LOCALLY DECODABLE CODES AND THE FAILURE OF COTYPE FOR PROJECTIVE TENSOR PRODUCTS

JOP BRIËT, ASSAF NAOR, AND ODED REGEV

Abstract. It is shown that for every $p \in (1, \infty)$ there exists a Banach space X of finite cotype such that the projective tensor product $\ell_p \widehat{\otimes} X$ fails to have finite cotype. More generally, if $p_1, p_2, p_3 \in (1, \infty)$ satisfy $\frac{1}{p_1} + \frac{1}{p_2} + \frac{1}{p_3} \leqslant 1$ then $\ell_{p_1} \widehat{\otimes} \ell_{p_2} \widehat{\otimes} \ell_{p_3}$ does not have finite cotype. This is proved via a connection to the theory of locally decodable codes.

1. introduction

Throughout this paper all Banach spaces are assumed to be over the reals, though our results apply (with the same proofs) to complex Banach spaces as well. We shall use standard Banach space notation and terminology, e.g., as in [1]. We shall also use the asymptotic notation $\lesssim, \gtrsim$ to indicate the corresponding inequalities up to universal constant factors, and we shall denote equivalence up to universal constant factors by $\asymp$, i.e., $A \asymp B$ is the same as $(A \lesssim B) \wedge (A \gtrsim B)$.

The *projective tensor product* of two Banach spaces $(X, \|\cdot\|_X)$ and $(Y, \|\cdot\|_Y)$, denoted $X \widehat{\otimes} Y$, is the completion of their algebraic tensor product $X \otimes Y$, equipped with the norm

$$\|z\|_{X\widehat{\otimes}Y} = \inf\left\{ \sum_{i=1}^n \|x_i\|_X \cdot \|y_i\|_Y : \exists\, n \in \mathbb{N}, \exists\{(x_i, y_i)\}_{i=1}^n \subseteq X \times Y, \right.$$
$$\left. \text{such that } z = \sum_{i=1}^n x_i \otimes y_i \right\}.$$

Thus, if X, Y are finite dimensional then the unit ball of $X \widehat{\otimes} Y$ is the convex hull in $X \otimes Y$ of all the vectors of the form $x \otimes y$, where x is a unit vector in X and y is a unit vector in Y. To state two concrete

J. B. was supported by an NWO Vici grant and the EU project QCS. A. N. was supported by NSF grant CCF-0832795, BSF grant 2010021, the Packard Foundation and the Simons Foundation. Part of this work was completed while A. N. was visiting Université Pierre et Marie Curie, Paris, France. O. R. was supported by a European Research Council (ERC) Starting Grant.

examples of this construction, one always has $\ell_1 \widehat{\otimes} X = \ell_1(X)$, and $\ell_2 \widehat{\otimes} \ell_2$ can be naturally identified with the Schatten trace class S_1, i.e., the space of all compact operators $T : \ell_2 \to \ell_2$, equipped with the norm $\|T\|_{S_1} = \mathrm{trace}(\sqrt{T^*T})$. For these facts, and much more information on projective tensor products, we refer to [15, 24, 12].

The literature contains a significant amount of work on the permanence of various key Banach space properties under projective tensor products; see the survey [11] for some of the known results along these lines. Here we will be mainly concerned with geometric properties of projective tensor products with $L_p(\mu)$ spaces, $p \in (1,\infty)$, in which case examples of known results include that $L_p \widehat{\otimes} X$ is weakly sequentially complete iff X is [18], $L_p \widehat{\otimes} X$ has the Radon-Nikodým property iff X does [9, 8], and $L_p \widehat{\otimes} X$ contains a copy of c_0 iff X does [10].

When one does not consider projective tensor products with $L_p(\mu)$ spaces, the above permanence properties are known to fail [21, 7]. Specifically, Bourgain and Pisier [7] showed that there exist a weakly sequentially complete Banach space X with the Radon-Nikodým property, such that $X \widehat{\otimes} X$ contains a copy of c_0 (thus $X \widehat{\otimes} X$ fails weak sequential completeness and the Radon-Nikodým property).

Here we will be concerned with the permanence of finite cotype under projective tensor products. For $q \in [2,\infty)$, a Banach space $(X, \|\cdot\|_X)$ is said to have cotype q if there exists $C \in (0,\infty)$ such that for every $n \in \mathbb{N}$ and every $x_1, \ldots, x_n \in X$ we have

$$\left(\sum_{i=1}^{n} \|x_i\|_X^q\right)^{1/q} \leqslant C \left(\mathbb{E}\left[\left\|\sum_{i=1}^{n} \varepsilon_i x_i\right\|_X^2\right]\right)^{1/2}, \tag{1}$$

where the expectation in (1) is taken with respect to uniformly distributed $\varepsilon = (\varepsilon_1, \ldots, \varepsilon_n) \in \{-1,1\}^n$. Thus L_p has cotype $\max\{p,2\}$ for for every $p \in [1,\infty)$ (see, e.g., [1]). The infimum over those $C \in (0,\infty)$ for which (1) holds true is denoted $C_q(X, \|\cdot\|_X)$, or, if the norm is clear from the context, simply $C_q(X)$. Given $k \in \mathbb{N}$ and a norm $\|\cdot\|$ on $\mathbb{R}^k$, it will also be convenient to denote $C^{(q)}_{\|\cdot\|} = C_q(\mathbb{R}^k, \|\cdot\|)$. If X has cotype q for some $q \in [2,\infty)$ then we say that X has finite cotype, or simply that X has cotype. The Maurey-Pisier theorem [19] implies that X fails to have finite cotype if and only if it is universal in the sense that there exists $K \in (0,\infty)$ such that *all* finite dimensional Banach spaces embed into X with distortion at most K (equivalently, ℓ_∞^n embeds into X with distortion at most K for all $n \in \mathbb{N}$). We are therefore interested in the permanence under projective tensor products of the failure of the above universality property.

Tomczak-Jaegermann proved [25] that $\ell_2\widehat{\otimes}\ell_2 = S_1$ has cotype 2, and Pisier proved [22, 23] that if $p,q\in[2,\infty)$ then $L_p\widehat{\otimes}L_q$ has cotype $\max\{p,q\}$ (see [22] for a more general result along these lines). Other than these facts and the easy fact that $L_1\widehat{\otimes}X = L_1(X)$ always inherits the cotype of X, we do not know of other permanence results for cotype under projective tensor products. In particular, it is open whether $L_p\widehat{\otimes}L_q$ has finite cotype when $p\in(1,2)$ and $q\in(1,2]$, and whether $\ell_2\widehat{\otimes}S_1 = \ell_2\widehat{\otimes}\ell_2\widehat{\otimes}\ell_2$ has finite cotype (these questions are stated in [23]).

A remarkable theorem of Pisier [21] asserts that there exist two Banach spaces X and Y of finite cotype such that $X\widehat{\otimes}Y$ does not have finite cotype. Specifically, by a famous theorem of Bourgain [5], L_1/H^1 has cotype 2 (H^1 is the closed span of $\{\theta\mapsto e^{2\pi in\theta}\}_{n=0}^{\infty}\subseteq L_1$), and Pisier constructs [21] a Banach space Z of cotype 2 such that $Z\widehat{\otimes}(L_1/H^1)$ contains a copy of c_0.

We have seen that projective tensor products with $L_p(\mu)$ spaces preserve a variety of geometric properties, but that similar results often fail for projective tensor products between general Banach spaces. In this vein, for $p\in(1,\infty)$ it was unknown whether $L_p\widehat{\otimes}X$ has finite cotype if X has finite cotype. This question was explicitly asked in [11, p. 59], and here we answer it negatively by showing that for every $p\in(1,\infty)$ there exists a Banach space X of finite cotype such that $\ell_p\widehat{\otimes}X$ fails to have finite cotype. Thus, $L_p\widehat{\otimes}X$ contains copies $\{\ell_\infty^n\}_{n=1}^{\infty}$ with distortion bounded by a constant independent of n; contrast this statement with the theorem of Bu and Dowling [10] quoted above that asserts that $L_p\widehat{\otimes}Y$ contains a copy of c_0 iff Y itself contains a copy of c_0. Note that when $p=2$ we see that even the projective tensor product with Hilbert space need not preserve finite cotype.

Our main result is the following theorem.

Theorem 1.1. *Fix $p_1,p_2,p_3\in(1,\infty)$ such that*

$$\frac{1}{p_1}+\frac{1}{p_2}+\frac{1}{p_3}\leqslant 1. \tag{2}$$

Then $\ell_{p_1}\widehat{\otimes}\ell_{p_2}\widehat{\otimes}\ell_{p_3}$ does not have finite cotype. Moreover, there exists a universal constant $c\in(0,\infty)$ such that for every $p_1,p_2,p_3\in(1,\infty)$ satisfying (2), every $q\in[2,\infty)$, and every integer $n>15$ we have

$$C_q\left(\ell_{p_1}^n\widehat{\otimes}\ell_{p_2}^n\widehat{\otimes}\ell_{p_3}^n\right)\gtrsim\frac{1}{\log n}\cdot\exp\left(\frac{c}{q}\cdot\frac{(\log\log n)^2}{\log\log\log n}\right). \tag{3}$$

It follows from Theorem 1.1 that for every $p\in(1,\infty)$, if we set $X=\ell_{2p/(p-1)}\widehat{\otimes}\ell_{2p/(p-1)}$ then $\ell_p\widehat{\otimes}X$ fails to have finite cotype. By the result of Pisier [22] quoted above, X has finite cotype. Another notable consequence of Theorem 1.1 is that there exists a Banach space Y such that $Y\widehat{\otimes}Y$ has finite cotype yet $Y\widehat{\otimes}Y\widehat{\otimes}Y$ fails to have finite cotype. We conjecture that (3) is not sharp, leaving open the determination of the asymptotic behavior of, say, $C_q\left(\ell_3^n\widehat{\otimes}\ell_3^n\widehat{\otimes}\ell_3^n\right)$.

Our proof of Theorem 1.1 is based on a connection between cotype of tensor products and results from theoretical computer science, namely the theory of locally decodable codes. This link allows us to use (as a "black box") delicate constructions that are available in the computer science literature in order to prove Theorem 1.1. Our initial hope was to use this connection in the reverse direction, namely, to use Banach space theory to address an important question about the length of locally decodable codes, but it turned out that instead locally decodable codes can be used to address the question in Banach space theory described above. Nevertheless, there is hope that the connection presented below, when combined with geometric insights about tensor norms, might lead to improved lower bounds for locally decodable codes. This hope will be made explicit in the following section.

1.1. **Locally decodable codes and cotype.** Definition 1.2 below is due to Katz and Trevisan [16]; see the surveys [26, 29] for more information on this notion (and the closely related notion of *private information retrieval*), as well as a description of some of its many applications in cryptography and computational complexity theory. We note that in the present paper no reference to Definition 1.2 will be made other than through the conclusion of Lemma 3.1 below.

Definition 1.2 (3-query locally decodable code)**.** *Fix $m,n\in\mathbb{N}$ and $\phi,\theta\in(0,1/2)$. A function*

$$C:\{-1,1\}^m\to\{-1,1\}^n$$

is called a 3-query locally decodable code of quality (ϕ,θ) if for every $t\in\{1,\ldots,m\}$ there exists a distribution $\mathcal{A}_t$ over 4-tuples (i,j,k,g), where $i,j,k\in\{1,\ldots,n\}$ and $g:\{-1,1\}^3\to\{-1,1\}$, with the property that for every $\varepsilon\in\{-1,1\}^m$ and every $\delta\in\{-1,1\}^n$ that differs from $C(\varepsilon)$ in at most $\phi\cdot n$ coordinates, with probability (with respect to the distribution $\mathcal{A}_t$) at least $\frac{1}{2}+\theta$ we have $g(\delta_i,\delta_j,\delta_k)=\varepsilon_t$.

The motivation behind Definition 1.2 is as follows. Just like standard error correcting codes, locally decodable codes provide a way to encode an m-bit message into a longer n-bit codeword in a way that allows one to recover the original message from the codeword, even if it is corrupted in any set of coordinates that isn't too large. However, while standard error correcting codes typically require reading essentially all the n bits of the corrupted codeword in order to recover even one bit of the message, a 3-query locally decodable code allows one to do this while reading only 3 bits.

It is an important open question to determine the asymptotic behavior in m of the smallest n for which 3-query locally decodable codes exist (for some fixed ϕ, θ, say, $\phi = \theta = 1/16$). The best known upper bound, due to Efremenko [13] using in part key ideas of Yekhanin [28] and a combinatorial construction of Grolmusz [14], is that for every $m \in \mathbb{N}$ there exists an integer $n \in \mathbb{N}$ satisfying

$$\log\log n \asymp \sqrt{\log m \log\log m}, \tag{4}$$

for which there exists a code $C : \{-1,1\}^m \to \{-1,1\}^n$ which is 3-query locally decodable of quality $\left(\phi, \frac{1}{2} - 6\phi\right)$ for all $\phi \in (0, 1/12)$. See [3] for an improvement of the implicit constant factor in (4).

The best known lower bound, due to Woodruff [27] as a logarithmic improvement over a lower bound of Kerenidis and de Wolf [17], is that for, say, $\phi = \theta = 1/16$ we necessarily have

$$n \gtrsim \frac{m^2}{\log m}. \tag{5}$$

In what follows, given $n \in \mathbb{N}$ we let $e_1, \ldots, e_n$ be the standard coordinate basis of $\mathbb{R}^n$. Let $\|\cdot\|$ be a norm on $\mathbb{R}^n \otimes \mathbb{R}^n \otimes \mathbb{R}^n$. For $K \in [1, \infty)$ say that $\|\cdot\|$ is *K-tensor-symmetric* if for every choice of permutations $\pi, \sigma, \tau \in S_n$, every choice of sign vectors $\varepsilon, \delta, \eta \in \{-1,1\}^n$, and every choice of scalars $\{a_{i,j,k}\}_{i=1}^n \subseteq \mathbb{R}$, we have

$$\left\| \sum_{i=1}^n \sum_{j=1}^n \sum_{k=1}^n \varepsilon_i \delta_j \eta_k a_{\pi(i),\sigma(j),\tau(k)} e_i \otimes e_j \otimes e_k \right\| \leqslant K \left\| \sum_{i=1}^n \sum_{j=1}^n \sum_{k=1}^n a_{i,j,k} e_i \otimes e_j \otimes e_k \right\|. \tag{6}$$

Theorem 1.3. *Fix $m, n \in \mathbb{N}$ and $\phi, \theta \in (0, 1/2)$. Suppose that there exists a 3-query locally decodable code $C : \{-1,1\}^m \to \{-1,1\}^n$ of quality (ϕ, θ). For every $K \in [1, \infty)$, if $\|\cdot\|$ is a K-tensor-symmetric norm on $\mathbb{R}^{3n} \otimes \mathbb{R}^{3n} \otimes \mathbb{R}^{3n}$ then for every $q \in [2, \infty)$ we have*

$$K^2 C^{(q)}_{\|\cdot\|} \cdot \frac{\left\| \sum_{i=1}^{3n} \sum_{j=1}^{3n} \sum_{k=1}^{3n} e_i \otimes e_j \otimes e_k \right\|}{\left\| \sum_{i=1}^{3n} e_i \otimes e_i \otimes e_i \right\|} \gtrsim \frac{\phi \theta^2 m^{1/q}}{\log(n+1)}.$$

Theorem 1.3 implies that if, say, $\phi = \theta = 1/16$ then there exists a universal constant $c \in (0,\infty)$ such that

$$n \geqslant \sup_{\|\cdot\|} \sup_{q\in[2,\infty)} \exp\left(\frac{cm^{1/q}\left\|\sum_{i=1}^{3n} e_i\otimes e_i\otimes e_i\right\|}{C_{\|\cdot\|}^{(q)}\left\|\sum_{i=1}^{3n}\sum_{j=1}^{3n}\sum_{k=1}^{3n} e_i\otimes e_j\otimes e_k\right\|}\right), \qquad (7)$$

where the first supremum in (7) is taken over all the 1-tensor-symmetric norms $\|\cdot\|$ on $\mathbb{R}^{3n}\otimes\mathbb{R}^{3n}\otimes\mathbb{R}^{3n}$. While our initial hope was to use (7) to narrow the large gap between (4) and (5), we do not know if there exists a norm on $\mathbb{R}^{3n}\otimes\mathbb{R}^{3n}\otimes\mathbb{R}^{3n}$ with respect to which (7) exhibits an asymptotic improvement over (5). This question is arguably the most important question that the present paper leaves open. However, Theorem 1.3 contains new information when one contrasts it with Efremenko's upper bound (4), thus yielding the following corollary.

Corollary 1.4. *There exists a universal constant $c\in(0,\infty)$ such that for every integer $n>15$, every $q\in[2,\infty)$ and every $K\in[1,\infty)$, any K-tensor-symmetric norm $\|\cdot\|$ on $\mathbb{R}^n\otimes\mathbb{R}^n\otimes\mathbb{R}^n$ satisfies*

$$C_{\|\cdot\|}^{(q)} \gtrsim \frac{\left\|\sum_{i=1}^{n} e_i\otimes e_i\otimes e_i\right\|}{\left\|\sum_{i=1}^{n}\sum_{j=1}^{n}\sum_{k=1}^{n} e_i\otimes e_j\otimes e_k\right\|}\cdot\frac{\exp\left(\frac{c}{q}\cdot\frac{(\log\log n)^2}{\log\log\log n}\right)}{K^2\log n}.$$

Suppose that $p_1,p_2,p_3\in(1,\infty)$ satisfy (2) and define $r\in[1,\infty)$ by

$$\frac{1}{r} \stackrel{\mathrm{def}}{=} \frac{1}{p_1}+\frac{1}{p_2}+\frac{1}{p_3}.$$

Denoting $e=\sum_{i=1}^n e_i\in\mathbb{R}^n$, we have

$$\begin{aligned}\left\|\sum_{i=1}^{n}\sum_{j=1}^{n}\sum_{k=1}^{n} e_i\otimes e_j\otimes e_k\right\|_{\ell_{p_1}^n\widehat{\otimes}\ell_{p_2}^n\widehat{\otimes}\ell_{p_3}^n} &= \|e\otimes e\otimes e\|_{\ell_{p_1}^n\widehat{\otimes}\ell_{p_2}^n\widehat{\otimes}\ell_{p_3}^n}\\ &= \|e\|_{\ell_{p_1}^n}\cdot\|e\|_{\ell_{p_2}^n}\cdot\|e\|_{\ell_{p_3}^n} = n^{1/p_1}\cdot n^{1/p_2}\cdot n^{1/p_3} = n^{1/r}. \qquad (8)\end{aligned}$$

It is also well known (see, e.g., Theorem 1.3 in [2]) that

$$\left\|\sum_{i=1}^{n} e_i\otimes e_i\otimes e_i\right\|_{\ell_{p_1}^n\widehat{\otimes}\ell_{p_2}^n\widehat{\otimes}\ell_{p_3}^n} = n^{1/r}. \qquad (9)$$

Since $\ell_{p_1}^n\widehat{\otimes}\ell_{p_2}^n\widehat{\otimes}\ell_{p_3}^n$ is 1-tensor-symmetric, it follows from (8) and (9) that Theorem 1.1 is a consequence of Corollary 1.4.

Acknowledgements. We are very grateful to Gilles Pisier for his encouragement and many insightful suggestions.

2. Preliminaries

In this section we briefly recall some standard notation and results on vector-valued Fourier analysis.

For $n \in \mathbb{N}$, the Walsh functions $\{W_A : \{-1,1\}^n \to \{-1,1\}\}_{A \subseteq \{1,\ldots,n\}}$ are given by $W_A(\varepsilon) = \prod_{i \in A} \varepsilon_i$. If $(X, \|\cdot\|_X)$ is a Banach space then for every $f : \{-1,1\}^n \to X$ and $A \subseteq \{1,\ldots,n\}$ we write

$$\widehat{f}(A) = \mathbb{E}\left[W_A(\varepsilon) f(\varepsilon)\right], \tag{10}$$

where the expectation in (10) is with respect to $\varepsilon \in \{-1,1\}^n$ chosen uniformly at random. Then,

$$\forall\, \varepsilon \in \{-1,1\}^n, \quad f(\varepsilon) = \sum_{A \subseteq \{1,\ldots,n\}} W_A(\varepsilon) \widehat{f}(A).$$

The *Rademacher projection* of f, denoted $\mathbf{Rad}(f) : \{-1,1\}^n \to X$, is defined by

$$\forall\, \varepsilon \in \{-1,1\}^n, \quad \mathbf{Rad}(f)(\varepsilon) = \sum_{i=1}^{n} \varepsilon_i \widehat{f}(\{i\}).$$

Pisier's famous bound on the K-convexity constant [20] asserts that if X is finite dimensional then every $f : \{-1,1\}^n \to X$ satisfies

$$\sqrt{\mathbb{E}\left[\|\mathbf{Rad}(f)(\varepsilon)\|_X^2\right]} \lesssim \log\left(\dim(X) + 1\right) \cdot \sqrt{\mathbb{E}\left[\|f(\varepsilon)\|_X^2\right]}. \tag{11}$$

Recall that the implied constant in (11) is universal, and thus it does not depend on n, f, $(X, \|\cdot\|_X)$ or $\dim(X)$. Bourgain proved [6] that the logarithmic dependence on $\dim(X)$ in (11) cannot be improved in general.

3. Relating locally decodable codes to cotype

Locally decodable codes will be used in what follows via the following lemma which is a slight variant of a result that appears in Appendix B of [4] (the proof in [4] is itself a variant of an argument in [17]).

Lemma 3.1 ([4])**.** *Fix $m, n \in \mathbb{N}$ and $\phi, \theta \in (0, 1/2)$. Suppose that $C : \{-1,1\}^m \to \{-1,1\}^n$ is a 3-query locally decodable code of quality (ϕ, θ). Then there exists a function $C' : \{-1,1\}^m \to \{-1,1\}^{3n}$ with the following properties. For every $i \in \{1,\ldots,m\}$ there exist three permutations $\pi_i, \sigma_i, \tau_i \in S_{3n}$, and for every $j \in \{1,\ldots,\lceil \phi\theta n/9 \rceil\}$ there exists a sign $\delta_i^j \in \{-1,1\}$, such that if $\varepsilon \in \{-1,1\}^m$ is chosen uniformly at random then with probability at least $\frac{1}{2} + \frac{\theta}{16}$ we have*

$$C'(\varepsilon)_{\pi_i(j)} C'(\varepsilon)_{\sigma_i(j)} C'(\varepsilon)_{\tau_i(j)} = \delta_i^j \varepsilon_i. \tag{12}$$

Proof. By Appendix B of [4], for every $i \in \{1,\dots,m\}$ there exists a family of nonempty disjoint subsets $\mathcal{F}_i$ of $\{1,\dots,n\}$ such that

- $|\mathcal{F}_i| \geqslant \frac{\phi\theta n}{9}$,
- each $S \in \mathcal{F}_i$ satisfies $|S| \leqslant 3$,
- for each $S \in \mathcal{F}_i$ there exists a sign $\delta_i(S) \in \{-1,1\}$ such that if $\varepsilon \in \{-1,1\}^m$ is chosen uniformly at random then

$$\mathrm{Prob}\left[\prod_{s\in S} C(\varepsilon)_s = \delta_i(S)\varepsilon_i\right] \geqslant \frac{1}{2} + \frac{\theta}{16}. \tag{13}$$

Define $C' : \{-1,1\}^m \to \{-1,1\}^{3n}$ by setting the first n coordinates of $C'(x)$ to be equal to $C(x)$, and defining the remaining $2n$ coordinates of $C'(x)$ to be equal to 1. One can then add $3-|S|$ elements from $\{n+1,\dots,3n\}$ to each set $S \in \mathcal{F}_i$ so that $\mathcal{F}_i$ becomes a family of disjoint subsets of $\{1,\dots,3n\}$ of size equal to 3, while not changing the validity of (13) with C replaced by C'. Write $\mathcal{F}_i = \{\{\pi_i(j),\sigma_i(j),\tau_i(j)\}\}_{j=1}^{|\mathcal{F}_i|}$ for some $\pi_i,\sigma_i,\tau_i \in S_{3n}$. Letting $\delta_i^j = \delta_i(\{\pi_i(j),\sigma_i(j),\tau_i(j)\})$, the validity of (12) with probability at least $\frac12 + \frac{\theta}{16}$ is the same as (13). □

Remark 3.1. An inspection of the proof of Efremenko's result [13] reveals that it directly gives a function C' as in Lemma 3.1. Therefore, strictly speaking, Lemma 3.1 is only required for statements like Theorem 1.3 that involve arbitrary locally decodable codes, and not for statements like Theorem 1.1 and Corollary 1.4 that use Efremenko's construction. We also note that the function C' given by Efremenko's construction has properties that are slightly stronger than those guaranteed by Lemma 3.1: it satisfies (12) for every $\varepsilon \in \{-1,1\}^m$, and moreover one can take $\delta_i^j = 1$ for all i,j. It is easy to see, however, that the latter property can be ensured in general, with only a slight loss in constants (say by replacing $3n$ with $6n$).

Fix $n \in \mathbb{N}$ and let $\|\cdot\|$ be a seminorm on $(\mathbb{R}^n)^{\otimes 3} \stackrel{\mathrm{def}}{=} \mathbb{R}^n \otimes \mathbb{R}^n \otimes \mathbb{R}^n$. Write

$$\mathcal{O}_{\|\cdot\|} \stackrel{\mathrm{def}}{=} \max_{\varepsilon\in\{-1,1\}^n} \|\varepsilon\otimes\varepsilon\otimes\varepsilon\|. \tag{14}$$

For $\alpha,\beta \in (0,1)$ consider the subset $S(\alpha,\beta) \subseteq (\mathbb{R}^n)^{\otimes 3}$ defined by

$$S(\alpha,\beta) \stackrel{\mathrm{def}}{=} \bigcup_{\pi,\sigma,\tau\in S_n} \bigcap_{j=1}^{\lceil \beta n\rceil} \left\{x \in (\mathbb{R}^n)^{\otimes 3} :\ \left|\left\langle e_{\pi(j)}\otimes e_{\sigma(j)}\otimes e_{\tau(j)}, x\right\rangle\right| \geqslant \alpha\right\}, \tag{15}$$

and write

$$\mathcal{S}_{\|\cdot\|}(\alpha,\beta) \stackrel{\mathrm{def}}{=} \min_{x\in S(\alpha,\beta)} \|x\|. \tag{16}$$

Theorem 3.2. *Fix $m,n\in\mathbb{N}$ and $\phi,\theta\in(0,1/2)$. Suppose that there exists a 3-query locally decodable code $C:\{-1,1\}^m\to\{-1,1\}^n$ of quality (ϕ,θ). Then for every seminorm $\|\cdot\|$ on $\mathbb{R}^{3n}\otimes\mathbb{R}^{3n}\otimes\mathbb{R}^{3n}$ and every $q\in[2,\infty)$ we have*

$$\frac{m^{1/q}}{\log(n+1)} \lesssim \frac{C^{(q)}_{\|\cdot\|}\cdot\mathcal{O}_{\|\cdot\|}}{\mathcal{S}_{\|\cdot\|}(\theta/8,\phi\theta/27)}. \tag{17}$$

Proof. Let $C':\{-1,1\}^m\to\{-1,1\}^{3n}$ be the function from Lemma 3.1. Define $f:\{-1,1\}^m\to\mathbb{R}^{3n}\otimes\mathbb{R}^{3n}\otimes\mathbb{R}^{3n}$ by

$$f(\varepsilon)=C'(\varepsilon)\otimes C'(\varepsilon)\otimes C'(\varepsilon).$$

Recalling the definition (14), we have $\|f(\varepsilon)\|\leqslant\mathcal{O}_{\|\cdot\|}$ for all $\varepsilon\in\{-1,1\}^m$. Combined with Pisier's bound on the K-convexity constant (11), we therefore have

$$\begin{aligned}\log\left((3n)^3+1\right)\cdot\mathcal{O}_{\|\cdot\|} &\gtrsim \left(\mathbb{E}\left\|\sum_{i=1}^m \varepsilon_i\widehat{f}(\{i\})\right\|^2\right)^{1/2}\\ &\geqslant \frac{1}{C^{(q)}_{\|\cdot\|}}\left(\sum_{i=1}^m\left\|\widehat{f}(\{i\})\right\|^q\right)^{1/q},\end{aligned} \tag{18}$$

where in the last step of (18) we used the definition of the cotype q constant $C^{(q)}_{\|\cdot\|}$.

Using the notation of Lemma 3.1, fix $i\in\{1,\ldots,m\}$ and for every $j\in\{1,\ldots,\lceil\phi\theta n/9\rceil\}$ write

$$P_i^j \stackrel{\mathrm{def}}{=} \mathrm{Prob}\left[\left\langle e_{\pi_i(j)}\otimes e_{\sigma_i(j)}\otimes e_{\tau_i(j)}, f(\varepsilon)\right\rangle=\delta_i^j\varepsilon_i\right], \tag{19}$$

where the probability in (19) is over $\varepsilon\in\{-1,1\}^m$ chosen uniformly at random. Recalling the definition of f, it follows from (12) that

$$\forall (i,j)\in\{1,\ldots,m\}\times\{1,\ldots,\lceil\phi\theta n/9\rceil\},\quad P_i^j\geqslant\frac12+\frac{\theta}{16}. \tag{20}$$

Now, for every $(i,j)\in\{1,\ldots,m\}\times\{1,\ldots,\lceil\phi\theta n/9\rceil\}$ we have

$$\begin{aligned}\delta_i^j&\left\langle e_{\pi_i(j)}\otimes e_{\sigma_i(j)}\otimes e_{\tau_i(j)},\widehat{f}(\{i\})\right\rangle\\ &= \left\langle \delta_i^j e_{\pi_i(j)}\otimes e_{\sigma_i(j)}\otimes e_{\tau_i(j)},\mathbb{E}\left[\varepsilon_i f(\varepsilon)\right]\right\rangle\\ &= \mathbb{E}\left[\delta_i^j\varepsilon_i\left\langle e_{\pi_i(j)}\otimes e_{\sigma_i(j)}\otimes e_{\tau_i(j)},f(\varepsilon)\right\rangle\right]\\ &\stackrel{(19)}{=} P_i^j-\left(1-P_i^j\right)\stackrel{(20)}{\geqslant}\frac{\theta}{8}.\end{aligned}\tag{21}$$

Recalling (15), it follows from (21) that $\widehat{f}(\{i\})\in S(\theta/8,\phi\theta/27)$ for all $i\in\{1,\ldots,m\}$. The definition (16) therefore implies that

$$\min_{i\in\{1,\ldots,m\}}\left\|\widehat{f}(\{i\})\right\|\geqslant \mathcal{S}_{\|\cdot\|}(\theta/8,\phi\theta/27),$$

which gives the desired estimate (17) due to (18). □

By substituting (4) into Theorem 3.2 we deduce that any seminorm on $\mathbb{R}^n\otimes\mathbb{R}^n\otimes\mathbb{R}^n$ must obey the following nontrivial restriction.

Corollary 3.3. *There exist universal constants $\alpha,\beta,c\in(0,1)$ such that for every integer $n>15$, if $\|\cdot\|$ is a seminorm on $\mathbb{R}^n\otimes\mathbb{R}^n\otimes\mathbb{R}^n$ and $q\in[2,\infty)$ then*

$$\frac{C_{\|\cdot\|}^{(q)}\cdot\mathcal{O}_{\|\cdot\|}}{\mathcal{S}_{\|\cdot\|}(\alpha,\beta)}\gtrsim\frac{1}{\log n}\cdot\exp\left(\frac{c}{q}\cdot\frac{(\log\log n)^2}{\log\log\log n}\right),\tag{22}$$

Proof. By Efremenko's bound (4) combined with Theorem 3.2, there exist universal constants $\alpha_1,\beta_1,c_1\in(0,1)$ and a sequence of integers $\{n_m\}_{m=3}^\infty\subseteq\mathbb{N}$ satisfying

$$\log\log n_m\asymp\sqrt{\log m\log\log m},\tag{23}$$

such that for every integer $m\geqslant 3$ and $q\in[2,\infty)$, if $|\cdot|$ is a seminorm on $\mathbb{R}^{3n_m}\otimes\mathbb{R}^{3n_m}\otimes\mathbb{R}^{3n_m}$ then

$$\frac{C_{|\cdot|}^{(q)}\cdot\mathcal{O}_{|\cdot|}}{\mathcal{S}_{|\cdot|}(\alpha_1,\beta_1)}\gtrsim\frac{m^{1/q}}{\log n_m}\stackrel{(23)}{\gtrsim}\frac{1}{\log n_m}\cdot\exp\left(\frac{c_1}{q}\cdot\frac{(\log\log n_m)^2}{\log\log\log n_m}\right).\tag{24}$$

Due to (23), there is $N_0\in\mathbb{N}$ such that if $n\geqslant N_0$ then there exists an integer $m\geqslant 3$ for which

$$3\left(1-\frac{\beta_1}{7}\right)n_m\leqslant n\leqslant 3n_m.\tag{25}$$

Observe that by adjusting the constant c, the desired asymptotic inequality (22) holds true if $n\in(15,N_0)$. We may therefore assume that

$n \geqslant N_0$, in which case we apply (24) to the trivial extension of $\|\cdot\|$ to a seminorm $|\cdot|$ on $\mathbb{R}^{3n_m} \otimes \mathbb{R}^{3n_m} \otimes \mathbb{R}^{3n_m}$, i.e., for every $\{a_{i,j,k}\}_{i,j,k=1}^{3n_m}$ set

$$\left|\sum_{i=1}^{3n_m}\sum_{j=1}^{3n_m}\sum_{k=1}^{3n_m} a_{i,j,k} e_i \otimes e_j \otimes e_k\right| \stackrel{\mathrm{def}}{=} \left\|\sum_{i=1}^{n}\sum_{j=1}^{n}\sum_{k=1}^{n} a_{i,j,k} e_i \otimes e_j \otimes e_k\right\|.$$

Then $C_{|\cdot|}^{(q)} = C_{\|\cdot\|}^{(q)}$ and $\mathcal{O}_{|\cdot|} = \mathcal{O}_{\|\cdot\|}$, and due to (25) we also have $\mathcal{S}_{|\cdot|}(\alpha_1, \beta_1) \geqslant \mathcal{S}_{\|\cdot\|}(\alpha_1, \beta_1/2)$. The desired estimate (22) is therefore a consequence of (24). $\square$

Due to the following simple lemma, Theorem 1.3 and Corollary 1.4 follow from Theorem 3.2 and Corollary 3.3, respectively.

Lemma 3.4. *Fix $n \in \mathbb{N}$ and $\alpha, \beta \in (0,1)$. For $K \in [1,\infty)$, if $\|\cdot\|$ is a K-tensor-symmetric norm on $\mathbb{R}^n \otimes \mathbb{R}^n \otimes \mathbb{R}^n$ then*

$$\mathcal{O}_{\|\cdot\|} \leqslant K \left\|\sum_{i=1}^{n}\sum_{j=1}^{n}\sum_{k=1}^{n} e_i \otimes e_j \otimes e_k\right\|. \tag{26}$$

and

$$\mathcal{S}_{\|\cdot\|}(\alpha, \beta) \geqslant \frac{\alpha\beta}{K}\left\|\sum_{i=1}^{n} e_i \otimes e_i \otimes e_i\right\|. \tag{27}$$

Proof. (26) is an immediate consequence of the definitions (6) and (14). Next, fix $x \in S(\alpha, \beta)$. Writing $x = \sum_{i=1}^n \sum_{j=1}^n \sum_{k=1}^n a_{i,j,k} e_i \otimes e_j \otimes e_k$ for some $\{a_{i,j,k}\}_{i,j,k=1}^n \subseteq \mathbb{R}$, and recalling (15), there exist $\pi, \sigma, \tau \in S_n$ such that

$$\forall\, i \in \{1, \ldots, \lceil \beta n \rceil\}, \quad \left|a_{\pi(i),\sigma(i),\tau(i)}\right| \geqslant \alpha. \tag{28}$$

For $\varepsilon, \delta, \eta \in \{-1,1\}^n$ and $\rho \in S_n$ define

$$x_{\varepsilon,\delta,\eta}^{\rho} \stackrel{\mathrm{def}}{=} \sum_{i=1}^{n}\sum_{j=1}^{n}\sum_{k=1}^{n} \varepsilon_i \delta_j s_k(\varepsilon, \delta, \eta, \rho) a_{\pi\circ\rho(i),\sigma\circ\rho(j),\tau\circ\rho(k)} e_i \otimes e_j \otimes e_k, \tag{29}$$

where

$$s_k(\varepsilon, \delta, \eta, \rho) \stackrel{\mathrm{def}}{=} \begin{cases} \eta_k & \text{if } \rho(k) > \lceil \beta n \rceil, \\ \varepsilon_k \delta_k \mathrm{sign}(a_{\pi\circ\rho(k),\sigma\circ\rho(k),\tau\circ\rho(k)}) & \text{otherwise.} \end{cases}$$

Thus, if $(\varepsilon, \delta, \eta, \rho) \in \{-1,1\}^n \times \{-1,1\}^n \times \{-1,1\}^n \times S_n$ is chosen uniformly at random then

$$\mathbb{E}\left[x_{\varepsilon,\delta,\eta}^{\rho}\right] = \frac{\sum_{i=1}^{\lceil \beta n \rceil} \left|a_{\pi(i),\sigma(i),\tau(i)}\right|}{n} \sum_{j=1}^{n} e_j \otimes e_j \otimes e_j. \tag{30}$$

Consequently,

$$\alpha\beta\left\|\sum_{j=1}^{n} e_j\otimes e_j\otimes e_j\right\| \overset{(28)\wedge(30)}{\leqslant} \left\|\mathbb{E}\left[x^{\rho}_{\varepsilon,\delta,\eta}\right]\right\| \leqslant \mathbb{E}\left[\left\|x^{\rho}_{\varepsilon,\delta,\eta}\right\|\right] \overset{(6)\wedge(29)}{\leqslant} K\|x\|. \quad (31)$$

Recalling (16), the validity of (31) for all $x\in S(\alpha,\beta)$ implies (27). □

References

[1] F. Albiac and N. J. Kalton. *Topics in Banach space theory*, volume 233 of *Graduate Texts in Mathematics*. Springer, New York, 2006.

[2] A. Arias and J. D. Farmer. On the structure of tensor products of l_p-spaces. *Pacific J. Math.*, 175(1):13–37, 1996.

[3] A. Beimel, Y. Ishai, E. Kushilevitz, and I. Orlov. Share conversion and private information retrieval. In *Proc. 27th IEEE Conf. on Computational Complexity (CCC'12)*, pages 258–268, 2012.

[4] A. Ben-Aroya, O. Regev, and R. de Wolf. A hypercontractive inequality for matrix-valued functions with applications to quantum computing and LDCs. In *49th Annual IEEE Symposium on Foundations of Computer Science*, pages 477–486, 2008. Available at `http://arxiv.org/abs/0705.3806`.

[5] J. Bourgain. New Banach space properties of the disc algebra and H^∞. *Acta Math.*, 152(1-2):1–48, 1984.

[6] J. Bourgain. On martingales transforms in finite-dimensional lattices with an appendix on the K-convexity constant. *Math. Nachr.*, 119:41–53, 1984.

[7] J. Bourgain and G. Pisier. A construction of $\mathcal{L}_\infty$-spaces and related Banach spaces. *Bol. Soc. Brasil. Mat.*, 14(2):109–123, 1983.

[8] Q. Bu. Observations about the projective tensor product of Banach spaces. II. $L^p(0,1)\widehat{\otimes}X,\ 1<p<\infty$. *Quaest. Math.*, 25(2):209–227, 2002.

[9] Q. Bu and J. Diestel. Observations about the projective tensor product of Banach spaces. I. $l^p\widehat{\otimes}X,\ 1<p<\infty$. *Quaest. Math.*, 24(4):519–533, 2001.

[10] Q. Bu and P. N. Dowling. Observations about the projective tensor product of Banach spaces. III. $L^p[0,1]\widehat{\otimes}X,\ 1<p<\infty$. *Quaest. Math.*, 25(3):303–310, 2002.

[11] J. Diestel, J. Fourie, and J. Swart. The projective tensor product. I. In *Trends in Banach spaces and operator theory (Memphis, TN, 2001)*, volume 321 of *Contemp. Math.*, pages 37–65. Amer. Math. Soc., Providence, RI, 2003.

[12] J. Diestel, J. H. Fourie, and J. Swart. *The metric theory of tensor products*. American Mathematical Society, Providence, RI, 2008. Grothendieck's résumé revisited.

[13] K. Efremenko. 3-query locally decodable codes of subexponential length. In *STOC'09—Proceedings of the 2009 ACM International Symposium on Theory of Computing*, pages 39–44. ACM, New York, 2009.

[14] V. Grolmusz. Superpolynomial size set-systems with restricted intersections mod 6 and explicit Ramsey graphs. *Combinatorica*, 20(1):71–85, 2000.

[15] A. Grothendieck. Résumé de la théorie métrique des produits tensoriels topologiques. *Bol. Soc. Mat. São Paulo*, 8:1–79, 1953.

[16] J. Katz and L. Trevisan. On the efficiency of local decoding procedures for error-correcting codes. In *Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing*, pages 80–86 (electronic), New York, 2000. ACM.

[17] I. Kerenidis and R. de Wolf. Exponential lower bound for 2-query locally decodable codes via a quantum argument. *J. Comput. System Sci.*, 69(3):395–420, 2004.

[18] D. R. Lewis. Duals of tensor products. In *Banach spaces of analytic functions (Proc. Pelczynski Conf., Kent State Univ., Kent, Ohio, 1976)*, pages 57–66. Lecture Notes in Math., Vol. 604. Springer, Berlin, 1977.

[19] B. Maurey and G. Pisier. Séries de variables aléatoires vectorielles indépendantes et propriétés géométriques des espaces de Banach. *Studia Math.*, 58(1):45–90, 1976.

[20] G. Pisier. Un théorème sur les opérateurs linéaires entre espaces de Banach qui se factorisent par un espace de Hilbert. *Ann. Sci. École Norm. Sup. (4)*, 13(1):23–43, 1980.

[21] G. Pisier. Counterexamples to a conjecture of Grothendieck. *Acta Math.*, 151(3-4):181–208, 1983.

[22] G. Pisier. Factorization of operator valued analytic functions. *Adv. Math.*, 93(1):61–125, 1992.

[23] G. Pisier. Random series of trace class operators. In *Proceedings Cuarto CLAPEM Mexico 1990. Contribuciones en probabilidad y estadistica matematica*, pages 29–42, 1992. Available at `http://arxiv.org/abs/1103.2090`.

[24] R. A. Ryan. *Introduction to tensor products of Banach spaces*. Springer Monographs in Mathematics. Springer-Verlag London Ltd., London, 2002.

[25] N. Tomczak-Jaegermann. The moduli of smoothness and convexity and the Rademacher averages of trace classes $S_p(1 \leqslant p < \infty)$. *Studia Math.*, 50:163–182, 1974.

[26] L. Trevisan. Some applications of coding theory in computational complexity. In *Complexity of computations and proofs*, volume 13 of *Quad. Mat.*, pages 347–424. Dept. Math., Seconda Univ. Napoli, Caserta, 2004.

[27] D. P. Woodruff. New lower bounds for general locally decodable codes. *Electronic Colloquium on Computational Complexity (ECCC)*, 14(006), 2007.

[28] S. Yekhanin. Towards 3-query locally decodable codes of subexponential length. *J. ACM*, 55(1):Art. 1, 16, 2008.

[29] S. Yekhanin. Locally decodable codes. *Found. Trends Theor. Comput. Sci.*, 7(1):1–117, 2011.

Centrum Wiskunde & Informatica (CWI), Science Park 123, 1098 SJ Amsterdam, The Netherlands

E-mail address: `j.briet@cwi.nl`

Courant Institute, New York University, 251 Mercer Street, New York NY 10012, USA

E-mail address: `naor@cims.nyu.edu`

École normale supérieure, Département d'informatique, 45 rue d'Ulm, Paris, France

E-mail address: `regev@di.ens.fr`