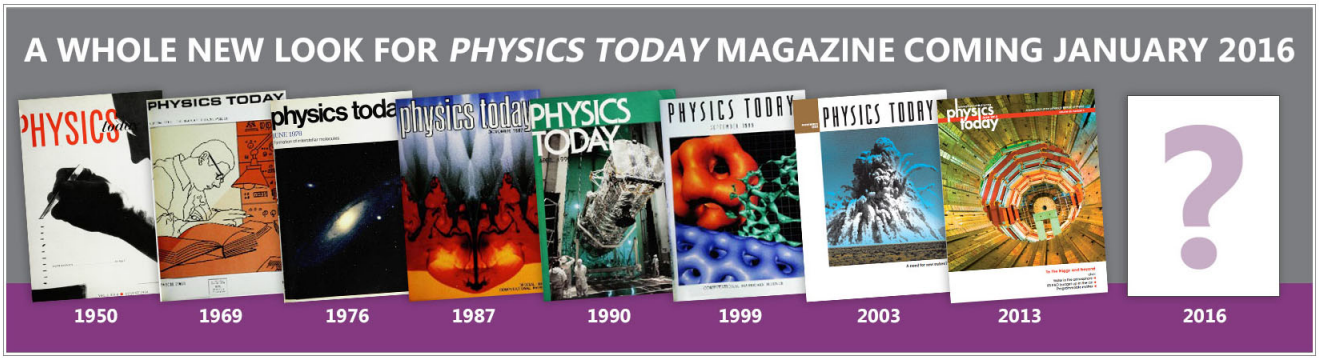
AIP | Journal of Mathematical Physics

# Nonadditivity of Rényi entropy and Dvoretzky's theorem

Guillaume Aubrun, Stanisław Szarek, and Elisabeth Werner

Citation: Journal of Mathematical Physics **51**, 022102 (2010); doi: 10.1063/1.3271044
View online: http://dx.doi.org/10.1063/1.3271044
View Table of Contents: http://scitation.aip.org/content/aip/journal/jmp/51/2?ver=pdfcov
Published by the AIP Publishing





# Nonadditivity of Rényi entropy and Dvoretzky's theorem

Guillaume Aubrun,[1,a)] Stanisław Szarek,[2,3,b)] and Elisabeth Werner[3,4,c)]
[1]*Institut Camille Jordan, Université Claude Bernard Lyon 1, 43 Boulevard du 11 Novembre 1918, 69622 Villeurbanne Cedex, France*
[2]*Equipe d'Analyse Fonctionnelle, Institut de Mathématiques de Jussieu, Université Pierre et Marie Curie-Paris 6, 4 Place Jussieu, 75252 Paris, France*
[3]*Department of Mathematics, Case Western Reserve University, Cleveland, Ohio 44106, USA*
[4]*UFR de Mathématique, Université de Lille 1, 59655 Villeneuve d'Ascq, France*

(Received 13 October 2009; accepted 10 November 2009; published online 1 February 2010)

The goal of this note is to show that the analysis of the minimum output $p$-Rényi entropy of a typical quantum channel essentially amounts to applying Milman's version of Dvoretzky's theorem about almost Euclidean sections of high-dimensional convex bodies. This conceptually simplifies the (nonconstructive) argument by Hayden–Winter, disproving the additivity conjecture for the minimal output $p$-Rényi entropy (for $p>1$). © *2010 American Institute of Physics.*
[doi:10.1063/1.3271044]

## I. INTRODUCTION

Many major questions in quantum information theory can be formulated as additivity problems. These questions have received considerable attention in recent years, culminating in Hastings' work showing that the minimal output von Neumann entropy of a quantum channel is not additive. He used a random construction inspired by previous examples due to Winter and Hayden, who proved nonadditivity of the minimal output $p$-Rényi entropy for any $p>1$. In this short note, we show that the Hayden–Winter analysis can be simplified (at least conceptually) by appealing to Dvoretzky's theorem. Dvoretzky's theorem is a fundamental result of asymptotic geometric analysis, which studies the behavior of geometric parameters associated with norms in $\mathbb{R}^n$ (or, equivalently, with convex bodies) when $n$ becomes large. Such connections between quantum information theory and high-dimensional convex geometry promise to be very fruitful.

## II. NOTATION

If $\mathcal{H}$ is a Hilbert space, we will denote by $\mathcal{B}(\mathcal{H})$ the space of bounded linear operators on $\mathcal{H}$, and by $\mathcal{D}(\mathcal{H})$ the set of *density matrices* on $\mathcal{H}$, i.e., positive semidefinite trace one operators on $\mathcal{H}$ [or *states* on $\mathcal{H}$, or—more properly—states on $\mathcal{B}(\mathcal{H})$]. Most often, we will have $\mathcal{H}=\mathbb{C}^n$ for some $n\in\mathbb{N}$, and we will then write $\mathcal{M}_n$ for $\mathcal{B}(\mathbb{C}^n)$.

For $p\geq 1$, the *p-Rényi entropy* of a state $\rho$ is defined as

$$S_p(\rho)=\frac{1}{1-p}\log(\operatorname{tr}\rho^p).$$

(For $p=1$, this should be understood as a limit and coincides with the von Neumann entropy.)

A linear map $\Phi:\mathcal{M}_m\to\mathcal{M}_d$ is called a *quantum channel* if it is completely positive and trace preserving. The *minimal output* $p$-Rényi entropy of $\Phi$ is then defined as

[a)]Electronic mail: aubrun@math.univ-lyon1.fr.
[b)]Electronic mail: szarek@math.jussieu.fr.
[c)]Electronic mail: elisabeth.werner@case.edu.

$$S_p^{\min}(\Phi) = \min_{\rho \in \mathcal{D}(\mathbb{C}^m)} S_p(\Phi(\rho)).$$

## III. THE ADDITIVITY CONJECTURE

The *additivity conjecture*[1] asserted that the following equality held for every pair $\Phi$, $\Psi$ of quantum channels

$$S_p^{\min}(\Phi \otimes \Psi) \stackrel{?}{=} S_p^{\min}(\Phi) + S_p^{\min}(\Psi). \tag{1}$$

The most important case, $p=1$, has been shown to be equivalent to a number of central questions in quantum information theory.[27] Of course, had the conjecture been true for every $p>1$, it would have held also for $p=1$ by continuity.

The conjecture has been recently disproved for *all* values of $p \geq 1$. Early (explicit) counterexamples for $p>4.79$ were due to Holevo and Werner.[31] Subsequently, the case $p>1$ was settled by Hayden and Winter in Ref. 17, and finally Hastings found a counterexample to the additivity conjecture for $p=1$.[16] The latter two papers used nonconstructive methods (see Sec. IV for more comments on this aspect of the story). Hastings' presentation was rather concise, but more detailed expositions of his approach can be found in, e.g., Refs. 10, 3, and 9.

We want to show in this note that a large part of the analysis by Hayden and Winter is actually a fallout of Dvoretzky's theorem, a classical result in high-dimensional convex geometry dating to the 1960s.[7,21] We note that this approach, at least in its present form, does not cover Hastings' construction.

## IV. MULTIPLICATIVE FORM

It will be more convenient to study a multiplicative version of the conjecture, already considered in Ref. 1. Instead of the Rényi entropy, we will work with the Schatten $p$-norm $\|\sigma\|_p = (\mathrm{tr}(\sigma^\dagger \sigma)^{p/2})^{1/p}$. (The limit case $\|\cdot\|_\infty$ is the operator, or "spectral," norm.)

If $p>1$ and $\rho$ is a state, then $S_p(\rho) = p/(1-p) \log\|\rho\|_p$, and so the study of $S_p^{\min}(\Phi)$ is replaced by that of $\max_{\rho \in \mathcal{D}(\mathbb{C}^m)} \|\Phi(\rho)\|_p$, or the *maximum output p-norm*. The latter quantity has a nice functional-analytic interpretation: it equals $\|\Phi\|_{1\to p}$, i.e., the norm of $\Phi$ as an operator from $(\mathcal{M}_m, \|\cdot\|_1)$ to $(\mathcal{M}_d, \|\cdot\|_p)$. This allows one to rewrite conjecture (1) in a multiplicative form

$$\|\Phi \otimes \Psi\|_{1\to p} \stackrel{?}{=} \|\Phi\|_{1\to p} \|\Psi\|_{1\to p}. \tag{2}$$

The inequality "$\geq$" is trivial, so the conjecture asked if "$\leq$" was always true.

We point out that the argument that follows deals directly with the maximum output $p$-norm and not with $\|\Phi\|_{1\to p}$, so the knowledge that the two are equal is not really needed. Note that it is only obvious that the maximum output $p$-norm is equal—for any linear map $\Phi$—to the norm of the restriction of $\Phi$ to the $\mathbb{R}$-linear space $\mathcal{M}_m^H$ of $m \times m$ Hermitian matrices. The fact that it coincides—for quantum channels, or even for all 2-positive maps—with the *a priori* larger norm $\|\Phi\|_{1\to p}$ is also elementary, but less immediate[30] (see also Refs. 2 and 29 for short proofs of the more general version).

Finally, let us observe that $\|\Phi\|_{1\to p}$ never exceeds 1 if $\Phi$ is a quantum channel. If, additionally, $\Phi$ is $\mathcal{M}_d$-valued, then $\|\Phi\|_{1\to p}$ is at least $d^{1/p-1}$ (the $p$-norm of the maximally mixed state in $\mathcal{M}_d$).

## V. CHANNELS AS SUBSPACES

Let $\mathcal{W}$ be a subspace of $\mathbb{C}^d \otimes \mathbb{C}^d$ of dimension $m$. Then $\Phi: \mathcal{B}(\mathcal{W}) \to \mathcal{M}_d$ defined by $\Phi(\rho) = \mathrm{tr}_2(\rho)$ [*partial trace* in the second factor, i.e., $\mathrm{tr}_2(\rho_1 \otimes \rho_2) = \mathrm{tr}(\rho_2)\rho_1$] is a quantum channel. Alternatively (and perhaps more properly), we could identify $\mathcal{W}$ with $\mathbb{C}^m$ via an isometry $V: \mathbb{C}^m \to \mathbb{C}^d \otimes \mathbb{C}^d$ whose range is $\mathcal{W}$ and set, for $\rho \in \mathcal{M}_m$, $\Phi(\rho) = \mathrm{tr}_2(V\rho V^\dagger)$; then $\Phi$ goes from $\mathcal{M}_m$ to $\mathcal{M}_d$.

(One could also consider here subspaces $\mathcal{W}\subset\mathbb{C}^d\otimes\mathbb{C}^r$, where possibly $r\neq d$; this would allow to preserve full generality, but would lead to more involved notation.)

By convexity, the maximum output $p$-norm, and hence also $\|\Phi\|_{1\to p}$, is attained on pure states. In other words,

$$\|\Phi\|_{1\to p}=\max_{x\in\mathbb{C}^m,|x|=1}\|\Phi(|x\rangle\langle x|)\|_p,$$

where $|\cdot|$ is the Euclidean norm. A standard and well-known argument shows that eigenvalues of $\Phi(|x\rangle\langle x|)$ are exactly squares of $s_j(x)$, the "Schmidt coefficients" of $x$, so

$$\|\Phi\|_{1\to p}=\max_{x\in\mathcal{W},|x|=1}\left(\sum_{j=1}^{d}s_j(x)^{2p}\right)^{1/p}=\max_{x\in\mathcal{W},|x|=1}\|x\|_{2p}^2,$$

where in the last expression we identify $x\in\mathcal{W}\subset\mathbb{C}^d\otimes\mathbb{C}^d$ (or, to be more precise, $\mathbb{C}^d\otimes\overline{\mathbb{C}^d}$—a distinction we will ignore) with an element of $\mathcal{M}_d$ via the canonical map induced by $u\otimes v\to|u\rangle\langle v|$. (Schmidt coefficients of an element of $\mathbb{C}^d\otimes\mathbb{C}^d$ become singular values of the corresponding element of $\mathcal{M}_d$.)

In other words, $\|\Phi\|_{1\to p}$ is the square of the maximum of the ratio $\|x\|_{2p}/\|x\|_2$ over the $m$-dimensional subspace of $\mathcal{M}_d$ that corresponds to $\mathcal{W}$ under the canonical identification, and that we will still call $\mathcal{W}$,

$$\|\Phi\|_{1\to p}=\max_{x\in\mathcal{W}}(\|x\|_{2p}/\|x\|_2)^2. \tag{3}$$

## VI. THE HAYDEN–WINTER COUNTEREXAMPLE

The Hayden–Winter construction can be described as follows. Let $V:\mathbb{C}^m\to\mathbb{C}^d\otimes\mathbb{C}^d$ be a random isometry (chosen with respect to the Haar measure) and $\Phi:\rho\mapsto\mathrm{tr}_2(V\rho V^\dagger)$ be the corresponding quantum channel from $\mathcal{M}_m$ into $\mathcal{M}_d$. We show in Sec. VII that Dvoretzky's theorem implies that for $m\sim d^{1+1/p}$, such random quantum channel typically satisfies

$$\|\Phi\|_{1\to p}\sim d^{1/p-1}. \tag{4}$$

Here, and throughout the remainder of the paper, $\sim$means "equivalent up to a universal multiplicative constant."

Take as the second channel the (complex) conjugate channel $\bar{\Phi}$ and let $|\psi\rangle$ be the maximally entangled state in $\mathbb{C}^m\otimes\mathbb{C}^m$. It is shown in Ref. 17 (Lemma 3.3) that $(\Phi\otimes\bar{\Phi})(|\psi\rangle\langle\psi|)$ has an eigenvalue $\geq m/d^2$, which implies that with the above choice of $m$,

$$\|\Phi\otimes\bar{\Phi}\|_{1\to p}\geq\|\Phi\otimes\bar{\Phi}\|_{1\to\infty}\geq m/d^2\sim d^{1/p-1}.$$

On the other hand, again with the same choice of $m$, by (4)

$$\|\Phi\|_{1\to p}=\|\bar{\Phi}\|_{1\to p}\sim d^{1/p-1},$$

and thus

$$\|\Phi\|_{1\to p}\|\bar{\Phi}\|_{1\to p}\sim(d^{1/p-1})^2\ll d^{1/p-1}, \tag{5}$$

so that we obtain a violation of the multiplicativity provided that $d^{1/p-1}\leq 1/C$, i.e., $d\geq C^{p/(p-1)}$, where $C$ is the absolute constant hidden behind the $\sim$ symbol. Moreover, this violation is asymptotically extremal. Indeed, while the inequality $\|\Phi\otimes\bar{\Phi}\|_{1\to p}\leq\|\Phi\|_{1\to p}=\|\bar{\Phi}\|_{1\to p}^{-1}\|\Phi\|_{1\to p}\|\bar{\Phi}\|_{1\to p}$ always holds (this follows from results from Ref. 1), in this example the reverse inequality also holds up to an absolute multiplicative constant. At the same time, $\|\bar{\Phi}\|_{1\to p}^{-1}\sim d^{1-1/p}$ is of largest

possible order in the class of $\mathcal{M}_d$-valued quantum channels (see the observation at the end of Sec. IV).

The lower estimate for $\|\Phi\otimes\bar{\Phi}\|_{1\to p}$ was the relatively simple part of the argument from Ref. 17; the authors referred to the proof of their Lemma 3.3 as "an easy calculation." Of course, it is "easy" only after the fact, and the crucial point was coming up with the right pair of channels to analyze.

Finally, as pointed out in Ref. 16, the random approach allows working initially with real spaces ($\mathbb{R}^m$, $\mathbb{R}^d\otimes\mathbb{R}^d$, etc.) and producing channels $\Phi$ fitting into the Hayden–Winter scheme, whose representation in the computational basis is real. In particular, $\Phi=\bar{\Phi}$, so we have channels (acting on complex spaces) for which $\|\Phi\otimes\Phi\|_{1\to p}\gg\|\Phi\|_{1\to p}^2$ and $S_p^{\min}(\Phi\otimes\Phi)<2S_p^{\min}(\Phi)$.

## VII. DVORETZKY'S THEOREM

By (3), $\|\Phi\|_{1\to p}=\max_{x\in\mathcal{W}}(\|x\|_{2p}/\|x\|_2)^2$, where $\mathcal{W}\subset\mathcal{M}_d$ is an $m$-dimensional subspace. The behavior of the ratio between the Euclidean norm and some other norms on subspaces of given dimension is a quantity that has been extensively studied in geometry of Banach spaces. The most classical result in this direction is Dvoretzky's theorem.

*Given $m\in\mathbb{N}$ and $\varepsilon>0$, there is $N=N(m,\varepsilon)$ such that, for any norm on $\mathbb{R}^N$ (or $\mathbb{C}^N$) there is an $m$-dimensional subspace on which that ratio is (approximately) constant, up to a multiplicative factor $1+\varepsilon$.*

This reveals a striking geometric phenomenon: any high-dimensional convex body, no matter how peaked it may be, has sections that are close to Euclidean balls.

For specific norms this statement can be made much more precise, both in describing the dependence $N=N(m,\varepsilon)$ and in identifying the constant of (approximate) proportionality of norms. The version of Dvoretzky's theorem that is relevant here is due to Milman.[21] (Alternative good expositions are, for example, Refs. 8, 24, and 25; the last one presents a proof based on the Gaussian analysis, which allows one to bypass the—deep and not so easy to prove—spherical isoperimetric inequality.)

**Dvoretzky's Theorem:** (Tangible version) *Consider the $n$–dimensional Euclidean space (real or complex) endowed with the Euclidean norm $|\cdot|$ and some other norms $\|\cdot\|$ such that, for some $b>0$, $\|\cdot\|\leq b|\cdot|$. Denote $M=\mathbb{E}\|X\|$, where $X$ is a random variable uniformly distributed on the unit Euclidean sphere. Let $\varepsilon>0$ and let $m\leq c\varepsilon^2(M/b)^2n$, where $c>0$ is an appropriate (computable) universal constant. Then, for most $m$-dimensional subspaces $E$ (in the sense of the invariant measure on the corresponding Grassmannian), we have*

$$\forall x\in E,(1-\varepsilon)M|x|\leq\|x\|\leq(1+\varepsilon)M|x|.$$

*Remarks:* (i) The above result is usually stated with the hypothesis $a^{-1}|\cdot|\leq\|\cdot\|\leq b|\cdot|$ (for some $a,b>0$). However, the parameter $a$ does not enter into the assertion; lower bounds on $\|\cdot\|$ are related to lower bounds on $M$, needed to obtain nontrivial values of $m$ [and the function $N(m,\varepsilon)$ mentioned earlier] in the abstract setting.
(ii) Standard and most elementary proofs yield the assertion only for $m\leq c\varepsilon^2/\log(1/\varepsilon)(M/b)^2n$; the dependence on $\varepsilon$ of the order of $\varepsilon^2$ was obtained in the important papers.[12,26] However, for our purposes it is enough to have, say, $\varepsilon=\frac{1}{2}$, so this aspect of the story is not important.

## VIII. DVORETZKY'S THEOREM FOR SCHATTEN CLASSES

In the Hayden–Winter construction, $\mathcal{W}\subset\mathcal{M}_d$ is a random $m$-dimensional subspace distributed according to the Haar measure on the Grassmann manifold and [cf. (3) and (4)] we want to control the ratio $\|x\|_{2p}/\|x\|_2$ uniformly on $\mathcal{W}$, where $2p=:q>2$. Thus, the context in which one needs to apply Dvoretzky's theorem is the Schatten $q$-norm on the complex space $\mathcal{M}_d$ for $q>2$, in particular, $n=d^2$, $\|\cdot\|=\|\cdot\|_q$, and $|\cdot|=\|\cdot\|_2$, the Hilbert–Schmidt norm. This has been done, e.g., in the 1977 paper[8] (see Example 3.3 there; Ref. 8 focuses on real spaces, but it is noted that all proofs carry over to the complex case). The conclusion is that if $m\sim d^{1+2/q}=d^{1+1/p}$, then the inequality

$$d^{1/q-1/2}\|x\|_2 \leq \|x\|_q \leq Cd^{1/q-1/2}\|x\|_2 \tag{6}$$

holds (for some constant $C \geq 1$ that does not depend on $d$ nor—less crucially—on $q$) for all $x$ in a typical $m$-dimensional subspace of $\mathcal{M}_d$. (If we used the normalized trace to define Schatten norms, the powers of $d$ would disappear.) Combining (6) with (3) yields that when $m \sim d^{1+1/p}$, then $\|\Phi\|_{1\to p} \sim d^{2/q-1} = d^{1/p-1}$ for a typical $\Phi$, which are exactly the values needed for the Hayden–Winter example.

For completeness, let us comment on the details of the derivation of (6) from Dvoretzky's theorem. What we need is to find (or estimate) the quantities $b, M$ appearing in the theorem. Clearly, for all $x \in \mathcal{M}_d$,

$$d^{1/q-1/2}\|x\|_2 \leq \|x\|_q \leq \|x\|_2, \tag{7}$$

which yields the value of the parameter $b=1$, the lower (trivial, and not actually needed for the multiplicativity problem) estimate from (6) and, *a fortiori*, the bound $M \geq d^{1/q-1/2}$. The upper estimate in (6) will now follow once we establish that $M$ is *precisely* of the order of $d^{1/q-1/2}$. Indeed, using (the tangible version of) Dvoretzky's theorem with $\varepsilon = \frac{1}{2}$, we are then led to $m \geq c(\frac{1}{2})^2(M/b)^2 n \sim (d^{1/q-1/2})^2 d^2 = d^{1+2/q}$, and to an upper estimate $\frac{3}{2}M \sim d^{1/q-1/2}$ in (6) (i.e., on a "typical" $m$-dimensional subspace).

As we mentioned above, the fact that $M \sim d^{1/q-1/2}$ is implicit in the argument from Ref. 8. [It is shown in Ref. 8 that $m \sim d^{1+2/q}$ is the optimal (i.e., the largest) dimension for which (approximate) proportionality of norms does hold. Now, if we have had $M \gg d^{1/q-1/2}$, Dvoretzky's theorem would have yielded a nearly Euclidean subspace of dimension $m \gg d^{1+2/q}$ (just repeat the argument from the preceding paragraph with $\gg$ instead of $\sim$), which contradicts the optimality assertion.] However, it is instructive to note that it may also be obtained by many other "standard" methods developed in geometric functional analysis and in random matrix theory. One (*by far* not the easiest, but most precise, at least in the appropriate asymptotic regime) was used by Collins–Nechita.[4] A simple argument to get an upper bound for $M$ goes as follows. Let $X$ be a random variable uniformly distributed on the Hilbert–Schmidt sphere in $\mathcal{M}_d$. It is easy to check, using an elementary $\varepsilon$-net argument, that the expectation of $\|X\|_\infty$ is bounded by $C_0 d^{-1/2}$ for some absolute constant $C_0$. Using the (pointwise) inequality $\|X\|_q \leq \|X\|_2^{2/q}\|X\|_\infty^{1-2/q}$ and Hölder's inequality, we get

$$M = \mathbb{E}\|X\|_q \leq (\mathbb{E}\|X\|_\infty)^{1-2/q} \leq (C_0 d^{-1/2})^{1-2/q} = C_0^{1-2/q} d^{1/q-1/2}.$$

If we are interested in good values of numerical constants, the best possible choice is $C_0 = 2$—the same "2" as in the Wigner's semicircle law. The needed generality and precision can be extracted—at least in the real case—from Ref. 11 [see also Refs. 15 and 6 (Theorem 2.11) or Ref. 28 (Appendix F) for related calculations].

## IX. DERANDOMIZATION

Similarly as the approaches to the additivity conjectures by Hayden–Winter and Hastings, Milman's proof of Dvoretzky's theorem relies on concentration of measure via Lévy's lemma, and so it is highly nonconstructive. Some effort has been put recently in finding explicit subspaces satisfying the conclusion of the theorem. Of course, this must depend on the choice of the initial norm $\|\cdot\|$. The prominent example is the case of the $\ell_1$ norm on $\mathbb{R}^n$, which is relevant to (classical) theoretical computer science, for example, to compressed sensing. In this case the dimension of the subspace is proportional to $n$. Although no explicit construction of such a subspace exists yet, recent results are promising (see Refs. 18, 14, and 19 and references therein). We might hope to adapt such techniques to obtain constructive counterexamples to the additivity conjectures. However, to date the best result in this direction seems to be Ref. 13, with an explicit example which works for all $p > 2$. An explicit counterexample to the companion problem concerning the range $p \in [0,1)$ is exhibited in Ref. 5 (it works for $p$ close to 0).

## X. SHRINKING UNDER RANDOM PROJECTIONS AND RELATED REMARKS

The Hayden–Winter construction requires only an *upper* estimate on $\|x\|_q$ for all $x$ in a (random) subspace of $\mathcal{M}_d$ [cf. (3) and (5)]. This observation leads to counterexamples to additivity conjecture based on a phenomenon that is conceptually simpler (even if less known) than Dvoretzky's theorem. One way to express it is as follows: *if, in the notation of Dvoretzky's theorem,* $(M/b)^2 n =: m_0 \leq m \leq n$, then the one sided estimate $\|x\| \leq C\sqrt{m/n}\, b\, |x|$ holds for all $x$ in a typical $m$-dimensional subspace.

While the choice $m \sim d^{1+1/p}$ (in the construction of a random channel) results in an extremal violation of multiplicativity, the above remark shows that similar calculations for, e.g., all $m \geq d^{1+1/p}$ lead to estimates of the order $m/d^2$ on all the norms $\|\Phi\|_{1\to p}$, $\|\bar{\Phi}\|_{1\to p}$ and $\|\Phi \otimes \bar{\Phi}\|_{1\to p}$, and so a violation occurs as long as $m/d^2$ is small enough, i.e., smaller than a certain numerical constant $c>0$. However, it should be noted that the restrictions $cd^2 > m \geq d^{1+1/p}$ still imply that $d \to \infty$ as $p \to 1$.

It may be more geometrically compelling to express the phenomenon referred to above in its dual form. First, the dual reformulation of Dvoretzky's theorem states that if $K$ is a symmetric body in the $n$-dimensional Euclidean space, then there is (relatively large) $m_0$ such that a typical orthogonal $m_0$-dimensional projection of $K$ is approximately a Euclidean ball. (Determining the threshold $m_0$ involves considering the norm, for which $K$ is the unit ball, and then calculating parameters $M$ and $b$ for the *dual* norm.) The relaxed version states that if $m_0 \leq m \leq n$, then the diameter of a typical $m$-dimensional projection of $K$ does not exceed $C\sqrt{m/n}$ times the diameter of $K$. References for these remarks are, e.g., Refs. 22 and 23 (Sec. 2.3.1), but the phenomenon can, in fact, be traced back (at least) to Ref. 12 or Ref. 20 among others.

## ACKNOWLEDGMENTS

The research of the first named author was partially supported by the Agence Nationale de la Recherche under Grant No. ANR-08-BLAN-0311-03. The research of the second and third named authors was partially supported by their respective grants from the National Science Foundation (USA) and from the U.S.-Israel Binational Science Foundation. The second named author thanks the organizers and fellow participants (particularly F. Brandao and C. King) of the Workshop on Operator Structures in Quantum Information (*Fields Institute*, July 2009), which served as a catalyst for this project.

[1] G. G. Amosov, A. S. Holevo, and R. F. Werner, "On some additivity problems in quantum information theory," Probl. Inf. Transm. **36**, 25 (2000), e-print arXiv:math-ph/0003002.
[2] K. M. R. Audenaert, "A note on the $p \to q$ norms of 2-positive maps," Numer. Linear Algebra Appl. **430**, 1436 (2009), e-print arXiv:math-ph/0505085.
[3] F. G. S. L. Brandao and M. Horodecki, "On Hastings' counterexamples to the minimum output entropy additivity conjecture," e-print arXiv:0907.3210.
[4] B. Collins and I. Nechita, "Random quantum channels. II: Entanglement of random subspaces, Rényi entropy estimates and additivity problems," e-print arXiv:0906.1877.
[5] T. Cubitt, A. W. Harrow, D. Leung, A. Montanaro, and A. Winter, "Counterexamples to additivity of minimum output $p$-Rényi entropy for $p$ close to 0," Commun. Math. Phys. **284**, 281 (2008).
[6] K. R. Davidson and S. J. Szarek, "Local operator theory, random matrices and Banach spaces," in *Handbook of the Geometry of Banach Spaces*, edited by W. B. Johnson and J. Lindenstrauss (North-Holland, Amsterdam, 2001), Vol. 1, pp. 317–366; *Handbook of the Geometry of Banach Spaces*, edited by W. B. Johnson and J. Lindenstrauss (North-Holland, Amsterdam, 2003), Vol. 2, pp. 1819–1820.
[7] A. Dvoretzky, "Some results on convex bodies and Banach spaces," in *Proc. Internat. Sympos. Linear Spaces (Jerusalem, 1960)* (Jerusalem Academic Press, Jerusalem, Pergamon, Oxford, 1961), pp. 123–160.
[8] T. Figiel, J. Lindenstrauss, and V. D. Milman, "The dimension of almost spherical sections of convex bodies," Acta Math. **139**, 53 (1977).
[9] M. Fukuda and C. King, "Entanglement of random subspaces via the Hastings bound," e-print arXiv:0907.5446.
[10] M. Fukuda, C. King, and D. Moser, "Comments on Hastings' additivity counterexamples," e-print arXiv:0905.3697.
[11] S. Geman, "A limit theorem for the norm of random matrices," Ann. Probab. **8**, 252 (1980).
[12] Y. Gordon, "Some inequalities for Gaussian processes and applications," Isr. J. Math. **50**, 265 (1985).
[13] A. Grudka, M. Horodecki, and L. Pankowski, "Constructive counterexamples to additivity of minimum output Renyi entropy of quantum channels for p>2," e-print arXiv:0911-2515
[14] V. Guruswami, J. R. Lee, and A. Wigderson, "Euclidean sections of $\ell_1^N$ with sublinear randomness and error-correction

over the reals," in *Proceedings of the 12th International Workshop on Randomization and Combinatorial Optimization: Algorithms and Techniques (RANDOM)*, Lecture Notes in Comput. Sci., vol. 5171 (Springer, Berlin, Heidelberg, 2008), pp. 444–454.
[15] U. Haagerup and S. Thorbjørnsen, "Random matrices with complex Gaussian entries," Expo. Math. **21**, 293 (2003).
[16] M. B. Hastings, "Superadditivity of communication capacity using entangled inputs," Nat. Phys. **5**, 255 (2009).
[17] P. Hayden and A. Winter, "Counterexamples to the maximal $p$-norm multiplicativity conjecture for all $p>1$," Commun. Math. Phys. **284**, 263 (2008), e-print arXiv:0807.4753.
[18] P. Indyk, "Uncertainty principles, extractors, and explicit embeddings of L2 into L1," in *STOC'07-Proceedings of the 39th Annual ACM Symposium on Theory of Computing* (ACM, New York, 2007) pp. 615–620.
[19] P. Indyk and S. J. Szarek, "A simple construction of almost-Euclidean subspaces of $\ell_1^n$ via tensor products," e-print arXiv:1001.0041.
[20] W. Johnson and J. Lindenstrauss, "Extensions of Lipschitz mappings into a Hilbert space," in *Conference in Modern Analysis and Probability (New Haven, Conn., 1982)*, Contemp. Math., vol. 26 (American Mathematical Society, Providence, RI, 1984), pp. 189–206.
[21] V. Milman, "A new proof of the theorem of A. Dvoretzky on sections of convex bodies," Funct. Anal. Appl. **5**, 28 (1971).
[22] V. Milman, "A note on a low $M^*$-estimate," in *Geometry of Banach Spaces (Strobl, 1989)*, London Mathematical Society Lecture Note Series Vol. 158 (Cambridge University Press, Cambridge, 1990), pp. 219–229.
[23] V. Milman, "Topics in asymptotic geometric analysis," in *Visions in mathematics. Towards 2000 (Tel Aviv, 1999)*, Geom. Funct. Anal., Special Volume, Part II (Birkhäuser, Basel, 2000), pp. 792–815.
[24] V. D. Milman and G. Schechtman, *Asymptotic Theory of Finite-Dimensional Normed Spaces. With an Appendix by M. Gromov*, Lecture Notes in Mathematics Vol. 1200 (Springer-Verlag, Berlin, 1986).
[25] G. Pisier, *The Volume of Convex Bodies and Banach Space Geometry*, Cambridge Tracts in Mathematics Vol. 94 (Cambridge University Press, Cambridge, 1989).
[26] G. Schechtman, "A remark concerning the dependence on ε in Dvoretzky's theorem," in *Geometric aspects of functional analysis (1987–88)*, Lecture Notes in Math., vol. 1376 (Springer, Berlin, 1989), pp. 274–277
[27] P. W. Shor, "Equivalence of additivity questions in quantum information theory," Commun. Math. Phys. **246**, 453 (2004).
[28] S. J. Szarek, "The volume of separable states is super-doubly-exponentially small in the number of qubits," Phys. Rev. A **72**, 032304 (2005).
[29] S. J. Szarek, "On norms of completely positive maps," in *Proceedings of IWOTA 2008*, Oper. Theory Adv. Appl., vol. 202 (Birkhäuser, Basel, 2009), pp. 535–538, e-print arXiv:quant-ph/0603110.
[30] J. Watrous, "Notes on super-operator norms induced by Schatten norms," Quantum Inf. Comput **5**, 58 (2005).
[31] R. F. Werner and A. S. Holevo "Counterexample to an additivity conjecture for output purity of quantum channels," J. Math. Phys. **43**, 4353 (2002), e-print arXiv:quant-ph/0203003.