Convexity, Complexity, and High Dimensions

Stanislaw J. Szarek *

Abstract. We discuss metric, algorithmic and geometric issues related to broadly understood complexity of high dimensional convex sets. The specific topics we bring up include metric entropy and its duality, derandomization of constructions of normed spaces or of convex bodies, and different fundamental questions related to geometric diversity of such bodies, as measured by various isomorphic (as opposed to isometric) invariants.

Mathematics Subject Classification (2000). Primary 46B20; Secondary 46B09, 47B06, 52A21, 52C17, 15A52, 90C25, 94B75.

Keywords. Convex body, high dimension, complexity, metric entropy, asymptotic geometric analysis

1. Introduction

When modeling complex (real-life or abstract) systems with many degrees of freedom, we are frequently led to mathematical objects whose dimension can be related to the number of free parameters in the underlying system and, as a consequence, is very large. Since many naturally appearing relationships between, or constraints on the parameters are linear or at least convex, we are thus led to high dimensional convex sets. Two areas of traditional mathematics that come to mind when faced with the problem of analyzing such sets are *classical geometry* and *functional analysis*. However, geometry is usually focused on obtaining very precise information for a fixed, not-too-large dimension. Functional analysis, on the other hand, is typically concerned with the infinite-dimensional setting (which frequently is an idealization of a very large dimension), but often provides only qualitative information. Fortunately, there is a middle ground between these two approaches and it has turned out to be quite fertile. The last few decades witnessed the development of a quite powerful quantitative methodology in geometric functional analysis that, together with similar advances in areas such as combinatorics or theoretical computer science, has been lately referred to as *asymptotic geometric analysis*. In a nutshell, the prescription for success of the asymptotic theory depends on identifying and exploiting *approximate* symmetries of various problems that escaped the earlier "too qualitative" or "too rigid" methods of classical functional analysis

*Supported in part by a grant from the National Science Foundation (U.S.A.).

and classical geometry. More specifically, an important feature of the area is the predominantly *isomorphic* (as opposed to *isometric*) character of the questions: one is usually after the rough (i.e., "up to a universal constant") asymptotic order of the quantities studied and not their more precise behavior. This sometimes makes the problem solvable. [See the article [48] by B. Klartag in this collection for a discussion of developments in the so-called "almost isometric" theory.] However, universal estimates are required, independent of the particular instance of the problem, most notably of the dimension. As is very well known to specialists, but perhaps not fully appreciated by non-experts, this last feature is absolutely crucial because it allows for applications to infinite dimensional functional analysis and to quantitative questions in applied fields. This framework led to discoveries of many surprising phenomena, which may be subsumed in the following "experimental" observation: low-dimensional intuitions are often *very* wrong in high dimensions. However, as opposed to other fields such as topology, high-dimensional curiosities generally do not appear via a quantum jump; say, when passing from dimension 3 to 4, or from 7 to 8. Instead, small changes accumulate as the dimension increases, leading ultimately to a qualitatively new picture.

In the present article we shall focus on those aspects of the theory that are relevant to broadly defined *complexity* of convex sets. To exemplify what we mean by complexity, we will now hint at three alternative viewpoints on the notion. Below K will stand for a generic *convex body* in $\mathbb{R}^n$ (i.e., compact convex set with nonempty interior).

(i) *The algorithmic complexity* How difficult is it to describe K? A prime example (which we mention mainly for demonstration purposes) is here the algorithmic complexity of the *membership oracle*: How difficult is it to decide whether a point belongs to K? Another class of questions is: Suppose that the existence of K with certain properties is given by a non-constructive proof, or by probabilistic considerations; is it possible to give an explicit example, or an efficient derandomized algorithm?

(ii) *The geometric complexity, or diversity* How complicated (in an appropriate geometric sense) is K? To what extent do convex bodies of the same dimension exhibit common features? In particular, to what extent do they resemble the arguably most regular body, the Euclidean ball?

(iii) *The metric entropy* Here we need an underlying metric structure, typically given by a norm. Given $\varepsilon > 0$, how many balls of radius ε do we need to cover K? The logarithm (to base 2) of the minimal cardinality of such cover is called the *metric entropy function* of K and can be interpreted as the complexity of K, measured in bits, at the level of resolution ε with respect to the metric in question.

In what follows we will provide some background information concerning these three aspects of complexity, describe recent developments in each area, and list related open problems. Each of the viewpoints (i)-(iii) will correspond to one section in the exposition; however, we will reverse the order. On the other hand, we emphasize that the three points of view are intimately interconnected. For example, one aspect of geometric diversity involves approximating convex bodies by simple ones, a problem which has obvious algorithmic ramifications. A sample such

question, approximating by polytopes, has been extensively studied and reported on in [14], see also [92].

Notation will be introduced as we proceed, but we list below a few general rules and conventions that will be used throughout the paper. We will sometimes use unexplained (but standard in the field) notation in side remarks. For this and for more background on the issues discussed here we refer the reader to monographs [75, 108, 84] and, for more up-to-date expositions, to surveys contained in [41], especially the chapters [42, 18, 24, 30, 43, 50, 56, 59, 63, 64], and – particularly for the motivational aspects – to the 1996 ECM and the 1998 ICM talks by V. Milman [72, 73].

If X is a normed space, we will write B_X for its unit ball (centered at the origin). In the other direction, if K is a convex body in $\mathbb{R}^n$ containing the origin in its interior, $\|\cdot\|_K$ will stand for the gauge of K (i.e., $\|x\|_K := \inf\{t > 0 : x \in tK\}$); if K is symmetric with respect to the origin, the gauge of K is just the norm for which K is the unit ball. Thus, in a way, the body K (symmetric with respect to the origin) is identified with the normed space $(\mathbb{R}^n, \|\cdot\|_K)$; this is the main reason for the interplay of geometric and functional analytic ideas.

The letters $C, c_0, C' \ldots$ will stand for absolute positive constants, independent of the particular instance of the problem considered, most notably of the dimension. However, the numerical values corresponding to the same symbol may vary between occurrences. Similarly, $C(\alpha)$ will denote a constant depending only on the parameter α, and so on. For two functions f, g (depending on the same or on different parameters), $f \sim g$ will mean that f and g are of the same order, i.e., $cf \le g \le Cf$ (with $C, c > 0$ independent of the parameters involved, as required by the previous convention).

2. Metric entropy and its duality

While in many applications *calculating* the metric entropy of *specific* sets is the primary objective, here we will mention applications only in passing and concentrate instead on the more fundamental properties of the notion, particularly those connected to duality considerations.

2.1. Notation and historical background, the duality conjecture.

If K, B are subsets of a vector space, the *covering number* of K by B, denoted $N(K, B)$, is the minimal number of translates of B needed to cover K. Similarly, the *packing* number $M(K, B)$ is the maximal number of disjoint translates of B by elements of K. [Note that geometers usually require only that the *interiors* of the translates be disjoint.] The two concepts are closely related, particularly if B is centrally symmetric; we have then $N(K, 2B) \le M(K, B) \le N(K, B)$. If B is a ball in a normed space and K a subset of that space (the setting and the point of view we will usually employ), these notions reduce to considerations involving the smallest ε-nets or the largest ε-separated (or 2ε-separated) subsets of K.

Besides the immediate geometric framework, packing and covering numbers appear naturally in numerous subfields of mathematics, ranging from classical and functional analysis through operator theory and probability theory (particularly when studying stochastic processes, see [26, 95, 61, 53]) to information theory and computer science (where, for example, a code is typically a packing). As with other notions touching on convexity, an important role is played by considerations involving duality. The central problem in this area is the 1972 *duality conjecture for covering numbers* due to Pietsch [79], which has been originally formulated in the operator-theoretic context (see below), but which in the present setting can be stated as

Conjecture 2.1 (The Duality Conjecture). *There exist numerical constants $a, b \geq 1$ such that for any dimension n and for any two symmetric convex bodies K, B in $\mathbb{R}^n$ one has*

$$b^{-1} \log N(B^\circ, aK^\circ) \leq \log N(K, B) \leq b \log N(B^\circ, a^{-1}K^\circ) \ . \tag{1}$$

Above and in what follows $A^\circ := \{u \in \mathbb{R}^n : \sup_{x\in A}\langle x, u\rangle \leq 1\}$ is the polar body of A; "symmetric" is a shorthand for "symmetric with respect to the origin" and, for definiteness, all logarithms are to the base 2. For simplicity, we will generally restrict our attention to symmetric sets; however, most statements can be formulated without the symmetry assumption. Of course, due to the bipolar theorem, K and B are exchangeable in (1) and so it is enough to prove only one of the two inequalities. We emphasize that the "equivalence" of the quantities in (1), and overall in this section, is more involved than the relation $\sim$ defined in the introduction.

In our preferred setting of a normed space X, the proper generality is achieved by considering $\log N(K, t\,B_X)$, where $t > 0$ and K is a general (convex, symmetric) subset of X. The polars should then be thought of as subsets of X^*, with $(B_X)^\circ$ coinciding with B_{X^*}, the unit ball of that space, and (1) becomes

$$b^{-1} \log N(B_{X^*}, atK^\circ) \leq \log N(K, tB_X) \leq b \log N(B_{X^*}, a^{-1}tK^\circ) \tag{2}$$

With minimal care, infinite-dimensional spaces and sets may be likewise considered. To avoid stating boundedness/compactness hypotheses, which are peripheral to the phenomena in question, it is convenient to allow $N(\cdot,\cdot)$, $M(\cdot,\cdot)$ etc. to take the value $+\infty$. Finally, the original operator-theoretic formulation of the conjecture is as follows. Given (linear bounded, or compact) operator $u : Y \to X$ between two normed spaces we define *entropy numbers* of u as $e_k(u) := \inf\{\varepsilon > 0 : N(uB_Y, \varepsilon B_X) \leq 2^{k-1}\}$. Do we have then

$$a^{-1} e_{bk}(u) \leq e_k(u^*) \leq a e_{k/b}(u^*) \tag{3}$$

(where $u^* : X^* \to Y^*$ is the adjoint of u) uniformly over spaces X, Y, operators u and $k \geq 1$?

2.2. The Hilbert space case. To indicate where the difficulty of the problem lies, we shall comment on the enlightening special cases when, in the language

of (3), X and/or Y is a Hilbert space. If *both* X and Y are Hilbert spaces, the situation is nearly trivial. Indeed, entropy numbers of a Hilbert space operator depend only on its singular numbers, and the singular numbers of an operator and its adjoint are identical. In the setting of (1), this corresponds to the bodies K, B (and hence K°, B°) being ellipsoids with the pair (K, B) affinely equivalent to the pair (B°, K°) (in that order!). As a consequence, (1), (3), and the appropriate version of (2), hold with $a = b = 1$. At the other extreme, in the general case, the four bodies K, B, K°, B° appearing in (1) may be *all* very different and so the reasons for the duality result (if it indeed does hold) must be much deeper. Finally, if one of the spaces (say, X) is a Hilbert space, looking at the equivalence (2) we see that it expresses what seems to be a rather fundamental property of *all* convex subsets of the Hilbert space.

Let us also point out that if $\dim X = \dim K := k < \infty$ (and K is bounded), then standard considerations show that, as $t \to 0^+$, both metric entropy functionals $\log N(K, t\,B_X)$ and $\log N(B_{X^*}, tK^\circ)$ are equivalent to $k \log(1/t)$. In fact, it is even true that the differences between the functionals and $k \log(1/t)$ are bounded. However, the bounds for the two differences depend in an intricate way on K, not allowing for any meaningful quantitative inferences, nor for deriving any conclusions about reasonably general infinite dimensional sets. [Comments in this paragraph are not dependent on X being a Hilbert (i.e., Euclidean) space.]

2.3. Duality results. The three decades following the statement of the conjecture brought many useful partial and/or related results, see [91, 51, 107, 19, 78, 33, 85] and their references. However, only in the last few years substantial progress was achieved with respect to the original problem. We have (see [8, 9])

Theorem 2.2. *There exist universal constants $a, b \geq 1$ such that* (2) *holds if X is a Hilbert space, uniformly over all symmetric convex sets $K \subset X$ and over $t > 0$. Moreover, the same is true if X is K-convex, with a, b depending on the K-convexity constant of X.*

The notion of *K-convexity* (the notation which, by the way, has nothing to do with our convex set K) goes back to [65] and is well known to specialists; we refer to [84, 64] for a precise definition, background and properties. Requiring K-convexity imposes a rather mild geometric restriction on the underlying space. For example, the class of K-convex spaces includes all L_p-spaces for $1 < p < \infty$ (classical or non-commutative), and similarly all uniformly convex and all uniformly smooth spaces. While many interesting descriptions of this class are possible (see [56, 64]), here we just mention that K-convexity is equivalent (see [82]) to the absence of large subspaces resembling (in the sense of the next section) finite-dimensional ℓ_1-spaces, and that it can be nicely quantified: there is a parameter called the *K-convexity constant*, which can be defined both for finite and infinite dimensional normed spaces, and which has good permanence properties with respect to standard functors of functional analysis.

Translating Theorem 2.2 to the other formulations is straightforward. For example, we get that (3) holds if one of the spaces X, Y is a Hilbert space or,

more generally, is K-convex. Similarly, if (say) B is an ellipsoid, then (1) holds uniformly over $n \in \mathbb{N}$ and over (symmetric convex bodies) $K \subset \mathbb{R}^n$ etc. Regarding constants, we know how to prove (2) for the Hilbert space with any $a > 2$, with $b = b(a)$; improvements (to "any $a > 1$") would follow if a certain geometric statement conjectured in [76] was true.

2.4. The convexified packing. An interesting feature of [9] is the formal introduction and an initial study of a modified notion of packing that has already been implicit in [19]. We will provide now some details since this will allow us to present a sketch of the proof of Theorem 2.2 and to pinpoint the ingredients that are missing in the general case of Conjecture 2.1; at the same time, the new notion appears to be interesting by itself. A sequence $x_1, \ldots, x_m$ is called a *convexified B-packing* iff

$$(x_j + B) \ \cap \ \mathrm{conv} \bigcup_{i<j} (x_i + B) \ = \ \emptyset$$

for $j = 2, \ldots, m$. [We emphasize that, as opposed to the usual notions of packing and covering, the *order* of the points *is* important here.] Next, the *convexified packing number* $\hat{M}(K, B)$ is the maximal length of a sequence in K which is a convexified B-packing. It turns out that for this modified notion the duality in the sense analogous to (1)-(3) does hold, and that it is (essentially) a consequence of a Hahn-Banach type separation theorem. For example, we have (see [9])

If $K, B \subset \mathbb{R}^n$ are convex symmetric bodies, then $\hat{M}(K, B) \le \hat{M}(B^\circ, K^\circ/2)^2$.

Accordingly, if we knew that the numbers $M(\cdot, \cdot)$ and $\hat{M}(\cdot, \cdot)$ were in the appropriate sense equivalent, the original duality conjecture would follow immediately. While clearly $\hat{M}(K, B) \le M(K, B)$, any general inequality going in the opposite direction appears at the first sight unlikely. However, the following reduction (shown in [8]) simplifies the matter substantially.

For a given space X, if (2) holds for $t = 1$ and all $K \subset X$ verifying $B_X/4 \subset K \subset 4B_X$, then it holds (perhaps with different $a, b > 0$) for all K and all $t > 0$.

In other words, it is enough to prove (1) (or even the first inequality in (1)) for K, B such that $B/4 \subset K \subset 4B$. This reduction allows us to close the loop, at least under some additional mild geometric assumptions about the ambient normed space.

For bounded sets in a K-convex space X, $M(\cdot, B_X)$ and $\hat{M}(\cdot, B_X)$ are comparable.

More precisely, we have $\log M(T, B_X) \le \beta \log \hat{M}(T, B_X/4)$ where β depends only on the diameter of the convex set T and (the upper bound on) the K-convexity constant of X. Moreover, the roles of B and T can be reversed if T is symmetric and $T \supset rB$ for some $r > 0$ (with β depending on r). Proofs of both these facts (contained in [9]) are based on the so-called Maurey's lemma (see [81]) and on the ideas from [19].

Theorem 2.2 follows now by combining (more or less) formally the three statements above. The argument suggests several natural questions.

Problem 2.3. Are the quantities $M(\cdot, B_X)$ and $\hat{M}(\cdot, B_X)$ always (in the appropriate sense) comparable? Comparable uniformly over well-bounded subsets of (an arbitrary) normed space X? Comparable uniformly over subsets of a Hilbert space X (without restriction on the diameter)?

An affirmative answer to the second question would imply an affirmative answer to Conjecture 2.1 in full generality. Similarly, an affirmative answer for a specific non-K-convex space X would imply the form (2) of the conjecture for that space (and the form (3), with the second space Y arbitrary). An interesting test case is $X = \ell_1$.

While equivalence of $M(\cdot, B_X)$ and $\hat{M}(\cdot, B_X)$ over all convex subsets of X (i.e., in absence of a uniform upper bound on the diameter, the first and the third part of Problem 2.3) is not required for the corresponding case of the Duality Conjecture 2.1, good understanding of the relationship between the two quantities may have implications for complexity theory. Indeed, a standard device in constructing geometric algorithms is a *separation oracle* (cf. [35]): if T is a convex set then, for a given x, the oracle either attests that $x \in T$ or returns a functional efficiently separating x from T. It is arguable that quantities of the type $\hat{M}(T, \cdot)$ correctly describe complexities of the set T with respect to many such algorithms.

3. Geometric complexity of convex bodies and their diversity

When comparing shapes of convex bodies, it is most natural in our context to not distinguish K from its images via invertible affine maps. This may be thought of as choosing for each body the coordinate system that is most appropriate for the particular property that is being studied, and leads to the concept of the *Banach-Mazur distance*. For (symmetric) convex bodies $U, V \subset \mathbb{R}^n$ one sets

$$d(U, V) := \inf\{\lambda > 0 : \exists w \in GL(n) \;\; U \subset wV \subset \lambda U\}.$$

This definition is usually formulated in the language of normed spaces: $d(X, Y) := \inf\{\|w\| \cdot \|w^{-1}\| \;\; : \;\; w : X \to Y \;\; \text{an isomorphism}\}$. We refer to the monograph [108] for an exhaustive study of issues related to this notion.

3.1. The structure of the Banach-Mazur compactum. The set of (classes of affinely equivalent) symmetric convex bodies in $\mathbb{R}^n$ (or, equivalently, of classes of isometric n-dimensional normed spaces), endowed with the Banach-Mazur distance, is usually called the (nth) *Banach-Mazur compactum* or the *Minkowski compactum*. [See [1] for most recent results about the *topological* structure of this set.] It is actually $\log d(\cdot, \cdot)$ which has the usual properties of a distance function, but it is customary to abuse the notation and talk about $d(\cdot, \cdot)$ as if it was a metric. It is a fundamental result due to F. John [40]) that for any n-dimensional symmetric convex body K its distance $d(K, B_2^n)$ to the Euclidean ball B_2^n may be at most $\sqrt{n}$, and it is easy to see that this bound can not be

in general improved. It follows right away that the *diameter* of the compactum is at most n, and the remarkable result of Gluskin [31] shows that this bound can not be substantially improved: we do have pairs K, B of n-dimensional symmetric convex bodies for which $d(K, B) \geq cn$ (where $c > 0$ is, according to our convention, a universal constant independent of n). We take this opportunity to point out several unsolved problems in this general direction. First, it would be interesting to determine the *exact* diameter of the Banach-Mazur compactum for specific low dimensions; in fact, the only case when the diameter of the compactum is precisely known is $n = 2$ (see [11]), and the complex analogue is unknown even in dimension 2. A more serious problem is the question of finding (the order of) the maximal distance of specific important convex bodies to general ones of the same dimension. For the *n-dimensional cube* B_∞^n (the unit ball of ℓ_∞^n), the easy lower and upper bounds of $\sqrt{n}$ and n were improved only around 1990 in, respectively, [98] and [20]. The lower bound $cn \log n$ from [98] remains the best known, while the upper one has been tightened in [101] and in a series of papers by Giannopoulos culminating in $Cn^{5/6}$ in [29]. Clearly, a wide gap still persists. Another wide open question is that about the diameter of the compactum of the *not-necessarily-symmetric* n-dimensional convex bodies, with the definition of the distance involving additionally a minimum over translations. The analogue of John's result (also contained in [40]) yields the value n for the radius with center at B_2^n. The resulting estimate n^2 on the diameter has been improved in [86] (see also [13]) to $n^{4/3}$ (times a logarithmic factor). For a more general discussion of the isomorphic theory of non-symmetric convex bodies we refer to the recent articles [54, 74, 34] and their references.

3.2. Quotient of a subspace theorem and its aftermath. It follows from the results quoted in section 3.1 that convex bodies/normed spaces can be quite distant in the Banach-Mazur sense. Accordingly, it was a major surprise when Milman ([69]) discovered in the mid 1980's that, in some sense, every convex body hides somewhere inside its structure an ellipsoid of nearly full dimension. More precisely, we have (in the language of normed spaces)

Theorem 3.1 (Quotient of a subspace theorem). *Given $\theta \in (0, 1)$ and an n-dimensional normed space X there exists a* subspace of a quotient *of X whose dimension is $\geq \theta n$ and whose Banach-Mazur distance to the Euclidean space does not exceed $C(\theta)$. Moreover, $C(\theta)$ can be chosen to verify* $\lim_{\theta \to 0^+} = 1$.

In other words, every n-dimensional symmetric convex body admits a central section and an affine image (not necessarily bijective) of that section which is of dimension $\geq \theta n$ and which is $C(\theta)$-equivalent (in the sense of the Banach-Mazur distance) to a Euclidean ball. Theorem 3.1 should be compared with the much earlier celebrated Dvoretzky theorem (see [27], and [68] for the improved version quoted here) which, in the same context, asserts existence of almost Euclidean *sections*, or subspaces, whose dimension is just of order $\log n$. It is easy to see that, in general, if we only use the operation of passing to a subspace (or, dually, only the operation of passing to a quotient), then this logarithmic order can not be improved. [We discuss some remarkable special cases when it can be dramati-

cally improved in the next section.] Still, it is conceivable that *some* considerable regularity can be achieved by a single operation of passing to a "proportional" subspace (or to a "proportional" quotient). In the wake of his quotient of a subspace theorem Milman stated in his 1986 ICM lecture ([70]) several specific problems going in that direction. All these problems were recently answered in the negative due to the discovery of a new phenomenon which we will next describe.

3.3. The saturation phenomenon. The following result from [103] is a sample illustration of the phenomenon.

Theorem 3.2 (The saturation phenomenon). *Let n and m_0 be positive integers with $\sqrt{n}\log n \le m_0 \le n$. Then, for every finite dimensional normed space W with*

$$\dim W \le c_1 m_0/\sqrt{n} \tag{4}$$

there exists an n-dimensional normed space X such that every subspace Y of X with $\dim Y \ge m_0$ contains a contractively complemented subspace isometric to W.

Loosely speaking, Theorem 3.2 says that the space X is so "saturated" with subspaces isometric to W (copies of W), that such subspaces persist in every "sufficiently large" subspace of X. Furthermore, due to the complementability clause in the assertion of Theorem 3.2, the statement can be dualized, i.e., "every subspace Y of X" can be replaced by "every quotient Y of X." Thus, in general, passing to large subspaces *or* large quotients can not erase k-dimensional features of a space if k is below certain threshold value. This is in stark contrast to the operation of passing to a large quotient of a subspace, which – by Theorem 3.1 – may lead, in a sense, to losing *all* information about the original space, no matter how complicated that space was.

Let us point out that, under the hypotheses of the Theorem, the dimension $k := \dim W$ is always nontrivial (i.e., large, if n is large), and in the most interesting case when $m_0 \sim n$ (say, $m_0 \approx n/2$) we can have $k \sim \sqrt{n}$. It follows that Theorem 3.2 imposes strict limits on properties that may be achieved (or improved) by passing to a large subspace (resp., quotient). Indeed, no property of normed spaces whose violation can be witnessed inside subspaces of dimension $\ll \sqrt{\dim X}$ (and which is inherited by complemented subspaces of a space) can be in general achieved by passing to a subspace (resp., quotient) of X whose dimension is comparable to that of X. To demonstrate that, we choose any space W with $\dim W \ll \sqrt{n}$ which does not have the property in question and use Theorem 3.2 to construct an n-dimensional space; then every sufficiently large subspace (resp., quotient) of X contains a contractively complemented subspace isometric to W and consequently can not have our property. Examples of properties which can be so "prevented" include being of nontrivial type or cotype, which immediately settles in the negative (and in a very strong sense) Problem 1 from [70]: *Does every n-dimensional normed space admit a quotient of dimension $\ge n/2$ whose cotype 2 constant is bounded by a universal numerical constant?*

Statements similar to Theorem 3.2 hold if it is additionally required that X has certain regularity properties. For example, if we insist that the cotype q constant

of X (for some $q \in (2, \infty)$) be controlled, it is possible to construct X which is saturated with copies of any given space W whose cotype q constant is not too large, provided $\dim W$ verifies a condition resembling (4). These topics were developed in [103, 104] and led to negative answers to Problems 2 and 3 from [70].

All the above notwithstanding, some *global* regularity of bodies/spaces may be achievable by passing to proportional quotient or subspaces. For example, already in [69], as a step in the proof of Theorem 3.1, it was established that every finite dimensional normed space admits a "proportional" quotient of well-bounded *volume ratio*, a volumetric characteristic of a convex body closely related to cotype 2 property of the corresponding normed space. It would be important to find more examples of, and/or limitations on such results. As a sample problem we mention the following

Problem 3.3. Given a finite dimensional normed space X, does there exist a subspace $Y \subset X$ with $m := \dim Y \geq \dim X/2$ and a basis $y_1, \ldots, y_m$ of Y such that, denoting by $y_1^*, \ldots, y_m^*$ the dual basis of Y^* we have

$$\mathrm{Ave}_{\varepsilon_i=\pm 1} \left\| \sum_{i=1}^m \varepsilon_i y_i \right\| \cdot \mathrm{Ave}_{\eta_j=\pm 1} \left\| \sum_{j=1}^m \eta_j y_j^* \right\| \leq Cm \ ?$$

It is in fact an open problem whether a similar property holds for every normed space *without* passing to a subspace. [For example, a slightly weaker form of this last question was stated as Problem 6 in [70].]

3.4. Products of convex bodies and the Nontrivial Projection Problem. A measure of geometric complexity of a high dimensional convex body K is whether it can be "reduced," in some meaningful sense, to bodies of substantially lower dimension. One such natural reduction would be approximating K, in the sense of Banach-Mazur distance, by Cartesian products of (two or more) convex bodies, each of which has a reasonably large dimension. The so phrased problem makes sense also for non-symmetric bodies, but in the symmetric case it reduces to the well known *nontrivial projection problem*.

Problem 3.4. Do there exist $C > 0$ and a sequence $k_n \to +\infty$ such that for every n-dimensional normed space X there is a projection P on X with $\|P\| \leq C$ and $\min\{\mathrm{rank}P, \mathrm{rank}(I-P)\} \geq k_n$?

A question about somewhat stronger property, the *finite-dimensional basis problem* was resolved in early 1980s (after having been open for about 50 years) in [32] and [97] (see also [60]), where it was shown that the statement from Problem 3.4 can not hold with k_n substantially larger than $\sqrt{n}$ (more precisely, with $k_n \gg \sqrt{n \log n}$) and that, in general, we can not find projections on X whose rank and corank are of the same order as $\dim X$ and whose norm is $o(\sqrt{\dim X})$. [Note that every k-dimensional subspace of a normed space is complemented via a projection of norm $\leq \sqrt{k}$, see [44], or even slightly smaller, see [52, 50].] Various versions of Problem 3.4 were stated in the ICM talks by Milman (1986, [70]) and, most notably, by

Pisier (1983, [83]), with the latter reporting also on the definitive treatment of the case when $\dim X = \infty$: it may then happen that, for any finite rank projection P on X one has $\|P\| \geq c\sqrt{\mathrm{rank}P}$. [The purely infinite dimensional counterexample to splitting into a nontrivial Cartesian product, or even to a weaker property, is provided by the Gowers-Maurey *hereditarily indecomposable* spaces, see [63].]

In spite of all these negative results it is still conceivable that the answer to Problem 3.4 is affirmative, even with $k_n \sim \sqrt{n}$; this threshold is precise (on the power scale) in the case of "the usual suspects," Gluskin-type random spaces, (see [60]) and – perhaps for a reason – parallels some thresholds related to the saturation phenomenon from section 3.2. In fact, improvements on the extremal order $\sqrt{\mathrm{rank}P}$ for norms of projections have been known for quite a while, see [80, 83]. The following bound ([105]) can be obtained by combining known techniques (in a not-so-straightforward manner, though).

Theorem 3.5. *There exist $C, c > 0$ and a sequence $k_n \geq \exp(c\sqrt{\log n})$ such that, for every n-dimensional normed space X, there is a projection P on X with $\min\{\mathrm{rank}P, \mathrm{rank}(I-P)\} \geq k_n$ and $\|P\| \leq C(\log k_n)^2$.*

Going even further, we do not see easy counterexamples to the following (sample) statement stronger than the one in Problem 3.4: *Given n-dimensional normed space X and an integer m with $\sqrt{n} < m \leq n$, the space X can be split into a direct sum of m subspaces $E_1, \ldots, E_m$ of approximately equal dimensions, and such that if P_j is the projection onto E_j that annihilates all E_i with $i \neq j$, then* $\max_{1 \leq j \leq m} \|P_j\| \leq C$. This would be a generalization of the classical Auerbach lemma which asserts that the answer is yes, with $C = 1$, if $m = n$. However, it is possible that, at least for some range of m, an argument in the spirit of [98] may yield a counterexample.

4. Algorithmic complexity and derandomization, pseudorandom matrices

Many results in asymptotic geometric analysis, including virtually all cited in the preceding section, have been obtained by *probabilistic* considerations. For example, when the objective is to prove the existence of a convex body (or a normed space) with certain property, the strategy is to come up with an appropriate random variable whose values are convex bodies, and then to show that with nonzero (and typically close to 1) probability the property in question is satisfied. [The arguments usually involve precise metric entropy estimates for various subsets of $\mathbb{R}^n$, or for sets of operators on $\mathbb{R}^n$, combined with large deviation and, particularly, small ball estimates for vector-valued random variables; the latter two are aspects of the celebrated *measure concentration phenomenon*, the standard form of which is more adapted to almost isometric questions than to isomorphic ones.] For many more examples of similar arguments in other contexts see [5].

In all such cases, a natural question is: *Is it possible to give an explicit example, or a derandomized algorithm?* An explicit example must have an explicit

reason, and this should presumably be reflected by the presence of some additional structure and a more natural, "nicer" end-product. Even more importantly, if a question is motivated by applications, it is usually imperative that the solution be explicit, or at least easily verifiable. In this section we will sketch several sample contexts when a derandomized proof would be desirable, and describe a few attempts at derandomization (or partial derandomization) of constructions that were originally obtained using probabilistic methods.

Very often the object one constructs (a convex body, a normed space, or a subspace or a quotient) can be fully described by a matrix, which in a probabilistic construction will be random. [This link is even more explicit when the objective is to find an operator.] Since we aim at producing explicit matrices that behave like random ones, one may say that this section is mostly about *pseudorandom matrices*.

4.1. Kashin decompositions and linear vs. quadratic programming. We begin by recalling the following spectacular result motivated by questions in approximation theory and usually referred to as *Kashin decomposition* (see [45, 96, 102, 84])

Theorem 4.1 (Kashin decomposition). *Given $m = 2n \in 2\mathbb{N}$, there exist two orthogonal m-dimensional subspaces $E_1, E_2 \subset \mathbb{R}^m$ such that*

$$\frac{1}{8}\|x\|_2 \le \frac{1}{\sqrt{m}}\|x\|_1 \le \|x\|_2 \quad \textit{for all} \quad x \in E_i,\ i = 1, 2. \tag{5}$$

In other words, the space ℓ_1^{2n} is an orthogonal (in the ℓ_2^{2n} sense) sum of two *nearly Euclidean* subspaces. The existence of such a decomposition was surprising because, as is easily seen, on the *entire* space $\mathbb{R}^m$, the ratio between the ℓ_1 and ℓ_2 norms varies between 1 and $\sqrt{m}$ (in fact, the Banach-Mazur distance between ℓ_1^m and ℓ_2^m equals $\sqrt{m}$). [See [84], p.95, for an exposition of the equally striking infinite-dimensional analogue due to Krivine and independently to Kashin.] A slightly different form of the theorem (the original one) asserts the existence of a matrix $V \in O(n)$ such that

$$\forall x \in \mathbb{R}^n \qquad \max\{\|x\|_1, \|Vx\|_1\} \ge c\sqrt{n}\|x\|_2 \ ;$$

the graphs of V and $-V$ yield then a desired decomposition of $\mathbb{R}^m$ (with $\frac{1}{8}$ in (5) replaced by $\frac{c}{2}$). In both formulations the standard arguments yield that, for large n, the assertion holds for nearly all decompositions $E_1 \oplus E_2$ or, resp., for nearly all $V \in O(n)$ (with respect to the corresponding Haar measure); see [7, 90, 55] and their references for an in-depth discussion of other random models. However, no explicit families of E_1, E_2 or V with $n \to \infty$ are known. This leads naturally to

Problem 4.2. Given $n \in \mathbb{N}$, exhibit an explicit Kashin decomposition of ℓ_1^{2n}.

A formally easier, and perhaps more to the point, as it corresponds to *constructive Dvoretzky theorem* for ℓ_1^m (cf. section 3.2), is the question (also stated as Problem 7 in [70]) about exhibiting explicit proportional nearly Euclidean subspaces of ℓ_1^m,

i.e., subspaces $E \subset \ell_1^m$ with $k := \dim E \geq cm$ and $d(E, \ell_2^k) \leq C$. The best to date result of this nature is due to Rudin [88] and yields merely $k = O(\sqrt{m})$. The construction in [88] was based on finite fields and difference sets (or the so called *finite geometries*), and the topic directly considered was that of exact Λ_p-sets for even integers $p \geq 4$. This leads to another question: finding explicit exact Λ_p-sets for other values of p; for definitions and probabilistic results see [17, 106, 18].

A very interesting result (whose relevance is not completely clear yet) in the direction of Problem 4.2 was obtained in [15], which – in our language – contains a constructive version of the quotient of a subspace Theorem 3.1 for the simplex. [See also [77], where this and many more related issues are discussed.]

Theorem 4.3. *Given $n \in \mathbb{N}$, there exists a set $S \subset \mathbb{R}^n$ which is an explicit affine image of an explicit section of the $5n$-dimensional simplex and which verifies*

$$B_2^n \subset S \subset CB_2^n$$

Moreover, C can be replaced by $1+\varepsilon$, for $\varepsilon \in (0,1)$, if we use a simplex of dimension $\geq C_1 n \log(2/\varepsilon)$.

One thus finds an explicit approximate of the n-dimensional Euclidean ball B_2^n "hidden" in the $5n$-dimensional simplex. The original motivation for Theorem 4.3 was approximating *quadratic programming* problems by *linear programming* problems while increasing the size of a problem only moderately. Here n is the size of the original quadratic problem related to the Euclidean ball, or to an ellipsoid. The dimension of the simplex corresponds to the size of the linear problem (its faces represent constraints), with the increase in size related to the number of auxiliary variables. Representing auxiliary variables in terms of the original variables corresponds to a section of the simplex, and the affine image, or projection, corresponds to verifying whether there is a point with certain coordinates pre-assigned which verifies the constraints. Finally, ε is the precision of the approximation. We emphasize the very weak dependence of the increase in dimension on ε; it is more standard in similar statements in geometric functional analysis to have in place of $\log(2/\varepsilon)$ a factor which is a power of ε (we again refer to the article [48] in this collection for a more detailed discussion of the almost isometric theory, where this particular issue more properly belongs). This is another indication of possible advantages of explicit objects over random ones.

It is not clear whether the approach of [15] can be developed to handle the symmetric case corresponding to a constructive Dvoretzky theorem for ℓ_1^m (closely related to Problem 4.2), or even to a constructive version of Theorem 3.1 for that space. In any case, it seems that the more directly relevant point of view is here the dual form of the Dvoretzky theorem, or of the Kashin decomposition: find an explicit projection, or an affine image, of the m-dimensional cube (the unit ball of ℓ_∞^m) which approximates a Euclidean ball of dimension $\approx cm$.

A vaguely similar topic in that it connects algorithmic issues (approximating, this time in the *isomorphic* sense, problems in combinatorial optimization by their *semi-definite relaxations*) with functional analytic phenomena (*Grothendieck-type inequalities* and the geometry of various high dimensional convex sets) has been

studied, among others, in [4, 67, 3, 47]; see the first three of these articles and [77], and their references, for the background. The same circle of ideas, related to inhomogeneity of high dimensional cubes and linked to some of the issues discussed in section 3, led to the solution – in the negative, for large dimensions – of the following (central case of the) well-known problem of Knaster stated in 1946 in the *New Scottish Book* and published in 1947 in [49]: *Given a continuous function on the sphere in* $\mathbb{R}^n$ *and a configuration of* n *points on that sphere, is there a rotation of the configuration on which the function is constant?* See [46] for details and for the background. We refer to [39] for improvements yielding (negative) solutions also for moderate dimensions (at this point the answer is unknown for n between 4 and about 60; the answer is affirmative for $n < 4$) and to [71] for a link between Knaster-like statements and precise versions of Dvoretzky theorem. [Some such statements may still be true, see [46].]

4.2. Decreasing randomness and expander graphs. A significant step in the direction of the problems stated or hinted in the preceding subsection was made in [10]. The approach of that paper uses the paradigm introduced earlier in combinatorics and computer science: if we don't know how to completely dispense with randomness in certain construction, let us at least reduce the number of random bits needed to implement the construction; see [2] for an early article in that direction, usually referred to as the *combinatorial derandomization*. As in [2], pseudorandomness is brought in by *pseudorandom expander graphs* based on Kazhdan property T for groups (see [62, 57]). Rather than flipping the coin $2n^2$ times to obtain a $n \times 2n$ matrix of ± 1's, which represents a linear map from $\mathbb{R}^{2n}$ to $\mathbb{R}^n$ whose kernel is typically an n-dimensional subspace of $\mathbb{R}^{2n}$, one identifies the 2^{2n} possible rows of such matrix (i.e., vectors of length $2n$ with ± 1 coordinates) with vertices of an appropriate explicit expander graph, and then decides which vertices/rows to use by performing a random walk on that graph. Obtaining n rows requires n (or $n-1$) steps, for which we need approximately $n \log_2 d$ random bits (where d is the degree of the graph), to which we need to add $2n$ bits for a random choice of the starting point. Specifics depend on a particular problem considered (the technical details are no longer primarily combinatorial, but field specific), for example to obtain a nearly Euclidean n-dimensional subspace of ℓ_1^{2n} (or a partially derandomized Dvoretzky theorem for that space), d can be chosen to be polynomial in n and so the cost in random bits is of order $n \log n$.

This is an extremely interesting and promising approach. In addition to Dvoretzky theorem for ℓ_1^n, the authors of [10] partially derandomize, among others, the quotient of a subspace Theorem 3.1. Full derandomization doesn't seem to be possible there since the initial space X is not concrete; alternatively, the hypothesis would need to include conditions on the presentation of X. This example, while pointing to the "more correct" questions that should be asked in certain contexts, also reveals the limitations of the approach. However, progress beyond those limitations may conceivably be possible if one uses the more sophisticated pseudorandom techniques from, say, [58, 89], the contributions whose full implications haven't been completely "digested" yet.

It is interesting to note that, in addition to the *classical* theoretical computer science, the same paradigm (from randomizing to partial derandomizing) and the same underlying techniques have been exploited in the *quantum information theory*, see [36, 6]; this circle of ideas also vaguely relates to random codes from subsection 4.4 below. Thus one may hope that the interaction of asymptotic geometric analysis and the quantum theory expands beyond the initial encounters such as [12, 100].

4.3. Reducibility of matrices and the property τ. An $n \times n$ matrix M is said to be reducible if, in some orthonormal basis, it can be written as a block matrix

$$M = \begin{bmatrix} M_1 & 0 \\ 0 & M_2 \end{bmatrix},$$

where M_1 and M_2 are square matrices of sizes which are (necessarily) between 1 and $n-1$. This is equivalent to M commuting with a nontrivial orthogonal projection. Based on an analysis of a large class of natural examples it was suggested around 1980 that, as n increases to ∞, the reducible matrices may become more and more dense in the space of all $n \times n$ matrices. A confirmation of this fact from "experimental mathematics" would have had interesting consequences in the theory of quasidiagonal operators, and (likely) some useful implications for numerical linear algebra. However, this hope was soon laid to rest by the following result [37]

Theorem 4.4. *There is a computable constant $c > 0$ such that for every $n \geq 2$ there is an $n \times n$ (real or complex) matrix of norm one which cannot be approximated within c by a reducible matrix.*

The argument given in [37] was non-constructive, the "poorly" reducible matrices being random (albeit of a somewhat special form), and the value of c obtained there was of order 10^{-7}. A construction yielding explicit pseudorandom matrices which are poorly approximable by reducible matrices was given recently in [16] (cf. [99, 109]). The construction in [16] is based on property τ from representation theory. [A preprint containing a simpler, but weaker, version using Kazhdan's property T was circulated among some specialists in 2002.] The construction depends on noting that a unitary representation $g \to \pi(g)$ on $\mathbb{C}^n$ is irreducible iff the adjoint representation $g \to Ad_\pi(g)$, defined by $Ad_\pi(g)(X) := \pi(g)X\pi(g)^*$, doesn't have non-trivial fixed points when restricted to (the invariant subspace of) trace zero $n \times n$ matrices . On the other hand, the property T (or τ) of a group G says, roughly, that every failure of a unitary representation ρ of G to have non-trivial fixed points can be witnessed in a uniform way on the finite set $S = \{\rho(g_1), \ldots, \rho(g_k)\}$, where $g_1, \ldots, g_k$ are generators of G (independent of ρ). Careful but elementary calculations involving various matrix ideal norms show then that irreducibility of ρ can be likewise (uniformly) witnessed on S, and the argument is concluded, as in [37], by producing an appropriate block matrix some of whose entries are elements of S. The key point in the argument is that k and the estimates quantifying irreducibility and lack of non-trivial fixed points are independent of the dimension of the representation (of course, to begin with, we

need to choose a group which – in addition to possessing property τ – has many finite dimensional representations; e.g., $SL_2(\mathbb{Z})$ fulfills this role well). Again, as a bonus, we get a constant c which is better than that in [37] by several orders of magnitude.

While this argument appears to be tightly connected to the Hilbert space structure and, accordingly, not immediately applicable to our more general setting of normed spaces, it is conceivable that (for example) by considering specific instances of the principle that is behind the construction, and by appealing in a deeper way to their structure, one may obtain pseudorandom matrices that are of relevance to some of the questions suggested elsewhere in this article. [The fact that Hilbert spaces are *the* setting for property T or τ is not disqualifying *per se*; in fact, constructions of, say, random bodies typically appeal to Euclidean structures of the underlying spaces by working, e.g., with Gaussian measures.]

4.4. Random linear codes and other topics. Other situations calling for pseudorandom models that have been mentioned in this article are Gluskin-type random Banach spaces [31, 32, 97, 98, 59], some of which are implicit in section 3.1, or the spaces exemplifying the saturation phenomenon from section 3.3. We point out that while the latter spaces depend on the initial, *a priori* arbitrary lower dimensional space W with which we saturate them, the dependence is very canonical. Indeed, what really counts is the arrangement of a finite family of lower dimensional subspaces in the larger space, just as Gluskin-type spaces exploited, in a sense, arrangements of finite sets of points. A construction that comes to mind here is [52], which, in particular, contains a successful derandomization of the example of a space with several extremal parameters, including the so called unconditional basis constant, given previously in [28] as an application of non-constructive Kashin decomposition (Theorem 4.1). However, the approach of [52] is based on spherical codes constructed via finite geometries and so its applicability seems somewhat limited, cf. our discussion of [88] in the paragraph following Theorem 4.1.

Another, quite different question is related to modeling free random variables in *free probability* (see [110, 112, 111, 38]) with independent random matrices of increasing size. Due to the apparent central role of the idea of *freeness* in the subject of random matrices it would be very interesting to have also sufficiently canonical pseudorandom models (we note that there exist here constructions based on Clifford matrices [110, 94] which are, however, not fully satisfactory).

We conclude by describing briefly one more development that occurred recently on the border of high-dimensional convexity and computer science and which concerns self-correcting linear codes. The context is roughly as follows. We want to transmit a signal which is a vector $x \in \mathbb{R}^n$. Since some coordinates may get corrupted in the transmission, we introduce some *redundancy* by transmitting instead the vector $y = Ax \in \mathbb{R}^N$, where A is an $N \times n$ matrix independent of x and N is larger, but *not much larger* than n. We then hope that if not too many of the coordinates of y get corrupted in the transmission, then we will be able to recover, in a robust way, the original signal x. In this context, some specific efficient strate-

gies (based on linear programming) for recovery of the original signal along this line were proposed by Donoho and his collaborators (see, e.g., [25] and references in [22]), and existence of very efficient codes, with redundancy close to the theoretical minimum (which depends, of course, on the reliability of the transmission channel) was shown in [23, 87, 22]. However, in a twist which is reminiscent of the classical random *Shannon codes* [93], in the most efficient encoding schemes the matrix A is not explicit! This is not the worst possible scenario since once an appropriate A (of given size) is found in the pre-processing stage, it subsequently can be repeatedly used to encode *all possible* signals $x \in \mathbb{R}^n$. However, in spite of some promising leads, fully satisfactory constructive and algorithmically efficient methods for producing large encoding matrices are still missing here.

We refer the reader to [21] for more background on the topic mentioned above and for other information/communication theory problems that have a similar flavor, and to [66] for a study of linear encoding for random models more general than that of [23, 87, 22] (but still employing the same setup involving vectors from $\mathbb{R}^n$ and $\mathbb{R}^N$).

References

[1] Ageev, S. M., Bogatyĭ, S. A., Repovsh, D., The Banach-Mazur compactum is an Aleksandrov compactification of a Q-manifold. (Russian) *Mat. Zametki* **76** (2004), no. 1, 3–10; English translation: *Math. Notes* **76** (2004), no. 1-2, 3–9.

[2] Ajtai, M., Komlós, J., Szemerédi, E., Deterministic simulation in logspace. In *Proc. 19th Annual ACM Symp. on Theory of Computing*, ACM Press 1987, 132–140.

[3] Alon, N., Makarychev, K., Makarychev, Y., Naor, A., Quadratic forms on graphs. *Invent. Math.* **163** (2006), no. 3, 499–522.

[4] Alon, N., Naor, A., Approximating the Cut-Norm via Grothendieck's Inequality. In *Proc. of the 36 ACM STOC*, ACM Press, Chicago 2004, 72–80; SIAM J. Computing, in press.

[5] Alon, N., Spencer, J. H., *The probabilistic method. With an appendix on the life and work of Paul Erdös.* 2nd edition. Wiley-Interscience Series in Discrete Mathematics and Optimization. Wiley-Interscience, New York, 2000.

[6] Ambainis, A., Smith, A., Small Pseudo-random Families of Matrices: Derandomizing Approximate Quantum Encryption. In *Approximation, Randomization, and Combinatorial Optimization: Algorithms and Techniques*, Lecture Notes in Comput. Sci. 3122, Springer, Berlin 2004, 249–260.

[7] Anderson, G. W., Integral Kašin splittings. *Israel J. Math.* **138** (2003), 139–156.

[8] Artstein, S., Milman, V. D., Szarek, S. J., Duality of Metric Entropy. *Ann. of Math.* (2) **159** (2004), no. 3, 1313–1328.

[9] Artstein, S., Milman, V. D., Szarek, S. J., Tomczak-Jaegermann, N., On convexified packing and entropy duality. *Geom. Funct. Anal.* **14** (2004), no. 5, 1134–1141.

[10] Artstein-Avidan, S., Milman, V. D., Logarithmic reduction of the level of randomness in some probabilistic constructions. *J. Funct. Anal.* **235**, no. 1 (2006), 297–329.

[11] Asplund, E., Comparison between plane symmetric convex bodies and parallelograms. *Math. Scand.* **8** (1960), 171–180.

[12] Aubrun, G., Szarek, S. J., Tensor products of convex sets and the volume of separable states on N qudits. *Phys. Rev. A.* **73**, 022109 (2006).

[13] Banaszczyk, W., Litvak, A. E., Pajor A., Szarek, S. J., The flatness theorem for nonsymmetric convex bodies via the local theory of Banach spaces. *Math. Oper. Res.* **24** (1999), no. 3, 728–750.

[14] Bárány, I., Random points, convex bodies, lattices. In *Proceedings of the International Congress of Mathematicians* (Beijing, 2002), Vol. III, Higher Ed. Press, Beijing, 2002, 527–535.

[15] Ben-Tal, A., Nemirovski, A., On polyhedral approximations of the second-order cone. *Math. Oper. Res.* **26** (2001), no. 2, 193–205.

[16] Benveniste, E. J., Szarek, S. J., Property T, property τ, and irreducibility of matrices, in preparation.

[17] Bourgain, J., Bounded orthogonal systems and the $\Lambda(p)$-set problem. *Acta Math.* **162** (1989), 227–245.

[18] Bourgain, J., Λ_p-sets in analysis: results, problems and related aspects. In [41], Vol. 1, 195–232.

[19] Bourgain, J., Pajor, A., Szarek, S. J., Tomczak-Jaegermann, N., On the duality problem for entropy numbers of operators. In *Geometric aspects of functional analysis (1987–88).* Lecture Notes in Math. 1376, Springer, Berlin-New York 1989, 50–63.

[20] Bourgain, J., Szarek, S.J., The Banach-Mazur distance to the cube and the Dvoretzky-Rogers factorization. *Israel J. Math.* **62** (1988), no. 2, 169–180.

[21] Candès, E. J., Compressive sampling, this collection.

[22] Candès, E., Rudelson, M., Vershynin, R., Tao, T., Error correction via Linear Programming. FOCS 2005 (46th Annual Symposium on Foundations of Computer Science), 295–308.

[23] Candès, E. J., Tao., T., Decoding by linear programming. Available on the arXiv preprint server: math.MG/0502327

[24] Diestel, J., Jarchow, H., Pietsch, A., Operator ideals. In [41], Vol. 1, 437–496; Addenda and corrigenda: Vol. 2, 1821.

[25] Donoho, D. L., Huo., X., Uncertainty principles and ideal atomic decomposition. *IEEE Transactions on Information Theory* **47** (2001), 2845–2862.

[26] Dudley, R. M., The sizes of compact subsets of Hilbert space and continuity of Gaussian processes. *J. Funct. Anal.* **1** (1967) 290–330.

[27] Dvoretzky, A., Some results on convex bodies and Banach spaces. In *Proc. Internat. Sympos. Linear Spaces (Jerusalem, 1960).* Jerusalem Academic Press, Jerusalem; Pergamon Oxford, 1961, 123–160.

[28] Figiel, T., Kwapień, S., Pełczyński, A., Sharp estimates for the constants of local unconditional structure of Minkowski spaces. *Bull. Acad. Polon. Sci.* (Sér. Sci. Math. Astronom. Phys.) **25** (1977), no. 12, 1221–1226.

[29] Giannopoulos, A. A., A note on the Banach-Mazur distance to the cube. In *Geometric aspects of functional analysis (Israel, 1992–1994)*, Oper. Theory Adv. Appl. 77, Birkhäuser, Basel, 1995, 67–73.

[30] Giannopoulos, A. A., Milman, V. D., Euclidean structure in finite dimensional normed spaces. In [41], Vol. 1, 707–779.

[31] Gluskin, E. D., The diameter of Minkowski compactum roughly equals to n. *Funct. Anal. Appl.* **15** (1981), 57–58 (English translation).

[32] Gluskin, E. D., Finite-dimensional analogues of spaces without a basis. (Russian) *Dokl. Akad. Nauk SSSR* **261** (1981), no. 5, 1046–1050.

[33] Gordon, Y., König, H., Schütt, C., Geometric and probabilistic estimates for entropy and approximation numbers of operators. *J. Approx. Theory* **49** (1987), no. 3, 219–239.

[34] Gordon, Y., Litvak, A.E., Meyer, M., Pajor, A., John's Decomposition in the General Case and Applications. *J. Differential Geom.* **68** (2004), no. 1, 99–119.

[35] Grötschel, M., Lovász, L., Schrijver, A., *Geometric algorithms and combinatorial optimization.* Algorithms and Combinatorics 2, Springer-Verlag, Berlin, 1993.

[36] Hayden, P., Leung, D., Shor, P. W., Winter, A., Randomizing quantum states: Constructions and applications. *Commun. Math. Phys.* **250** (2) 2004, 371-391.

[37] Herrero, D., Szarek, S. J., How well can an $n \times n$ matrix be approximated by reducible ones? *Duke Math. J.* **53** (1986), 233-248.

[38] Hiai, F., Petz, D., *The semicircle law, free random variables and entropy.* Mathematical Surveys and Monographs 77, American Mathematical Society, Providence, RI, 2000.

[39] Hinrichs, A., Richter, C., The Knaster problem: more counterexamples. *Israel J. Math.* **145** (2005), 311–324.

[40] John, F., Extremum problems with inequalities as subsidiary conditions. In *Studies and Essays Presented to R. Courant on his 60th Birthday, January 8, 1948.* 187–204. Interscience Publishers, Inc., New York, N. Y. 1948.

[41] *Handbook of the geometry of Banach spaces* (ed. by W. B. Johnson and J. Lindenstrauss). North-Holland, Amsterdam, Vol. 1, 2001 and Vol. 2, 2003.

[42] Johnson, W. B., Lindenstrauss, J., Basic concepts in the geometry of Banach spaces. In [41], Vol. 1, 1–84

[43] Johnson, W. B., Schechtman, G. Finite dimensional subspaces of L_p. In [41], Vol. 1, 837–870.

[44] Kadets , M. Ĭ., Snobar, M. G., Certain functionals on the Minkowski compactum. (Russian) *Mat. Zametki* **10** (1971), 453–457.

[45] Kashin, B. S., The widths of certain finite-dimensional sets and classes of smooth functions. (Russian) *Izv. Akad. Nauk SSSR* (Ser. Mat.) **41** (1977), no. 2, 334–351, 478.

[46] Kashin, B.S., Szarek, S.J., The Knaster problem and the geometry of high-dimensional cubes. *C. R. Math. Acad. Sci. Paris* **336** (2003), no. 11, 931–936.

[47] Kashin, B.S., Szarek, S.J., On the Gram Matrices of Systems of Uniformly Bounded Functions. *Proc. Steklov Inst. Math.* **243** (2003), 227–233 (English translation).

[48] Klartag, B., Isomorphic and almost-isometric problems in high dimensional convex geometry, this collection.

[49] Knaster, B., Problem 4. *Colloq. Math.* **30** (1947), 30–31.

[50] Koldobsky, A., König, H., Aspects of the isometric theory of Banach spaces. In [41], Vol. 1, 899–939.

[51] König, H., Milman, V. D., On the covering numbers of convex bodies. In *Geometric aspects of functional analysis (1985–86)*. Lecture Notes in Math., vol. 1267, Springer, Berlin-New York (1987) 82–95.

[52] König, H., Tomczak-Jaegermann, N., Bounds for projection constants and 1-summing norms. *Trans. Amer. Math. Soc.* **320** (1990), no. 2, 799–823.

[53] Kuelbs, J., W. V. Li, Metric entropy and the small ball problem for Gaussian measures. *J. Funct. Anal.* **116** (1993), no. 1, 133–157.

[54] Lassak, M., Approximation of convex bodies by centrally symmetric bodies. *Geom. Dedicata* **72** (1998), no. 1, 63–68.

[55] Litvak, A. E., Pajor, A., Rudelson, M., Tomczak-Jaegermann, N., Vershynin, R., Euclidean embeddings in spaces of finite volume ratio via random matrices. *J. Reine Angew. Math.* **589** (2005), 1–19.

[56] Ledoux, M., Zinn, J., Probabilistic limit theorems in the setting of Banach spaces. In [41], Vol. 2, 1177–1200.

[57] Lubotzky, A. *Discrete groups, expanding graphs and invariant measures. With an appendix by Jonathan D. Rogawski.* Progress in Mathematics 125, Birkhäuser Verlag, Basel, 1994.

[58] Lubotzky, A., Phillips, R., Sarnak, P., Ramanujan graphs. *Combinatorica* **8** (1988), no. 3, 261–277.

[59] Mankiewicz, P., Tomczak-Jaegermann, N., Quotients of finite-dimensional Banach spaces; random phenomena. In [41], Vol. 2, 1201–1246.

[60] Mankiewicz, P., Szarek, S. J., Random Banach Spaces. The limitations of the method. *Mathematica* **41** (1994), 239–250; Corrigenda: *Mathematica* **42** (1995), 220–221.

[61] Marcus, M. B., Pisier, G., Characterizations of almost surely continuous p-stable random Fourier series and strongly stationary processes. *Acta Math.* **152** (1984), no. 3-4, 245–301.

[62] Margulis, G. A., Explicit constructions of expanders. (Russian) *Problemy Peredači Informacii* **9** (1973), 71–80; *Problems Inform. Transmission* **9** (1973), 325–332 (English translation).

[63] Maurey, B., Banach spaces with few operators. In [41], Vol. 2, 1247–1297.

[64] Maurey, B., Type, cotype and K-convexity. In [41], Vol. 2, 1299–1332.

[65] Maurey, B., Pisier, G., Séries de variables aléatoires vectorielles indépendantes et propriétés géométriques des espaces de Banach. (French) *Studia Math.* **58** (1976), no. 1, 45–90.

[66] Mendelson, S., Pajor, A., Tomczak-Jaegermann, N., Reconstruction and subgaussian operators. Available on the arXiv preprint server: math.FA/0506239

[67] Megretski, A., Relaxation of Quadratic Programs in Operator Theory and System Analysis. In *Systems, Approximation, Singular Integral Operators, and Related Topics (Bordeaux, 2000)*, Birkhäuser, Basel 2001, 365–392.

[68] Milman, V. D., A new proof of the theorem of A. Dvoretzky on sections of convex bodies. *Funct. Anal. Appl.* **5** (1971), 28–37 (English translation).

[69] Milman, V. D., Almost Euclidean quotient spaces of subspaces of a finite-dimensional normed space. *Proc. Amer. Math. Soc.* **94** (1985), no. 3, 445–449.

[70] Milman, V. D., The concentration phenomenon and linear structure of finite-dimensional normed spaces. In *Proceedings of the International Congress of Mathematicians (Berkeley, Calif., 1986)*, Vol. 2, Amer. Math. Soc., Providence, RI, 1987, 961–975.

[71] Milman, V. D., A few observations on the connections between local theory and some other fields. In *Geometric aspects of functional analysis (1986/87)*, Lecture Notes in Math. 1317, Springer, Berlin 1988, 283–289.

[72] Milman, V. D., Surprising geometric phenomena in high-dimensional convexity theory. In *European Congress of Mathematics (Budapest, 1996)*, Vol. II. Progr. Math. 169, Birkhäuser, Basel 1998, 73–91.

[73] Milman, V. D., Randomness and pattern in convex geometric analysis. In *Proceedings of the International Congress of Mathematicians (Berlin, 1998)*, Vol. II. Doc. Math. 1998, Extra Vol. II, 665–677.

[74] Milman, V. D., Pajor, A., Entropy and asymptotic geometry of non-symmetric convex bodies. *Adv. Math.* **152** (2000), no. 2, 314–335.

[75] Milman, V. D., Schechtman, G. *Asymptotic theory of finite-dimensional normed spaces. With an appendix by M. Gromov.* Lecture Notes in Math. 1200, Springer-Verlag, Berlin 1986.

[76] Milman, V. D., Szarek, S. J., A geometric approach to duality of metric entropy. *C. R. Acad. Sci. Paris* (Sér. I Math.) **332** (2001), no. 2, 157–162.

[77] Nemirovski, A., Advances in Convex Optimization: Conic Programming, this collection.

[78] Pajor, A., Tomczak-Jaegermann, N., Volume ratio and other s-numbers of operators related to local properties of Banach spaces. *J. Func. Anal.* **87** (2) (1989), 273–293.

[79] Pietsch, A., *Theorie der Operatorenideale (Zusammenfassung)*, (German) Friedrich-Schiller-Universität, Jena 1972.

[80] Pisier, G., Un théorème sur les opérateurs linéaires entre espaces de Banach qui se factorisent par un espace de Hilbert. (French) *Ann. Sci. Ecole Norm. Sup.* (4) **13** (1980), no. 1, 23–43.

[81] Pisier, G., Remarques sur un résultat non publié de B. Maurey. (French) *Séminaire d'Analyse Fonctionnelle, 1980–1981*, Exp. No. V, 13 pp. École Polytechnique, Palaiseau 1981.

[82] Pisier, G., Holomorphic semigroups and the geometry of Banach spaces. *Ann. of Math.* (2) **115** (1982), no. 2, 375–392.

[83] Pisier, G., Finite rank projections on Banach spaces and a conjecture of Grothendieck. In *Proceedings of the International Congress of Mathematicians (Warsaw, 1983)*, Vol. 2., PWN, Warsaw 1984, 1027–1039.

[84] Pisier, G., *The Volume of Convex Bodies and Banach Space Geometry.* Cambridge Tracts in Mathematics 94, Cambridge University Press, Cambridge 1989.

[85] Pisier, G., A new approach to several results of V. Milman. *J. Reine Angew. Math.* **393** (1989), 115-131.

[86] Rudelson, M., Distances between non-symmetric convex bodies and the MM^*-estimate. *Positivity* **4** (2000), no. 2, 161–178.

[87] Rudelson, M., Vershynin, R., Geometric approach to error correcting codes and reconstruction of signals. *Internat. Math. Res. Notices* **2005**, no. 64, 4019–4041.

[88] Rudin, W., Trigonometric series with gaps. *J. Math. Mech.* **9** (1960), 203–227.

[89] Sarnak, P., *Some applications of modular forms.* Cambridge Tracts in Mathematics 99. Cambridge University Press, Cambridge 1990.

[90] Schechtman, G., Special orthogonal splittings of L_1^{2k}. *Israel J. Math.* **139** (2004), 337–347.

[91] Schütt, C., Entropy numbers of diagonal operators between symmetric Banach spaces. *J. Approx. Theory* **40** (1984), no. 2, 121–128.

[92] Schütt, C., Werner, E., Polytopes with vertices chosen randomly from the boundary of a convex body. In *Geometric aspects of functional analysis*, Lecture Notes in Math. 1807, Springer-Verlag, Berlin 2003, 241–422.

[93] Shannon, C. E., Weaver, W., *The Mathematical Theory of Communication.* The University of Illinois Press, Urbana, Ill., 1949.

[94] Shlyakhtenko, D., Limit distributions of matrices with bosonic and fermionic entries. In *Free probability theory (Waterloo, ON, 1995)*, Fields Inst. Commun. 12, Amer. Math. Soc., Providence, RI, 1997, 241–252.

[95] Sudakov, V. N., Gaussian random processes, and measures of solid angles in Hilbert space. (Russian) *Dokl. Akad. Nauk SSSR* **197** (1971), 43–45. English translation: *Soviet Math. Dokl.* 12 (1971), 412–415.

[96] Szarek, S. J., On Kashin's almost Euclidean orthogonal decomposition of ℓ_1^n. *Bull. Acad. Polon. Sci.* (Sér. Sci. Math. Astronom. Phys.) **26** (1978), no. 8, 691–694.

[97] Szarek, S. J., The finite-dimensional basis problem with an appendix on nets of Grassmann manifolds. *Acta Math.* **151** (1983), no. 3-4, 153–179.

[98] Szarek, S. J., Spaces with large distance to ℓ_∞^n and random matrices. *Amer. J. Math.* **112** (1990), no. 6, 899–942.

[99] Szarek, S. J., An exotic quasidiagonal operator. *J. Funct. Anal.* **89** (1990), 274–290.

[100] Szarek, S. J., The volume of separable states is super-doubly-exponentially small in the number of qubits. *Phys. Rev. A* **72**, 032304 (2005).

[101] Szarek, S. J., Talagrand, M., An "isomorphic" version of the Sauer-Shelah lemma and the Banach-Mazur distance to the cube. In *Geometric aspects of functional analysis (1987–88)*, Lecture Notes in Math. 1376, Springer, Berlin 1989, 105–112.

[102] Szarek, S. J., Tomczak-Jaegermann, N., On nearly Euclidean decomposition for some classes of Banach spaces. *Compositio Math.* **40** (1980), no. 3, 367–385.

[103] Szarek, S. J., Tomczak-Jaegermann, N., Saturating constructions for normed spaces. *Geom. Funct. Anal.* **14** (2004), no. 6, 1352–1375

[104] Szarek, S. J., Tomczak-Jaegermann, N., Saturating constructions for normed spaces II. *J. Funct. Anal.* **221** (2005), no. 2, 407–438.

[105] Szarek, S. J., Tomczak-Jaegermann, N., On the nontrivial projection problem, in preparation

[106] Talagrand, M., Sections of smooth convex bodies via majorizing measures. *Acta Math.* **175** (1995), 273–300.

[107] Tomczak-Jaegermann, N., Dualité des nombres d'entropie pour des opérateurs à valeurs dans un espace de Hilbert. (French) *C. R. Acad. Sci. Paris* (Sér. I Math.) **305** (1987), no. 7, 299–301.

[108] Tomczak-Jaegermann, N., *Banach-Mazur distances and finite-dimensional operator ideals.* Pitman Monographs and Surveys in Pure and Applied Mathematics 38, Longman, Harlow; Wiley, New York 1989.

[109] Voiculescu, D., Property T and approximations of operators. *Bull. London Math. Soc.* **22** (1990), 25–30.

[110] Voiculescu, D., Limit laws for random matrices and free products. *Invent. Math.* **104** (1991), 201–220.

[111] Voiculescu, D., Free probability theory: random matrices and von Neumann algebras. In *Proceedings of the International Congress of Mathematicians (Zürich, 1994)*, Vol. 1, Birkhäuser, Basel 1995, 227–241.

[112] Voiculescu, D., Dykema, K., Nica, A., *Free random variables. A noncommutative probability approach to free products with applications to random matrices, operator algebras and harmonic analysis on free groups.* CRM Monograph Series 1, American Mathematical Society, Providence, RI, 1992.

Case Western Reserve University, Department of Mathematics, Cleveland, Ohio 44106-7058, U.S.A. *and*
Université Pierre et Marie Curie-Paris6, UMR 7586-Institut de Mathématiques, Analyse Fonctionnelle, BC 186, 75252 Paris, France

E-mail: szarek@case.edu