ISRAEL JOURNAL OF MATHEMATICS **139** (2004), 337–347

SPECIAL ORTHOGONAL SPLITTINGS OF L_1^{2k}

BY

GIDEON SCHECHTMAN*

Department of Mathematics, Weizmann Institute of Science
Rehovot, Israel
e-mail: gideon@wisdom.weizmann.ac.il

ABSTRACT

We show that for each positive integer k there is a $k \times k$ matrix B with ± 1 entries such that putting E to be the span of the rows of the $k \times 2k$ matrix $[\sqrt{k}I_k, B]$, then $E, E^{\perp}$ is a Kashin splitting: The L_1^{2k} and the L_2^{2k} are universally equivalent on both E and $E^{\perp}$. Moreover, the probability that a random ± 1 matrix satisfies the above is exponentially close to 1.

1. Introduction

For $0 < p < \infty$ and $n \in \mathbb{N}$ let L_p^n denote $\mathbb{R}^n$ with the norm

$$\|x\|_{L_p^n} = (n^{-1}\sum_{i=1}^{n} |x_i|^p)^{1/p},$$

where $x = (x_1, x_2, \ldots, x_n)$. A celebrated theorem of Kashin [Ka] states that L_1^{2k} can be decomposed into two orthogonal (with respect to the inner product induced by $\|\cdot\|_{L_2^{2k}}$) k-dimensional subspaces on each of which the two norms $\|\cdot\|_{L_1^n}$ and $\|\cdot\|_{L_2^n}$ are universally equivalent, i.e., putting, for a subset $E \subseteq L_1^n$,

$$C_n(E) = \sup\{\|x\|_{L_2^n}/\|x\|_{L_1^n}; x \in E, x \neq 0\},$$

we can find a k-dimensional subspace of L_1^{2k} for which

$$C_{2k}(E), C_{2k}(E^{\perp}) \leq C$$

* Supported by the Israel Science Foundation.
Received March 11, 2003

where $C < \infty$ is some universal constant. We shall call such a choice of (orthogonal) subspace(s) a Kashin splitting with constant C.

The proof(s) of the Kashin theorem are probabilistic and do not produce an explicit subspace E as above. For example, it is shown that with high probability over the orthogonal group $O(k)$ (where the probability is the Haar measure), the span of the rows of the $k \times 2k$ matrix $[U_1, U_2]$, where $U_1, U_2 \in O(k)$ are chosen independently, is such a subspace.

In a recent paper Anderson [An] found an explicit determinantal formula for $C_{2k}(E)$ and $C_{2k}(E^\perp)$ for any k-dimensional subspace E (involving determinants of $k \times k$ submatrices of the $k \times 2k$ matrix whose rows are any basis of E). Anderson then continues and presents a discretization of (a variant of) the random decomposition, reducing the search of a Kashin splitting to a search among $k \times 2k$ matrices with integer entries (ranging in some bounded, though of size exponential in k, set). The point is that this suggests a possibility of finding an *explicit* Kashin splitting. It also permits a (not very efficient) search algorithm for finding a good Kashin splitting (although, it seems, for that the main point in the paper, the determinantal formulas, can be avoided).

In this paper we take this direction one step farther by showing that one can replace the integral matrices by matrices whose entries are taken only from the set $\{0, \sqrt{k}, 1, -1\}$. More precisely, we show in Theorem 1 that with high probability for a random choice of $k \times k$ matrix B with entries being independent Bernoulli ± 1 variables, the span of the rows of the matrix $[\sqrt{k}I, B]$ form a Kashin splitting with some universal constant. (Since $\sqrt{k}$ is not necessarily an integer, one may wonder whether this is, strictly speaking, a strengthening of Anderson's result. However, in the proof of Theorem 1 below one can easily replace $\sqrt{k}$ with $[\sqrt{k}]$ everywhere and get such a formal strengthening.)

We would like next to indicate what Anderson's determinantal formula gives for such matrices. For R, C two subsets of $\{1, 2, \ldots, k\}$ denote by $B_{R,C}$ the submatrix of B formed by the rows in R and the columns in C. For a submatrix $D = B_{R,C}$ of B and row $i \in R$ let D_{-i} be the matrix $B_{R \setminus \{i\}, C}$; similarly for a $j \notin C$ let D^{+j} be the matrix $B_{R, C \cup \{j\}}$. For $l = 1, 2, \ldots, k-1$, a $(l+1) \times l$ submatrix $D = B_{R,C}$ of B and $p = 1, 2$ denote

$$\Delta_p(D, B) = \left(k^{p/2} \sum_{i \in R} |\det D_{-i}|^p + \sum_{j \notin C} |\det D^{+j}|^p \right)^{1/p}.$$

Using Anderson's determinantal formulas one gets, as we shall indicate in Corollary 1, that for a $k \times k$ matrix B the rows of $[\sqrt{k}I, B]$ form a Kashin decomposition with constant

$$\sqrt{2k}\max\left\{\max\left\{\frac{\Delta_2(D,B)}{\Delta_1(D,B)}\right\},\max\left\{\frac{\Delta_2(D,B^*)}{\Delta_1(D,B^*)}\right\}\right\},$$

where the two inner max are taken over all $l = 1, 2, \ldots, k-1$, and over all $(l+1)\times l$ submatrix D of B, for the first max, and of B^*, for the second.

It follows from our main theorem that there is a $k \times k$ matrix B with ± 1 entries for which

$$\sqrt{2k}\max\left\{\max\left\{\frac{\Delta_2(D,B)}{\Delta_1(D,B)}\right\},\max\left\{\frac{\Delta_2(D,B^*)}{\Delta_1(D,B^*)}\right\}\right\} \tag{1}$$

is bounded by a constant independent of k and for such a matrix this gives the splitting constant.

This of course gives an algorithm (still not very efficient) for searching for a Kashin splitting, but more importantly, it suggests that there might be an algebraic or combinatorial method of finding an explicit splitting. The formula (1) gives an explicit criterion for deciding whether a ± 1 matrix produces such a splitting.

2. The main result

We shall denote by $\|a\|_p$ the ℓ_p^k norm of $a = (a_1, a_2, \ldots, a_n)$,

$$\|a\|_p = (\sum_{i=1}^{n} |a_i|^p)^{1/p}$$

(notice the difference with $\|x\|_{L_p^n}$ defined earlier). Denote by S^{k-1} the Euclidean unit sphere in $\mathbb{R}^k$ and by B_p^k the unit ball of ℓ_p^k, $0 < p \leq \infty$. Given $a = (a_1, a_2, \ldots, a_n) \in \mathbb{R}^k$ denote

$$E_p(a) = \text{Ave}\left(k^{-1}\sum_{j=1}^{k}|\sum_{i=1}^{k} a_i\varepsilon_{i,j}|^p\right)^{1/p}$$

where the average is taken over all sequences of signs $\{\varepsilon_{i,j}\}$. As is well known $2^{-1/2} \leq E_1(a) \leq E_2(a) \leq 1$. (See [Sz] for the stated explicit lower bound; we only need some absolute positive lower bound which follows from Khinchine's inequality.) In the sequel P denotes the natural probability measure on $\{-1,1\}^{k^2}$ and the general element in this probability space is denoted by $\{\varepsilon_{i,j}\}_{i,j=1}^{k}$. We begin with two concentration inequalities.

LEMMA 1: *There is an absolute positive constant η such that for all k, all $a \in \mathbb{R}^n$ and all $0 < C < \infty$,*

$$P\Big(|k^{-1}\sum_{j=1}^{k}|\sum_{i=1}^{k} a_i\varepsilon_{i,j}| - E_1(a)| > CE_1(a)\Big) \le e^{-\eta C^2 k} \tag{2}$$

and

$$P\Big(|(k^{-1}\sum_{j=1}^{k}(\sum_{i=1}^{k} a_i\varepsilon_{i,j})^2)^{1/2} - E_2(a)| > CE_2(a)\Big) \le e^{-\eta C^2 k}. \tag{3}$$

Proof: Let $f, g\colon \mathbb{R}^{k^2} \to \mathbb{R}$ be the functions defined by

$$f(x) = k^{-1}\sum_{j=1}^{k}\left|\sum_{i=1}^{k} a_i x_{i,j}\right| \quad \text{and} \quad g(x) = \left(k^{-1}\sum_{j=1}^{k}\left(\sum_{i=1}^{k} a_i x_{i,j}\right)^2\right)^{1/2}$$

for $x = \{x_{i,j}\}_{i,j=1}^{k}$. Both functions are convex and Lipschitz with constant $\|a\|_2$ with respect to the $\ell_2^{k^2}$ norm. The latter statement can be proved by computing the norm of the gradients of the functions at their points of differentiability. The analogous inequality to (2), where $E_1(a)$ is replaced with the median of f, follows from the main result of [Ta]. That the median can be replaced with the mean is simple, well known, and can be found, e.g., in [MS] Proposition V.4. Inequality (3) is dealt with similarly. ∎

For $1 \le l \le k$ denote

$$F_l^k = \{a = (a_1, a_2, \ldots, a_k) \in B_2^k; a_i \ne 0 \text{ for at most } l \text{ values of } i\}.$$

We now extend the concentration inequalities of Lemma 1 to simultaneous inequalities for the sets F_l^k.

PROPOSITION 1: *There are absolute positive constants η and α such that for all k and $l \le \alpha k$,*

$$P\left(\left|k^{-1}\sum_{j=1}^{k}\left|\sum_{i=1}^{k} a_i\varepsilon_{i,j}\right| - E_1(a)\right| > E_1(a)/4, \text{ for some } a \in F_l^k\right) \le e^{-\eta k}$$

and

$$P\left(\left|\left(k^{-1}\sum_{j=1}^{k}\left(\sum_{i=1}^{k} a_i\varepsilon_{i,j}\right)^2\right)^{1/2} - E_2(a)\right| > E_2(a)/4, \text{ for some } a \in F_l^k\right) \le e^{-\eta k}.$$

Proof: Given two sets A, B in a linear space we denote by $N(A, B)$ the minimal number of shifts of B whose union covers A.

For $\sigma \subseteq \{1,2,\ldots,k\}$ denote $F_\sigma^k = \{(a_1,a_2,\ldots,a_k) \in B_2^k; a_i = 0 \text{ for } i \notin \sigma\}$. Fix some $1 \le l \le k$, then by the usual volume estimates (see, e.g., [MS]) for each subset $\sigma \subseteq \{1,2,\ldots,k\}$ of cardinality l and for all $0 < \delta < 1$, $N(F_\sigma^k, \delta B_2^k) \le (2\delta^{-1})^l$. It follows from Lemma 1 that for some absolute $\eta > 0$,

$$P\left(\left|k^{-1}\sum_{j=1}^k\left|\sum_{i=1}^k a_i\varepsilon_{i,j}\right| - E_1(a)\right| > E_1(a)/8, \text{ for some } a \in \mathcal{N}\right) \le e^{l\log(2/\delta)-\eta k}$$

where $\mathcal{N}$ is some δ-net in F_σ^k. If δ is a small enough positive universal constant and l/k is small enough with respect to the universal constants δ and η (so that $e^{l\log(2/\delta)-\eta k} < e^{-\eta k/2}$), it now follows by successive approximation (see, e.g., [MS]) that

$$(4)\quad P\left(\left|k^{-1}\sum_{j=1}^k\left|\sum_{i=1}^k a_i\varepsilon_{i,j}\right| - E_1(a)\right| > E_1(a)/4, \text{ for some } a \in F_\sigma^k\right) \le e^{-\eta k/2}.$$

Put $\alpha = l/k$; assume $\alpha \le 1/2$ and also small enough for (4) to hold. Notice that, by Stirling's formula, the number of subsets of $\{1,2,\ldots,k\}$ of cardinality l can be evaluated as

$$\binom{k}{l} \le e^{3k\alpha\log(1/\alpha)}.$$

It follows from (4) that

$$P\left(\left|k^{-1}\sum_{j=1}^k\left|\sum_{i=1}^k a_i\varepsilon_{i,j}\right| - E_1(a)\right| > E_1(a)/4, \text{ for some } a \in F_l^k\right) \le e^{3k\alpha\log(1/\alpha)-\eta k/2}.$$

Finally, if $\alpha\log(1/\alpha) < \eta/12$, the last quantity is less than $e^{-\eta k/4}$, which finishes the proof of the first assertion. The second is proved very similarly. ∎

LEMMA 2: *Let $a = (a_1,a_2,\ldots,a_k)$ be a norm one vector in ℓ_2^k and let $0 < \gamma < 1$. Assume $k^{-1/2}\sum_{i=1}^k |a_i| \le \gamma$. Then*

$$\left(\sum_{i=l}^k (a_i^*)^2\right)^{1/2} \le l^{-1}\gamma\sqrt{k(k-l+1)}$$

for all $1 \le l \le k$, where $\{a_i^*\}$ denotes the decreasing rearrangement of $\{|a_i|\}$.

Proof: For each $1 \le l \le k$, $(k-l+1)(a_l^*)^2 \ge \sum_{i=l}^k (a_i^*)^2$. It follows that

$$\gamma \ge k^{-1/2}\sum_{i=1}^k |a_i| \ge lk^{-1/2}a_l^* \ge l(k(k-l+1))^{-1/2}\left(\sum_{i=l}^k (a_i^*)^2\right)^{1/2}$$

from which the conclusion follows. ∎

For $0<\gamma<1$, $k\in\mathbb{N}$, denote

$$A_\gamma^k=\Big\{a\in S^{k-1}; k^{-1/2}\sum_{i=1}^k |a_i|\le\gamma\Big\}=\Big\{a\in S^{k-1}; \frac{\|a\|_{L_1^k}}{\|a\|_{L_2^k}}\le\gamma\Big\}.$$

Next we extend the concentration inequalities to the sets A_γ^k.

PROPOSITION 2: *There are absolute constants $0<\gamma<1$ and $\eta>0$ such that for all k,*

$$P\bigg(\Big|k^{-1}\sum_{j=1}^k\Big|\sum_{i=1}^k a_i\varepsilon_{i,j}\Big|-E_1(a)\Big|>E_1(a)/2, \text{ for some } a\in A_\gamma^k\bigg)\le e^{-\eta k}$$

and

$$P\bigg(\Big|\Big(k^{-1}\sum_{j=1}^k\Big(\sum_{i=1}^k a_i\varepsilon_{i,j}\Big)^2\Big)^{1/2}-1\Big|>1/2, \text{ for some } a\in A_\gamma^k\bigg)\le e^{-\eta k}.$$

Proof: Notice first that by the usual ε-net considerations starting with Lemma 1, there are some absolute $C<\infty$ and $\eta>0$ such that

$$P\bigg(k^{-1}\sum_{j=1}^k\Big|\sum_{i=1}^k a_i\varepsilon_{i,j}\Big|>C\|a\|_2, \text{ for some } a\in\mathbb{R}^k\bigg)\le e^{-\eta k}$$

and

$$P\bigg(\Big(k^{-1}\sum_{j=1}^k\Big(\sum_{i=1}^k a_i\varepsilon_{i,j}\Big)^2\Big)^{1/2}>C\|a\|_2, \text{ for some } a\in\mathbb{R}^k\bigg)\le e^{-\eta k}.$$

(Actually, the first assertion follows trivially from the second.) Let $l=[\alpha k]$ where α is the constant from Proposition 1. Now choose $\gamma>0$ such that, putting $\delta=l^{-1}\gamma\sqrt{k(k-l+1)}$, $3C\delta<1/4\sqrt{2}$.

By Lemma 2, each $a\in A_\gamma^k$ can be split as $a=b+c$ with $b\in F_l^k$ and $\|c\|_2\le\delta$. Let $\{\varepsilon_{i,j}\}$ be such that both

$$\Big|k^{-1}\sum_{j=1}^k\Big|\sum_{i=1}^k b_i\varepsilon_{i,j}\Big|-E_1(b)\Big|\le E_1(b)/4 \tag{5}$$

and

$$k^{-1}\sum_{j=1}^k\Big|\sum_{i=1}^k c_i\varepsilon_{i,j}\Big|\le C\|c\|_2. \tag{6}$$

Then the condition on δ implies that

$$\left| k^{-1} \sum_{j=1}^{k} \left| \sum_{i=1}^{k} a_i \varepsilon_{i,j} \right| - E_1(a) \right| \leq E_1(a)/2.$$

Since, by Proposition 1 and the first paragraph of this proof, the probability that at least one of inequalities (5) or (6) does not hold is less than $e^{-\eta k}$, we get the first assertion of the Proposition (with a different absolute η). The second assertion is proved very similarly. ∎

Given signs $\{\varepsilon_{i,j}\}_{i,j=1}^{k}$, we shall denote by B the $k \times k$ matrix with entries $\{\varepsilon_{i,j}\}_{i,j=1}^{k}$ and by $A = [\sqrt{k}I, B]$ the $k \times 2k$ matrix whose first k columns form $\sqrt{k}I_k$ and the last k columns form B. We shall also denote $\bar{A} = [-B^*, \sqrt{k}I]$ with the obvious meaning (where B^* is the transpose of B). Note that the row spans of A and of $\bar{A}$ form orthogonal subspaces of L_2^{2k}. We are now ready to state and prove our main result.

THEOREM 1: *For some absolute $\eta > 0$ and $C < \infty$ and for all k there are signs $\{\varepsilon_{i,j}\}_{i,j=1}^{k}$ such that for all $a \in S^{k-1}$,*

$$C^{-1} \leq \|aA\|_{L_1^{2k}} \leq \|aA\|_{L_2^{2k}} \leq C$$

and

$$C^{-1} \leq \|a\bar{A}\|_{L_1^{2k}} \leq \|a\bar{A}\|_{L_2^{2k}} \leq C.$$

Moreover, this holds with probability larger than $1 - e^{-\eta k}$.

Proof: As in the beginning of the proof of Proposition 2, it follows from Lemma 1 that for some absolute C and η and with probability at least $1 - e^{-\eta k}$,

$$k^{-1} \sum_{j=1}^{k} \left| \sum_{i=1}^{k} a_i \varepsilon_{i,j} \right| \leq \left(k^{-1} \sum_{j=1}^{k} \left(\sum_{i=1}^{k} a_i \varepsilon_{i,j} \right)^2 \right)^{1/2} \leq C$$

for all $a \in S^{k-1}$. Of course, the same holds also if we replace $\varepsilon_{i,j}$ with $-\varepsilon_{j,i}$ everywhere. It follows easily that, with probability $1 - e^{-\eta k}$,

$$\|aA\|_{L_1^{2k}} \leq \|aA\|_{L_2^{2k}} \leq (1 + C^2)^{1/2}/\sqrt{2}$$

and

$$\|a\bar{A}\|_{L_1^{2k}} \leq \|a\bar{A}\|_{L_2^{2k}} \leq (1 + C^2)^{1/2}/\sqrt{2}$$

for all $a \in S^{k-1}$.

For the lower bound let γ be the constant from Proposition 2. Then, with probability $1 - e^{-\eta k}$,

$$k^{-1} \sum_{j=1}^{k} \left| \sum_{i=1}^{k} a_i \varepsilon_{i,j} \right| > 1/2\sqrt{2}$$

for all $a \in A_\gamma^k$ (and the same holds with $-\varepsilon_{j,i}$ instead of $\varepsilon_{i,j}$). For the other $a \in S^{k-1}$,

$$k^{-1/2} \sum_{i=1}^{k} |a_i| > \gamma.$$

It follows easily that, with probability at least $1 - e^{-\eta k}$,

$$\|aA\|_{L_2^{2k}} \geq \|aA\|_{L_1^{2k}} \geq \min\{\gamma/2, 1/4\sqrt{2}\}$$

and

$$\|a\bar{A}\|_{L_2^{2k}} \geq \|a\bar{A}\|_{L_1^{2k}} \geq \min\{\gamma/2, 1/4\sqrt{2}\}$$

for all $a \in S^{k-1}$. ∎

Recall the definition of $\Delta_p(D, B)$ appearing in the Introduction.

COROLLARY 1: *There is a constant $C < \infty$ such that for all k there is a $k \times k$ matrix B with ± 1 entries such that*

$$\sqrt{2k} \max \left\{ \max\left\{ \frac{\Delta_2(D, B)}{\Delta_1(D, B)} \right\}, \max\left\{ \frac{\Delta_2(D, B^*)}{\Delta_1(D, B^*)} \right\} \right\} \leq C, \tag{7}$$

where the first inner max is taken over all $l = 1, 2, \ldots, k-1$, and over all $(l+1) \times l$ submatrix D of B for which the denominator is not zero, while the second inner max is taken over all $l = 1, 2, \ldots, k-1$, and over all $(l+1) \times l$ submatrix D of B^*.

Moreover, the left hand side of (7) is equal to $\max\{C_{2k}(E), C_{2k}(E^\perp\}$, where E is the span of the rows of $[\sqrt{k}I, B]$.

Proof: By Theorem 1 we only need to address the "Moreover" part. This follows easily from section 2.5 in Anderson [An], in which it is shown, in our notation, that for a $k \times 2k$ matrix A and for E being the span of its rows,

$$C_{2k}(E) = \sqrt{\frac{2k}{k+1}} \max \frac{\left(\frac{1}{k+1} \sum_{j \notin C} |\det D^{+j}|^2\right)^{1/2}}{\frac{1}{k+1} \sum_{j \notin C} |\det D^{+j}|}$$

where the max is taken over all $k \times (k-1)$ submatrices $D = D_{\{1,\ldots,k\},C}$ for which the denominator does not vanish.

As we remarked in the Introduction, Corollary 1 gives an explicit criterion for deciding whether a ± 1 matrix gives a good Kashin splitting and the assurance that there are (many) such matrices. We hope this will help in a search for an explicit construction of a Kashin splitting.

Remark: It is easy to see that Theorem 1 implies that for each positive integer k, with probability larger than $1 - e^{-\eta k}$, a $k \times k$ matrix B with independent ± 1 entries satisfies the following: Letting K_1 be $\{x; Bx \in \sqrt{k}B_1^k\}$ and K_2 be the symmetric convex hull of $\sqrt{k}$ times the canonical unit vector basis in $\mathbb{R}^k$ $(= \sqrt{k}B_1^k)$, then $K_1 \cap K_2$ lies between two universal multiples of the Euclidean unit ball, B_2^k.

3. Some related results and remarks

Kashin also proved that for *any* $0 < \lambda < 1$ and any n there is a $[\lambda n]$-dimensional subspace E of L_1^n which is $C(\lambda)$-isomorphic to a Hilbert space where $C(\lambda)$ depends only on λ (actually, he proved that $C_n(E) \le C(\lambda)$). A similar statement holds for almost isometries, although we need to replace "any $0 < \lambda < 1$" with "some $0 < \lambda < 1$": For every $\varepsilon > 0$ there is a $\lambda = \lambda(\varepsilon)$ such that for any n there is a subspace of L_1^n of dimension at least λn which is $(1+\varepsilon)$-isomorphic to a Hilbert space. This is proved in [FLM] (and, without stating it explicitly, already in [Mi]). The proofs are again probabilistic and we are far from having any explicit embeddings.

What about embeddings given by a span of rows of matrices whose entries take values in some small set of values? It is not very hard to see that a similar proof to the one here gives, for any $0 < \lambda < 1$ and any n, a subspace E of L_1^n on which $C_n(E) \le C(\lambda)$ and which is spanned by vectors whose entries are taken from a four point set (actually, the set consists of $0, \pm 1$ and one other specific value, only the ± 1 are chosen randomly). Moreover, there is a corresponding determinantal formula for determining whether a space from this collection satisfies $C_n(E) \le C(\lambda)$. These subjects will be detailed in a forthcoming MSc thesis of Boris Levant written at the Weizmann Institute.

It is also possible to find, for every $0 < \lambda < 1$, a good Hilbertian subspace of L_1^n of dimension $[\lambda n]$ spanned by rows of a $[\lambda n] \times n$ matrix with ± 1 entries. This follows from the main result of [Sc] where a similar statement with *some* $0 < \lambda < 1$ instead of *every* $0 < \lambda < 1$ is proved, together with the method of [JS] where it is shown that whenever E is a k-dimensional subspace of L_1^n then, for all $a > 1$, the restriction operator onto some $[ak]$ of the n coordinates is a C-isomorphism when restricted to E and where C depends on k/n only. The proof in [Sc] uses a concentration inequality similar to the one in the first part of Lemma 1. Using a variation on the second part of that lemma as well (and the restriction method of [JS]) one can get a bit more.

PROPOSITION 3: *For all $0 < \lambda < 1$ and all n there is a $[\lambda n] \times n$ matrix A with ± 1 entries such that for all $a \in S^{[\lambda n]-1}$,*

$$C^{-1}(\lambda) \leq \|aA\|_{L_1^n} \leq \|aA\|_{L_2^n} \leq C(\lambda)$$

where $C(\lambda)$ depends on λ only.

The details of the proof will be given in Levant's thesis.

Remark: Going back to the search for an explicit ± 1 matrix B for which the span of the rows of $[\sqrt{k}I, B]$ gives a good Kashin splitting, a first candidate to look for is the Walsh matrix. However, it is easy to see that this is not the case. Assume $k = 2^t$; reindex the columns $1, \ldots, k$ as $\{-1,1\}^t$ and the rows by $\{\sigma\}_{\sigma \subseteq \{1,\ldots,t\}}$ and let the σ, ε term of the matrix B be $W_\sigma(\varepsilon) = \prod_{i \in \sigma} \varepsilon_i$. Consider the vector of coefficients $a = (a_\sigma)$ where a_σ is 1 whenever σ is a subset of $\{1, \ldots, t/2\}$ (assuming t is even) and 0 otherwise. Then it is not hard to see that $\|\sqrt{k}a\|_{L_2^k} = \|aB\|_{L_2^k} = k^{1/4}$, while $\|\sqrt{k}a\|_{L_1^k} = \|aB\|_{L_1^k} = 1$.

The method of the proof of the main theorem may be useful for other applications. The idea of the proof was that we split the sphere S^{k-1} into two sets. On one of them the L_1^k and L_2^k are well equivalent and the other one (A_γ^k) is "small". Of course the measure of A_γ^k is basically known and is very small. This estimate was not good enough for our purposes and we needed another measure of "smallness" (which was $A_\gamma^k \subset F_l^k + \delta B_2^k$ for some (not too small) l and (small) δ). There is another measure of smallness that follows easily from the proof here and may be useful elsewhere. Again, it was not good enough for our purposes. Recall that $A_\gamma^k = \{(a_1, a_2, \ldots, a_k) \in S^{k-1}; k^{-1/2}\sum_{i=1}^k |a_i| \leq \gamma\}$.

PROPOSITION 4: *Let $0 < \gamma < 1$ and $k \in \mathbb{N}$. Then, for all $\varepsilon > 4\gamma$,*

$$N(A_\gamma^k, \varepsilon B_2^k) \leq e^{\frac{6\gamma k}{\varepsilon}(\log \frac{\varepsilon}{2\gamma} + \log \frac{4}{\varepsilon})}.$$

Proof: Since for any $\sigma \subseteq \{1, 2, \ldots, k\}$ of cardinality l and for all $0 < \delta < 1$, $N(F_\sigma^k, \delta B_2^k) \leq (2\delta^{-1})^l$, and since the number of subsets of $\{1, 2, \ldots, k\}$ of cardinality $l \leq k/2$ can be evaluated as

$$\binom{k}{l} \leq e^{3l \log(k/l)},$$

it follows that

$$N(F_l^k, \delta B_2^k) \le e^{3l(\log \frac{k}{l} + \log \frac{2}{\delta})}. \tag{8}$$

By Lemma 2, $A_\gamma^k \subset F_l^k + \delta B_2^k$ with $\delta = l^{-1}\gamma\sqrt{k(k-l+1)}$. It follows that

$$N(A_\gamma^k, 2\delta B_2^k) \le e^{3l(\log \frac{k}{l} + \log \frac{2}{\delta})}.$$

Letting $\delta = \varepsilon/2$ and $l = [2\gamma\sqrt{k(k-l+1)}/\varepsilon] \le 2\gamma k/\varepsilon$, we get, for $\gamma < \varepsilon/4$ (to ensure $l < k/2$),

$$N(A_\gamma^k, 2\delta B_2^k) \le e^{\frac{6\gamma k}{\varepsilon}(\log \frac{\varepsilon}{2\gamma} + \log \frac{4}{\varepsilon})}. \quad \blacksquare$$

References

[An] G. W. Anderson, *Integral Kašin splittings*, Israel Journal of Mathematics, to appear.

[FLM] T. Figiel, J. Lindenstrauss and V. D. Milman, *The dimension of almost spherical sections of convex bodies*, Acta Mathematica **139** (1977), 53–94.

[Ka] B. Kashin, *Section of some finite-dimensional sets and classes of smooth functions*, Izvestiya Akademii Nauk SSSR **41** (1977), 334–351 (Russian).

[JS] W. B. Johnson and G. Schechtman, *Very tight embeddings of subspaces of L_p, $1 \le p < 2$, into ℓ_p^n*, Geometric and Functional Analysis **13** (2003), 845–851.

[Mi] V. D. Milman, *A new proof of A. Dvoretzky's theorem on cross-sections of convex bodies*, Funktsional. Analisis i Prilozen. **5** (1971), 28–37 (Russian).

[MS] V. D. Milman and G. Schechtman, *Asymptotic theory of finite-dimensional normed spaces*, Lecture Notes in Mathematics **1200**, Springer-Verlag, Berlin, 1986.

[Sc] G. Schechtman, *Random embeddings of Euclidean spaces in sequence spaces*, Israel Journal of Mathematics **40** (1981), 187–192.

[Sz] S. J. Szarek, *On the best constants in the Khinchin inequality*, Studia Mathematica **58** (1976), 197–208.

[Ta] M. Talagrand, *An isoperimetric theorem on the cube and the Kintchine–Kahane inequalities*, Proceedings of the American Mathematical Society **104** (1988), 905–909.