the UMD property due to Burkholder [32]—see also [33]:

$$\text{UMD}(X) \lesssim d(X, Y) \, \text{UMD}(Y).$$

Finally, with this at hand, we obtain the bound

$$\text{UMD}(M_{n,m}) \lesssim d(M_{n,m}, \mathcal{S}_p^{n,m}) \, \text{UMD}(\mathcal{S}_p^{n,m}) \lesssim n^{1/p} \, p.$$

Adjusting the parameter p as $p = \log(n)$ we obtain

$$\text{UMD}(M_{n,m}) \lesssim \log(n),$$

that is enough to conclude that

$$T_2(\mathcal{S}_1^{n,m} \otimes_\varepsilon \mathcal{S}_1^{n,m}) \lesssim \log(nm) \, \log^2(n) \, n^{1/2}.$$

$$\square$$

3. Cheating strategies for G_{Rad}

In this section we describe in detail the action of cheaters in our PV protocol G_{Rad}. Recall that in 1-D PV, we consider a privileged point x and a couple of verifiers, V_L, V_R, at locations $x \pm \delta$. See Sect. 1.1, page 7, for the definition of G_{Rad}. In the dishonest scenario two cheaters, Alice and Bob, hold locations $x \pm \delta'$ for some $0 < \delta' < \delta$. The strategy of Alice and Bob is restricted to the *s2w* scenario already described in Fig. 2.

A strategy in this scenario is determined by—cf. Fig. 2:

- a shared entangled state $\varphi \in \mathcal{D}(\mathcal{H}_{E_a} \otimes \mathcal{H}_{E_b})$ that we assume here to be pure[15]. From now on we use interchangeably the notations φ or $|\varphi\rangle\langle\varphi|$ to refer to that state;
- a family of tuples of four "local" channels: for each $\varepsilon \in \mathcal{Q}_{n^2}$,

$$\mathcal{A} \in \text{CPTP}(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_{E_a}, \mathcal{H}_{A \to A} \otimes \mathcal{H}_{A \to B}), \quad \mathcal{B}_\varepsilon \in \text{CPTP}(\mathcal{H}_{E_b}, \mathcal{H}_{B \to B} \otimes \mathcal{H}_{B \to A}),$$

$$\tilde{\mathcal{A}}_\varepsilon \in \text{CPTP}(\mathcal{H}_{A \to A} \otimes \mathcal{H}_{B \to A}, \mathcal{H}'_A), \quad \tilde{\mathcal{B}}_\varepsilon \in \text{CPTP}(\mathcal{H}_{B \to B} \otimes \mathcal{H}_{A \to B}, \mathcal{H}'_B).$$

For verification, $\mathcal{H}'_A$, $\mathcal{H}'_B$ should be communicated to V_L and V_R respectively. Therefore, according to the definition of the protocol, these registers should be isomorphic to the originals $\mathcal{H}_A$ and $\mathcal{H}_B$.

---

[15] It can be easily checked that, by convexity, the success probability achieved in G_{Rad} by strategies using mixed states is always upper bounded by the success probability when using pure states. Since the quantity we are interested in is the optimal cheating probability, restricting ourselves to strategies using pure states would be enough.

Understood as a family of quantum channels, the strategy defined by these elements reads:

$$\mathcal{S}_\varepsilon : \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B) \longrightarrow \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$$
$$\psi \mapsto \mathcal{S}_\varepsilon(\psi) = (\tilde{\mathcal{A}}_\varepsilon \otimes \tilde{\mathcal{B}}_\varepsilon) \circ (\mathcal{A} \otimes \mathcal{B}_\varepsilon)(\psi \otimes \varphi), \tag{15}$$

for each $\varepsilon \in \mathcal{Q}_{n^2}$.

The probability that the verifiers accept the output of such a strategy is given by:

$$\omega(G_{\mathrm{Rad}}; \{\mathcal{S}_\varepsilon\}_\varepsilon) := \mathbb{E}_\varepsilon \, \mathrm{Tr}\left[\, |\psi_\varepsilon\rangle\langle\psi_\varepsilon| \, (\mathrm{Id}_C \otimes \mathcal{S}_\varepsilon)(|\psi\rangle\langle\psi|) \,\right]. \tag{16}$$

Optimizing over any strategy allowed in the s2w scenario leads to the value:

$$\omega_{s2w}(G_{\mathrm{Rad}}) = \sup_{\{\mathcal{S}_\varepsilon\}_\varepsilon \in \mathfrak{S}_{s2w}} \omega(G_{\mathrm{Rad}}; \{\mathcal{S}_\varepsilon\}_\varepsilon), \tag{17}$$

where $\mathfrak{S}_{s2w}$ denotes the set of strategies in the s2w scenario.

In this language, the existence of general attacks for arbitrary PV protocols translates into the coincidence of the value in the $s2w$ scenario with the honest value:

$$\omega_{s2w}(G_{\mathrm{Rad}}) = 1. \tag{18}$$

As we said in the introduction, the main question we are interested in is the amount of entanglement necessary to establish this equality. It is natural then to define a restricted version of $\omega_{s2w}(G_{\mathrm{Rad}})$ considering only strategies using a limited amount of resources. Here, we restrict the local dimension at any time during the protocol. For $\tilde{k}, k \in \mathbb{N}$ we define the scenario $\mathfrak{S}_{s2w,\tilde{k},k}$ as the set of strategies in the form of (15) but with the following restrictions:

$$\dim(\mathcal{H}_{E_{a(b)}}) \le k, \qquad \dim(\mathcal{H}_{A(B) \to A(B)}) \times \dim(\mathcal{H}_{A(B) \to B(A)}) \le \tilde{k}.$$

I.e., we restrict,

$$\varphi \in \mathcal{D}(\ell_2^{k^2})$$

and, for each $\varepsilon \in \mathcal{Q}_{n^2}$,

$$\mathcal{A} \in \mathrm{CPTP}(\ell_2^{n^2 k}, \ell_2^{\tilde{k}}), \quad \mathcal{B}_\varepsilon \in \mathrm{CPTP}(\ell_2^k, \ell_2^{\tilde{k}}),$$
$$\tilde{\mathcal{A}}_\varepsilon \in \mathrm{CPTP}(\ell_2^{\tilde{k}}, \ell_2^n), \quad \tilde{\mathcal{B}}_\varepsilon \in \mathrm{CPTP}(\ell_2^{\tilde{k}}, \ell_2^n).$$

Given this model, we define:

$$\omega_{s2w;\tilde{k},k}(G_{\mathrm{Rad}}) := \sup_{\{\mathcal{S}_\varepsilon\}_\varepsilon \in \mathfrak{S}_{s2w;\tilde{k},k}} \omega(G_{\mathrm{Rad}}; \{\mathcal{S}_\varepsilon\}_\varepsilon). \tag{19}$$

Clearly,

$$\lim_{\tilde{k},k \to \infty} \omega_{s2w;\tilde{k},k}(G_{\mathrm{Rad}}) = \omega_{s2w}(G_{\mathrm{Rad}}) = 1. \tag{20}$$

We want to study the rate of convergence of this limit. To the best of our knowledge, it is not even known whether the limit is in general attained for finite k, $\tilde{k}$. We worry about lower bounds in k, $\tilde{k}$ when a given degree of approximation is achieved in (20). More precisely, we upper bound $\omega_{s2w;\tilde{k},k}(G_{\mathrm{Rad}})$ in terms of k, $\tilde{k}$ and properties of the strategies considered. However, we postpone those results until Sect. 4. Before that, we need to provide here two reductions to the kind of strategies we consider in order to prepare the ground for next section.

3.1. Use of classical communication in cheating strategies. First, we consider the role of classical communication between Alice and Bob. In our model, we regard this resource as free and, in fact, we built into the structure of the considered strategies the free communication of the classical information about ε (in the second round of local operations this parameter was considered as public). This is justified by the fact that our interest is in bounding the *quantum* resources used for attacking G_{Rad}, which are assumed to be much more expensive than classical communication. However, there is a potential problem with this approach. That is the possibility of the players using further classical communication apart from that of ε—*extra classical communication* from now on. In our model, this extra classical communication would be included in the definition of the channels $\mathcal{A}$ and $\mathcal{B}_\varepsilon$. In the $\mathfrak{S}_{s2w,\tilde{k},k}$ scenario, this would affect the dimension $\tilde{k}$ being no longer a reliable witness for the quantum resources spent by a given strategy: $\tilde{k}$ would also include the dimension of the extra classical messages shared by Alice and Bob. Nonetheless, we show that the amount of *useful* extra classical communication in our setting is bounded by the initial dimension of the quantum system manipulated by the players, that is, by k and n. The following lemma lets us control the contribution of the classical part of players action to $\tilde{k}$.

Lemma 3.1. *The optimization over $\mathcal{S} \in \mathfrak{S}_{s2w,\tilde{k},k}$ in* (19) *can be restricted to strategies using extra classical communication of local dimension* $\tilde{k}_{cl} \leq n^4 k^2$.

Proof. The result follows from convexity taking into account that the extreme points of the set of instruments acting on a given Hilbert space of dimension d has at most d^2 outcomes. See, for instance, [34, Rmk. 7.9., p.158] (also [17, Corollary 1.36]).

Consider an arbitrary strategy $\mathcal{S} = \{\tilde{\mathcal{A}}_\varepsilon, \tilde{\mathcal{B}}_\varepsilon, \mathcal{A}, \mathcal{B}_\varepsilon, \varphi\} \in \mathfrak{S}_{s2w;m,k}$ using extra classical communication of local dimension m_{cl}. The dimensions m, m_{cl} are free parameters that will be fixed at the end of the proof. Therefore, we can further specify these classical messages in the structure of the channels $\mathcal{A}$ and $\mathcal{B}_\varepsilon$:

$$\mathcal{A}(\,\cdot\,) = \sum_{c_a=1}^{m_{cl}} \mathcal{A}^{c_a}(\,\cdot\,) \otimes |c_a\rangle\langle c_a| \quad : \quad \mathcal{A}^{c_a} \in \text{CP}(\ell_2^{n^2 k}, \ell_2^{m/m_{cl}}) \text{ for any } c_a,$$

$$\mathcal{B}_\varepsilon(\,\cdot\,) = \sum_{c_b=1}^{m_{cl}} \mathcal{B}_\varepsilon^{c_b}(\,\cdot\,) \otimes |c_b\rangle\langle c_b| \quad : \quad \mathcal{B}_\varepsilon^{c_b} \in \text{CP}(\ell_2^{k}, \ell_2^{m/m_{cl}}) \text{ for any } c_b.$$

These expressions are nothing else than the description of some instruments in $\text{Ins}(\ell_2^{k}, \ell_2^{m/m_{cl}})$ ($\text{Ins}(\ell_2^{n^2 k}, \ell_2^{m/m_{cl}})$ in the first case) with m_{cl} outcomes each. As we said at the beginning of the proof, the extreme points of $\text{Ins}(\ell_2^{k}, \ell_2^{m/m_{cl}})$ consist of instruments with at most k^2 outcomes ($n^4 k^2$ in the first case). Therefore, we can rewrite the channels $\mathcal{A}, \mathcal{B}_\varepsilon$ as a convex combination of such extreme points:

$$\mathcal{A}(\,\cdot\,) = \sum_s \alpha_s \mathcal{A}_s(\,\cdot\,),$$

$$\mathcal{B}_\varepsilon(\,\cdot\,) = \sum_s \beta_{\varepsilon,s} \mathcal{B}_{\varepsilon,s}(\,\cdot\,),$$

where, for each s, ε:

- $0 \leq \alpha_s, \beta_{\varepsilon,s} \leq 1 : \sum_s \alpha_s = 1 = \sum_s \beta_{\varepsilon,s}$;

- $\mathcal{A}_s \in \mathrm{Ins}(\ell_2^{n^4 k^2}, \ell_2^{m/m_{cl}}), \mathcal{B}_{\varepsilon;s} \in \mathrm{Ins}(\ell_2^k, \ell_2^{m/m_{cl}})$ with at most $n^4 k^2$ and k^2 outcomes, respectively. For simplicity we just fix $\tilde{k}_{cl}$ bounded by the largest of these bounds, $\tilde{k}_{cl} \leq n^4 k^2$.

Denote $\mathcal{S}_{s,s'}$ the strategy specified by elements $\{\tilde{\mathcal{A}}_\varepsilon, \tilde{\mathcal{B}}_\varepsilon, \mathcal{A}_s, \mathcal{B}_{\varepsilon,s'}, \varphi\}_\varepsilon$ and $\mathcal{S}_{\varepsilon;s,s'}(\cdot)$ the corresponding channels, defined by the generic prescription (15). Notice that $\mathcal{S}_\varepsilon(\cdot) = \sum_{s,s'} \alpha_s \beta_{s'} \mathcal{S}_{\varepsilon;s,s'}(\cdot)$. Now, focus on the value achieved in G_{Rad}. It turns out that $\omega(G_{\mathrm{Rad}}; \mathcal{S})$ is linear in $\mathcal{S}$, fact that allows us to write:

$$\omega(G_{\mathrm{Rad}}; \mathcal{S}) = \sum_s \alpha_s \, \mathbb{E}_\varepsilon \sum_{s'} \beta_{\varepsilon,s} \, \omega(G_{\mathrm{Rad}}; \{\mathcal{S}_{\varepsilon;s,s'}\}_\varepsilon)$$

$$\leq \max_s \left\{ \mathbb{E}_\varepsilon \max_{s'} \left\{ \omega(G_{\mathrm{Rad}}; \{\mathcal{S}_{\varepsilon;s,s'}\}_\varepsilon) \right\} \right\}.$$

Denoting s^*, $s_\varepsilon'^*$ the indexes at which the maxima above are attained, the strategy $\{\tilde{\mathcal{A}}_\varepsilon, \tilde{\mathcal{B}}_\varepsilon, \mathcal{A}_{s^*}, \mathcal{B}_{\varepsilon,s_\varepsilon'^*}, \varphi\}_\varepsilon$, that uses extra classical communication of local dimension at most $\tilde{k}_{cl} \leq n^4 k^2$, can be now regarded as an element in $\mathfrak{S}_{s2w;\tilde{k},k}$ with $\tilde{k} = m\tilde{k}_{cl}/m_{cl}$. This proves the claim. $\square$

3.2. Pure strategies. The second reduction consists in purifying arbitrary strategies. We start fixing some notation. We say that a strategy $\mathcal{S} = \{\tilde{\mathcal{A}}_\varepsilon, \tilde{\mathcal{B}}_\varepsilon, \mathcal{A}, \mathcal{B}_\varepsilon, \varphi\}_\varepsilon \in \mathfrak{S}_{s2w}$ is *pure* if the channels $\tilde{\mathcal{A}}_\varepsilon, \tilde{\mathcal{B}}_\varepsilon, \mathcal{A}, \mathcal{B}_\varepsilon$ can be written as:

$$\mathcal{A}(\cdot) = V(\cdot)V^\dagger, \qquad\qquad \mathcal{B}_\varepsilon(\cdot) = W_\varepsilon(\cdot)W_\varepsilon^\dagger, \qquad\qquad (21)$$

$$\tilde{\mathcal{A}}_\varepsilon(\cdot) = \mathrm{Tr}_{anc_a} \tilde{V}_\varepsilon(\cdot)\tilde{V}_\varepsilon^\dagger, \qquad \tilde{\mathcal{B}}_\varepsilon(\cdot) = \mathrm{Tr}_{anc_b} \tilde{W}_\varepsilon(\cdot)\tilde{W}_\varepsilon^\dagger, \qquad (22)$$

for some contractive operators

$$V : \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_{E_a} \longrightarrow \mathcal{H}_{A \to A} \otimes \mathcal{H}_{A \to B}, \qquad W_\varepsilon : \mathcal{H}_{E_b} \longrightarrow \mathcal{H}_{B \to B} \otimes \mathcal{H}_{B \to A},$$

$$\tilde{V}_\varepsilon : \mathcal{H}_{A \to A} \otimes \mathcal{H}_{B \to A} \longrightarrow \mathcal{H}_A \otimes \mathcal{H}_{anc_a}, \qquad \tilde{W}_\varepsilon : \mathcal{H}_{B \to B} \otimes \mathcal{H}_{A \to B} \longrightarrow \mathcal{H}_B \otimes \mathcal{H}_{anc_b},$$

where $\mathcal{H}_{anc_a}, \mathcal{H}_{anc_b}$ are arbitrary ancillary Hilbert spaces. In the restricted scenario $\mathfrak{S}_{s2w;\tilde{k},k}$, these operators are of the form:

$$V : \ell_2^{n^2 k} \longrightarrow \ell_2^{\tilde{k}}, \qquad W_\varepsilon : \ell_2^k \longrightarrow \ell_2^{\tilde{k}}, \qquad \tilde{V}_\varepsilon, \tilde{W}_\varepsilon : \ell_2^{\tilde{k}} \longrightarrow \ell_2^{nr}, \qquad (23)$$

where r is some (arbitrary) natural number. For convenience, we identify pure strategies with families of such *pure* objects, setting the notation $\mathcal{S}^{\mathcal{U}} = \{\tilde{V}_\varepsilon, \tilde{W}_\varepsilon, V, W_\varepsilon, |\varphi\rangle\}_\varepsilon$.

We further denote $\mathfrak{S}_{s2w}^{\mathcal{U}}$ the subset of pure strategies in the s2w scenario and $\mathfrak{S}_{s2w;\tilde{k},k}^{\mathcal{U}}$ the corresponding subset in the model with limited dimension. Due to Stinespring dilation theorem [35], it turns out that $\mathfrak{S}_{s2w}^{\mathcal{U}} = \mathfrak{S}_{s2w}$. However, when we restrict the dimension of the considered strategies, the situation is a bit subtler and the Stinespring dilation of the channels involved affects the relevant dimensions defining the models $\mathfrak{S}_{s2w;\tilde{k},k}$ and $\mathfrak{S}_{s2w;\tilde{k},k}^{\mathcal{U}}$. This is taken care of by the following lemma:

Lemma 3.2. *Any strategy* $\mathcal{S} \in \mathfrak{S}_{s2w;\tilde{k},k}$ *can be regarded as a pure strategy* $\mathcal{S}^{\mathcal{U}} \in \mathfrak{S}_{s2w;\tilde{k}',k}^{\mathcal{U}}$ *where* $\tilde{k}' \leq n^2 k \tilde{k}^2$. *That is, the chain of containments* $\mathfrak{S}_{s2w;\tilde{k},k}^{\mathcal{U}} \subseteq \mathfrak{S}_{s2w;\tilde{k},k} \subseteq \mathfrak{S}_{s2w;\tilde{k}',k}^{\mathcal{U}}$ *holds.*

Proof. Set a strategy $\mathcal{S} = \{\tilde{\mathcal{A}}_\varepsilon, \tilde{\mathcal{B}}_\varepsilon, \mathcal{A}, \mathcal{B}_\varepsilon, \varphi\}$ in $\mathfrak{S}_{s2w;\tilde{k},k}$.

We are going to consider Stinespring dilations to purify the corresponding channels

$$\mathcal{S}_\varepsilon(\,\cdot\,) = (\tilde{\mathcal{A}}_\varepsilon \otimes \tilde{\mathcal{B}}_\varepsilon) \circ (\mathcal{A} \otimes \mathcal{B}_\varepsilon)(\,\cdot\, \otimes \varphi). \tag{24}$$

We start with

$$\tilde{\mathcal{A}}_\varepsilon, \tilde{\mathcal{B}}_\varepsilon \in \mathrm{CPTP}(\ell_2^{\tilde{k}}, \ell_2^n).$$

These channels can be lifted (due to a Stinespring dilation) to be of the form:

$$\tilde{\mathcal{A}}_\varepsilon(\,\cdot\,) = \mathrm{Tr}_{\widetilde{anc}} \tilde{V}_\varepsilon(\,\cdot\,)\tilde{V}_\varepsilon^\dagger, \qquad \tilde{\mathcal{B}}_\varepsilon(\,\cdot\,) = \mathrm{Tr}_{\widetilde{anc}} \tilde{W}_\varepsilon(\,\cdot\,)\tilde{W}_\varepsilon^\dagger,$$

where $\tilde{V}_\varepsilon, \tilde{W}_\varepsilon : \ell_2^{\tilde{k}} \longrightarrow \ell_2^n \otimes \mathcal{H}_{\widetilde{anc}}$ are Stinespring isometries and $\dim(\mathcal{H}_{\widetilde{anc}})$ can be upper bounded by $n\tilde{k}$.

Proceeding similarly with $\mathcal{A} \in \mathrm{CPTP}(\ell_2^{n^2 k}, \ell_2^{\tilde{k}})$ and $\mathcal{B}_\varepsilon \in \mathrm{CPTP}(\ell_2^k, \ell_2^{\tilde{k}})$ we obtain:

$$\mathcal{A}(\,\cdot\,) = \mathrm{Tr}_{anc_1} V(\,\cdot\,)V^\dagger, \qquad \mathcal{B}_\varepsilon(\,\cdot\,) = \mathrm{Tr}_{anc_2} W_\varepsilon(\,\cdot\,)W_\varepsilon^\dagger,$$

for Stinespring dilations $V : \ell_2^{n^2 k} \longrightarrow \ell_2^{\tilde{k}} \otimes \mathcal{H}_{anc_1}$, $W_\varepsilon : \ell_2^k \longrightarrow \ell_2^{\tilde{k}} \otimes \mathcal{H}_{anc_2}$ such that $\dim(\mathcal{H}_{anc_1}) \leq n^2 k\tilde{k}$, $\dim(\mathcal{H}_{anc_2}) \leq k\tilde{k}$.

With all that, and denoting $\mathcal{H}_{anc_a} \equiv \mathcal{H}_{anc_1} \otimes \mathcal{H}_{\widetilde{anc}}$, $\mathcal{H}_{anc_b} \equiv \mathcal{H}_{anc_2} \otimes \mathcal{H}_{\widetilde{anc}}$, we define the channels

$$\tilde{\mathcal{A}}_\varepsilon^{\mathcal{U}}(\,\cdot\,) := \mathrm{Tr}_{anc_a}(\tilde{V}_\varepsilon \otimes \mathrm{Id}_{anc_1})(\,\cdot\,)(\tilde{V}_\varepsilon^\dagger \otimes \mathrm{Id}_{anc_1}),$$

$$\tilde{\mathcal{B}}_\varepsilon^{\mathcal{U}}(\,\cdot\,) := \mathrm{Tr}_{anc_b}(\tilde{W}_\varepsilon \otimes \mathrm{Id}_{anc_2})(\,\cdot\,)(\tilde{W}_\varepsilon^\dagger \otimes \mathrm{Id}_{anc_2}),$$

$$\mathcal{A}^{\mathcal{U}}(\,\cdot\,) := V_\varepsilon(\,\cdot\,)V_\varepsilon^\dagger, \qquad \mathcal{B}_\varepsilon^{\mathcal{U}}(\,\cdot\,) := W_\varepsilon(\,\cdot\,)W_\varepsilon^\dagger.$$

Then, we can rewrite (24) as:

$$\mathcal{S}_\varepsilon(\,\cdot\,) = (\tilde{\mathcal{A}}_\varepsilon^{\mathcal{U}} \otimes \tilde{\mathcal{B}}_\varepsilon^{\mathcal{U}}) \circ (\mathcal{A}^{\mathcal{U}} \otimes \mathcal{B}_\varepsilon^{\mathcal{U}})(\,\cdot\, \otimes |\varphi\rangle\langle\varphi|).$$

But clearly the strategy $\mathcal{S}^{\mathcal{U}} := \{\tilde{\mathcal{A}}_\varepsilon^{\mathcal{U}}, \tilde{\mathcal{B}}_\varepsilon^{\mathcal{U}}, \mathcal{A}^{\mathcal{U}}, \mathcal{B}_\varepsilon^{\mathcal{U}}, \varphi\}_\varepsilon$ is pure, finishing the proof of the lemma. A careful look at the definition of the channels defining $\mathcal{S}^{\mathcal{U}}$ reveals that $\mathcal{S}^{\mathcal{U}} \in \mathfrak{S}_{s2w;\tilde{k}',k}^{\mathcal{U}}$ with $\tilde{k}' \leq n^2 k\tilde{k}^2$. $\square$

With Lemmas 3.1 and 3.2 at hand we can focus now on the study of strategies in $\mathfrak{S}_{s2w;\tilde{k}',k}^{\mathcal{U}}$. Given a general strategy $\mathcal{S} \in \mathfrak{S}_{s2w;\tilde{k},k}$, Lemma 3.1 guarantees that $\mathcal{S}$ can be taken such that the dimension of the classical resources used is upper bounded by

$$\tilde{k}_{cl} \leq n^4 k^2. \tag{25}$$

Then, Lemma 3.2 allows us to relate $\mathcal{S}$ with a pure strategy $\mathcal{S}^{\mathcal{U}} \in \mathfrak{S}_{s2w;\tilde{k}',k}^{\mathcal{U}}$ such that

$$\tilde{k}' \leq n^2 k\tilde{k}^2. \tag{26}$$

Accordingly, in the rest of this manuscript we work in the model $\mathfrak{S}_{s2w;\tilde{k}',k}^{\mathcal{U}}$ redirecting the reader to (26) and (25) for the relation with the resources used by more general strategies. However, notice that these correspondences are at most polynomial in n, k and $\tilde{k}$ and, in fact, will only introduce corrections by constant factors in the bounds we

state later on. In this sense, the precise exponents in (26), (25) are irrelevant. This will become clearer in the next section. In order to obtain a cleaner notation, from now on we will use $\tilde{k}$ to refer to the same as $\tilde{k}'$ above.

For convenience, we finish this section recalling the expression of $\omega(G_{\text{Rad}}; \mathcal{S}^{\mathcal{U}})$, Eq. (16), particularized for pure strategies $\mathcal{S}^{\mathcal{U}} = \{\tilde{V}_\varepsilon, \tilde{W}_\varepsilon, V, W_\varepsilon, \varphi\}$:

$$\omega(G_{\text{Rad}}; \mathcal{S}^{\mathcal{U}}) = \mathbb{E}_\varepsilon \, \text{Tr}\left[|\psi_\varepsilon\rangle\langle\psi_\varepsilon| \, (\text{Id}_C \otimes \mathcal{S}^{\mathcal{U}}_\varepsilon) \left(|\psi\rangle\langle\psi|\right) \right], \qquad (27)$$

where now:

$$\mathcal{S}^{\mathcal{U}}_\varepsilon(\cdot) = \text{Tr}_{\mathcal{H}_{anc_a} \otimes anc_b} \left[(\tilde{V}_\varepsilon \otimes \tilde{W}_\varepsilon)(V \otimes W_\varepsilon)(\cdot \otimes |\varphi\rangle\langle\varphi|)(V^\dagger \otimes W^\dagger_\varepsilon)(\tilde{V}^\dagger_\varepsilon \otimes \tilde{W}^\dagger_\varepsilon) \right].$$

Notice that for strategies in the more specific model $\mathfrak{S}^{\mathcal{U}}_{s2w;\tilde{k}',k}$, the operators $\tilde{V}_\varepsilon$, $\tilde{W}_\varepsilon$, V, W_ε are specified as in (23) and, therefore, $\mathcal{H}_{anc_a}$ and $\mathcal{H}_{anc_b}$ in this case are identified with ℓ_2^r for some $r \in \mathbb{N}$. Finally, we provide an alternative expression for (27) that establishes a first connection with normed spaces:

Proposition 3.3. *For any pure strategy* $\mathcal{S}^{\mathcal{U}} = \{\tilde{V}_\varepsilon, \tilde{W}_\varepsilon, V, W_\varepsilon, \varphi\}$:

$$\omega(G_{\text{Rad}}; \mathcal{S}^{\mathcal{U}}) = \mathbb{E}_\varepsilon \left\| \frac{1}{n^2} \sum_{i,j} \varepsilon_{ij} (\langle i|\tilde{V}_\varepsilon \otimes \langle j|\tilde{W}_\varepsilon)(V|ij\rangle \otimes W_\varepsilon)|\varphi\rangle \right\|^2_{\mathcal{H}_{anc_a} \otimes \mathcal{H}_{anc_b}}.$$

Before showing the easy proof of this proposition, let us clarify the notation used above. By $V|ij\rangle$ we mean the operator $V \in M_{\tilde{k}',n^2k}$ with its indices corresponding to $\ell_2^{n^2}$ contracted with the vector $|ij\rangle$. That is, if we expand V on its coordinates, $V = \sum_{k,l=1}^n \sum_{m=1}^k \sum_p^{\tilde{k}'} V_{p,klm}|p\rangle\langle klm|$, and then $V|ij\rangle = \sum_{m=1}^k \sum_p^{\tilde{k}'} V_{p,ijm}|p\rangle\langle m| \in M_{\tilde{k}',k}$. Similarly with $\langle i|\tilde{V}_\varepsilon$ and $\langle j|\tilde{W}_\varepsilon$.

Proof. The proof is completely elementary and follows the next lines:

In the first place, we notice that for any vectors $|\xi\rangle \in \mathcal{H}$, $|\eta\rangle \in \mathcal{H}'$ and any operator $U \in \mathcal{B}(\mathcal{H}', \mathcal{H} \otimes \mathcal{K})$

$$\text{Tr}\left[|\xi\rangle\langle\xi| \, \text{Tr}_{\mathcal{K}} U \, |\eta\rangle\langle\eta| \, U^\dagger \right] = \text{Tr}\left[(|\xi\rangle\langle\xi| \otimes \text{Id}_{\mathcal{K}}) U \, |\eta\rangle\langle\eta| \, U^\dagger \right]$$
$$= \langle\eta|U^\dagger(|\xi\rangle \otimes \text{Id}_{\mathcal{K}})(\langle\xi| \otimes \text{Id}_{\mathcal{K}}) U \, |\eta\rangle$$
$$= \left\| (\langle\xi| \otimes \text{Id}_{\mathcal{K}}) U \, |\eta\rangle \right\|^2_{\mathcal{K}}.$$

Applying this elementary identity to $|\psi_\varepsilon\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C \equiv \mathcal{H}$, $|\psi\rangle \otimes |\varphi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C \otimes \mathcal{H}_E \equiv \mathcal{H}'$ and the operator $\text{Id}_C \otimes (\tilde{V}_\varepsilon \otimes \tilde{W}_\varepsilon)(V \otimes W_\varepsilon) \in \mathcal{B}(\mathcal{H}', \mathcal{H} \otimes \mathcal{H}_{anc_a} \otimes \mathcal{H}_{anc_b})$ we have that, for each $\varepsilon \in \mathcal{Q}_{n^2}$:

$$\text{Tr}\left[|\psi_\varepsilon\rangle\langle\psi_\varepsilon| \, (\text{Id}_C \otimes \mathcal{S}^{\mathcal{U}}_\varepsilon) \left(|\psi\rangle\langle\psi|\right) \right]$$
$$= \mathbb{E}_\varepsilon \left\| (\langle\psi_\varepsilon| \otimes \text{Id}_{anc_a \otimes anc_b}) \left(\text{Id}_C \otimes (\tilde{V}_\varepsilon \otimes \tilde{W}_\varepsilon)(V \otimes W_\varepsilon) \right) (|\psi\rangle \otimes |\varphi\rangle) \right\|^2_{\mathcal{H}_{anc_a} \otimes \mathcal{H}_{anc_b}}.$$

The claim in the Proposition is obtained from the last line above just recalling the definitions $|\psi_\varepsilon\rangle = \frac{1}{n} \sum_{i,j=1}^n \varepsilon_{ij}|ij\rangle_{AB} \otimes |ij\rangle_C$ and $|\psi\rangle = \frac{1}{n} \sum_{i,j=1}^n |ij\rangle_{AB} \otimes |ij\rangle_C$. $\square$

4. Bounds for "smooth" strategies: Theorem 1.1

This section is devoted to the proof of Theorem 1.1, which provides lower bounds on resources needed to break G_{Rad} by strategies characterized by regularity measures based on parameter σ defined in Sect. 2.3.3. When we refer here to a cheating strategy for G_{Rad}, unless the opposite is explicitly specified, we mean a pure strategy $\mathcal{S}^{\mathcal{U}} = \{\tilde{V}_\varepsilon, \tilde{W}_\varepsilon, V, W_\varepsilon, |\varphi\rangle\}_\varepsilon \in \mathfrak{S}^{\mathcal{U}}_{s2w;\tilde{k},k}$.

As explained in the introduction, the main idea leading to Theorem 1.1 is the understanding of cheating strategies for G_{Rad} as assignments on the hypercube $\mathcal{Q}_{n^2}$, i.e., vector-valued functions $\Phi : \mathcal{Q}_{n^2} \to X$ where X is a suitable Banach space. Given a strategy $\mathcal{S}^{\mathcal{U}}$, the corresponding assignment Φ must be related with the value $\omega(G_{\mathrm{Rad}}; \mathcal{S}^{\mathcal{U}})$. Ideally, we hope to bound $\omega(G_{\mathrm{Rad}}; \mathcal{S}^{\mathcal{U}})$ with the expected value of the norm of Φ, quantity for which we can use Corollary 2.17 to obtain upper bounds. Proposition 3.3 gives us a first hint on how to construct Φ. Given $\mathcal{S}^{\mathcal{U}} = \{\tilde{V}_\varepsilon, \tilde{W}_\varepsilon, V, W_\varepsilon, |\varphi\rangle\}_\varepsilon$, consider the map:

$$\Phi : \mathcal{Q}_{n^2} \longrightarrow \ell_2^{r^2}$$
$$\varepsilon \mapsto \Phi^i(\varepsilon) = \frac{1}{n^2} \sum_{ij} \varepsilon_{ij} \left(\langle i|\tilde{V}_\varepsilon \otimes \langle j|\tilde{W}_\varepsilon\right) (V|ij\rangle \otimes W_\varepsilon)|\varphi\rangle, \qquad (28)$$

where r is determined by the strategy, recall (23).

Proposition 3.3 can be now read as:

$$\omega(G_{\mathrm{Rad}}; \mathcal{S}^{\mathcal{U}}) = \mathbb{E}_\varepsilon \|\Phi(\varepsilon)\|^2_{\ell_2^{r^2}}, \qquad (29)$$

so we are on a good track. It is easy to check that, by construction, $\|\Phi(\varepsilon)\|_{\ell_2^{r^2}} \le 1$ for any $\varepsilon \in \mathcal{Q}^{n^2}$ and therefore the trivial bound $\mathbb{E}_\varepsilon \|\Phi(\varepsilon)\|^2_{\ell_2^{r^2}} \le \mathbb{E}_\varepsilon \|\Phi(\varepsilon)\|_{\ell_2^{r^2}}$ holds. With this and Corollary 2.17, we can obtain—recall Definition 2.14 for σ_Φ:

$$\omega(G_{\mathrm{Rad}}; \mathcal{S}^{\mathcal{U}}) \le \left\|\mathbb{E}_\varepsilon \Phi(\varepsilon)\right\|_{\ell_2^{r^2}} + C\, \sigma_\Phi \mathrm{T}_2^{(n^2)}(\ell_2^{r^2}).$$

Furthermore, $\mathrm{T}_2^{(n^2)}(\ell_2^{r^2}) = 1$ since, more generally, $\mathrm{T}_2(\ell_2^{r^2}) = 1$.

The main problem with this approach is that the quantity $\left\|\mathbb{E}_\varepsilon \Phi(\varepsilon)\right\|_{\ell_2^{r^2}}$ might be of the same order as $\omega(G_{\mathrm{Rad}}; \mathcal{S}^{\mathcal{U}})$, making the previous bound trivial. In fact, for any given Φ there exists a rather trivial modification of it that *does not affect any dimension involved* but provides a function Φ' for which $\left\|\mathbb{E}_\varepsilon \Phi'(\varepsilon)\right\|_{\ell_2^{r^2}} = \mathbb{E}_\varepsilon \left\|\Phi'(\varepsilon)\right\|_{\ell_2^{r^2}} = \omega(G_{\mathrm{Rad}}; \mathcal{S}^{\mathcal{U}})$. This modified version of Φ can be constructed as follows. For each $\varepsilon \in \mathcal{Q}_{n^2}$, consider a unitary R_ε that rotates the vector $\Phi(\varepsilon)$ into the direction of a reference unit vector $|0\rangle$. Φ' is defined simply as $\Phi'(\varepsilon) := R_\varepsilon \Phi(\varepsilon)$. Even when this adjustment is completely artificial—the unitaries R_ε do not correspond with anything implementable by the cheaters—the approach presented so far is unable to detect such an artifact. In part, this is due to the fact that the norm considered on the image of Φ does not encode any of the structure of the cheating action. We now look at alternative constructions for Φ that amend this issue.

What we do next, is simplifying the image of the map Φ considering more involved choices for the output Banach space. This allows us to preserve an equivalence of the kind of (29) while obtaining good upper bounds for $\left\|\mathbb{E}_\varepsilon \Phi(\varepsilon)\right\|_X$.

Given a strategy $\mathcal{S}^{\mathcal{U}} = \{\tilde{V}_\varepsilon, \ \tilde{W}_\varepsilon, \ V, \ W_\varepsilon, \ |\varphi\rangle\}_\varepsilon$ we define the following two alternatives to Φ:

$$\Phi^i : \mathcal{Q}_{n^2} \longrightarrow M_{r,k} \otimes_{min} M_{r,\tilde{k}}$$
$$\varepsilon \mapsto \Phi^i(\varepsilon) = \frac{1}{n^2} \sum_{ij} \ \varepsilon_{ij} \ (\langle i|\tilde{V}_\varepsilon \otimes \langle j|\tilde{W}_\varepsilon) \ (V|ij\rangle \otimes \mathrm{Id}_{\ell_2^{\tilde{k}}}),$$
$$\Phi^{ii} : \mathcal{Q}_{n^2} \longrightarrow \mathcal{S}_1^{\tilde{k},n} \otimes_{(\varepsilon,\pi)_{1/2}} \mathcal{S}_1^{\tilde{k},n}$$
$$\varepsilon \mapsto \Phi^{ii}(\varepsilon) = \frac{1}{n^2} \sum_{ij} \ \varepsilon_{ij} \ \langle i| \otimes \langle j| \otimes (V|ij\rangle \otimes W_\varepsilon) \ |\varphi\rangle.$$

These are the central objects we study to obtain Theorem 1.1. For Φ^i, recall Sect. 2.3.1 for the definition of the $\otimes_{min}$ norm, which in this particular case can be also understood as defined by the (completely) isometric equivalence $M_{r,k} \otimes_{min} M_{r,\tilde{k}} = M_{r^2, k\tilde{k}}$. In the case of Φ^{ii} the norm on the output space was defined at the end of Sect. 2.3.3 as the interpolation space $(\mathcal{S}_1^{m,n} \otimes_\varepsilon \mathcal{S}_1^{m,n}, \mathcal{S}_1^{m,n} \otimes_\pi \mathcal{S}_1^{m,n})_{1/2}$.

Now we comment on the idea behind the definitions of these maps: recall that a strategy $\mathcal{S}^{\mathcal{U}} = \{\tilde{V}_\varepsilon, \ \tilde{W}_\varepsilon, \ V, \ W_\varepsilon, \ |\varphi\rangle\}_\varepsilon$ consists of two rounds of local operations with a communication stage in between. Fixing the first round, that is related to V, W_ε and $|\varphi\rangle$, and understanding the optimization over any $\tilde{V}_\varepsilon$, $\tilde{W}_\varepsilon$ as computing a particular norm leads us to define Φ^{ii}. When we fix $\tilde{V}_\varepsilon$, $\tilde{W}_\varepsilon$ and V—this last one is ε-independent—, optimizing then over any possible $(\mathrm{Id}_{\ell_2^k} \otimes W_\varepsilon)|\varphi\rangle$, we obtain Φ^i.

Next we describe how these maps are related to G_{Rad}.

Lemma 4.1. *For any strategy $\mathcal{S}^{\mathcal{U}}$,*

$$\omega(G_{\mathrm{Rad}}; \mathcal{S}^{\mathcal{U}}) \leq \mathbb{E}_\varepsilon \left\| \Phi^{i(ii)}(\varepsilon) \right\|_{X^{i(ii)}},$$

where we have denoted $X^i = M_{r,k} \otimes_{min} M_{r,\tilde{k}}$ and $X^{ii} = \mathcal{S}_1^{\tilde{k},n} \otimes_{(\varepsilon,\pi)_{1/2}} \mathcal{S}_1^{\tilde{k},n}$.

Remark 4.2. For Φ^{ii}, the previous statement can be strengthened to

$$\omega(G_{\mathrm{Rad}}; \mathcal{S}^{\mathcal{U}}) \leq \mathbb{E}_\varepsilon \left\| \Phi^{ii}(\varepsilon) \right\|_{\tilde{X}^{ii}},$$

where $\tilde{X}^{ii} = \mathcal{S}_1^{\tilde{k},n} \otimes_{\mathfrak{S}_2^{w-cb}} \mathcal{S}_1^{\tilde{k},n}$. Recall Definition 2.4 for this last norm.

Proof. The proof of both items in the lemma follows the same structure. We start with the bound regarding Φ^i:

Recalling Proposition 3.3:

$$\omega(G_{\mathrm{Rad}}; \mathcal{S}^{\mathcal{U}}) = \mathbb{E}_\varepsilon \left\| \frac{1}{n^2} \sum_{i,j} \varepsilon_{ij} (\langle i|\tilde{V}_\varepsilon \otimes \langle j|\tilde{W}_\varepsilon) \ (V|ij\rangle \otimes W_\varepsilon) \ |\varphi\rangle \right\|_{\ell_2^{r^2}}^2.$$

We bound this quantity as follows:

$$\omega(G_{\text{Rad}}; \mathcal{S}^{\mathcal{U}}) = \mathbb{E}_\varepsilon \left\| \frac{1}{n^2} \sum_{i,j} \varepsilon_{ij}(\langle i|\tilde{V}_\varepsilon \otimes \langle j|\tilde{W}_\varepsilon)(V|ij\rangle \otimes \text{Id}_{\ell_2^{\tilde{k}}})(\text{Id}_{\ell_2^{\ell k}} \otimes W_\varepsilon)|\varphi\rangle \right\|_{\ell_2^{r2}}^2$$

$$\leq \mathbb{E}_\varepsilon \sup_{|\varphi\rangle \in B_{\ell_2^{\ell k \tilde{k}}}} \left\| \frac{1}{n^2} \sum_{i,j} \varepsilon_{ij}(\langle i|\tilde{V}_\varepsilon \otimes \langle j|\tilde{W}_\varepsilon)(V|ij\rangle \otimes \text{Id}_{\ell_2^{\tilde{k}2}})|\varphi\rangle \right\|_{\ell_2^{r2}}^2$$

$$= \mathbb{E}_\varepsilon \sup_{|\varphi\rangle \in B_{\ell_2^{\ell k \tilde{k}}}} \left\| \Phi^i(\varepsilon)(|\varphi\rangle) \right\|_{\ell_2^{r2}}^2 = \mathbb{E}_\varepsilon \left\| \Phi^i(\varepsilon) \right\|_{M_{r2,k\tilde{k}}}^2$$

$$\leq \mathbb{E}_\varepsilon \left\| \Phi^i(\varepsilon) \right\|_{M_{r2,k\tilde{k}}} \equiv \mathbb{E}_\varepsilon \left\| \Phi^i(\varepsilon) \right\|_{X^i}.$$

The inequality in the last line holds since $\left\| \Phi^i(\varepsilon) \right\|_{M_{r2,k\tilde{k}}} \leq 1$ for any $\varepsilon \in \mathcal{Q}_{n^2}$. This can be checked by direct calculation or, alternatively, as a consequence of Remark 4.7.

For Φ^{ii}, we prove the stronger result stated in Remark 4.2. That is, considering the map Φ^{ii} taking values on the space $\tilde{X}^{ii} = \mathcal{S}_1^{\tilde{k},n} \otimes_{\mathfrak{S}_2^{w-cb}} \mathcal{S}_1^{\tilde{k},n}$, we show that:

$$\omega(G_{\text{Rad}}; \mathcal{S}^{\mathcal{U}}) \leq \mathbb{E}_\varepsilon \left\| \Phi^{ii}(\varepsilon) \right\|_{\tilde{X}^{ii}}. \tag{30}$$

Since the norm in $\tilde{X}^{ii}$ is smaller than in X^{ii}, recall Proposition 2.10, the statement of the lemma is also true. Following the proof of the first item, we start bounding:

$$\omega(G_{\text{Rad}}; \mathcal{S}^{\mathcal{U}}) = \mathbb{E}_\varepsilon \left\| \frac{1}{n^2} \sum_{i,j} \varepsilon_{ij}(\langle i|\tilde{V}_\varepsilon \otimes \langle j|\tilde{W}_\varepsilon)(V|ij\rangle \otimes W_\varepsilon)|\varphi\rangle \right\|_{\ell_2^{r2}}^2$$

$$\leq \mathbb{E}_\varepsilon \sup_{\tilde{V},\tilde{W} \in B_{M_{nr,\tilde{k}}}} \left\| \frac{1}{n^2} \sum_{i,j} \varepsilon_{ij}(\langle i|\tilde{V} \otimes \langle j|\tilde{W})(V|ij\rangle \otimes W_\varepsilon)|\varphi\rangle \right\|_{\ell_2^{r2}}^2$$

$$= \mathbb{E}_\varepsilon \sup_{\tilde{V},\tilde{W} \in B_{M_{nr,\tilde{k}}}} \left\| (\tilde{V} \otimes \tilde{W})\left(\frac{1}{n^2} \sum_{i,j} \varepsilon_{ij}(\langle i| \otimes \langle j| \otimes V|ij\rangle \otimes W_\varepsilon)|\varphi\rangle \right) \right\|_{\ell_2^{r2}}^2$$

$$= \mathbb{E}_\varepsilon \sup_{\tilde{V},\tilde{W} \in B_{M_{nr,\tilde{k}}}} \left\| (\tilde{V} \otimes \tilde{W})\left(\Phi^{ii}(\varepsilon) \right) \right\|_{\ell_2^{r2}}^2$$

$$\overset{(\text{Lemma 2.6})}{\leq} \mathbb{E}_\varepsilon \left\| \Phi^{ii}(\varepsilon) \right\|_{\mathcal{S}_1^{\tilde{k},n} \otimes_{\mathfrak{S}_2^{w-cb}} \mathcal{S}_1^{\tilde{k},n}}^2$$

$$\leq \mathbb{E}_\varepsilon \left\| \Phi^{ii}(\varepsilon) \right\|_{\mathcal{S}_1^{\tilde{k},n} \otimes_{\mathfrak{S}_2^{w-cb}} \mathcal{S}_1^{\tilde{k},n}} \equiv \mathbb{E}_\varepsilon \left\| \Phi^{ii}(\varepsilon) \right\|_{\tilde{X}^{ii}}.$$

As before, the last inequality is true given that $\left\| \Phi^{ii}(\varepsilon) \right\|_{\mathcal{S}_1^{\tilde{k},n} \otimes_{\mathfrak{S}_2^{w-cb}} \mathcal{S}_1^{\tilde{k},n}} \leq 1$ for any $\varepsilon \in \mathcal{Q}^{n^2}$. Again, this fact can be shown by direct computation (see Remark 4.7 for an alternative proof). $\square$

The regularity of the maps $\Phi^{i(ii)}$ can be characterized by parameters $\sigma_{\mathcal{S}^{\mathcal{U}}}^i := \sigma_{\Phi^i}$ and $\sigma_{\mathcal{S}^{\mathcal{U}}}^{ii} := \sigma_{\Phi^{ii}}$—recall Definition 2.14. More explicitly:

$$\sigma_{\mathcal{S}^{\mathcal{U}}}^{i(ii)} = \log(n^2)\, \mathbb{E}_\varepsilon \left(\sum_{i,j} \|\partial_{ij} \Phi^{i(ii)}(\varepsilon)\|_{X^{i(ii)}}^2 \right)^{1/2}. \tag{31}$$

In the case of an arbitrary (possibly *non-pure*) strategy $\mathcal{S}$, we can assign parameters $\sigma_{\mathcal{S}}^i$, $\sigma_{\mathcal{S}}^{ii}$ with the simple prescription:

$$\sigma_{\mathcal{S}}^{i(ii)} := \inf_{\substack{\mathcal{S}^{\mathcal{U}} \\ \text{purifying } \mathcal{S}}} \sigma^{i(ii)}.$$

From now on, we omit the subindex specifying the strategy, which is always determined by the context, and refer to these parameters as σ^i, σ^{ii}.

The above expressions for σ^i, σ^{ii} can be bounded by the easier expressions appearing in the introduction. See "Appendix A" for details. In Eq. (31) the analytic nature of these parameters is clearer while the approximate expressions in Sect. 1 are closer to an operational interpretation of them.

With definition (31) at hand and taking into account Corollary 2.17, we can obtain:

Lemma 4.3. *For any strategy $\mathcal{S}^{\mathcal{U}}$,*

i.

$$\omega(G_{\mathrm{Rad}}; \mathcal{S}^{\mathcal{U}}) \leq \left\| \mathbb{E}_\varepsilon \Phi^i(\varepsilon) \right\|_{X^i} + C\, \sigma^i\, \mathrm{T}_2^{(n^2)}\left(X^i \right),$$

ii.

$$\omega(G_{\mathrm{Rad}}; \mathcal{S}^{\mathcal{U}}) \leq \left\| \mathbb{E}_\varepsilon \Phi^{ii}(\varepsilon) \right\|_{\tilde{X}^{ii}} + C\, \sigma^{ii}\, \mathrm{T}_2^{(n^2)}\left(X^{ii} \right).$$

Comment 4.4. Notice the change of norms in the second item of the lemma. This refinement is needed later on in order to obtain Proposition 4.6 below.

Proof. The first item is a direct consequence of Corollary 2.17 applied to the bound in Lemma 4.1, i.

The second item proceeds similarly but with a small detour. Using now Pisier's inequality, Lemma 2.16 (with $p = 1$ and a trivial triangle inequality, as in the proof of Corollary 2.17), in the stronger inequality (30) we obtain

$$\mathbb{E}_\varepsilon \left\| \Phi^{ii}(\varepsilon) \right\|_{\tilde{X}^{ii}} \leq \left\| \mathbb{E}_\varepsilon \Phi^{ii}(\varepsilon) \right\|_{\tilde{X}^{ii}} + C\, \log(n)\, \mathbb{E}_{\varepsilon,\tilde{\varepsilon}} \left\| \sum_{k,l=1}^n \tilde{\varepsilon}_{kl} \partial_{kl} \Phi^{ii}(\varepsilon) \right\|_{\tilde{X}^{ii}}.$$

Now, according to Proposition 2.10, we can upper bound the last summand above changing the norm $\tilde{X}^{ii}$ by X^{ii}. Considering that (recall again Comment 2.12)

$$\mathbb{E}_{\varepsilon,\tilde{\varepsilon}} \left\| \sum_{k,l=1}^n \tilde{\varepsilon}_{kl} \partial_{kl} \Phi^{ii}(\varepsilon) \right\|_{X^{ii}} \lesssim \mathrm{T}_2^{(n^2)}(X^{ii})\, \mathbb{E}_\varepsilon \left(\sum_{k,l=1}^n \|\partial_{kl} \Phi^{ii}(\varepsilon)\|_{X^{ii}}^2 \right)^{1/2},$$

we have:

$$\omega(G_{\mathrm{Rad}}; \mathcal{S}^{\mathcal{U}}) \leq \left\| \mathbb{E}_\varepsilon \Phi^{ii}(\varepsilon) \right\|_{\tilde{X}^{ii}} + C \, \log(n) \, \mathrm{T}_2^{(n^2)}(X^{ii}) \, \mathbb{E}_\varepsilon \left(\sum_{k,l=1}^n \|\partial_{kl} \Phi^{ii}(\varepsilon)\|_{X^{ii}}^2 \right)^{1/2}.$$

We obtain Lemma 4.3, ii., identifying σ^{ii} above. $\quad\square$

Lemma 4.3 allows us to somehow exchange the lack of control on the behaviour of a general strategy by the control of some properties of the Banach spaces involved. Bounding the quantities appearing there, we obtain our main result:

Theorem 4.5 (Formal statement of Theorem 1.1). *Given an arbitrary (possibly non-pure) strategy* $\mathcal{S} \in \mathfrak{S}_{s2w;\tilde{k},k}$,

I.

$$\omega(G; \mathcal{S}) \leq C_1 + C_2 \, \sigma^i \, \log^{1/2}(k\tilde{k}) + O\left(\frac{1}{n^{1/2}}\right);$$

II.

$$\omega(G; \mathcal{S}) \leq \tilde{C}_1 + C_3 \, \tilde{\sigma}^{ii} \, \log^{1/2}(nk\tilde{k}) + O\left(\frac{1}{n^{1/2}} + \frac{\log(n) \log^{1/2}(nk\tilde{k})}{n}\right),$$

where we have denoted $\tilde{\sigma}^{ii} = n^{3/4} \log(n) \, \sigma^{ii}$.

Above, C_1, $\tilde{C}_1 < 1$, C_2, C_3 *are positive constants.*

The following proposition precisely takes care of bounding part of the terms appearing in Lemma 4.3, as a key step to prove the theorem.

Proposition 4.6. *For any pure strategy* $\mathcal{S}^{\mathcal{U}} \in \mathfrak{S}_{s2w;\tilde{k},k}$:

i.

$$\left\| \mathbb{E}_\varepsilon \Phi^i(\varepsilon) \right\|_{X^i} \leq \frac{3}{4} + \frac{C}{\sqrt{n}}.$$

ii.

$$\left\| \mathbb{E}_\varepsilon \Phi^{ii}(\varepsilon) \right\|_{\tilde{X}^{ii}} \leq \frac{\sqrt{3}}{2} + \frac{C}{\sqrt{n}} + C' \frac{\log(n) \log^{1/2}(k\tilde{k})}{n},$$

where C, C' *are universal constants.*

The sequence leading to Theorem 4.5 is the following: Proposition 4.6.i $\Rightarrow$ Theorem 4.5.I $\Rightarrow$ Proposition 4.6.ii $\Rightarrow$ Theorem 4.5.II. To simplify the presentation, we will first write the proof of both statements of Theorem 4.5, assuming the corresponding statements of Proposition 4.6. Then we will prove Proposition 4.6, using Theorem 4.5.I in the proof of statement (ii).

Proof of Theorem 4.5. To obtain the statement of the theorem, as we already said, we start considering Lemma 4.3. Then, we need to bound:

1. the type constants $T_2^{(n^2)}(X^i)$ and $T_2^{(n^2)}(X^{ii})$. These bounds are already provided in Eqs. (11) and (13), respectively. We recall these bounds here for reader's convenience:

$$T_2^{(n^2)}(X^i) \leq T_2(X^i) \lesssim \log^{1/2}(k\tilde{k}), \qquad T_2^{(n^2)}(X^{ii}) \lesssim n^{3/4} \log(n) \log^{1/2}(n\tilde{k});$$

2. the terms $\left\| \mathbb{E}_\varepsilon \Phi^i(\varepsilon) \right\|_{X^i}$ and $\left\| \mathbb{E}_\varepsilon \Phi^{ii}(\varepsilon) \right\|_{\tilde{X}^{ii}}$. These quantities are controlled by Proposition 4.6.

With this we obtain the stated bound in the case of pure strategies. Nonetheless, statements about pure strategies can be transformed into statements about general strategies taking into account the relation (26). As we said at the end of Sect. 3, this relation is polynomial in the parameters involved and therefore, the change from pure to general strategies only induces corrections by constant factors that we absorbed in the constants C_2, C_3 present in the statement. Similar considerations deal with the amount of classical communication included in $\tilde{k}$, in this case one has to recall Eq. (25). See "Appendix B" for further details. □

Proof of Proposition 4.6, i. The norm in the L.H.S. of Proposition 4.6, i., is attained at unit vectors $|\varphi\rangle \in \ell_2^{k\tilde{k}}$, $|\xi\rangle \in \ell_2^{r^2}$ (independent of ε)[16]:

$$\left\| \mathbb{E}_\varepsilon \Phi^i(\varepsilon) \right\|_{M_{r^2,k\tilde{k}}} = \left| \mathbb{E}_\varepsilon \langle\xi| \Phi^i(\varepsilon) |\varphi\rangle \right| \leq \mathbb{E}_\varepsilon \left| \langle\xi| \Phi^i(\varepsilon) |\varphi\rangle \right|.$$

Expanding this expression we have:

$$\left\| \mathbb{E}_\varepsilon \Phi^i(\varepsilon) \right\|_{M_{r^2,k\tilde{k}}} \leq \mathbb{E}_\varepsilon \left| \frac{1}{n^2} \sum_{ij} \varepsilon_{ij} \langle\xi| \left(\langle i|\tilde{V}_\varepsilon \otimes \langle j|\tilde{W}_\varepsilon \right) \left(V |ij\rangle \otimes \mathrm{Id}_{\ell_2^{\tilde{k}}} \right) |\varphi\rangle \right|$$

$$= \mathbb{E}_\varepsilon \left| \langle\overline{\xi}_\varepsilon | \overline{\varphi}\rangle \right|,$$

where we have defined the unit vectors:

$$\langle\overline{\xi}_\varepsilon| := \frac{1}{n} \sum_{i,j} \varepsilon_{ij} \langle ij|_C \otimes \langle\xi| \left(\langle i|\tilde{V}_\varepsilon \otimes \langle j|\tilde{W}_\varepsilon \right),$$

$$|\overline{\varphi}\rangle := \frac{1}{n} \sum_{i,j} |ij\rangle_C \otimes \left(V |ij\rangle \otimes \mathrm{Id}_{\ell_2^{\tilde{k}'}} \right) |\varphi\rangle.$$

Now, notice that there exists at least one ε^* such that $|\langle\overline{\xi}_{\varepsilon^*} | \overline{\varphi}\rangle| \geq \|\mathbb{E}_\varepsilon \Phi^i(\varepsilon)\|_{M_{r^2,k\tilde{k}}}$. Consider this ε^* to rewrite $|\overline{\varphi}\rangle = |\overline{\xi}_{\varepsilon^*}\rangle + (|\overline{\varphi}\rangle - |\overline{\xi}_{\varepsilon^*}\rangle)$. An application of Cauchy–Schwarz inequality gives us the following:

$$\|\mathbb{E}_\varepsilon \Phi^i(\varepsilon)\|_{M_{r^2,k\tilde{k}}} \leq \mathbb{E}_\varepsilon \left| \langle\overline{\xi}_\varepsilon|\overline{\varphi}\rangle \right| \leq \mathbb{E}_\varepsilon \left| \langle\overline{\xi}_\varepsilon|\overline{\xi}_{\varepsilon^*}\rangle \right| + \left| \langle\overline{\varphi} - \overline{\xi}_{\varepsilon^*}|\overline{\varphi} - \overline{\xi}_{\varepsilon^*}\rangle \right|^{1/2}. \qquad (32)$$

Now we bound both summands in the R.H.S. of the previous expression separately:

---

16 Recall the isometric identity $M_{r,k} \otimes_{min} M_{r,\tilde{k}} = M_{r^2,k\tilde{k}}$.

- For the second:

$$\left| \langle \overline{\varphi} - \overline{\xi}_{\varepsilon*} | \overline{\varphi} - \overline{\xi}_{\varepsilon*} \rangle \right|^{1/2} \leq \left(2(1 - \langle \overline{\xi}_{\varepsilon*} | \overline{\varphi} \rangle) \right)^{1/2} \leq \left(2(1 - \|\mathbb{E}_{\varepsilon} \, \Phi(\varepsilon)\|_{M_{r^2,k\bar{k}}}) \right)^{1/2}$$
$$\leq \frac{7}{4} - \frac{4}{3} \|\mathbb{E}_{\varepsilon} \, \Phi^i(\varepsilon)\|_{M_{r^2,k\bar{k}}},$$

where the last inequality is based on an elementary linear approximation of $\sqrt{2(1-x)}$ (simply by the line tangent to the function in a suitably chosen point).

- For the first one, we will find that:

$$\mathbb{E}_{\varepsilon} \left| \langle \overline{\xi}_{\varepsilon} | \overline{\xi}_{\varepsilon*} \rangle \right| = O\left(\frac{1}{\sqrt{n}} \right).$$

In order to show this bound, we start observing that:

$$\mathbb{E}_{\varepsilon} \left| \langle \overline{\xi}_{\varepsilon} | \overline{\xi}_{\varepsilon*} \rangle \right| = \mathbb{E}_{\varepsilon} \left| \frac{1}{n^2} \sum_{ij} \varepsilon_{ij} \varepsilon_{ij}^* \langle \xi | \left(\langle i | \tilde{V}_{\varepsilon} \, \tilde{V}_{\varepsilon*}^{\dagger} | i \rangle \otimes \langle j | \tilde{W}_{\varepsilon} \, \tilde{W}_{\varepsilon*}^{\dagger} | j \rangle \right) | \xi \rangle \right|$$

$$\leq \mathbb{E}_{\varepsilon} \sup_{\substack{|\xi_i\rangle, |\varphi_j\rangle \in B_{\ell_2^{r^2}} \\ \text{for } i,j=1,\ldots,n}} \left| \frac{1}{n^2} \sum_{ij} \varepsilon_{ij} \varepsilon_{ij}^* \langle \xi_i | \varphi_j \rangle \right|.$$

An application of the Grothendieck inequality [36] allows us to restrict $r = 1$ in the last supremum at the cost of the complex Grothendieck constant $K_G^{\mathbb{C}}$. Furthermore, Krivine's result that the two dimensional Grothendieck constant is equal to $\sqrt{2}$ [37] allows to further restrict the supremum to the choice of signs loosing another factor of $\sqrt{2}$ (see [38, Claim 4.7] for an explicit argument). In conclusion, we have the following bound:

$$\mathbb{E}_{\varepsilon} \sup_{\substack{|\xi_i\rangle, |\varphi_j\rangle \in B_{\ell_2^{r^2}} \\ \text{for } i,j=1,\ldots,n}} \left| \frac{1}{n^2} \sum_{ij} \varepsilon_{ij} \varepsilon_{ij}^* \langle \xi_i | \varphi_j \rangle \right| \leq \sqrt{2} K_G^{\mathbb{C}} \, \mathbb{E}_{\varepsilon} \sup_{\substack{t_i, s_j \in \{\pm 1\} \\ \text{for } i,j=1,\ldots,n}} \frac{1}{n^2} \sum_{ij} \varepsilon_{ij} \varepsilon_{ij}^* t_i s_j$$

But the last quantity is of order $O(1/\sqrt{n})$. One can understand this as a consequence of Hoeffding's inequality [39]: for each choice $(s_i, t_j)_{i,j} \in \{\pm 1\}^n \times \{\pm 1\}^n$ the probability that $\frac{1}{n^2} \sum_{ij} \varepsilon_{ij} \varepsilon_{ij}^* t_i s_j$ is larger than $2/\sqrt{n}$ is upper bounded by e^{-2n}. Then, a union bound over the 2^{2n} possible sequences $(s_i, t_j)_{i,j} \in \{\pm 1\}^n \times \{\pm 1\}^n$ concludes the argument.

Joining everything in (32) we obtain the bound in Proposition 4.6, i.   □

Proof Proposition 4.6, ii. Remember that we can already use Theorem 4.5.I here. It turns out that Proposition 4.6, ii. is a consequence of this first part of our main theorem.

The key idea is understanding the norm $\left\| \mathbb{E}_{\varepsilon} \Phi^{ii \cdot} \right\|_{\tilde{X}^{ii}}$ as the optimization over some family of strategies with small enough parameter σ^i. Concretely, considering the characterization of the norm $\tilde{X}^{ii}$ given in Lemma 2.6, we can prove that

$$\left\| \mathbb{E}_{\varepsilon} \Phi^{ii}(\varepsilon) \right\|_{\tilde{X}^{ii}} \leq \sup_{\substack{r \in \mathbb{N} \\ \tilde{V}, \tilde{W} \in B_{M_{nr,\bar{k}'}}}} \omega \left(G_{\text{Rad}}; \{\tilde{V}, \tilde{W}, V, W_{\varepsilon}, |\varphi\rangle\}_{\varepsilon} \right)^{1/2}. \tag{33}$$

The desired bound follows now from realizing that in the strategies on which this optimization is performed, the second round of local operations, $\tilde{V} \otimes \tilde{W}$, is ε-independent. Therefore, for these strategies, according to Example 2.15, $\sigma^i \approx \frac{\log(n)}{n}$, which, in conjunction with Theorem 4.5, I., leads to the desired statement. To obtain the precise statement appearing there, we have considered the elementary inequality $(1+x)^{1/2} \leq 1 + x/2$.

Then, to finish, let us prove the claim (33).

Recall that, according to Lemma 2.6 we can write:

$$\left\| \mathbb{E}_\varepsilon \Phi^{ii}(\varepsilon) \right\|_{\tilde{X}^{ii}} = \sup_{\substack{r \in \mathbb{N} \\ \tilde{V}, \tilde{W} \in B_{M_{nr,\tilde{k}}}}} \left\| \mathbb{E}_\varepsilon \left(\tilde{V} \otimes \tilde{W} \right) \left(\frac{1}{n^2} \sum_{i,j} \varepsilon_{ij} \left(\langle i| \otimes \langle j| \right) (V|ij\rangle \otimes W_\varepsilon) |\varphi\rangle \right) \right\|_{\ell_2^{r2}}$$

$$\leq \sup_{\substack{r \in \mathbb{N} \\ \tilde{V}, \tilde{W} \in B_{M_{nr,\tilde{k}}}}} \mathbb{E}_\varepsilon \left\| \frac{1}{n^2} \sum_{i,j} \varepsilon_{ij} \left(\langle i|\tilde{V} \otimes \langle j|\tilde{W} \right) (V|ij\rangle \otimes W_\varepsilon) |\varphi\rangle \right\|_{\ell_2^{r2}}.$$

Furthermore, considering the elementary bound $\mathbb{E}_\varepsilon \phi(\varepsilon) \leq \left(\mathbb{E}_\varepsilon \phi(\varepsilon)^2 \right)^{\frac{1}{2}}$, valid for any function $\phi : \mathcal{Q}_{n^2} \to \mathbb{R}$, we can finally write:

$$\left\| \mathbb{E}_\varepsilon \Phi^{ii}(\varepsilon) \right\|_{\tilde{X}^{ii}} \leq \sup_{\substack{r \in \mathbb{N} \\ \tilde{V}, \tilde{W} \in B_{M_{nr,\tilde{k}}}}} \left(\mathbb{E}_\varepsilon \left\| \frac{1}{n^2} \sum_{i,j} \varepsilon_{ij} \left(\langle i|\tilde{V} \otimes \langle j|\tilde{W} \right) (V|ij\rangle \otimes W_\varepsilon) |\varphi\rangle \right\|_{\ell_2^{r2}}^2 \right)^{\frac{1}{2}}$$

$$= \sup_{\substack{r \in \mathbb{N} \\ \tilde{V}, \tilde{W} \in B_{M_{nr,\tilde{k}}}}} \omega \left(G_{\mathrm{Rad}}; \{ \tilde{V}, \tilde{W}, V, W_\varepsilon, |\varphi\rangle \}_\varepsilon \right)^{1/2},$$

as claimed. □

We make a final comment that, in some sense, connects with the next section where we will discuss possible extensions of the approach presented up to this point.

Remark 4.7. The appearance of the norms $X^i = M_{r,k} \otimes_{min} M_{r,\tilde{k}}$, $X^{ii} = \mathcal{S}_1^{\tilde{k},n} \otimes_{(\varepsilon,\pi)_{1/2}} \mathcal{S}_1^{\tilde{k},n}$ above might seem, at some point, arbitrary, in the sense that we have used these norms merely to *upper* bound the value $\omega(G_{\mathrm{Rad}}, \mathcal{S}^{\mathcal{U}})$. Part of the motivation to consider these spaces is the fact that we are able to properly understand their type properties. But we can wonder: is any norm upper bounding $\omega(G_{\mathrm{Rad}}, \mathcal{S}^{\mathcal{U}})$ a reasonable choice provided that we can control the relevant type constants? Obviously, this is not the case. Actually, in Sect. 5 we explore further this issue. By now, let us note that the chosen norms also satisfy some basic normalization conditions. In particular, it can be shown that the elements constituting Φ^i, Φ^{ii} are well normalized when regarded as elements in X^i and X^{ii}, respectively. Concretely, for each $i, j \in [n]$

$$\left\| (\langle i|\tilde{V}_\varepsilon \otimes \langle j|\tilde{W}_\varepsilon) (V|ij\rangle \otimes \mathrm{Id}_{\ell_2^{\tilde{k}}}) \right\|_{X^i} \leq 1,$$

for any contractive operators $\tilde{V}_\varepsilon$, $\tilde{W}_\varepsilon$, V, W_ε, and

$$\| |i\rangle \otimes |j\rangle \otimes (V|ij\rangle \otimes W_\varepsilon) |\varphi\rangle \|_{X^{ii}} \leq 1,$$

for any unit vector $|\varphi\rangle$ and contractive V, W_ε.

The first bound is straightforward. Since $\tilde{V}_\varepsilon \otimes \tilde{W}_\varepsilon$ and $V \otimes \mathrm{Id}_{\ell_2^{\tilde{k}}}$ are contractive operators, $\langle i|\tilde{V}_\varepsilon \otimes \langle j|\tilde{W}_\varepsilon$ and $V|ij\rangle \otimes \mathrm{Id}_{\ell_2^{\tilde{k}}}$ are also contractive and the same applies to their composition.

For the second bound, fixing i, j, we first notice that $|\tilde{\varphi}\rangle := (V|ij\rangle \otimes \mathrm{Id}_{\ell_2^{\tilde{k}^2}})(\mathrm{Id}_{\ell_2^k} \otimes W_\varepsilon)|\varphi\rangle$ has norm $\||\tilde{\varphi}\rangle\|_{\ell_2^{\tilde{k}^2}} \leq 1$. Furthermore, considering the norm-one injections ι_i :
$\ell_2^{\tilde{k}} \ni |\varphi\rangle \mapsto |i\rangle \otimes |\varphi\rangle \in \mathcal{S}_1^{\tilde{k},n}$, we have that $|i\rangle \otimes |j\rangle \otimes |\tilde{\varphi}\rangle = \iota_i \otimes \iota_j(|\tilde{\varphi}\rangle)$. Therefore

$$\big\||i\rangle \otimes |j\rangle \otimes |\tilde{\varphi}\rangle\big\|_{\mathcal{S}_1^{\cdot n} \otimes_{(\varepsilon,\pi)_{1/2}} \mathcal{S}_1^{\cdot n}} \leq \big\||\tilde{\varphi}\rangle\big\|_{\ell_2^{\tilde{k}^2}} \big\|\iota_i \otimes \iota_j : \ell_2^{\tilde{k}} \to \mathcal{S}_1^{\tilde{k},n} \otimes_{(\varepsilon,\pi)_{1/2}} \mathcal{S}_1^{\tilde{k},n}\big\| \leq 1.$$

It remains to justify that, in fact,

$$\big\|\iota_i \otimes \iota_j : \ell_2^{\tilde{k}} \to \mathcal{S}_1^{\tilde{k},n} \otimes_{(\varepsilon,\pi)_{1/2}} \mathcal{S}_1^{\tilde{k},n}\big\| \leq 1.$$

This can be proved recalling that $\mathcal{S}_1^{\tilde{k},n} \otimes_{(\varepsilon,\pi)_{1/2}} \mathcal{S}_1^{\tilde{k},n}$ is the interpolation space $(\mathcal{S}_1^{\tilde{k},n} \otimes_\varepsilon \mathcal{S}_1^{\tilde{k}',n}, \mathcal{S}_1^{\tilde{k},n} \otimes_\pi \mathcal{S}_1^{\tilde{k},n})_{\frac{1}{2}}$ and $\ell_2^{\tilde{k}^2}$ can be also regarded as the space $\left(\ell_2^{\tilde{k}} \otimes_\varepsilon \ell_2^{\tilde{k}}, \ell_2^{\tilde{k}} \otimes_\pi \ell_2^{\tilde{k}}\right)_{\frac{1}{2}}$. The last assertion can be shown noticing that $\ell_2^{\tilde{k}} \otimes_\varepsilon \ell_2^{\tilde{k}} = M_{\tilde{k}}$ and $\ell_2^{\tilde{k}} \otimes_\pi \ell_2^{\tilde{k}} = \mathcal{S}_1^{\tilde{k}}$. Given that, the isometric equivalence (recall Theorem 2.9) $(M_{\tilde{k}}, \mathcal{S}_1^{\tilde{k}})_{1/2} = \mathcal{S}_2^{\tilde{k}} = \ell_2^{\tilde{k}^2}$ provides the stated fact. Then,

$$\big\|\iota_i \otimes \iota_j : \ell_2^{\tilde{k}} \to \mathcal{S}_1^{\tilde{k},n} \otimes_{(\varepsilon,\pi)_{1/2}} \mathcal{S}_1^{\tilde{k},n}\big\|$$
$$\leq \big\|\iota_i \otimes \iota_j : \ell_2^{\tilde{k}} \otimes_\varepsilon \ell_2^{\tilde{k}} \to \mathcal{S}_1^{\tilde{k},n} \otimes_\varepsilon \mathcal{S}_1^{\tilde{k},n}\big\|^{\frac{1}{2}} \big\|\iota_i \otimes \iota_j : \ell_2^{\tilde{k}} \otimes_\pi \ell_2^{\tilde{k}} \to \mathcal{S}_1^{\tilde{k},n} \otimes_\pi \mathcal{S}_1^{\tilde{k},n}\big\|^{\frac{1}{2}}$$
$$\leq \big\|\iota_i : \ell_2^{\tilde{k}} \to \mathcal{S}_1^{\tilde{k},n}\big\| \big\|\iota_j : \ell_2^{\tilde{k}} \to \mathcal{S}_1^{\tilde{k},n}\big\| \leq 1.$$

5. A Conjecture Towards Unconditional Lower Bounds

In the previous section, we have modified the naïve choice (28) for Φ in order to circumvent the problem that $\big\|\mathbb{E}_\varepsilon \Phi(\varepsilon)\big\|_{\ell_2^{r^2}}$ can be in general too large, damning that way the bounds obtained through Corollary 2.17 to be trivial. The variations Φ^i, Φ^{ii} allowed us to obtain the bounds in Theorem 4.5. An unsatisfactory feature of this result is that, in order to obtain concrete bounds on the quantum resources employed by a given strategy for G_{Rad}, we still need to make some additional assumption on that strategy. Recall that, in particular, the bounds in Theorem 4.5 depend on the regularity parameters σ^i, σ^{ii}. Ideally, we would like to obtain bounds only depending on the dimension of the quantum systems Alice and Bob manipulate.

Following this line of thought, one could ask whether, given a strategy, is possible to construct a corresponding assignment Φ that additionally displays the property of being regular enough, that is, with $\sigma_\Phi \lesssim_{\log} 1/n$. The answer is affirmative, but the cost of doing so is that the output Banach space of Φ becomes more involved and its type properties escape from the techniques used in this work. We define:

$$\Phi^{iii} : \mathcal{Q}_{n^2} \longrightarrow \left(\mathcal{S}_1^{\tilde{k},n} \otimes_{\mathfrak{S}_2^{cb-w}} \mathcal{S}_1^{\tilde{k},n}\right) \otimes_\varepsilon \ell_2^{k\tilde{k}}$$
$$\varepsilon \mapsto \Phi^{iii}(\varepsilon) = \frac{1}{n^2} \sum_{ij} \varepsilon_{ij} \langle i| \otimes \langle j| \otimes (V|ij\rangle \otimes \mathrm{Id}_{\ell_2^{\tilde{k}}}) \tag{34}$$

that relates with the value of the game G_{Rad} as stated in the following

Lemma 5.1. *For any pure strategy $\mathcal{S}^{\mathcal{U}} \in \mathfrak{S}_{s2w;\tilde{k},k}$:*

$$\omega(G_{\mathrm{Rad}}; \mathcal{S}^{\mathcal{U}})^{1/2} \lesssim \mathbb{E}_{\varepsilon} \, \|\Phi^{iii}(\varepsilon)\|_{X^{iii}},$$

where $X^{iii} := \left(\mathcal{S}_1^{\tilde{k},n} \otimes_{\mathfrak{S}_2^{cb-w}} \mathcal{S}_1^{\tilde{k},n} \right) \otimes_{\varepsilon} \ell_2^{k\tilde{k}}$

Proof. For each $\varepsilon \in \mathcal{Q}_{n^2}$, we have to interpret the tensor $\Phi^{iii}(\varepsilon)$ as the mapping:

$$\Phi^{iii}(\varepsilon) : \ell_2^{k\tilde{k}} \longrightarrow \mathcal{S}_1^{\tilde{k},n} \otimes_{\mathfrak{S}_2^{cb-w}} \mathcal{S}_1^{\tilde{k},n}$$
$$|\varphi\rangle \mapsto \Phi^{iii}(\varepsilon)(|\varphi\rangle) = \frac{1}{n^2} \sum_{ij} \varepsilon_{ij} \, \langle i | \otimes \langle j | \otimes (V|ij\rangle \otimes \mathrm{Id}_{\ell_2^{\tilde{k}}}) |\varphi\rangle.$$

Then, the norm of this map is

$$\|\Phi^{iii}(\varepsilon)\| = \sup_{|\varphi\rangle \in B_{\ell_2^{k\tilde{k}}}} \left\| \frac{1}{n^2} \sum_{ij} \varepsilon_{ij} \, \langle i | \otimes \langle j | \otimes (V|ij\rangle \otimes \mathrm{Id}_{\ell_2^{\tilde{k}}}) |\varphi\rangle \right\|_{\mathcal{S}_1^{\tilde{k},n} \otimes_{\mathfrak{S}_2^{cb-w}} \mathcal{S}_1^{\tilde{k},n}}$$

$$= \sup_{W \in B_{M_{\tilde{k}}}} \sup_{|\varphi\rangle \in B_{\ell_2^{k\tilde{k}}}} \left\| \frac{1}{n^2} \sum_{ij} \varepsilon_{ij} \, \langle i | \otimes \langle j | \otimes (V|ij\rangle \otimes W) |\varphi\rangle \right\|_{\mathcal{S}_1^{\tilde{k},n} \otimes_{\mathfrak{S}_2^{cb-w}} \mathcal{S}_1^{\tilde{k},n}}.$$

Recalling once more Lemma 2.6, we can write explicitly the norm above as:

$$\|\Phi^{iii}(\varepsilon)\| = \sup_{\substack{m \in \mathbb{N} \\ \tilde{V}, \tilde{W} \in B_{M_{\tilde{k},nm}}}} \sup_{\substack{W \in B_{M_{\tilde{k}}} \\ |\varphi\rangle \in B_{\ell_2^{k\tilde{k}}}}} \left\| \frac{1}{n^2} \sum_{ij} \varepsilon_{ij} \, (\langle i | \tilde{V} \otimes \langle j | \tilde{W}) \, (V|ij\rangle \otimes W) |\varphi\rangle \right\|_{\ell_2^{m^2}}.$$

Finally, squaring this last expression and taking the expectation over ε we conclude that:

$$\mathbb{E}_{\varepsilon} \, \|\Phi^{iii}(\varepsilon)\|^2 = \mathbb{E}_{\varepsilon} \sup_{\substack{m \in \mathbb{N} \\ \tilde{V}, \tilde{W} \in B_{M_{\tilde{k},nm}}}} \sup_{\substack{W \in B_{M_{\tilde{k}}} \\ |\varphi\rangle \in B_{\ell_2^{k\tilde{k}}}}} \left\| \frac{1}{n^2} \sum_{ij} \varepsilon_{ij} \, (\langle i | \tilde{V} \otimes \langle j | \tilde{W}) \, (V|ij\rangle \otimes W) |\varphi\rangle \right\|_{\ell_2^{m^2}}^2$$

$$\geq \mathbb{E}_{\varepsilon} \left\| \frac{1}{n^2} \sum_{ij} \varepsilon_{ij} \, (\langle i | \tilde{V}_{\varepsilon} \otimes \langle j | \tilde{W}_{\varepsilon}) \, (V|ij\rangle \otimes W_{\varepsilon}) |\varphi\rangle \right\|_{\ell_2^{m^2}}^2 = \omega(G_{\mathrm{Rad}}; \mathcal{S}^{\mathcal{U}}),$$

where we have considered that $\mathcal{S}^{\mathcal{U}} = \{\tilde{V}_{\varepsilon}, \tilde{W}_{\varepsilon}, V, W_{\varepsilon}, |\varphi\rangle\}_{\varepsilon}$. With that we are almost done. This last expression is enough to obtain

$$\omega(G_{\mathrm{Rad}}; \mathcal{S}^{\mathcal{U}}) \leq \mathbb{E}_{\varepsilon} \, \|\Phi^{iii}(\varepsilon)\|^2 \approx \left(\mathbb{E}_{\varepsilon} \, \|\Phi^{iii}(\varepsilon)\| \right)^2,$$

where the last equality (up to constants) can be obtained using Kahane inequality [26]. This is the claim of the lemma. $\square$

Now, notice that Φ^{iii} is by construction a linear map of the kind of Example 2.15, and, consequently, $\sigma_{\Phi^{iii}} \lesssim \log(n)/n$. Furthermore, by symmetry, $\mathbb{E}_{\varepsilon} \Phi^{iii}_{\mathcal{S}^{\mathcal{U}}} = 0$. Therefore, Corollary 2.17 applied to the statement of Lemma 5.1 implies:

$$\omega(G_{\mathrm{Rad}}; \mathcal{S}^{\mathcal{U}}) \lesssim_{\log} \left(\frac{\mathrm{T}_2^{(n^2)}(X^{iii})}{n} \right)^2. \tag{35}$$

The problem now reduces to find a good estimate for the type-2 constant in the last expression.

We note that the norm X^{iii} is the smallest one for which we were able to prove an equivalent to Lemma 5.1. However, the whole argument from this lemma until here would be valid for any norm larger than X^{iii} fulfilling a normalization condition with respect to the elements that sum up to $\Phi^{iii}(\varepsilon)$. We will be more explicit later on. An example of such a norm is $X^{ii} \otimes_\varepsilon \ell_2^{k\tilde{k}}$ where $X^{ii} = \mathcal{S}_1^{\tilde{k},n} \otimes_{(\varepsilon,\pi)^{1/2}} \mathcal{S}_1^{\tilde{k},n}$. Motivated by the result obtained previously about the type of X^{ii}, Eq. (13), we are led to conjecture that:

Conjecture 1 (strongest form). *For any natural numbers* n, m, p:

$$\mathrm{T}_2^{(n^2)} \left(\left(\mathcal{S}_1^{m,n} \otimes_{(\varepsilon,\pi)^{1/2}} \mathcal{S}_1^{m,n} \right) \otimes_\varepsilon \ell_2^p \right) \lesssim_{\log} \mathrm{T}_2^{(n^2)} \left(\mathcal{S}_1^{p,n} \otimes_{(\varepsilon,\pi)^{1/2}} \mathcal{S}_1^{p,n} \right) \lesssim_{\log} n^{3/4}.$$

(36)

A weaker conjecture which would also imply the desired bounds in the setting of PBC is:

Conjecture 1 (weaker form).

$$\mathrm{T}_2^{(n^2)} \left(\left(\mathcal{S}_1^{m,n} \otimes_{(\varepsilon,\pi)^{1/2}} \mathcal{S}_1^{m,n} \right) \otimes_\varepsilon \ell_2^p \right) \lesssim_{\log} n^\beta \quad \textit{for some } \beta < 1.$$

(37)

According to what we explained above, there is a plethora of norms for which the positive resolution of the corresponding conjecture would imply unconditional exponential lower bounds for the resources in attacks for PBC. Next, we formalize this discussion characterizing those norms and then we rewrite the Conjecture in a unified form.

First, we characterize what we need from a norm X to follow the previous argument substituting X^{iii} by this X. In this section we refer to X as a *valid norm* if it satisfies:

P.i. X is a norm on the algebraic tensor product $\mathcal{S}_1^{m,n} \otimes \mathcal{S}_1^{m,n} \otimes \ell_2^p$;
P.ii. $\|x\|_X \gtrsim \|x\|_{X^{iii}}$ for any $x \in X$;
P.iii. $\left\| |i\rangle \otimes |j\rangle \otimes (V|ij\rangle \otimes \mathrm{Id}_{\ell_2^{\tilde{k}'}}) \right\|_X \leq 1$ for any contraction V.

Notice that P.ii. guarantees a relation with the value of G_{Rad} in analogy with Lemma 5.1 and P.iii. guarantees that $\Phi^{iii} : \mathcal{Q}_{n_2} \to X$ still falls in the setting of Example 2.15, i.e., we still have $\sigma_{\Phi^{iii}} \lesssim \log(n)/n$. These two properties therefore translate in the fact that the bound (35) is still true with the type-2 constant of any valid norm X instead of X^{iii}.

We can state

Conjecture 1 (even weaker form). *For some valid norm, i.e. a norm X satisfying properties* P.i., P.ii. *and* P.iii. *above, and some dimension independent constant* $\beta < 1$:

$$\mathrm{T}_2^{(n^2)} (X) \lesssim_{\log} n^\beta.$$

(38)

Now, to state our conjecture in its weakest form we need to introduce the notion of type constant of an operator $F : X \to Y$. The type-2 constant of a linear map $F : X \to Y$ is the infimum of the constants T such that

$$\left(\mathbb{E}_\varepsilon \left[\| \sum_i \varepsilon_i F(x_i) \|_Y^2 \right] \right)^{1/2} \leq \mathrm{T} \left(\sum_i \|x_i\|_X^2 \right)^{1/2},$$

for any finite sequence $\{x_i\}_i \subset X$. In analogy with the case of the type constant of a Banach space, when the cardinal of this sequence is restricted, we refer to the type-2 constant with m vectors of $F : X \to Y$ and denote $T_2^{(m)}(F : X \to Y)$.

We are interested here in the type of the identity map $\text{Id} : X \to X^{iii}$, being X a *valid norm*. In fact, the final statement of our conjecture is as follows:

Conjecture 1 (weakest form). *For some valid norm, i.e. a norm X satisfying properties* P.i., P.ii. *and* P.iii. *above, and some dimension independent constant* $\beta < 1$:

$$T_2^{(n^2)}\left(\text{Id} : X \to X^{iii}\right) \lesssim_{\log} n^{\beta}. \tag{39}$$

Remark 5.2. Notice that in particular, $T_2^{(n^2)}\left(\text{Id} : X \to X^{iii}\right) \lesssim T_2^{(n^2)}(Y)$ for any *valid norm Y* such that $\|x\|_{X^{iii}} \lesssim \|x\|_Y \lesssim \|x\|_X$. Therefore, the last statement for our conjecture, Eq. (39), is indeed weaker than the previous ones.

Within the family of *valid* norms characterized by properties P.i., P.ii., P.iii. we obviously find the spaces X^{iii} and $\left(\mathcal{S}_1^{m,n} \otimes_{(\varepsilon,\pi)_{1/2}} \mathcal{S}_1^{m,n}\right) \otimes_{\varepsilon} \ell_2^p$. But also, the space $\left(\mathcal{S}_1^{m,n} \otimes_{\mathfrak{S}_2^w} \mathcal{S}_1^{m,n}\right) \otimes_{\varepsilon} \ell_2^p$, see Sect. 2.3.1 for the definition. An obstruction for the techniques used in this work to obtain upper bounds for the type constants of these spaces is the pathological behaviour of the injective tensor product with respect to interpolation methods [40]. In order to support the validity of the stated conjecture, we explore next the most direct approaches to disprove it, lower bounding the type-2 constant of the spaces involved. We find that these approaches do not lead to bounds stronger than $T_2(X) \gtrsim_{\log} n^{3/4}$ for at least some *valid* norm X.

In first place, one can obtain lower bounds for the type constants of a space X by estimating the type constant of its subspaces, since $T_p(X) \geq T_p(S)$ for any subspace $S \subseteq X$. Restricting to the case of valid norms, the type constants of the simplest subspaces are not large enough to disprove our conjecture (see [17, Section 4.7.1] for details). As we explain in the next section, another, less trivial, way to obtain lower bounds for the type 2-constant of a normed space X is by studying its volume ratio.

5.1. Volume ratio. Although the Banach spaces that appear in this work are prominently complex, for the sake of simplicity we will restrict ourselves to real spaces in this section. There exist standard tools [41–44] to transfer results in this case to the complex domain, albeit some technicalities might appear in that process [45]. Since our aim here is restricted to showing some evidence in favour of our conjecture, we do not think that these intricacies add anything of essential importance to the following discussion.

A standard approach to understand the type/cotype properties of a space X consists in the computation of its volume ratio, $\text{vr}(X)$, a notion originated in [46,47]. The reason is that this parameter provides a lower bound for the cotype-2 constant. This is the content of the following result due to Milman and Bourgain:

Theorem 5.3. ([48]) *For a Banach space X,*

$$C_2(X) \log\left(2\,C_2(X)\right) \gtrsim \text{vr}(X).$$

Taking into account the duality between type and cotype constants, Eq. (9), the last result translates into a lower bound for the type-2 constant of the dual space:

$$T_2(X) \geq C_2(X^*) \gtrsim_{\log} \text{vr}(X^*),$$

giving as another technique to try to disprove (38). In this section we upper bound the volume ratio of various *valid* norms obtaining results that are again compatible with a positive resolution of the conjecture of the previous section.

We start defining the volume ratio of a normed space X, $\mathrm{vr}(X)$. Given a d-dimensional Banach space X,

$$\mathrm{vr}(X) = \left(\frac{\mathrm{vol}_d(B_X)}{\mathrm{vol}_d(\mathcal{E}_X)}\right)^{1/d}, \tag{40}$$

where $\mathcal{E}_X$ is the ellipsoid of maximal volume contained in B_X and $\mathrm{vol}_d(\,\cdot\,)$ denotes the d-dimensional Lebesgue measure. Before stating the main result of this section, we make now a tiny digression about the relation between volume ratio and cotype. In few words, this relation is still far from being well understood. The question about the existence of some direct relation between the volume ratio of a space and its cotype—in the opposite direction to Theorem 5.3—was already asked in the seminal work [47] and also in the more recent [49]. While it is known that volume ratio and cotype cannot be equivalent in general[17], it is not known whether a converse to Theorem 5.3 might hold (maybe up to factors that are logarithmic in the dimension) for spaces with additional structure such as tensor norms on tensor products of ℓ_p spaces, for instance. Studying further these questions is an extremely interesting avenue to tackle the problems we are concerned with in this work, at the same time as shedding light on the relation between two very fundamental notions in local Banach space theory.

We focus on spaces of the form $\left(\mathcal{S}_1^{m,n} \otimes_\alpha \mathcal{S}_1^{m,n}\right) \otimes_\varepsilon \ell_2^p$, where $\mathcal{S}_1^{m,n}$ must be understood as $\ell_2^m \otimes_\pi \ell_2^n$ and the ℓ_2 spaces that appear from now on, as real Hilbert spaces unless the opposite is indicated. We prove:

Theorem 5.4. *Let α be a* tensor norm *such that, for any $x \in \mathcal{S}_1^{m,n} \otimes_\alpha \mathcal{S}_1^{m,n}$:*

1. $\|x\|_{\mathcal{S}_1^{m,n} \otimes_\alpha \mathcal{S}_1^{m,n}} \leq \|x\|^{1/2}_{\mathcal{S}_1^{m,n} \otimes_\pi \mathcal{S}_1^{m,n}} \|x\|^{1/2}_{\mathcal{S}_1^{m,n} \otimes_\varepsilon \mathcal{S}_1^{m,n}}$;
2. $\|x\|_{\ell_2^{n^2 m^2}} \leq \|x\|_{\mathcal{S}_1^{m,n} \otimes_\alpha \mathcal{S}_1^{m,n}}$.

Then, considering $X = \left(\mathcal{S}_1^{m,n} \otimes_\alpha \mathcal{S}_1^{m,n}\right) \otimes_\varepsilon \ell_2^p$,

$$\mathrm{vr}(X^*) \lesssim n^{3/4}.$$

The proof uses several standard tools from geometric Banach space theory, mainly following the approach of [49]. But before going into the proof, we note that some of our *valid* norms indeed fulfill the conditions of the theorem. For illustrative purposes, we briefly comment on the case of the (complex) spaces $(\mathcal{S}_1^{m,n} \otimes_{\mathfrak{S}_2^w} \mathcal{S}_1^{m,n}) \otimes_\varepsilon \ell_2^p$ and $(\mathcal{S}_1^{m,n} \otimes_{(\varepsilon,\pi)_{1/2}} \mathcal{S}_1^{m,n}) \otimes_\varepsilon \ell_2^p$ that have appeared before in our work. Both fulfil conditions 1 and 2 in the statement above. Let's see that:

From Proposition 2.10 we know that

$$\|x\|_{\mathcal{S}_1^{m,n} \otimes_{\mathfrak{S}_2^w} \mathcal{S}_1^{m,n}} \leq \|x\|_{\mathcal{S}_1^{m,n} \otimes_{(\varepsilon,\pi)_{1/2}} \mathcal{S}_1^{m,n}}. \tag{41}$$

---

[17] It can be seen that the volume ratio of the space $\ell_\infty^{n^\alpha} \oplus_\infty \ell_2^n$ is bounded by a universal constant for any $n \in \mathbb{N}$ and any $0 < \alpha < 1$. However, the cotype-2 constant of this space is of order $n^{\alpha/2}$. We are indebted to Elisabeth Werner for kindly communicating us this counterexample.

Standard properties of interpolation (Theorem 2.7) guarantee that $(\varepsilon, \pi)_{1/2}$ is a tensor norm[18] fulfilling

$$\|x\|_{(Y_0, Y_1)_{1/2}} \leq \|x\|_{Y_0}^{1/2} \|x\|_{Y_1}^{1/2} \quad , \text{ for any finite dimensional Banach spaces } Y_0, \ Y_1. \tag{42}$$

In order to see this last inequality, just apply, for a given $x \in Y_0 \otimes Y_1$, Theorem 2.7 with $X_0 = X_1 = \mathbb{R}$ and $f(\lambda) = \lambda x$.

Finally, using the fact that $\mathfrak{S}_2^w$ coincides with the Euclidean (or Hilbert–Schmidt) norm in the tensor product of Hilbert spaces (fact that follows directly from the definition of the $\mathfrak{S}_2^w$ norm), together with the facts that it is a tensor norm and the identity map $\mathcal{S}_1^{m,n} \to \mathcal{S}_2^{m,n}$ has norm ≤ 1, one gets

$$\|x\|_{\ell_2^{n^2 m^2}} \leq \|x\|_{\mathcal{S}_1^{m,n} \otimes_{\mathfrak{S}_2^w} \mathcal{S}_1^{m,n}}. \tag{43}$$

The desired claim follows putting together Eqs. (41), (42) and (43). An important point to stress here is that, in order to apply Theorem 5.4, real versions of these spaces must be considered. In the first case, one obtains a real version of $\mathfrak{S}_2^w$ just restricting the underlying field to $\mathbb{R}$ in Definition 2.3. The second case is a bit more subtle since the complex interpolation method is inherently defined over complex normed spaces. A way to formalize the discussion at this point is considering the real interpolation method [22, Chapter 3]. Following the standpoint fixed at the beginning of this section, we leave aside these technicalities that we think do not add much to our discussion.

An important feature of spaces of the form $\left(\mathcal{S}_1^{m,n} \otimes_\alpha \mathcal{S}_1^{m,n}\right) \otimes_\varepsilon \ell_2^p$ is the fact that, by construction, they *have enough symmetries*. This will be exploited in the following proof with no further mention. The reader can find some additional information in Appendix C.

Proof. We start noticing that α being a tensor norm translates into the fact that *X has enough symmetries*. This means that the only operator on that space that commutes with every isometry is the identity (or a multiple of it). The same happens with the dual X^*. Next we give an alternative way to compute the volume ratio using this property. To simplify notation, denote $d = \dim(X) = n^2 m^2 p$. Then, we can bound (40) as follows:

$$\begin{aligned}
\mathrm{vr}(X^*) &\stackrel{(i.)}{=} \left(\frac{\mathrm{vol}_d(B_{X^*})}{\mathrm{vol}_d(B_{\ell_2^d})}\right)^{1/d} \left\|\mathrm{Id} : \ell_2^d \to X^*\right\| \\
&\stackrel{(ii.)}{\leq} \left(\frac{\mathrm{vol}_d(B_{\ell_2^d})}{\mathrm{vol}_d(B_X)}\right)^{1/d} \left\|\mathrm{Id} : \ell_2^d \to X^*\right\| \\
&\stackrel{(iii.)}{\leq} \frac{\left\|\mathrm{Id} : \ell_2^d \to X^*\right\|}{\sqrt{d}} \left(\frac{1}{\mathrm{vol}_d(B_X)}\right)^{1/d} \\
&\stackrel{(iv.)}{\leq} \frac{\left\|\mathrm{Id} : \ell_2^d \to X^*\right\|}{\sqrt{d}} \mathbb{E} \|G\|_X,
\end{aligned} \tag{44}$$

where $G = \sum_{i,j,k,l,h} g_{ijklh} |i\rangle\langle j| \otimes |k\rangle\langle l| \otimes \langle h|$ is a tensor in X^* with i.i.d. gaussian entries g_{ijklh}. The expectation is over these random variables. With respect to the chain of claims

---

[18] At least in the category of all finite dimensional normed spaces, which is the relevant setup for this work.

implicit in the previous manipulation: (i.) follows from the fact that the maximal volume ellipsoid $\mathcal{E}_{X^*}$ coincides with $\left\| \mathrm{Id} : \ell_2^d \to X^* \right\|^{-1} B_{\ell_2^d}$ when X^* has enough symmetries [25, Section 16], in (ii.) we have used the famous Blaschke–Santaló inequality [21, Section 7], in (iii.), the standard volume estimate for the Euclidean ball $\mathrm{vol}_d(\mathsf{ball}(\ell_2^d)) \approx d^{-d/2}$ and (iv.) follows from Lemma 3.4. in [49].

As a consequence, to obtain the stated bound we have to estimate the quantities $\left\| \mathrm{Id} : \ell_2^d \to X^* \right\|$ and $\mathbb{E} \left\| G \right\|_X$.

- Upper bounding $\left\| \mathrm{Id} : \ell_2^d \to X^* \right\|$:

We show two complementary bounds for this quantity. The first one uses the second condition in the statement of the theorem, that can be equivalently stated as: $\left\| \mathrm{Id} : \mathcal{S}_1^{m,n} \otimes_\alpha \mathcal{S}_1^{m,n} \longrightarrow \ell_2^{n^2 m^2} \right\| \leq 1$. This allows us to bound:

$$
\begin{aligned}
\left\| \mathrm{Id} : \ell_2^d \to X^* \right\| &= \left\| \mathrm{Id} : X \to \ell_2^d \right\| \\
&= \left\| \mathrm{Id} : \left(\mathcal{S}_1^{m,n} \otimes_\alpha \mathcal{S}_1^{m,n} \right) \otimes_\varepsilon \ell_2^p \longrightarrow \ell_2^{n^2 m^2 p} \right\| \\
&\leq \left\| \mathrm{Id} : \ell_2^{n^2 m^2} \otimes_\varepsilon \ell_2^p \longrightarrow \ell_2^{n^2 m^2 p} \right\| \\
&\leq \sqrt{p}.
\end{aligned}
$$

The mentioned hypothesis was used in the first inequality above.

Our second bound comes from the observation that the operator norm we want to bound is indeed upper bounded by the 2-summing norm of the identity between $\mathcal{S}_1^{m,n} \otimes_\alpha \mathcal{S}_1^{m,n}$ and $\ell_2^{n^2 m^2}$. We can alternatively understand the studied norm as:

$$
\begin{aligned}
\left\| \mathrm{Id} : \ell_2^d \to X^* \right\| &= \left\| \mathrm{Id} : X \to \ell_2^d \right\| \\
&= \left\| \mathrm{Id} : \ell_2^p \otimes_\varepsilon \left(\mathcal{S}_1^{m,n} \otimes_\alpha \mathcal{S}_1^{m,n} \right) \longrightarrow \ell_2^p (\ell_2^{n^2 m^2}) \right\| \\
&\leq \sup_{p \in \mathbb{N}} \left\| \mathrm{Id} : \ell_2^p \otimes_\varepsilon \left(\mathcal{S}_1^{m,n} \otimes_\alpha \mathcal{S}_1^{m,n} \right) \longrightarrow \ell_2^p (\ell_2^{n^2 m^2}) \right\| \\
&= \pi_2 \left(\mathrm{Id} : \mathcal{S}_1^{m,n} \otimes_\alpha \mathcal{S}_1^{m,n} \longrightarrow \ell_2^{n^2 m^2} \right),
\end{aligned}
$$

where the last equality is simply the definition of the 2-summing norm of the indicated map—recall (5). While now we don't need the hypothesis used before, we need to invoke the tensor norm properties of α. Hopefully, thanks to this property[19], Lemma 5.2. of [50] provides us a satisfactory way to compute the above norm. Under the consideration that $\mathcal{S}_1^{m,n} \otimes_\alpha \mathcal{S}_1^{m,n}$ as well as $\ell_2^{n^2 m^2}$ have *enough symmetries in the orthogonal group*—see Appendix C—, the cited lemma allows to write the following identity:

$$
\pi_2 \left(\mathrm{Id} : \mathcal{S}_1^{m,n} \otimes_\alpha \mathcal{S}_1^{m,n} \longrightarrow \ell_2^{n^2 m^2} \right) = \frac{nm}{\left\| \mathrm{Id} : \ell_2^{n^2 m^2} \longrightarrow \mathcal{S}_1^{m,n} \otimes_\alpha \mathcal{S}_1^{m,n} \right\|}.
$$

Taking into account the two bounds above, we can state that, under the conditions in the theorem:

$$
\left\| \mathrm{Id} : \ell_2^d \to X^* \right\| \leq \min \left(\sqrt{p}, \ \frac{nm}{\left\| \mathrm{Id} : \ell_2^{n^2 m^2} \longrightarrow \mathcal{S}_1^{m,n} \otimes_\alpha \mathcal{S}_1^{m,n} \right\|} \right). \tag{45}
$$

---

[19] See again Appendix C for clarification.

- Upper bounding $\mathbb{E}\,\|G\|_X$:

The upper estimate of this quantity follows from Chevet's inequality [51], see also [25, Section 43]. According to that:

$$\mathbb{E}\,\|G\|_X = \mathbb{E}\,\|G\|_{(\mathcal{S}_1^{m,n} \otimes_\alpha \mathcal{S}_1^{m,n}) \otimes_\varepsilon \ell_2^p}$$

$$\leq \sup_{\varphi \in B_{(\mathcal{S}_1^{m,n} \otimes_\alpha \mathcal{S}_1^{m,n})^*}} \left(\sum_{i,j,k,l} \left| \varphi\left(|i\rangle\langle j| \otimes |k\rangle\langle l| \right) \right|^2 \right)^{1/2} \mathbb{E}\,\left\| \sum_h g_h \langle h| \right\|_{\ell_2^p}$$

$$+ \sup_{\varphi \in B_{(\ell_2^p)^*}} \left(\sum_h |\varphi(\langle h|)|^2 \right)^{1/2} \mathbb{E}\,\left\| \sum_{i,j,k,l} g_{ijkl} |i\rangle\langle j| \otimes |k\rangle\langle l| \right\|_{\mathcal{S}_1^{m,n} \otimes_\alpha \mathcal{S}_1^{m,n}}.$$

Here we note the coincidence of the 2-sums above with the norm of the following identity maps (in both equations below, the LHS is merely the explicit expression of the norms in the RHS):

$$\sup_{\varphi \in B_{(\mathcal{S}_1^{m,n} \otimes_\alpha \mathcal{S}_1^{m,n})^*}} \left(\sum_{i,j,k,l} |\varphi(|i\rangle\langle j| \otimes |k\rangle\langle l|)|^2 \right)^{1/2} = \left\| \mathrm{Id} : \left(\mathcal{S}_1^{m,n} \otimes_\alpha \mathcal{S}_1^{m,n} \right)^* \longrightarrow \ell_2^{n^2 m^2} \right\|,$$

$$\sup_{\varphi \in B_{(\ell_2^p)^*}} \left(\sum_h |\varphi(\langle h|)|^2 \right)^{1/2} = \left\| \mathrm{Id} : \ell_2^p \longrightarrow \ell_2^p \right\|.$$

Furthermore, to simplify the presentation we also introduce the notation $\boldsymbol{g} = \sum_{i,j,k,l} g_{ijkl} |i\rangle\langle j| \otimes |k\rangle\langle l|$. With these comments, we can write

$$\mathbb{E}\,\|G\|_X \leq \left\| \mathrm{Id} : \left(\mathcal{S}_1^{m,n} \otimes_\alpha \mathcal{S}_1^{m,n} \right)^* \longrightarrow \ell_2^{n^2 m^2} \right\| \mathbb{E}\,\left\| \sum_h g_h \langle h| \right\|_{\ell_2^p}$$

$$+ \left\| \mathrm{Id} : \ell_2^p \longrightarrow \ell_2^p \right\| \mathbb{E}\,\|\boldsymbol{g}\|_{\mathcal{S}_1^{m,n} \otimes_\alpha \mathcal{S}_1^{m,n}}$$

$$\approx \left\| \mathrm{Id} : \left(\mathcal{S}_1^{m,n} \otimes_\alpha \mathcal{S}_1^{m,n} \right)^* \longrightarrow \ell_2^{n^2 m^2} \right\| \sqrt{p} + \mathbb{E}\,\|\boldsymbol{g}\|_{\mathcal{S}_1^{m,n} \otimes_\alpha \mathcal{S}_1^{m,n}}.$$

Now, it just left to bound $\mathbb{E}\,\|\boldsymbol{g}\|_{\mathcal{S}_1^{m,n} \otimes_\alpha \mathcal{S}_1^{m,n}}$. For that, we make use of hypothesis 1 in the statement, that is:

$$\mathbb{E}\,\|\boldsymbol{g}\|_{\mathcal{S}_1^{m,n} \otimes_\alpha \mathcal{S}_1^{m,n}} \leq \mathbb{E}\,\left(\|\boldsymbol{g}\|_{\mathcal{S}_1^{m,n} \otimes_\pi \mathcal{S}_1^{m,n}}^{1/2} \|\boldsymbol{g}\|_{\mathcal{S}_1^{m,n} \otimes_\varepsilon \mathcal{S}_1^{m,n}}^{1/2} \right)$$

$$\leq \left(\mathbb{E}\,\|\boldsymbol{g}\|_{\mathcal{S}_1^{m,n} \otimes_\pi \mathcal{S}_1^{m,n}} \right)^{1/2} \left(\mathbb{E}\,\|\boldsymbol{g}\|_{\mathcal{S}_1^{m,n} \otimes_\varepsilon \mathcal{S}_1^{m,n}} \right)^{1/2}.$$

The first term can be bounded as follows: we use the isometric equivalence $\mathcal{S}_1^{m,n} \simeq \ell_2^m \otimes_\pi \ell_2^n$ and the fact that the projective tensor norm is commutative to obtain that $\mathcal{S}_1^{m,n} \otimes_\pi \mathcal{S}_1^{m,n} \simeq \ell_2^n \otimes_\pi \ell_2^n \otimes_\pi \mathcal{S}_1^m$ isometrically. Furthermore, considering that $\|\mathrm{Id} : \ell_1^{n^2} \simeq \ell_1^n \otimes_\pi \ell_1^n \to \ell_2^n \otimes_\pi \ell_2^n\| \leq 1$ and $\|\mathrm{Id} : \mathcal{S}_2^m \to \mathcal{S}_1^m\| \leq \sqrt{m}$, it is also true that:

$$\mathbb{E}\,\|\boldsymbol{g}\|_{\ell_2^n \otimes_\pi \ell_2^n \otimes_\pi \mathcal{S}_1^m} \leq \sqrt{m}\,\mathbb{E}\,\|\boldsymbol{g}\|_{\ell_1^{n^2}(\mathcal{S}_2^m)}.$$

Similarly, using now that $\|\mathrm{Id} : \ell_2^{n^2} \to \ell_1^{n^2}\| \le n$,

$$\sqrt{m} \, \mathbb{E} \, \|\boldsymbol{g}\|_{\ell_1^{n^2}(\mathcal{S}_2^m)} \le n\sqrt{m} \, \mathbb{E} \, \|\boldsymbol{g}\|_{\ell_2^{n^2}(\mathcal{S}_2^m)} = n\sqrt{m} \, \mathbb{E} \, \|\boldsymbol{g}\|_{\ell_2^{n^2 m^2}}.$$

The estimate $\mathbb{E} \, \|\boldsymbol{g}\|_{\ell_2^{n^2 m^2}} \lesssim nm$ allows us to conclude:

$$\mathbb{E} \, \|\boldsymbol{g}\|_{\mathcal{S}_1^{m,n} \otimes_\pi \mathcal{S}_1^{m,n}} \lesssim n\sqrt{m} \, nm = n^2 m^{3/2}.$$

For the other term, we use again Chevet's inequality:

$$\mathbb{E} \, \Big\| \sum_{i,j,k,l} g_{ijkl} |i\rangle\langle j| \otimes |k\rangle\langle l| \Big\|_{\mathcal{S}_1^{m,n} \otimes_\varepsilon \mathcal{S}_1^{m,n}} \le 2 \, \big\| \mathrm{Id} : \big(\mathcal{S}_1^{m,n}\big)^*$$

$$\longrightarrow \ell_2^{nm} \, \big\| \, \mathbb{E} \, \Big\| \sum_{i,j} g_{ij} |i\rangle\langle j| \Big\|_{\mathcal{S}_1^{m,n}}$$

$$= 2\sqrt{n} \, \mathbb{E} \, \Big\| \sum_{i,j} g_{ij} |i\rangle\langle j| \Big\|_{\mathcal{S}_1^{m,n}}$$

$$\lesssim \sqrt{n} \, n\sqrt{m} = n^{3/2} m^{1/2}.$$

With the previous bounds, we obtain:

$$\mathbb{E} \, \|G\|_X \lesssim \big\| \mathrm{Id} : \ell_2^{n^2 m^2} \longrightarrow \mathcal{S}_1^{m,n} \otimes_\alpha \mathcal{S}_1^{m,n} \big\| \sqrt{p} + n^{7/4} m. \qquad (46)$$

To finish, we introduce in (44) the information given by (45) and (46):

$$\mathrm{vr}(X^*) \le \frac{\big\| \mathrm{Id} : \ell_2^d \to X^* \big\|}{\sqrt{d}} \, \mathbb{E} \, \|G\|_X$$

$$\lesssim \frac{\min\left(\sqrt{p}, \, \dfrac{nm}{\big\| \mathrm{Id} : \ell_2^{n^2 m^2} \longrightarrow \mathcal{S}_1^{m,n} \otimes_\alpha \mathcal{S}_1^{m,n} \big\|} \right)}{nm\sqrt{p}}$$

$$\left(\big\| \mathrm{Id} : \ell_2^{n^2 m^2} \longrightarrow \mathcal{S}_1^{m,n} \otimes_\alpha \mathcal{S}_1^{m,n} \big\| \sqrt{p} + n^{7/4} m \right)$$

$$\le \frac{nm}{nm\sqrt{p} \, \big\| \mathrm{Id} : \ell_2^{n^2 m^2} \longrightarrow \mathcal{S}_1^{m,n} \otimes_\alpha \mathcal{S}_1^{m,n} \big\|} \, \big\| \mathrm{Id} : \ell_2^{n^2 m^2} \longrightarrow \mathcal{S}_1^{m,n} \otimes_\alpha \mathcal{S}_1^{m,n} \big\| \sqrt{p}$$

$$+ \frac{\sqrt{p}}{nm\sqrt{p}} n^{7/4} m = 1 + n^{3/4},$$

that is enough to conclude the proof of the statement of the theorem.   □

6. Discussion

In this work we have proposed a protocol for PV, referred as G_{Rad} throughout the text, and proved lower bounds on the quantum resources necessary to break it. Our bounds, appearing in Theorem 4.5, do not answer in a definite way Question 1 and, in particular, are not enough for providing security guarantees for G_{Rad} in full generality. The reason is that the bounds presented in Theorem 4.5 depend on some additional properties of

the strategy under consideration: the parameters σ^i, σ^{ii}, related with the regularity of the strategy when regarded as a vector-valued assignment on the Boolean hypercube, cf. Sect. 4. However, our Theorem 4.5 is strong enough to encapsulate some previous results. As mentioned in Sect. 1, the hypotheses of Corollary 1.2 are satisfied by the teleportation based attacks of [9] and [2] and also by Universal Programmable Quantum Processors, rederiving in that way some results in [2,9,14]. Furthermore, we have related our Question 1 with the type/cotype properties of specific Banach spaces and, in fact, the obtained results led us to put forward a conjecture about these mathematical objects. The positive solution of this conjecture would imply a major progress in the understanding of G_{Rad}—see Sect. 5 for a formal statement of the conjecture and details about the connection with the security of G_{Rad}. In this last section we have also provided some estimates supporting the conjecture. We have proven bounds for the volume ratio of the spaces involved there relating, as a byproduct, our conjecture, and therefore the problem about the security of G_{Rad} with open problems in Banach space theory concerning the relation between cotype and volume ratio.

The future direction for this work is clear: trying to resolve the status of the security of G_{Rad}. Starting with the setting we introduced in Sect. 5, the most direct approach consists in developing new techniques to estimate type/cotype constants of tensor norm spaces. This is in fact an interesting avenue also in the context of local Banach space theory and we hope that this work could serve as motivation to pursue it. Extending the family of spaces whose type/cotype constants can be accurately estimated might shed new light on several poorly understood questions in this context, as it is the relation between volume ratio and cotype or the prevalence of type/cotype in tensor norms.

Coming back to our σ–dependent bounds, Theorem 4.5, it would be also a desirable development to achieve a better understanding of the regularity parameters introduced there, σ^i and σ^{ii}. For example, it would be very clarifying to understand how the structure of strategies is restricted under the assumption of these parameters being small (in the sense of Corollary 1.2) or whether general strategies can be *made more regular* in order to have a better behaviour in terms of these parameters. Another interesting question in this direction is understanding whether σ^i, σ^{ii} can be related with some physical properties of the strategies involved, such as their robustness against noise or the complexity of the operations performed.

Beyond the specific setting studied here, we have introduced a whole toolbox of constructions and connections that can be of interest in other related contexts. Firstly, most of the ideas we have used to study G_{Rad} can be explored in other quantum games. More specifically, we can consider a modified version of G_{Rad} in which the verifiers only have to communicate an n^2-dimensional quantum system to the prover—without the assistance of any further classical communication. A more detailed account of this tentative line of research was given in Sect. 1.1. Even when some of the results achieved in the present work carry over this modified setting, some new challenges appear whose exploration we leave for the future.

Being more speculative, the recent connection between PBC and AdS/CFT [5,6] seems to indicate that the tools we use here might have potential application to the understanding of holographic duality. Along this line, we can ask, for example, whether the notions of regularity studied here can be related with properties of the mapping between bulk and boundary theories in this context. In [6] it was claimed that properties of the AdS/CFT holographic correspondence allow to find cheating strategies that break PBC with polynomial resources. According to that, the exponential lower bounds in Corollary 1.2 opens the possibility to impose restrictions on the regularity of such holo-

graphic correspondence. This would be in consonance with a recent result of Kliesch and Koenig [52], based on previous work of Jones [53]. In [52], the continuum limit of discrete tensor-network toy models for holography was studied finding that, generically, this limit is extremely discontinuous.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

A. Handier expressions for σ^i, σ^{ii}

In this appendix we provide some expressions upper bounding σ^i and σ^{ii}. The advantage of these expressions is that they are easier to compute and can be expressed directly in terms of the elements of a given strategy. However, we stress that in general these bounds might be inaccurate.

Proposition A.1. *Given a pure strategy* $\mathcal{S}^{\mathcal{U}} = \{\tilde{V}_\varepsilon, \tilde{W}_\varepsilon, V, W_\varepsilon, |\varphi\rangle\}_\varepsilon \in \mathfrak{S}_{s2w}$,

i.

$$\sigma^i \lesssim_{\log} \mathbb{E}_\varepsilon \left(\sum_{i,j} \frac{1}{2} \left\| \tilde{V}_\varepsilon \otimes \tilde{W}_\varepsilon - \tilde{V}_{\overline{\varepsilon}^{ij}} \otimes \tilde{W}_{\overline{\varepsilon}^{ij}} \right\|_{M_{r^2, k\bar{k}'}}^2 \right)^{1/2} + O\left(\frac{1}{n}\right);$$

ii.

$$\sigma^{ii} \lesssim_{\log} \mathbb{E}_\varepsilon \left(\sum_{i,j} \frac{1}{2} \left\| \left(\mathrm{Id}_{\ell_2^{k'}} \otimes (W_\varepsilon - W_{\overline{\varepsilon}^{ij}}) \right) |\varphi\rangle \right\|_{\ell_2^{k\bar{k}'}}^2 \right)^{1/2} + O\left(\frac{1}{n}\right).$$

Proof. We provide simple, likely far from tight, bounds for the quantity

$$\left(\sum_{i,j} \left\| \partial_{ij} \Phi^{i(ii)}(\varepsilon) \right\|_{X^{i(ii)}}^2 \right)^{1/2}$$

appearing in (31) (recall that $X^i = M_{\tilde{k}/2, k\tilde{k}'}$, $X^{ii} = \mathcal{S}_1^{\tilde{k}', n} \otimes_{(\varepsilon,\pi)_{1/2}} \mathcal{S}_1^{\tilde{k}', n}$). Recall also that $\partial_{ij}\Phi(\varepsilon) = \frac{\Phi(\varepsilon_{11},\dots,\varepsilon_{ij},\dots,\varepsilon_{nn}) - \Phi(\varepsilon_{11},\dots,-\varepsilon_{ij},\dots,\varepsilon_{nn})}{2}$. In the rest of the proof we shorten notation denoting $(\varepsilon_{11}, \dots, -\varepsilon_{ij}, \dots, \varepsilon_{nn})$ as $\overline{\varepsilon}^{ij}$.

In the case of Φ^i,

$$\|\partial_{ij}\Phi^i(\varepsilon)\|_{M_{\tilde{k}/2, k\tilde{k}'}}$$

$$= \frac{1}{2}\left\| \frac{1}{n^2} \sum_{p,q\neq i,j} \varepsilon_{pq} \left((\langle p|\tilde{V}_\varepsilon \otimes \langle q|\tilde{W}_\varepsilon) - (\langle p|\tilde{V}_{\overline{\varepsilon}^{ij}} \otimes \langle q|\tilde{W}_{\overline{\varepsilon}^{ij}}) \right) (V|pq\rangle \otimes \mathrm{Id}_{\ell_2^{\tilde{k}'}}) \right.$$

$$\left. + \frac{1}{n^2} \varepsilon_{ij} \left((\langle i|\tilde{V}_\varepsilon \otimes \langle j|\tilde{W}_\varepsilon) + (\langle i|\tilde{V}_{\overline{\varepsilon}^{ij}} \otimes \langle j|\tilde{W}_{\overline{\varepsilon}^{ij}}) \right) (V|ij\rangle \otimes \mathrm{Id}_{\ell_2^{\tilde{k}'}}) \right\|_{M_{r^2, k\tilde{k}'}}$$

$$\leq \frac{1}{2}\left\| \frac{1}{n^2} \sum_{p,q} \varepsilon_{pq} \left((\langle p|\tilde{V}_\varepsilon \otimes \langle q|\tilde{W}_\varepsilon) - (\langle p|\tilde{V}_{\overline{\varepsilon}^{ij}} \otimes \langle q|\tilde{W}_{\overline{\varepsilon}^{ij}}) \right) (V|pq\rangle \otimes \mathrm{Id}_{\ell_2^{\tilde{k}'2}}) \right\|_{M_{r^2, k\tilde{k}'}}$$

$$+ \frac{2}{n^2}$$

$$= \frac{1}{2}\left\| \langle\psi_\varepsilon| \left[\left((\tilde{V}_\varepsilon \otimes \tilde{W}_\varepsilon) - (\tilde{V}_{\overline{\varepsilon}^{ij}} \otimes \tilde{W}_{\overline{\varepsilon}^{ij}}) \right) (V \otimes \mathrm{Id}_{\ell_2^{\tilde{k}'}}) \otimes \mathrm{Id}_{\mathcal{H}_C} \right] |\psi\rangle \right\|_{M_{r^2, k\tilde{k}'}} + O\left(\frac{1}{n^2}\right)$$

$$\leq \frac{1}{2}\left\| (\tilde{V}_\varepsilon \otimes \tilde{W}_\varepsilon) - (\tilde{V}_{\overline{\varepsilon}^{ij}} \otimes \tilde{W}_{\overline{\varepsilon}^{ij}}) \right\|_{M_{r^2, k\tilde{k}'}} + O\left(\frac{1}{n^2}\right).$$

For Φ^{ii},

$$\|\partial_{ij}\Phi^{ii}(\varepsilon)\|_{\mathcal{S}_1^{\tilde{k}', n} \otimes_{(\varepsilon,\pi)_{1/2}} \mathcal{S}_1^{\tilde{k}', n}}$$

$$= \frac{1}{2}\left\| \frac{1}{n^2} \sum_{p,q\neq i,j} \varepsilon_{pq} |p\rangle \otimes |q\rangle \otimes (V|pq\rangle \otimes \mathrm{Id}_{\ell_2^{\tilde{k}'2}})(\mathrm{Id}_{\ell_2^k} \otimes (W_\varepsilon - W_{\overline{\varepsilon}^{ij}}))|\varphi\rangle \right.$$

$$\left. + \frac{1}{n^2} \varepsilon_{ij} |i\rangle \otimes |j\rangle \otimes (V|ij\rangle \otimes \mathrm{Id}_{\ell_2^{\tilde{k}'}})(\mathrm{Id}_{\ell_2^k} \otimes (W_\varepsilon + W_{\overline{\varepsilon}^{ij}}))|\varphi\rangle \right\|_{\mathcal{S}_1^{\tilde{k}', n} \otimes_{(\varepsilon,\pi)_{1/2}} \mathcal{S}_1^{\tilde{k}', n}}$$

$$\overset{(*)}{\leq} \frac{1}{2}\left\| \frac{1}{n^2} \sum_{p,q} \varepsilon_{pq} |p\rangle \otimes |q\rangle \otimes (V|pq\rangle \otimes \mathrm{Id}_{\ell_2^{\tilde{k}'2}})(\mathrm{Id}_{\ell_2^k} \otimes (W_\varepsilon - W_{\overline{\varepsilon}^{ij}}))|\varphi\rangle \right\|_{\mathcal{S}_1^{\tilde{k}', n} \otimes_{(\varepsilon,\pi)_{1/2}} \mathcal{S}_1^{\tilde{k}', n}}$$

$$+ \frac{2}{n^2}$$

$$\leq \frac{1}{2n^2} \sum_{p,q} \left\| |p\rangle \otimes |q\rangle \otimes (V|pq\rangle \otimes \mathrm{Id}_{\ell_2^{\tilde{k}'2}})(\mathrm{Id}_{\ell_2^k} \otimes (W_\varepsilon - W_{\overline{\varepsilon}^{ij}}))|\varphi\rangle \right\|_{\mathcal{S}_1^{\tilde{k}', n} \otimes_{(\varepsilon,\pi)_{1/2}} \mathcal{S}_1^{\tilde{k}', n}}$$

$$+ O\left(\frac{1}{n^2}\right)$$

$$\overset{(**)}{\leq} \frac{1}{2n^2} \sum_{p,q} \left\| (V|pq\rangle \otimes \mathrm{Id}_{\ell_2^{\tilde{k}'2}})(\mathrm{Id}_{\ell_2^k} \otimes (W_\varepsilon - W_{\overline{\varepsilon}^{ij}}))|\varphi\rangle \right\|_{\ell_2^{\tilde{k}'2}} + O\left(\frac{1}{n^2}\right)$$

$$\leq \frac{1}{2n^2} \sum_{p,q} \left\| (\mathrm{Id}_{\ell_2^k} \otimes (W_\varepsilon - W_{\overline{\varepsilon}^{ij}}))|\varphi\rangle \right\|_{\ell_2^{k\tilde{k}'2}} + O\left(\frac{1}{n^2}\right)$$

$$\leq \frac{1}{2} \left\| (\mathrm{Id}_{\ell_2^k} \otimes (W_\varepsilon - W_{\bar{\varepsilon}^{ij}}))|\varphi\rangle \right\|_{\ell_2^{k\tilde{k}'/2}} + O\left(\frac{1}{n^2}\right).$$

The previous two bounds lead automatically to the claimed statement.

In (*) we have applied a simple triangle inequality and used the fact that the elements in the sum are well normalized in the considered norm, recall Remark 4.7. For (**), if we denote $|\tilde{\varphi}_{pq}\rangle := \left(V|pq\rangle \otimes \mathrm{Id}_{\ell_2^{\tilde{k}'/2}}\right)\left(\mathrm{Id}_{\ell_2^{k'}} \otimes (W_\varepsilon - W_{\bar{\varepsilon}^{ij}})\right)|\varphi\rangle$, we have to notice that, for each $p, q, |p\rangle \otimes |q\rangle \otimes |\tilde{\varphi}_{pq}\rangle = \iota_p \otimes \iota_q(|\tilde{\varphi}_{pq}\rangle)$, where ι_p, ι_q are the injections considered in Remark 4.7. In that remark, we have proven that $\iota_p \otimes \iota_q$ is a contractive map from $\mathcal{S}_1^{\tilde{k},n} \otimes_{(\varepsilon,\pi)_{1/2}} \mathcal{S}_1^{\tilde{k},n}$ into $\ell_2^{\tilde{k}'/2}$. Inequality (**) follows from this observation. $\quad\square$

B. Non-pure strategies in Theorem 4.5

We give here some further details towards the proof of Theorem 4.5. We first explicit the statement we obtain in the case of *pure* strategies and then, how to obtain the general statement appearing in 4.5.

Claim B.1. *For* $\mathcal{S}^{\mathcal{U}} \in \mathfrak{S}_{s2w;\tilde{k}',k}^{\mathcal{U}}$:

I.

$$\omega(G; \mathcal{S}^{\mathcal{U}}) \leq C_1 + C_2'\, \sigma^i\, \log^{1/2}(k\tilde{k}') + O\left(\frac{1}{n^{1/2}}\right);$$

II.

$$\omega(G; \mathcal{S}^{\mathcal{U}}) \leq \tilde{C}_1 + C_3'\, \tilde{\sigma}^{ii}\, \log^{1/2}(nk\tilde{k}') + O\left(\frac{1}{n^{1/2}} + \frac{\log(n)\log^{1/2}(k\tilde{k})}{n}\right),$$

where we have denoted $\tilde{\sigma}^{ii} = n^{3/4}\log(n)\,\sigma^{ii}$.

Above, $C_1, \tilde{C}_1 < 1, C_2', C_3'$ *are positive constants.*

Proof. Lemma 4.3 provides the following bounds:

$$\omega(G_{\mathrm{Rad}}; \mathcal{S}^{\mathcal{U}}) \leq \left\| \mathbb{E}_\varepsilon \Phi^i(\varepsilon) \right\|_{X^i} + C\, \sigma^i\, \mathrm{T}_2^{(n^2)}(X^i), \tag{47}$$

$$\omega(G_{\mathrm{Rad}}; \mathcal{S}^{\mathcal{U}}) \leq \left\| \mathbb{E}_\varepsilon \Phi^{ii}(\varepsilon) \right\|_{\tilde{X}^{ii}} + C\, \sigma^{ii}\, \mathrm{T}_2^{(n^2)}(X^{ii}). \tag{48}$$

Taking into account the estimates

$$\mathrm{T}_2^{(n^2)}(X^i) \leq \mathrm{T}_2(X^i) \lesssim \log^{1/2}(k\tilde{k}'), \qquad \mathrm{T}_2^{(n^2)}(X^{ii}) \lesssim n^{3/4}\log(n)\log^{1/2}(nk'),$$

and Proposition 4.6, Eqs. (47), (48) transform in:

$$\omega(G_{\mathrm{Rad}}; \mathcal{S}^{\mathcal{U}}) \lesssim \frac{3}{4} + O\left(\frac{1}{n^{1/2}}\right) + C\, \sigma^i\, \log^{1/2}(k\tilde{k}'),$$

$$\omega(G_{\mathrm{Rad}}; \mathcal{S}^{\mathcal{U}}) \lesssim \frac{\sqrt{3}}{2} + O\left(\frac{1}{\sqrt{n}} + \frac{\log(n)\log^{1/2}(k\tilde{k}')}{n}\right)$$

$$+ C\, \sigma^{ii}\, n^{3/4}\log(n)\log^{1/2}(n\tilde{k}').$$

$$\square$$

Now, we use Lemma 3.2 to translate the previous bound to the case of a general strategy $\mathcal{S}$, obtaining that way the statement appearing in the main text.

Claim B.2. *The previous claim implies, for any $\mathcal{S} \in \mathfrak{S}_{s2w;\tilde{k},k}$, the bounds:*

I.

$$\omega(G; \mathcal{S}) \le C_1 + C_2 \, \sigma^i \, \log^{1/2}(nk\tilde{k}) + O\left(\frac{1}{n^{1/2}}\right);$$

II.

$$\omega(G; \mathcal{S}) \le \tilde{C}_1 + C_3 \, \tilde{\sigma}^{ii} \, \log^{1/2}(nk\tilde{k}) + O\left(\frac{1}{n^{1/2}} + \frac{\log(n) \log^{1/2}(nk\tilde{k})}{n}\right),$$

where we have denoted $\tilde{\sigma}^{ii} = n^{3/4} \log(n) \, \sigma^{ii}$.

Above, C_1, $\tilde{C}_1 < 1$, C_2, C_3 are positive constants.

Proof. Lemma 3.2 allows us to consider $\mathcal{S}$ as a pure strategy in $\mathfrak{S}^{\mathcal{U}}_{s2w;\tilde{k}',k}$. The relevant estimate, also provided in that lemma, is that $\tilde{k}'$ can be taken to be lower or equal than $n^2 k\tilde{k}^4$. I.e., $\mathcal{S}$ satisfies Claim B.1 with $\tilde{k}' \le n^2 k\tilde{k}^4$. Furthermore, we can roughly bound

$$k\tilde{k}' \le nk\tilde{k}' \le (nk\tilde{k}')^{\alpha},$$

for some positive constant α. Since those factors appear in Claim B.1 only inside a logarithm, the exponent α only changes the constants C_2', C_3' appearing there. □

If one wants to state Theorem 4.5 in terms of the raw quantum dimension $\tilde{k}_q := \frac{\tilde{k}}{\tilde{k}_{cl}}$, where $\tilde{k}_{cl}$ was the dimension of the classical messages used in the strategy, it is possible to argue similarly as above using this time Lemma 3.1. The result is exactly the same, only the constants C_2, C_3 are affected.

C. Tensor norms and enough symmetries

In this appendix we give some additional information about spaces *with enough symmetries* and spaces *with enough symmetries in the orthogonal group*, properties used in our Theorem 5.4. Given a Banach space X, we refer to the group of isometries on that space as the *symmetry group* of X.

Definition C.1. A Banach space X has enough symmetries if the only operators on X that commutes with the symmetry group of the space are $\lambda \operatorname{Id}_X$ for some scalar λ.

It easy to see that if X has enough symmetries the same happens with X^*. Furthermore, it is a piece of folklore that tensor norms also respect this property. That is, for any tensor norm α, $X \otimes_\alpha Y$ has enough symmetries when X and Y have enough symmetries. This fact follows from noticing that for any isometries f, g in X and Y, respectively, $f \otimes g$ is also an isometry in $X \otimes_\alpha Y$. This is guaranteed by the metric mapping property (4). Finally, in [50] the notion of enough symmetries in the orthogonal group appears in the statement of [50, Lemma 5.2], result used in our proof of Theorem 5.4.

Definition C.2. An n-dimensional Banach space X has enough symmetries in the orthogonal group if the symmetry group of X includes a subgroup of GL(n) verifying the property that the only operators on X that commutes with that subgroup are $\lambda \operatorname{Id}_X$ for some scalar λ.

We finally comment that tensor norms also preserves the property of having enough symmetries in the orthogonal group. The reason is the same as in the previous case of simply having enough symmetries. Furthermore, it is obvious from the definition that ℓ_2^n has enough symmetries in the orthogonal group and, therefore, $\ell_2^n \otimes_\alpha \ell_2^{n'}$, $(\ell_2^n \otimes_\alpha \ell_2^{n'}) \otimes_{\alpha'} \ell_2^{n''}$, …are also spaces with enough symmetries in the orthogonal group when $\alpha, \alpha', \ldots$ are tensor norms. In particular, the spaces considered in Theorem 5.4 have this property.

References

1. Malaney, R.: The quantum car. IEEE Wirel. Commun. Lett. **5.6**, 624–627 (2016). https://doi.org/10.1109/LWC.2016.2607740
2. Beigi, S., Köonig, R.: Simplified instantaneous non-local quantum computation with applications to position-based cryptography. New J. Phys. **13.9**, 093036 (2011). https://doi.org/10.1088/1367-2630/13/9/093036
3. Speelman, F.: Instantaneous non-local computation of low T-depth quantum circuits (2015). arXiv:1511.02839 [quant-ph]
4. Buhrman, H., Fehr, S., Schaffner, C., Speelman, F.: The garden-hose model. In: Proceedings of the 4th Conference on Innovations in Theoretical Computer Science—ITCS '13 (2013). https://doi.org/10.1145/2422436.2422455
5. May, A.: Quantum tasks in holography (2019). arXiv:1902.06845 [hep-th]
6. May, A., Penington, G., Sorce, J.: Holographic scattering requires a connected entanglement wedge. J. High Energy Phys. **2020**, 8 (2020). https://doi.org/10.1007/JHEP08(2020)132
7. Chandran, N., Goyal, V., Moriarty, R., Ostrovsky, R.: Position based cryptography. In: CRYPTO2009, pp. 391–407 (2009). https://doi.org/10.1007/978-3-642-03356-8_23
8. Kent, A., Munro, W.J., Spiller, T.P.: Quantum tagging: Authenticating location via quantum information and relativistic signaling constraints. Phys. Rev. A 84(1) (2011). https://doi.org/10.1103/PhysRevA.84.012326. ISSN: 1094-1622
9. Buhrman, H., Chandran, N., Fehr, S., Gelles, R., Goyal, V., Ostrovsky, R., Schaffner, C.: Position-based quantum cryptography: impossibility and constructions. In: Rogaway, P. (ed.) Advances in Cryptology—CRYPTO 2011, pp. 429–446. Springer, Berlin (2011)
10. Vaidman, L.: Instantaneous measurement of nonlocal variables. Phys. Rev. Lett. (2003). https://doi.org/10.1103/PhysRevLett.90.010402
11. Tomamichel, M., Fehr, S., Kaniewski, J., Wehner, S.: A monogamy-of-entanglement game with applications to device-independent quantum cryptography. New J. Phys. **15**(10), 103002 (2013). https://doi.org/10.1088/1367-2630/15/10/103002
12. Unruh, D.: Quantum position verification in the random oracle model. In: Garay, J.A., Gennaro, R. (eds.) Advances in Cryptology—CRYPTO 2014, pp. 1–18. Springer, Berlin (2014)
13. Bluhm, A., Christandl, M., Speelman, F.: Position-based cryptography: single-qubit protocol secure against multi-qubit attacks (2021). arXiv:2104.06301 [quant-ph]
14. Kubicki, A.M., Palazuelos, C., Pérez-García, D.: Resource quantification for the no-programing theorem. Phys. Rev. Lett. **122**(8) (2019). https://doi.org/10.1103/physrevlett.122.080505. ISSN: 1079-7114
15. Nielsen, M.A., Chuang, I.L.: Programmable quantum gate arrays. Phys. Rev. Lett. **79**(2), 321–324 (1997). https://doi.org/10.1103/PhysRevLett.79.321
16. Pisier, G.: Random series of trace class operators. In: Proceedings Cuarto CLAPEM Mexico 1990. Contribuciones en probabilidad y estadistica matematica, pp. 29–42 (1990). arXiv:1103.2090
17. Kubicki, A.M.: Local Banach space theory and resource quantification in Quantum Information Processing. PhD thesis. Faculty of Mathematical Sciences, Universitat de València, (2021). https://roderic.uv.es/bitstream/handle/10550/80380/Thesis_AMKubicki.pdf?sequence=1&isAllowed=y
18. Pietsch, A.: Eigenvalues and S-numbers. Cambridge University Press, Cambridge (1986)
19. Defant, A., Floret, K.: Tensor Norms and Operator Ideals. North-Holland, Amsterdam (1993)

20. Effros, E.G., Ruan, Z.-J.: Operator Spaces. Oxford University Press, Oxford (2000)
21. Pisier, G.: The Volume of Convex Bodies and Banach Space Geometry. Cambridge Tracts in Mathematics. Cambridge University Press, Cambridge (1989). https://doi.org/10.1017/CBO9780511662454
22. Bergh, J., Löfström, J.: Interpolation Spaces. Springer, Berlin (1976). ISBN: 978-3-642-66451-9
23. Triebel, H.: Interpolation Theory, Function Spaces, Differential Operators. North-Holland Publishing Company, Amsterdam (1978)
24. Pisier, G.: Non-commutative vector valued Lp-spaces and completely p-summing maps. In: Asterique 247 (1998). http://www.numdam.org/issue/AST_1998__247__R1_0.pdf
25. Tomczak-Jaegermann, N.: Banach-Mazur Distances and Finite-Dimensional Operator Ideals, vol. 38. Pitman Monographs, Surveys in Pure, and Applied Mathematics, p. 395 (1989)
26. Kahane, J.P.: Some Random Series of Functions. Cambridge University Press, Cambridge (1993)
27. Maurey, B.: Type, cotype and K-convexity. In: Handbook of the Geometry of Banach Spaces, vol. 2, pp. 1299– 1332. North-Holland (2003)
28. Pisier, G.: On the duality between type and cotype. In: Chao, J.-A., Woyczyński, W.A. (eds.) Martingale Theory in Harmonic Analysis and Banach Spaces, pp. 131–144. Springer, Berlin (1982)
29. Pisie, G.: Probabilistic methods in the geometry of Banach spaces. In: Letta, G., Pratelli, M. (eds.) Probability and Analysis, pp. 167–241. Springer, Berlin (1986)
30. Pisier, G.: Factorization of operator valued analytic functions. In: Advances in Mathematics 93.1 (1992), pp 61–125. https://doi.org/10.1016/0001-8708(92)90025-G. ISSN: 0001-8708
31. Randrianantoanina, N.: Non-commutative martingale transforms. J Funct Anal **194**(1), 181–212 (2002). https://doi.org/10.1006/jfan.2002.3952
32. Burkholder, D.L.: A geometrical characterization of banach spaces in which martingale difference sequences are unconditional. Ann. Probab. **9**(6), 997–1011 (1981)
33. Burkholder, D.L.: Martingales and Fourier analysis in Banach spaces. In: Letta, G., Pratelli, M. (eds.) Probability and Analysis, pp. 61–108. Springer, Berlin (1986)
34. Busch, P., Lahti, P., Pellonpää, J.-P., Ylinen, K.: Quantum Measurement. Springer, Switzerland (2016). https://doi.org/10.1007/978-3-319-43389-9
35. Stinespring,W.F.: Positive Functions on C*-Algebras. In: Proceedings of the American Mathematical Society 6.2 (1955), 211–216. issn: 00029939, 10886826. http://www.jstor.org/stable/2032342
36. Grothendieck, A.:. Résumé de la théorie métrique des produits tensoriels topologiques. In: Boletim Da Sociedades de Matemática de S ao Paulo 8:1 (1953)
37. Krivine, J. L.: Constantes de Grothendieck et fonctions de type positif sur les sphères. fr. In: Séminaire d'Analyse fonctionnelle (dit "Maurey-Schwartz") (1977-1978). talk:1 et 2. http://www.numdam.org/item/SAF_1977-1978____A1_0/
38. Regev, O., Vidick, T.: Quantum XOR games. ACM Trans. Comput. Theory **7.4**, 1–43 (2015). https://doi.org/10.1145/2799560
39. Hoeffding, W.: Probability inequalities for sums of bounded random variables. J. Am. Stat. Assoc. **58**(301), 13–30 (1963)
40. Le Merdy, C.: The Schatten space S4 is a Q-algebra. Proc. Am. Math. Soc. **126**(3), 715–719 (1998)
41. Michal, A.D., Wyman, M.: Characterization of complex couple spaces. Engl. Ann. Math. (2) **42**, 247–250 (1941)
42. Taylor, A.E.: Analysis in complex Banach spaces. Engl. Bull. Am. Math. Soc. **49**, 652–669 (1943)
43. Wenzel, J.: Real and complex operator ideals. Quaest. Math. **18**(1–3), 271–285 (1995). https://doi.org/10.1080/16073606.1995.9631800
44. Muñoz, G., Sarantopoulos, Y., Tonge, A.: Complexifications of real Banach spaces, polynomials and multilinear maps. Eng. Studia Math. **134**(1), 1–33 (1999)
45. Wenzel, J.: A supplement to my paper on real and complex operator ideals. Quaest. Math. **20.4**, 663–665 (1997). https://doi.org/10.1080/16073606.1997.9632233
46. Szarek, S.: Kashins Almost Euclidean Orthogonal Decomposition of L1 fng. Bull. Acad. Polon. Sci. Ser. Sci. Math. Astron. Phys. **26**(8), 691–694 (1978)
47. Szarek, S., Tomczak-Jaegermann, N.: On nearly euclidean decomposition for some classes of Banach spaces. Compos. Math. **40**(3), 367–385 (1980)
48. Bourgain, J., Milman, V.D.: New volume ratio properties for convex symmetric bodies in Rn. Invent. Math. **88**(2), 319–340 (1987)
49. Giladi, O., Prochno, J., Schütt, C., Tomczak-Jaegermann, N., Werner, E.: On the geometry of projective tensor products. J. Funct. Anal. **273**(2), 471–495 (2017). https://doi.org/10.1016/j.jfa.2017.03.019
50. Defant, A., Mastyło, M., Michels, C.: Summing norms of identities between unitary ideals. Math. Z. **252**, 863–882 (2006). https://doi.org/10.1007/s00209-005-0893-7

51. Chevet, S: Séries de variables aléatoires gaussiennes à valeurs dans $E \hat{\otimes}_\epsilon F$. Application aux produits d'espaces de Wiener abstraits. In: Séminaire Analyse fonctionnelle ("dit Maurey-Schwartz"), pp. 1–15 (1978). http://www.numdam.org/item/SAF_1977-1978____A14_0/
52. Kliesch, A., König, R.: Continuum limits of homogeneous binary trees and the Thompson group. Phys. Rev. Lett. (2020). https://doi.org/10.1103/PhysRevLett.124.010601
53. Jones, V.F.: A no-go theorem for the continuum limit of a periodic quantum spin chain. Commun. Math. Phys. **357**(1), 295–317 (2018). https://doi.org/10.1007/s00220-017-2945-3