ISRAEL JOURNAL OF MATHEMATICS 101 (1997), 93–124

CONTACT POINTS OF CONVEX BODIES

BY

M. RUDELSON*

Institute of Mathematics, The Hebrew University of Jerusalem
Givat Ram, Jerusalem 91904, Israel
e-mail: mark@math.huji.ac.il

ABSTRACT

Let B be a convex body in $\mathbb{R}^n$ and let $\mathcal{E}$ be an ellipsoid of minimal volume containing B. By contact points of B we mean the points of the intersection between the boundaries of B and $\mathcal{E}$. By a result of P. Gruber, a generic convex body in $\mathbb{R}^n$ has $(n+3)\cdot n/2$ contact points. We prove that for every $\varepsilon > 0$ and for every convex body $B \subset \mathbb{R}^n$ there exists a convex body K having

$$m \leq C(\varepsilon)\cdot n \log^3 n$$

contact points whose Banach–Mazur distance to B is less than $1+\varepsilon$.

We prove also that for every $t > 1$ there exists a convex symmetric body $\Gamma \subset \mathbb{R}^n$ so that every convex body $D \subset \mathbb{R}^n$ whose Banach–Mazur distance to Γ is less than t has at least $(1 + c_0/t^2)\cdot n$ contact points for some absolute constant c_0.

We apply these results to obtain new factorizations of Dvoretzky–Rogers type and to estimate the size of almost orthogonal submatrices of an orthogonal matrix.

1. Introduction

Let K be a convex body in $\mathbb{R}^n$ and let $\mathcal{E}$ be the ellipsoid of minimal volume containing K. By the contact points of K we mean the points of the intersection between the boundaries of K and $\mathcal{E}$. The importance of contact points follows from the special role played by the minimal volume ellipsoid in the Local Theory of Banach Spaces and Convex Geometry. In particular, a special family of contact

* Research supported in part by a grant of the US–Israel BSF.
Received November 13, 1995

points was used by K. Ball to show that the n-dimensional simplex and cube have the maximal volume ratio among all convex and convex symmetric bodies in $\mathbb{R}^n$ respectively ([B1], [B2]). Contact points arise also in the problem of estimating the Banach–Mazur distance between a convex symmetric body and the cube of an appropriate dimension ([B-S], [S-T], [Gi1]).

To study contact points we need to introduce the notion of John's decomposition. By a celebrated theorem of F. John [J] there exists a unique ellipsoid of minimal volume containing a given convex body $K \in \mathbb{R}^n$. This ellipsoid will be called the John ellipsoid of K. If the body K is embedded in $\mathbb{R}^n$ so that its John ellipsoid is the standard Euclidean ball B_2^n, then there exist $M \leq N = (n+3)n/2$ contact points $x_1, \dots, x_M$ and M positive numbers $c_1, \dots, c_M$ satisfying the following system of equations:

$$\mathrm{id} = \sum_{i=1}^{M} c_i x_i \otimes x_i, \tag{1.1}$$

$$0 = \sum_{i=1}^{M} c_i x_i. \tag{1.2}$$

Here by id we denote the identity operator in $\mathbb{R}^n$. Besides it, John's proof shows that if $\tilde{K}$ is a convex subset of B_2^n containing the points $x_1, \dots, x_M$, then B_2^n is the John ellipsoid of $\tilde{K}$. The system (1.1) is called the John decomposition of the identity operator. This notion will be crucial in the study of contact points.

For a symmetric convex body it is enough to take $M \leq N_s = (n+1)n/2$ points in (1.1). Note that N_s is the dimension of the space of symmetric matrices and $N = N_s + n$.

Clearly, the number of contact points of a convex (respectively, convex symmetric) body in $\mathbb{R}^n$ cannot be less than $n+1$ (respectively, $2n$). However, for most convex bodies this number is much bigger. Before formulating this precisely let us recall the definition of the Banach–Mazur metric in the space of convex bodies.

Let $\bar{\mathcal{K}}$ be the set of all n-dimensional convex bodies. For $K, B \in \bar{\mathcal{K}}$ define a distance between K and B as

$$d(K,B) = \inf\{c \mid K + u \subset TB \subset c(K+u)\},$$

where the infimum is taken over all vectors $u \in \mathbb{R}^n$ and all invertible operators T. If K and B are symmetric, then $u = 0$ and d becomes the usual Banach–Mazur distance.

P. Gruber [Gr] proved that the set of all convex bodies for which the number of contact points differs from N (N_s in the symmetric case) is a set of the first Baire category in $\bar{\mathcal{K}}$. In Section 2 we give a simpler proof of this result. It follows also from the proof that the closure of the set of convex bodies having less than N contact points is nowhere dense in $\bar{\mathcal{K}}$.

However, it turns out that every convex body can be approximated by another one, for which the number of contact points is practically of order n. We prove the following

THEOREM 1.1: *Let B be a convex body in $\mathbb{R}^n$ and let $\varepsilon > 0$. There exists a convex body $K \subset \mathbb{R}^n$, so that $d(K, B) \leq 1 + \varepsilon$ and the number of contact points of K with its John ellipsoid is less than*

$$m(n, \varepsilon) = C(\varepsilon) \cdot n \cdot \log^3 n. \tag{1.3}$$

Moreover, if K is embedded in $\mathbb{R}^n$ so that its John ellipsoid is the standard Euclidean ball B_2^n, then the identity operator on $\mathbb{R}^n$ has the following decomposition:

$$\mathrm{id} = \sum_{i=1}^{m} a_i u_i \otimes u_i, \tag{1.4}$$

where $m \leq m(n, \varepsilon), u_1, \ldots, u_m$ are the only contact points of K with B_2^n,

$$\sum_{i=1}^{m} a_i u_i = 0 \tag{1.5}$$

and for every i, $\quad 1 - \varepsilon \leq \frac{m}{n} a_i \leq 1 + \varepsilon.$

The proof of Theorem 1.1 consists of two steps. In Section 3 we show that, given a John decomposition generated by the contact points $x_1, \ldots, x_M$, we can find a subsequence $x_{i_1}, \ldots, x_{i_m}$, remove from the John decomposition the other points and change the coefficients c_i so that the operator we get will be close to the identity. This method was previously introduced in [R] for convex symmetric bodies. The proof is based on estimates of the supremum of some family of Bernoulli random variables. Then in Section 4 we construct a body K, so that this approximate decomposition of the identity operator becomes the John decomposition for K.

Actually we are able to improve the estimate in (1.3) to

$$m \leq C(\varepsilon) \cdot n \cdot \log n.$$

This can be achived by applying Talagrand's method of majorizing measures ([T]). Since however the proof of this improvment is much more involved than that of (1.3), we shall present it in a different paper.

In Section 5 we study the question how much the number of contact points can be reduced, if instead of ε-approximation, we approximate a given body B by bodies whose distance to B is bounded by some large number t. We show that there exists a convex symmetric body $\Gamma \subset \mathbb{R}^n$ whose number of contact points cannot be reduced to $n + o(n)$. More precisely, we prove the following

THEOREM 1.2: *For every $t > 1$ and for every $n > n_0(t)$ there exists a convex symmetric body $\Gamma \subset \mathbb{R}^n$ such that*

(1) *every convex symmetric body K satisfying $d(\Gamma, K) \leq t$ has at least $(1 + c_0/t^2) \cdot 2n$ contact points;*
(2) *every convex body D satisfying $d(\Gamma, D) \leq t$ has at least $(1 + c_0/t^2) \cdot n$ contact points.*

Here c_0 is an absolute constant.

In Section 6 we use Theorem 1.1 for a symmetric body to derive a factorization theorem of Dvoretzky–Rogers type and Theorem 1.2 to obtain a lower bound related to such a factorization.

Finally, in Section 7 we apply the results of Section 3 (actually those of [R]) to solve a problem of B. Kashin and L. Tzafriri.

Let us introduce some notation. Let $K \subset \mathbb{R}^n$, $B \subset \mathbb{R}^m$ be convex bodies. If $0 \in K$ then by $\|\cdot\|_K$ we denote the Minkowski functional of K. For a linear operator $T: \mathbb{R}^m \to \mathbb{R}^n$ define a norm as

$$\|T: B \to K\| = \sup\{\|Tx\|_K \mid x \in B\}.$$

If K and B are symmetric this is a usual operator norm. The n-dimensional Euclidean ball will be denoted by B_2^n. Instead of $\|x\|_{B_2^n}$ and $\|T: B_2^n \to B_2^n\|$ we write $\|x\|$ and $\|T\|$ respectively. The letter $\mathcal{P}$ stands for probability and the letter $\mathbb{E}$ for the expectation of a random variable. By $C, c, \tilde{C}$ etc. we denote absolute constants whose value may change from line to line.

ACKNOWLEDGEMENT: I would like to thank Professor Lindenstrauss and Professor Gluskin for helpful discussions.

2. Typical number of contact points

Let $\bar{\mathcal{K}}$ ($\mathcal{K}$) be the set of all n-dimensional convex (convex symmetric) bodies equipped with the Banach–Mazur metric. It is known that $\bar{\mathcal{K}}$ and $\mathcal{K}$ are complete metric spaces. Denote by $\bar{\mathcal{D}}_m$ the set of all bodies $B \in \bar{\mathcal{K}}$ which have at most m contact points. Similarly, $\mathcal{D}_m$ stands for the set of all $B \in \mathcal{K}$ having at most m pairs of contact points. Obviously, none of the sets $\bar{\mathcal{D}}_m$, $\mathcal{D}_m$ is closed. However we have the following

THEOREM 2.1:

(1) *For every m, $n \le m < N_s$, $cl\mathcal{D}_m$ is a nowhere dense subset of $cl\mathcal{D}_{m+1}$.*
(2) *$\mathcal{K}\backslash\mathcal{D}_{N_s}$ is a set of the first Baire category in $\mathcal{K}$.*

Note that since $\mathcal{K}$ is complete, it follows from the theorem that a generic (in the sense of category) convex symmetric body has exactly N_s contact points.

For a general convex body we have a similar result.

THEOREM 2.1′:

(1) *For every m, $n \le m < N$, $cl\bar{\mathcal{D}}_m$ is a nowhere dense subset of $cl\bar{\mathcal{D}}_{m+1}$.*
(2) *$\bar{\mathcal{K}}\backslash\bar{\mathcal{D}}_N$ is a set of the first Baire category in $\bar{\mathcal{K}}$.*

Before proving the theorem let us introduce some notion. Let K be an n-dimensional convex body. We say that K is in standard position if the John ellipsoid of K is B_2^n. Let (1.4), (1.5) be a John decomposition for K. Note that this decomposition is not uniquely defined. By the length of the John decomposition we mean the number of different terms $x_i \otimes x_i$. This notion was studied by A. Pelczynski and N. Tomczak-Jaegermann [P-T-J]. In particular they proved that for every $n \le m \le N_s$ there exists a convex symmetric body which has a unique John decomposition of length m.

Proof of Theorem 2.1: Let $\mathcal{C}_m$ be a set of all n-dimensional convex symmetric bodies which have a John decomposition of length at most m. Obviously, for $m \le N_s$ we have that $\mathcal{D}_m \subset \mathcal{C}_m$. Moreover, LEMMA 2.1: *If $m \le N_s$ then $cl\mathcal{D}_m = \mathcal{C}_m$.*

Proof: We prove first that the set $\mathcal{C}_m$ is closed. Let $\{K_l\}_{l=1}^{\infty} \subset \mathcal{C}_m$ be a sequence of convex symmetric bodies converging to some body $K \in \mathcal{K}$. Suppose that K_l are taken in standard position and the John decomposition for K_l is

$$\mathrm{id} = \sum_{i=1}^{m} c_i^l x_i^l \otimes x_i^l.$$

Passing to a subsequence, we may assume that $c_i^l \to c_i$ and $x_i^l \to x_i$ for every $i \le m$. Hence, we have $\|x_i\| = 1$ and

$$\mathrm{id} = \sum_{i=1}^{m} c_i x_i \otimes x_i. \tag{2.1}$$

Let $T_l \colon \mathbb{R}^n \to \mathbb{R}^n$ be an operator so that

$$d_l^{-1} \cdot K_l \subset T_l K \subset K_l \subset B_2^n,$$

where $d_l = d(K_l, K) \to 1$. Passing again to a subsequence, we assume that $T_l \to T$. Then $TK \subset B_2^n$ and $x_i \in TK$ for all i. Thus, (2.1) is a John decomposition for K.

Now let $K \in \mathcal{C}_m$ and let $\varepsilon > 0$. We construct a new body $K_\varepsilon \in \mathcal{D}_m$ so that $d(K, K_\varepsilon) \le 1 + \varepsilon$. Let K be in standard position and let (2.1) be a John decomposition for K. Define K_ε by

$$K_\varepsilon = \text{abs conv}\left(\frac{1}{1+\varepsilon} \cdot K, x_1, \dots, x_m\right).$$

Then $K_\varepsilon \subset B_2^n$ and $\partial K_\varepsilon \cap \partial B_2^n = \{x_1, \dots, x_m\}$. So, B_2^n is the John ellipsoid of K_ε and

$$\frac{1}{1+\varepsilon} \cdot K \subset K_\varepsilon \subset K. \qquad \blacksquare$$

To obtain (1) we have to prove now that $\mathcal{C}_m$ is nowhere dense in $\mathcal{C}_{m+1}$. The proof goes by induction on m. For $m = n-1$, $\mathcal{C}_m = \emptyset$, so the statement is trivial. Let now $\bar{K} \in \mathcal{C}_m$. For given $\varepsilon > 0$ we have to construct a new body $\tilde{K} \in \mathcal{C}_{m+1} \backslash \mathcal{C}_m$ so that $d(\tilde{K}, \bar{K}) \le 1 + \varepsilon$. By the induction hypothesis $\bar{K}$ can be approximated by a body $K \in \mathcal{C}_m \backslash \mathcal{C}_{m-1}$. Suppose that K is in standard position and (2.1) is the John decomposition for K. We use the construction of Lemma 2.5 of [P-T-J]. Note that the tensors $x_i \otimes x_i$ are linearly independent. Indeed, if

$$0 = \sum_{i=1}^{m} a_i x_i \otimes x_i$$

then

$$\mathrm{id} = \sum_{i=1}^{m} (c_i - \alpha a_i) x_i \otimes x_i$$

and we can choose α so that all the coefficients except some i_0 are positive and $c_{i_0} - \alpha a_{i_0} = 0$. This contradicts $K \notin \mathcal{C}_{m-1}$.

Without loss of generality we may assume that the vectors $x_1, \dots, x_n$ are linearly independent. Then the tensors $x_i \otimes x_j + x_j \otimes x_i, \quad i,j = 1, \dots, n$ form a basis of the space of symmetric matrices. Since $m < N_s$, there exists a pair i, j with $i, j \leq n$, so that

$$x_i \otimes x_j + x_j \otimes x_i \notin \mathrm{span}(x_1 \otimes x_1, \dots, x_m \otimes x_m).$$

Suppose that this holds for $i = 1, \ j = 2$. For $\alpha > 0$ define

$$z_0' = \frac{\alpha}{\sqrt{2}} x_2, \qquad z_1' = \frac{x_1}{\sqrt{2}} - \frac{\alpha}{2} x_2, \qquad z_2' = \frac{x_1}{\sqrt{2}} + \frac{\alpha}{2} x_2,$$
$$z_1 = \frac{z_1'}{\|z_1'\|}, \qquad z_2 = \frac{z_2'}{\|z_2'\|}.$$

Then

$$z_0' \otimes z_0' + z_1' \otimes z_1' + z_2' \otimes z_2' = x_1 \otimes x_1 + \alpha^2 \cdot x_2 \otimes x_2,$$

so we have the following representation of the identity operator:

$$\text{(2.2)} \quad \mathrm{id} = c_1 \|z_1'\|^2 \cdot z_1 \otimes z_1 + c_1 \|z_2'\|^2 \cdot z_2 \otimes z_2 + \left(c_2 - \frac{c_1 \alpha^2}{2}\right) \cdot x_2 \otimes x_2 + \sum_{i=3}^{m} c_i x_i \otimes x_i.$$

For sufficiently small α all the coefficients are positive.

Define now

$$\tilde{K} = \mathrm{abs\ conv}\left(\frac{1}{1+\varepsilon} K, z_1, z_2, x_2, \dots, x_m\right).$$

For small α and ε, $\tilde{K}$ is arbitrary close to K. We claim that $\tilde{K} \in \mathcal{C}_{m+1} \setminus \mathcal{C}_m$. Indeed,

$$x_1 \otimes x_2 + x_2 \otimes x_1 \in \mathrm{span}(z_1 \otimes z_1, z_2 \otimes z_2, x_2 \otimes x_2).$$

Hence,

$$\dim \operatorname{span}(z_1 \otimes z_1, z_2 \otimes z_2, x_2 \otimes x_2, \dots, x_m \otimes x_m) = m + 1$$

and this means that the decomposition (2.2) is unique. ∎

(2) Let $\varepsilon > 0$ and let $\mathcal{F}(\varepsilon)$ be the set of all bodies $K \in \mathcal{K}$ having $N_s + 1$ contact points, so that if K is taken in the standard position, then the mutual distances between these points are at least ε. As in part (1) it can be easily shown that $\mathcal{F}(\varepsilon)$ is closed in the Banach–Mazur metric. Since $\mathcal{F}(\varepsilon) \cap \mathcal{D}_{N_s} = \emptyset$ and $\mathcal{D}_{N_s}$ is dense (by part (1)), the set $\mathcal{F}(\varepsilon)$ is nowhere dense. We have that

$$\mathcal{K} \setminus \mathcal{D}_{N_s} = \bigcup_{n \in \mathbb{N}} \mathcal{F}\left(\frac{1}{n}\right). \quad ∎$$

The proof of Theorem 2.1′ is similar, although it is more technical and we shall only sketch it. We proceed as in the proof of Theorem 2.1. The only difference is that (2.2) is not a John decomposition since

$$\begin{aligned} u =& c_1 \left\|z_1'\right\|^2 \cdot z_1 + c_2 \left\|z_2'\right\|^2 \cdot z_2 + \left(c_2 - \frac{c_1 \alpha^2}{2}\right) \cdot x_2 + \sum_{i=1}^{m} c_i x_i \otimes x_i \\ =& c_1 (\left\|z_1'\right\| z_1' + \left\|z_2'\right\| z_2' - x_1) - \frac{c_1 \alpha^2}{2} x_2 \neq 0 \end{aligned}$$

and (1.4) does not hold. However, $u \in \operatorname{span}\{z_1', x_2\}$ and $\|u\| = O(\alpha^2)$, so we can find coefficients d_1 and d_2 which are close to $c_1 \left\|z_1'\right\|$ and $c_2 - c_1 \alpha^2 / 2$ respectively so that the operator

$$T = d_1 z_1 \otimes z_1 + c_1 \left\|z_2'\right\| z_2 \otimes z_2 + d_2 x_2 \otimes x_2 + \sum_{i=3}^{m} c_i x_i \otimes x_i \tag{2.3}$$

satisfies $\|T - \mathrm{id}\| = O(\alpha^2)$ and

$$d_1 z_1 + c_1 \left\|z_2'\right\| z_2 + d_2 x_2 + \sum_{i=3}^{m} c_i x_i = 0. \tag{2.4}$$

Thus (2.3), (2.4) is an approximate John decomposition, and we can use the construction of Section 4 to obtain an approximating body $\tilde{K}$ with the desired properties. ∎

3. Approximate John decomposition

Before constructing a new body with a small number of contact points, we find for a given body an approximate decomposition of the identity operator. We get this decomposition in several steps. At each step we select randomly a subset of the contact points and after it move the body so as to preserve (1.5).

LEMMA 3.1: *Let B be a convex body in $\mathbb{R}^n$, so that its John ellipsoid is B_2^n. Then there exist*

$$m \leq C(\varepsilon) \cdot n \cdot \log^3 n$$

contact points $x_1, \ldots, x_m$ and a vector u, $\|u\| \leq \frac{C(\varepsilon)}{\sqrt{n}\log^{3/2} n}$, so that the identity operator in $\mathbb{R}^n$ has the following representation:

$$\text{id} = \frac{n}{m}\sum_{i=1}^{m}(x_i + u) \otimes (x_i + u) + S, \tag{3.1}$$

where

$$\sum_{i=1}^{m}(x_i + u) = 0 \tag{3.2}$$

and

$$\|S\colon \ell_2^n \to \ell_2^n\| < \varepsilon. \tag{3.3}$$

Remark 3.1: Denote $\tilde{B} = B + u$. Then from (3.2) it follows that $0 \in \text{Int}\tilde{B}$ and the Minkowski functional for $\tilde{B}$ is well defined.

Proof: Let $\varepsilon > 0$ and let

$$\text{id} = \sum_{j=1}^{k} \bar{c}_j \bar{x}_j \otimes \bar{x}_j,$$
$$\sum_{j=1}^{k} \bar{c}_j \bar{x}_j = 0$$

be a John decomposition for the body B. Set $M = \left[\frac{4nk}{\varepsilon}\right]$ and $N_j = \left[\frac{\bar{c}_j M}{n}\right]$ or $N_j = \left[\frac{\bar{c}_j M}{n}\right] + 1$, so that $\sum_{j=1}^{k} N_j = M$. Form the sequence $x_1, \ldots, x_M$ by repeating N_j times each term $\bar{x}_j$. Define

$$\bar{T}_0 = \frac{n}{M}\sum_{i=1}^{M} x_i \otimes x_i.$$

Then

$$\left\|\mathrm{id} - \bar{T}_0\right\| = \left\|\sum_{j=1}^{k}\left(\bar{c}_j - \frac{N_j n}{M}\right)\bar{x}_j \otimes \bar{x}_j\right\| \le \frac{n}{M}\sum_{j=1}^{k}\|\bar{x}_j \otimes \bar{x}_j\| \le \frac{\varepsilon}{4}$$

and

$$\left\|\frac{n}{M}\sum_{j=1}^{M} x_i\right\| = \left\|\sum_{j=1}^{k}\left(\bar{c}_j - \frac{N_j n}{M}\right)\bar{x}_j\right\| \le \frac{\varepsilon}{4}.$$

Put

$$u_0 = -\frac{1}{M}\sum_{i=1}^{M} x_i,$$

$$T_0 = \frac{n}{M}\sum_{i=1}^{M}(x_i + u_0) \otimes (x_i + u_0).$$

Then

$$\left\|T_0 - \bar{T}_0\right\| = \left\|\frac{n}{M}\sum_{i=1}^{M}(x_i \otimes u_0 + u_0 \otimes x_i) + n u_0 \otimes u_0\right\| = n\left\|u_0 \otimes u_0\right\| \le \frac{\varepsilon^2}{16n}.$$

Let $\mu_1, \dots, \mu_M$ be independent Bernoulli variables taking values 0 and 1 with probability 1/2. Define an operator

$$\bar{T}_1 = 2\frac{n}{M}\sum_{i \in I_1}(x_i + u_0) \otimes (x_i + u_0),$$

where I_1 is the set of indices i for which $\mu_i = 1$. With probability greater than 3/4, $M/4 \le |I_1| \le 3M/4$. To estimate the norm of $\bar{T}_1 - T_0$ use the following

LEMMA 3.2: *Let $y_1, \dots, y_M$ be vectors in $\mathbb{R}^n$, $\varepsilon_1, \dots, \varepsilon_M$ be independent Bernoulli variables, taking values $1, -1$ with probability 1/2. Then*

$$\mathbb{E}\left\|\sum_{i=1}^{M}\varepsilon_i y_i \otimes y_i\right\| \le C \log n \sqrt{\log M} \cdot \max_{i=1,\dots,m}\|y_i\| \cdot \left\|\sum_{i=1}^{M} y_i \otimes y_i\right\|^{1/2}$$

for some absolute constant C.

The proof of Lemma 3.2 is based on entropy estimates of Rademacher random variables and we postpone it to the end of the section. Taking $y_i = x_i + u_0$, we get from Lemma 3.2 that, with probability greater than 1/2,

$$\left\|\bar{T}_1 - T_0\right\| \le 4C\sqrt{\frac{n}{M}}\log n\sqrt{\log M}. \tag{3.4}$$

Denote

$$u_1 = -\frac{1}{|I_1|}\sum_{i\in I_1}(x_i+u_0).$$

Since $\sum_{i=1}^{M}(x_i+u_0)=0$,

$$\mathbb{E}\left\|\sum_{i=1}^{M}\mu_i(x_i+u_0)\right\| = \mathbb{E}\left\|\sum_{i=1}^{M}(\mu_i-\tfrac{1}{2})(x_i+u_0)\right\| \le \sqrt{M}.$$

Hence we can choose the set I_1 so that $|I_1|\ge M/4$, $\|u_1\|\le 4/\sqrt{|I_1|}$ and (3.4) holds. Define

$$T_1 = 2\frac{n}{M}\sum_{i\in I_1}(x_i+u_0+u_1)\otimes(x_i+u_0+u_1).$$

Then

$$\|T_1-\bar{T}_1\| = \frac{2n|I_1|}{M}\cdot\|u_1\otimes u_1\| \le \frac{32n}{M}.$$

Proceeding this way, we construct by induction a sequence of sets $\{1,\dots,M\} = I_0\supset I_1\supset\cdots\supset I_s$ and a sequence of vectors $u_0,u_1,\dots,u_s$, so that

$$|I_{j+1}| \le \frac{3}{4}\cdot|I_j|,$$

$$\|u_j\| \le \frac{4}{\sqrt{|I_j|}},$$

$$\sum_{i\in I_j}(x_i+u_0+\cdots+u_j)=0,$$

and for the operator

$$T_j = \frac{2^j\cdot n}{M}\sum_{i\in I_j}(x_i+u_0+\cdots+u_j)\otimes(x_i+u_0+\cdots+u_j)$$

one has

$$\|T_{j+1}-T_j\| \le C\cdot\sqrt{\frac{n}{|I_j|}}\cdot\log n\cdot\sqrt{\log|I_j|}. \tag{3.5}$$

Summing the inequalities (3.5) we get

$$\begin{aligned}\|\mathrm{id}-T_s\| &\le \|\mathrm{id}-T_0\| + \|T_0-T_1\| + \cdots + \|T_{s-1}-T_s\| \\ &\le \frac{\varepsilon}{4} + C\cdot\sqrt{n}\cdot\log n\cdot\left(\frac{\sqrt{\log|I_0|}}{\sqrt{|I_0|}} + \frac{\sqrt{\log|I_1|}}{\sqrt{|I_1|}} + \cdots + \frac{\sqrt{\log|I_{s-1}|}}{\sqrt{|I_{s-1}|}}\right).\end{aligned}$$

Choose s so that the last expression will be less than $\varepsilon/2$. Simple calculations show that in this case $|I_s| \le C(\varepsilon) n \log^3 n$ and

$$\|u_0 + u_1 + \cdots + u_s\| \le \frac{C(\varepsilon)}{\sqrt{n}\log^{3/2} n}$$

Denote $m = |I_s|$, $\quad u = u_1 + u_2 + \cdots + u_s$ and renumerate the sequence $1, \ldots, M$, so that I_s becomes its initial segment $\{1, \ldots, m\}$. Then, (3.2) holds and

$$\|\mathrm{id} - A \sum_{i=1}^{m} (x_i + u) \otimes (x_i + u)\| < \frac{\varepsilon}{2}, \tag{3.6}$$

where $A = 2^s n/M$. To get (3.1), (3.3) from this, take the trace. By (3.6), we have $|n - A \cdot m| < \frac{1}{2}\varepsilon \cdot n$, so

$$\left\|\mathrm{id} - \frac{n}{m} \sum_{i=1}^{m} (x_i + u) \otimes (x_i + u)\right\| < \varepsilon. \qquad ∎$$

Proof of Lemma 3.2: Without loss of generality, we may assume that $\max_{i=1,\ldots,m} \|y_i\| = 1$. By an inequality of Dudley [L-T],

$$\mathbb{E} \left\| \sum_{i=1}^{M} \varepsilon_i y_i \otimes y_i \right\| = \mathbb{E} \sup_{\|y\| \le 1} \left| \sum_{i=1}^{M} \varepsilon_i \langle y, y_i \rangle^2 \right| \le C \cdot \int_0^\infty \Big(\log N(B_2^n, \delta, u) \Big)^{1/2} du.$$

Here $N(B_2^n, \delta, u)$ is the maximal cardinality of a u-net in B_2^n in the metric δ, where

$$\delta(x, y) = \Big(\sum_{i=1}^{M} (\langle x, y_i \rangle^2 - \langle y, y_i \rangle^2)^2 \Big)^{1/2}.$$

Denote $\|y\|_Y = \sup_{i=1,\ldots,M} |\langle y, y_i \rangle|$. The metric δ can be easily estimated by this norm:

$$\begin{aligned} \delta(x, y) &\le \left(\sum_{i=1}^{M} (\langle x, y_i \rangle + \langle y, y_i \rangle)^2 \right)^{1/2} \cdot \sup_{i=1,\ldots,M} |\langle x - y, y_i \rangle| \\ &\le \left\| \sum_{i=1}^{M} y_i \otimes y_i \right\|^{1/2} \cdot \|x + y\| \cdot \|x - y\|_Y \le \rho \cdot \|x - y\|_Y, \end{aligned}$$

where $\rho = 2 \left\| \sum_{i=1}^{M} y_i \otimes y_i \right\|^{1/2}$. So

$$N(B_2^n, \delta, u) \le N\left(B_2^n, \|\cdot\|_Y, \frac{1}{\rho} u \right),$$

and

$$\mathbb{E}\left\|\sum_{i=1}^{M}\varepsilon_i y_i\otimes y_i\right\|\le C\rho\cdot\int_0^{\infty}\Big(\log N(B_2^n,\|\cdot\|_Y,v)\Big)^{1/2}dv.$$

If $v>1$, then $N(B_2^n,\|\cdot\|_Y,v)=1$, because $\|y\|_Y\le\|y\|$. A standard volume estimate gives

$$N(B_2^n,\|\cdot\|_Y,v)\le N(B_2^n,\|\cdot\|,v)\le\Big(1+\frac{2}{v}\Big)^n. \tag{3.7}$$

By an inequality of Pajor and Tomczak-Jaegermann [Pa-T-J], we get

$$\Big(\log N(B_2^n,\|\cdot\|_Y,v)\Big)^{1/2}\le\frac{c}{v}\mathbb{E}\ \|g\|_Y\,, \tag{3.8}$$

where g is a standard Gaussian vector in the space $\mathbb{R}^n$. The estimate of $\mathbb{E}\ \|g\|_Y$ is well known. Denote $g_i=\langle g,x_i\rangle, i=1,\dots,M$. Then

$$\begin{aligned}\mathbb{E}\ \|g\|_Y=\mathbb{E}\sup_{i=1,\dots,M}|g_i|&\le\mathbb{E}\left(\sum_{i=1}^{M}|g_i|^{\log M}\right)^{1/\log M}\\ &\le\left(\mathbb{E}\sum_{i=1}^{M}|g_i|^{\log M}\right)^{1/\log M}\le CM^{1/\log M}\cdot\sqrt{\log M}.\end{aligned} \tag{3.9}$$

Combining the estimates (3.7), (3.8) and (3.9), we have

$$\begin{aligned}\int_0^{\infty}\Big(\log N(B_2^n,\|\cdot\|_Y,v)\Big)^{1/2}dv&\le\int_0^{A}\Big(n\cdot\log(1+\frac{2}{v})\Big)^{1/2}dv+\int_A^{1}C\sqrt{\log M}\frac{dv}{v}\\ &\le A\cdot\sqrt{n}\cdot\log\left(1+\frac{2}{A}\right)+C\cdot\sqrt{\log M}\cdot\log\frac{1}{A}.\end{aligned}$$

To end the proof choose $A=1/\sqrt{n}$. ∎

Remark 3.2: Let B be a convex symmetric body whose John ellipsoid is B_2^n. Let $a_1,\dots,a_m$ be positive numbers and $u_1,\dots,u_m$ be contact points so that (1.4) holds. Then, adding to the collection $u_1,\dots,u_m$ the points $-u_1,\dots,-u_m$, we provide (1.5). Thus, in symmetric case we can always set $u=0$ in Lemma 3.1.

Remark 3.3: One cannot make the coefficient in Lemma 3.2 smaller than $C\sqrt{\log n}$. Indeed, suppose that $M=n\cdot k$ and $y_i=e_j$ for $(j-1)k<i\le jk$. Then,

$$\left\|\sum_{i=1}^{M}\varepsilon_i y_i\otimes y_i\right\|=\left\|\sum_{j=1}^{n}\left(\sum_{i=(j-1)k+1}^{jk}\varepsilon_i\right)e_j\otimes e_j\right\|=\max_{j=1,\dots,n}\left|\sum_{i=(j-1)k+1}^{jk}\varepsilon_i\right|.$$

For sufficiently large k, $k^{-1/2}\sum_{i=1}^{k}\varepsilon_i$ behaves like a Gaussian variable, so

$$\mathbb{E}\left\|\sum_{i=1}^{M}\varepsilon_i y_i\otimes y_i\right\|\geq C\sqrt{k}\sqrt{\log n}=C\sqrt{\log n}\cdot\left\|\sum_{i=1}^{M}y_i\otimes y_i\right\|^{1/2}.$$

4. Construction of the approximating body

Suppose that the body B is embedded into $\mathbb{R}^n$ so that its John ellipsoid is B_2^n. Using the approximate John decomposition (3.1) – (3.3) we construct a body K close to B, having m contact points with its John ellipsoid.

Let $\varepsilon>0$. Denote $\tilde{B}=B+u$, $y_i=x_i+u$ and set

$$T=\mathrm{id}-S=\frac{n}{m}\sum_{i=1}^{m}y_i\otimes y_i,$$

where $\|S\|<\varepsilon/8$. By (3.2)

$$\sum_{i=1}^{m}y_i=0. \tag{4.1}$$

Let $v\in\mathbb{R}^n$, and $\|v\|\leq\varepsilon/\sqrt{n}$ be a vector, which we shall define later. Denote

$$T_v=\frac{n}{m}\sum_{i=1}^{m}(y_i+v)\otimes(y_i+v),$$

$R_v=T_v^{1/2}$ and $\mathcal{E}=\mathcal{E}_v=R_vB_2^n$. By (4.1), for sufficiently small ε,

$$\|T_v-\mathrm{id}\|\leq\|T_v-T\|+\|S\|\leq n\cdot\|v\otimes v\|+\|S\|\leq\varepsilon^2+\frac{\varepsilon}{8}<\frac{\varepsilon}{4}. \tag{4.2}$$

So

$$\left(1-\frac{\varepsilon}{4}\right)\mathcal{E}\subset B_2^n\subset\left(1+\frac{\varepsilon}{4}\right)\mathcal{E}.$$

Denote

$$z_i=\frac{1}{\|y_i+v\|_{\mathcal{E}}}\cdot(y_i+v)$$

and set

$$\tilde{K}=\mathrm{conv}\left(\frac{1}{1+\varepsilon}(\tilde{B}+v),\ z_1,\dots,z_m\right).$$

Since $B\subset B_2^n$ and $\|v\|\leq\varepsilon/\sqrt{n}$, we get that the only contact points of $\tilde{K}$ with $\mathcal{E}$ are $z_1,\dots,z_m$. We prove now that

$$\frac{1}{1+\varepsilon}(\tilde{B}+v)\subset\tilde{K}\subset(1+2\varepsilon)(\tilde{B}+v).$$

The first inclusion is obvious. To prove the second, let $x \in \tilde{K}$ and consider a decomposition of x

$$x = \frac{\alpha_0}{1+\varepsilon} b + \sum_{i=1}^{m} \alpha_i z_i,$$

where $b \in \tilde{B} + v$, $\alpha_i \geq 0$ and $\sum_{i=0}^{m} \alpha_i \leq 1$. Note that $y_i = x_i + u$, $\tilde{B} = B + u$ and since $x_i \in \partial B$, $y_i + v \in \partial(\tilde{B} + v)$, so $\|y_i + v\|_{\tilde{B}+v} = 1$. Since

$$\|u\| \leq \frac{C(\varepsilon)}{\sqrt{n}\log^{3/2} n}, \quad \|v\| \leq \frac{\varepsilon}{\sqrt{n}},$$

we have $\|y_i + v\|_{\mathcal{E}} \geq 1 - \varepsilon$. Then from the triangle inequality it follows that

$$\begin{aligned}\|x\|_{\tilde{B}+v} &\leq \frac{\alpha_0}{1+\varepsilon} + \sum_{i=1}^{m} \alpha_i \cdot \frac{1}{\|y_i + v\|_{\mathcal{E}}} \cdot \|y_i + v\|_{\tilde{B}+v} \\ &\leq \frac{\alpha_0}{1+\varepsilon} + \frac{1}{1-\varepsilon} \sum_{i=1}^{m} \alpha_i \leq 1 + 2\varepsilon.\end{aligned}$$

Define now a decomposition of the identity operator

$$\text{(4.3)} \quad \mathrm{id} = R_v^{-1} \circ T \circ R_v^{-1} = \sum_{i=1}^{m} \frac{n}{m} \cdot \|y_i + v\|_{\mathcal{E}}^2 \cdot R_v^{-1} z_i \otimes R_v^{-1} z_i = \sum_{i=1}^{m} a_i u_i \otimes u_i,$$

where

$$a_i = \frac{n}{m} \cdot \|y_i + v\|_{\mathcal{E}}^2, \qquad u_i = R_v^{-1} y_i.$$

Finally, define a body $K = R_v^{-1}\tilde{K}$. Then $K \subset B_2^n$ and the only contact points of K with B_2^n are $u_1, \ldots, u_m$. If the vector v is chosen so that

$$\text{(4.4)} \qquad \sum_{i=1}^{m} a_i u_i = 0,$$

then (4.2), (4.3) become a John decomposition of the body K and, by [J] (see also [B]), B_2^n is the John ellipsoid of K. To end the proof of Theorem 1.1, it remains to find a vector v for which (4.4) holds. Note that by the definition of the norm $\|\cdot\|_{\mathcal{E}}$,

$$\begin{aligned}\sum_{i=1}^{m} a_i u_i &= \frac{n}{m} \cdot R_v^{-1} \left(\sum_{i=1}^{m} \left\| R_v^{-1}(y_i + v) \right\|^2 \cdot \frac{y_i + v}{\left\| R_v^{-1}(y_i + v) \right\|} \right) \\ &= \frac{n}{m} \cdot R_v^{-1} \left(\sum_{i=1}^{m} \langle y_i + v, T_v^{-1}(y_i + v) \rangle^{1/2} (y_i + v) \right).\end{aligned}$$

Thus what remains to prove is the following

LEMMA 4.1: *Let $\varepsilon > 0$, y_i, $i = 1, \ldots, m$ be as above. There exists a vector v, satisfying the following conditions:*

$$\text{(i)} \qquad \|v\| \le \frac{\varepsilon}{\sqrt{n}};$$

$$\text{(ii)} \qquad \sum_{i=1}^{m} \langle y_i + v, T_v^{-1}(y_i + v)\rangle^{1/2}(y_i + v) = 0,$$

where

$$T_v = \frac{n}{m} \sum_{i=1}^{m} (y_i + v) \otimes (y_i + v).$$

Proof: By (4.1), we can rewrite (ii) as

$$\sum_{i=1}^{m} \left(\langle y_i + v, T_v^{-1}(y_i + v)\rangle^{1/2} - 1 \right) y_i + \sum_{i=1}^{m} \langle y_i + v, T_v^{-1}(y_i + v)\rangle^{1/2} v = 0.$$

Define a function F: $\frac{\varepsilon}{\sqrt{n}} B_2^n \to \mathbb{R}^n$ by

$$F(v) = -\left(\sum_{i=1}^{m} \langle y_i + v, T_v^{-1}(y_i + v)\rangle^{1/2} \right)^{-1} \cdot \left(\sum_{i=1}^{m} \left(\langle y_i + v, T_v^{-1}(y_i + v)\rangle^{1/2} - 1 \right) y_i \right).$$

By the Brouwer fixed point theorem it is enough to prove that F maps $\frac{\varepsilon}{\sqrt{n}} B_2^n$ to itself. Let $\|v\| \le \varepsilon/\sqrt{n}$. Remark first that by (4.2),

$$\langle y_i + v, T_v^{-1}(y_i + v)\rangle^{1/2} \ge (1 - \varepsilon). \tag{4.5}$$

For any vector $w \in B_2^n$ and any $\alpha_1, \ldots, \alpha_m$,

(4.6)

$$\left| \langle \sum_{i=1}^{m} \alpha_i y_i, w\rangle \right| \le \sqrt{m} \max_{i=1,\ldots,m} |\alpha_i| \cdot \left(\sum_{i=1}^{m} \langle y_i, w\rangle^2 \right)^{1/2} \le \frac{m}{\sqrt{n}} \|T_0\| \cdot \max_{i=1,\ldots,m} |\alpha_i|,$$

where

$$T_0 = \frac{n}{m} \sum_{i=1}^{m} y_i \otimes y_i, \qquad \|T_0\| \le 1 + \frac{\varepsilon}{4}.$$

Let $1 \le i \le m$. For a sufficiently large n we have

$$\begin{aligned}\left|\langle y_i+v, T_v^{-1}(y_i+v)\rangle^{1/2}-1\right| &\le \left|\langle y_i+v,(y_i+v)\rangle^{1/2}-1\right| + 2\,\|\mathrm{id}-T_v\| \\ &\le \frac{2\varepsilon}{\sqrt{n}} + 2\cdot\frac{\varepsilon}{4} \le \frac{2\varepsilon}{3}.\end{aligned} \tag{4.7}$$

So by (4.6), (4.7),

$$\left\|\sum_{i=1}^{m}\left(\langle y_i+v, T_v^{-1}(y_i+v)\rangle^{1/2}-1\right)y_i\right\| \le \frac{m}{\sqrt{n}}(1+\varepsilon)\cdot\frac{2\varepsilon}{3}.$$

Finally, by (4.5), this means that $F(v) \in \frac{\varepsilon}{\sqrt{n}}B_2^n$. ∎

Remark 4.1: Let B be a convex symmetric body whose John ellipsoid is B_2^n. Then by Remark 3.2 we can take $u=0$. It is easy to see that in this case we can take also $v=0$. From the proof it follows that we can construct a convex symmetric body K and an operator R_0 so that the John ellipsoid of K is B_2^n,

$$\frac{1}{1+\varepsilon}B \subset R_0K \subset (1+\varepsilon)B$$

and $\|R_0-\mathrm{id}\| \le 1+\varepsilon$.

5. Lower estimate

In this section we prove Theorem 1.2. For convenience convex centrally symmetric bodies will be called balls. We show that there exists a ball $\Gamma \subset \mathbb{R}^n$ which cannot be approximated by any convex body having a small number of contact points. The ball Γ will be constructed by a random procedure. Let $g_1(\omega),\dots,g_{2n}(\omega) \in \mathbb{R}^n$, $\omega \in \Omega$ be independent Gaussian vectors. This means that the coordinates of each $g_i(\omega)$ are independent mean zero Gaussian variables normalized by $\mathbb{E}\,\|g_i\|^2 = 1$. Set

$$\Gamma(\omega) = \mathrm{abs\ conv}(g_1(\omega),\dots,g_{2n}(\omega)).$$

We prove that with probability close to 1 the ball $\Gamma(\omega)$ has the desired property. The balls $\Gamma(\omega)$ were introduced by Gluskin [G1] and they serve as a basic source of counterexamples in many problems of the Local Theory [G2], [B], [S1] etc. In particular in [S2] Szarek has shown that for some ω the ball $\Gamma(\omega)$ cannot be embedded in $\mathbb{R}^n$ between B_2^n and CB_∞^n, where C does not depend on n. We use here a modification of his argument.

Proof of Theorem 1.2: We begin to prove (1). We take as Γ the random ball $\Gamma(\omega)$ and show that the probability that $d(\Gamma(\omega), K) \leq t$ for some ball K having a small number of contact points is less than 1. We construct first a special embedding of the ball K.

LEMMA 5.1: *Let K be an n-dimensional ball in $\mathbb{R}^n$ having $2m$ contact points. Then K can be embedded into an n-dimensional subspace Y of $\mathbb{R}^m$ so that the John ellipsoid of K becomes $B_2^m \cap Y$ and, if $e_1, \ldots, e_m$ is the standard basis of $\mathbb{R}^m$, then*

$$P_Y e_j \in K \quad \text{for } j = 1, \ldots, m.$$

Here $P_Y\colon \mathbb{R}^m \to \mathbb{R}^m$ is the orthogonal projection onto Y.

Proof: First we embed K into $\mathbb{R}^n$ so that B_2^n becomes its John ellipsoid. Let

$$\text{id} = \sum_{i=1}^{\bar{m}} c_i u_i \otimes u_i, \quad \bar{m} \leq m \tag{5.1}$$

be the John decomposition for K. Let $f_1, \ldots, f_n$ be the standard basis of $\mathbb{R}^n$. We consider $\mathbb{R}^n$ as a coordinate subspace of $\mathbb{R}^{\bar{m}}$. Define vectors $v_1, \ldots, v_n \in \mathbb{R}^{\bar{m}}$ by

$$v_i(j) = \langle \sqrt{c_j} u_j, f_i \rangle, \qquad i = 1, \ldots, n, \quad j = 1, \ldots, \bar{m}.$$

By (5.1) the vectors $v_1, \ldots, v_n$ form an orthonormal system in $\mathbb{R}^{\bar{m}}$ and we can complete it to an orthonormal basis $v_1, \ldots, v_{\bar{m}}$. Let $e_1, \ldots, e_{\bar{m}}$ be the dual basis: $v_i(j) = e_j(i)$ for $i, j = 1, \ldots, \bar{m}$. Then the vectors $\sqrt{c_1} u_1, \ldots, \sqrt{c_{\bar{m}}} u_{\bar{m}}$ can be obtained from the vectors $e_1, \ldots, e_{\bar{m}}$ by restricting them to the n first coordinates. We shall consider $e_1, \ldots, e_{\bar{m}}$ as the standard basis of $\mathbb{R}^{\bar{m}}$. Denote Y the subspace of $\mathbb{R}^{\bar{m}}$ spanned by the vectors $u_1, \ldots, u_{\bar{m}}$ and let P_Y be the orthogonal projection onto it. Then the John ellipsoid of $K \subset Y$ is $B_2^m \cap Y$ and

$$P_Y e_i = \sqrt{c_i} u_i \qquad \text{for } i = 1, \ldots, \bar{m}.$$

Since $0 \leq c_i \leq 1$ and $u_i \in K$, we get that $P_Y e_i \in K$. Finally consider $\mathbb{R}^{\bar{m}}$ as a coordinate subspace of $\mathbb{R}^m$. ∎

Consider independent Gaussian vectors $g_1(\omega), \ldots, g_{2n}(\omega)$ in $\mathbb{R}^n$ and an $n \times 2n$ Gaussian matrix $G(\omega)$ whose columns are $g_1(\omega), \ldots, g_{2n}(\omega)$. Denote by B_1^N the unit ball of the space ℓ_1^N. Set

$$\Gamma(\omega) = G(\omega) B_1^{2n}.$$

Suppose that for some ω there exists a ball K having $2m \le (1+c_0/t^2)\cdot 2n$ contact points for which $d(\Gamma(\omega), K) \le t$. By Lemma 5.1 we can embed K into a subspace Y of $\mathbb{R}^m$ so that

$$P_Y B_1^m \subset K \subset P_Y B_2^m. \tag{5.2}$$

Let $S\colon Y \to \mathbb{R}^n$ be an operator such that

$$\|S\colon K \to \Gamma(\omega)\| = 1, \qquad \|S^{-1}\colon \Gamma(\omega) \to K\| = d(\Gamma(\omega), K) \le t.$$

We have the following diagram:

$$\begin{array}{ccccc}
B_1^m & \xrightarrow{P_Y} & K & \xrightarrow{\text{id}} & B_2^m \cap Y \\
 & & \Big\downarrow{\scriptstyle S} & & \\
B_1^{2n} & \xrightarrow{G(\omega)} & \Gamma(\omega) & &
\end{array}$$

By the lifting property there exists an operator $A\colon \mathbb{R}^m \to \mathbb{R}^{2n}$ so that $\|A\colon B_1^m \to B_1^{2n}\| \le 1$ and

$$SP_Y = G(\omega)A. \tag{5.3}$$

By (5.2), (5.3),

$$\frac{1}{t}S^{-1}\Gamma(\omega) \subset K \subset P_Y B_2^m = S^{-1}G(\omega)AB_2^m.$$

Hence the existence of the ball K implies that

$$g_j(\omega) \in t \cdot G(\omega)AB_2^m \qquad \text{for } j = 1, \dots, 2n.$$

Part (1) of the theorem follows now from the next lemma which is close to Theorem 1.2 of [S2]. For the proof of part (1) we take $P_0 = \text{id}$ in the lemma; the more general case will be used in the proof of part (2) and in Section 6.

LEMMA 5.2: *Let $t > 0$ and let $m \le (1 + c_0/t^2)\cdot n$ for some absolute constant c_0. Let $G(\omega)$ be an $n \times 2n$ Gaussian matrix whose columns are $g_1(\omega), \dots, g_{2n}(\omega)$. Then there exists an $\omega \in \Omega$ so that for every operator $A\colon \mathbb{R}^m \to \mathbb{R}^{2n}$, $\|A\colon B_1^m \to B_1^{2n}\| \le 1$ and for every orthogonal projection $P_0\colon \mathbb{R}^n \to \mathbb{R}^n$ with $\dim\ker P_0 \le c_0 n/t^2$,*

$$P_0 g_j(\omega) \notin t \cdot P_0 G(\omega)AB_2^m \tag{5.4}$$

for some $j \in \{1, \ldots, 2n\}$.

Before we prove Lemma 5.2 let us derive from it part (2) of the theorem. As before we take as Γ the random ball

$$\Gamma(\omega) = G(\omega)B_1^{2n}, \qquad \omega \in \Omega.$$

Suppose that for some $\omega \in \Omega$ there exists a convex body D having $m \leq (1 + c_0/t^2) \cdot n$ contact points so that $d(\Gamma(\omega), D) \leq t$. The body D is defined up to an affine transform. Embed it into $\mathbb{R}^n$ so that the John ellipsoid of it will be B_2^n. There is a linear operator $\tilde{S}: \mathbb{R}^n \to \mathbb{R}^n$ and a vector $u \in \mathbb{R}^n$ so that

$$\frac{1}{t}\tilde{S}^{-1}(\Gamma(\omega) + u) \subset D \subset \tilde{S}^{-1}(\Gamma(\omega) + u). \tag{5.5}$$

Define a ball

$$K = \operatorname{conv}(D, -D).$$

Then K has the same John ellipsoid as D and the number of the contact points of K is at most $2m$. Set

$$B(\omega) = \operatorname{conv}(\Gamma(\omega) + u, -(\Gamma(\omega) + u)).$$

By (5.5) we have

$$\frac{1}{t}B(\omega) \subset \tilde{S}K \subset B(\omega).$$

By Lemma 5.1, we can embed K into a subspace Y of $\mathbb{R}^m$ so that

$$P_Y B_1^m \subset K \subset P_Y B_2^m.$$

We shall consider $\tilde{S}$ as an operator from Y to $\mathbb{R}^n$.

Let $P_0: \mathbb{R}^n \to \mathbb{R}^n$ be an orthogonal projection so that $\ker P_0 = \operatorname{span}\{u\}$. Then

$$P_0 B(\omega) = P_0 \Gamma(\omega),$$

so

$$\frac{1}{t}P_0\Gamma(\omega) \subset P_0\tilde{S}K \subset P_0\Gamma(\omega). \tag{5.6}$$

Define $V: Y \to Y$ by

$$V = \tilde{S}^{-1}P_0\tilde{S}.$$

By the lifting property there exists an operator $A\colon \mathbb{R}^m \to \mathbb{R}^{2n}$ so that $\|A\colon B_1^m \to B_1^{2n}\| \le 1$ and

$$\tilde{S}VP_Y = G(\omega)P_0A. \tag{5.7}$$

We obtain the following commutative diagram:

$$\begin{array}{ccccccc}
B_1^m & \xrightarrow{P_Y} & K & \xrightarrow{V} & VK & \xrightarrow{\mathrm{id}} & V(B_2^m \cap Y) \\
 & & {\scriptstyle \tilde{S}}\downarrow & & \downarrow{\scriptstyle \tilde{S}} & & \\
A\downarrow & & B(\omega) & \xrightarrow{P_0} & P_0B(\omega) & & \\
 & & & & \downarrow{\scriptstyle \mathrm{id}} & & \\
B_1^{2n} & \xrightarrow{G(\omega)} & \Gamma(\omega) & \xrightarrow{P_0} & P_0\Gamma(\omega) & &
\end{array}$$

Thus by (5.6), (5.7) we have that

$$\frac{1}{t}P_0\Gamma(\omega) \subset \tilde{S}VK \subset \tilde{S}V(P_YB_2^m) = P_0G(\omega)AB_2^m,$$

and hence

$$P_0g_j(\omega) \in tP_0G(\omega)AB_2^m \qquad \text{for } j = 1, \ldots, 2n.$$

Part (2) of the theorem follows now from Lemma 5.2 ∎

Proof of Lemma 5.2: The proof of the lemma consists of two steps. First we estimate the measure of those ω for which (5.4) is satisfied for a fixed operator A. Then we use an ε-net argument to derive the lemma.

STEP 1: Let c_0 be a constant to be defined later. Set

$$\delta = c_0/t^2.$$

Recall the definition of Kolmogorov numbers. Let V be an operator in ℓ_2^m and let $k \le m$. Denote

$$d_k(V) = \min \|P_kV\|,$$

where the minimum is taken over all orthogonal projections P_k with k-dimensional kernel.

Let $\bar{G}(\omega)$ be an $m \times 2n$ Gaussian matrix. By Proposition 4.1 of [S2] for some absolute constants $\bar{C}, \tilde{c}, \tilde{C}, C_1$

$$\begin{aligned}\mathcal{P}\{d_k(\bar{G}(\omega)\bar{A}) \le \bar{C}\cdot\frac{m-k}{m} \text{ for all } \bar{A}\colon B_1^m \to B_1^{2n},\ \|\bar{A}\| \le 1\} \\ \ge 1 - \tilde{C}\exp(-\tilde{c}\cdot(m-k)^2)\end{aligned} \tag{5.8}$$

for every k satisfying $2^{-4}m \geq m - k \geq C_1(mn^3 \log m)^{1/5}$. Take $k = (1 - 2\delta)n$. Since the matrix $G(\omega)$ can be considered as the n first rows of the matrix $\bar{G}(\omega)$,

$$d_k(G(\omega)\bar{A}) \leq d_k(\bar{G}(\omega)\bar{A}). \tag{5.9}$$

From (5.8), (5.9), it follows that there exists a set $E_1 \subset \Omega$ of probability at most $\tilde{C} \cdot \exp(-\tilde{c} \cdot 9\delta^2 n^2)$ so that

$$d_{(1-2\delta)n}(G(\omega)\bar{A}) \leq \bar{C} \cdot 3\delta = C^*\delta$$

for all $\omega \notin E_1$ and all $\bar{A}\colon \mathbb{R}^m \to \mathbb{R}^{2n}$, $\|\bar{A}\colon B_1^m \to B_1^{2n}\| \leq 1$.

By the definition of Kolmogorov numbers,

$$\begin{aligned} &\min\{\|PG(\omega)A\| \mid \dim\ker P = (1-\delta)n,\ \ker P \supset \ker P_0\} \\ \leq &\min\{\|P_{(1-2\delta)n}G(\omega)A\| \mid \dim\ker P_{(1-2\delta)n} = (1-2\delta)n\} = d_{(1-2\delta)n}(G(\omega)A). \end{aligned}$$

Hence there exists an orthogonal projection $P\colon \mathbb{R}^m \to \mathbb{R}^m$ depending on $G(\omega)A$ so that $\operatorname{rank} P = \delta n$,

$$\ker P \supset \ker P_0 \tag{5.10}$$

and

$$PG(\omega)AB_2^m \subset C^*\delta \cdot PB_2^m. \tag{5.11}$$

It follows from (5.10) that $PP_0 = P$.

We are going to estimate the probability that $\|Pg_j(\omega)\| \leq Ct\delta$ for all $j = 1, \ldots, 2n$. For P which does not depend on ω it can be easily done. Although this is not the case, this estimate will be essentially the same as for P independent of ω. More precisely, let $Q\colon \mathbb{R}^{2n} \to \mathbb{R}^{2n}$ be an orthogonal projection onto $\operatorname{Im}(A)$ and set $\tilde{Q} = \mathrm{id} - Q$. Then $G(\omega)QA$ and $G(\omega)\tilde{Q}A$ are independent random matrices. Note that in fact the projection P depends only on $G(\omega)|_{\operatorname{Im}(A)}A = G(\omega)QA$. Since $\operatorname{rank}(A) = m$, $\operatorname{rank}\tilde{Q} = 2n - m \geq n/2$. Let $\tilde{g}$ be a normalized Gaussian vector independent from $G(\omega)$. It follows from [S2, p. 917–918] that there exist absolute constants C' and a, so that

$$\mathcal{P}\{\max_{j=1,\ldots,2n} \|Pg_j(\omega)\| \leq 3t \cdot C^*\delta\} \leq [\mathcal{P}\{\|P\tilde{g}\| \leq C' \cdot 3t \cdot C^*\delta\}]^{2an}.$$

Note that $P\tilde{g}$ is a δn-dimensional Gaussian variable normalized by $\mathbb{E}\,\|P\tilde{g}\|^2 = \delta$. Thus the above expression is less than

$$(e^{1/2}C' \cdot 3t \cdot C^*\sqrt{\delta})^{\delta n \cdot 2an}.$$

Set $c_0 = (e^{3/2} \cdot 3C^*C')^{-2}$. We conclude that

$$\mathcal{P}\left\{\max_{j=1,\dots,2n} \|Pg_j(\omega)\| \le \frac{3C^*c_0}{t}\right\} \le \exp\left(-\frac{2ac_0}{t^2}\cdot n^2\right). \tag{5.12}$$

STEP 2: The ε-net argument. Using (5.11) and (5.12) we prove that for some ω and for all operators A there exists $j \le m$, so that

$$P_0 g_j(\omega) \notin 3t \cdot P_0 G(\omega) A B_2^n.$$

For $\lambda > 0$ put

$$E_\lambda = \{\omega \mid \|G(\omega)\colon B_2^{2n} \to B_2^n\| > \lambda\}.$$

By Lemma 2.8 of [S2], there exists a λ for which $\mathcal{P}(E_\lambda) \le \exp(-Cn/8)$ for some absolute constant C. Set

$$\varepsilon = \frac{C^* c_0}{t^2\lambda}$$

and select an ε-net $\mathcal{A}$ from the set $\{A\colon \mathbb{R}^m \to \mathbb{R}^{2n} \mid \|A\colon B_1^m \to B_1^{2n}\| \le 1\}$ in $\|\cdot\|_{2\to 2}$ norm. By Claim 4.5(b) of [S2] we have

$$\operatorname{card}\mathcal{A} \le \exp\left(\frac{Cm\cdot(2n\log 2n)^{1/2}}{\varepsilon}\right) \le \exp(\bar{C}t^2 n^{3/2}\log^{1/2} n) \le \exp\left(\frac{ac_0}{t^2}\cdot n^2\right)$$

provided $t^4 \le (ac_0/\bar{C})\cdot n^{1/2}\log^{-1/2} n$. Hence with probability at least

$$\begin{aligned} &1 - \operatorname{card}\mathcal{A}\cdot\exp\left(-\frac{2ac_0}{t^2}\cdot n^2\right) - \mathcal{P}(E_1)\\ \le&1 - \exp\left(-\frac{ac_0}{t^2}\cdot n^2\right) - \tilde{C}\cdot\exp\left(-\tilde{c}\cdot\frac{9c_0^2}{t^2}\cdot n^2\right)\end{aligned}$$

for every $\bar{A} \in \mathcal{A}$ there exists a projection $P\colon \mathbb{R}^m \to \mathbb{R}^m$ with $\operatorname{rank} P = c_0 n/t^2$ so that

$$PP_0 = P, \tag{5.13}$$

$$PG(\omega)\bar{A}B_2^m \subset C^*\frac{c_0}{t^2}\cdot PB_2^m, \tag{5.14}$$

and

$$\max_{j=1,\ldots,2n} \|Pg_j(\omega)\| > \frac{3C^* c_0}{t}. \tag{5.15}$$

Choose $\omega \notin E_\lambda$ for which (5.13) – (5.15) hold for every $\bar{A} \in \mathcal{A}$. Let $A\colon \mathbb{R}^m \to \mathbb{R}^{2n}$ be an operator, $\|A\colon B_1^m \to B_1^{2n}\| \le 1$. There exists an operator $\bar{A} \in \mathcal{A}$ so that $\|A - \bar{A}\| \le \varepsilon$. Let P be a projection for which (5.13) – (5.15) hold for $\bar{A}$. Suppose that for every $j = 1, \ldots, 2n$,

$$P_0 g_j(\omega) \in t \cdot P_0 G(\omega) A B_2^m.$$

Then by (5.13), (5.14) for all j

$$\begin{aligned} Pg_j(\omega) \in& t \cdot PG(\omega)\bar{A}B_2^m + t \cdot PG(\omega)(A - \bar{A})B_2^m \\ &\subset \left(\frac{2C^* c_0}{t} + t \cdot \|G(\omega)\| \cdot \|(A - \bar{A})\|\right) \cdot PB_2^m. \end{aligned}$$

Hence

$$\max_{j=1,\ldots,2n} \|Pg_j(\omega)\| \le \frac{2C^* c_0}{t} + t\lambda\varepsilon \le \frac{3C^* c_0}{t}$$

and this contradicts (5.15). ∎

6. Dvoretzky–Rogers type factorizations

In this section we use the notation $\|T\colon X \to Y\|$ as well as $\|T\colon B_X \to B_Y\|$ for the norm of an operator T between Banach spaces X and Y with unit balls B_X and B_Y.

The classical result of Dvoretzky–Rogers states that for every Banach space X of dimension n^2 there exists an n-dimensional subspace Y and a factorization $\mathrm{id} = \alpha \circ \beta$ of the identity operator in $\mathbb{R}^n$, so that $\|\beta\colon \ell_2^n \to Y\| \cdot \|\alpha\colon Y \to \ell_\infty^n\| \le 8$. This means that some section of the unit ball of X can be embedded between the Euclidean ball and the cube. In [S2] Szarek proved that for every n there exists a convex symmetric body Γ which cannot be embedded into $\mathbb{R}^n$ between B_2^n and $t \cdot B_\infty^n$ if $t < C(n/\log n)^{1/10}$. However in [B-S] it was shown that every convex symmetric body possesses a section of a proportional dimension k which can be embedded between B_2^k and $C \cdot B_\infty^k$ for some constant C depending on k/n. The estimate of $C(k/n)$ was improved later in [S-T], [Gi1], [Gi2]. Up to now, the best result is the following

THEOREM 6.0 ([Gi2]): *Let X be an n-dimensional Banach space. For every $\varepsilon > 0$ and for some $m \geq (1-\varepsilon)n$ there exists a factorization* $\mathrm{id} = \alpha \circ \beta$, *where*

$$\|\alpha\colon \ell_2^m \to X\| \cdot \|\beta\colon X \to \ell_\infty^m\| \leq \frac{C}{\varepsilon}.$$

Using the decomposition (1.4) for convex symmetric bodies we can construct a factorization which is somehow dual to that of Theorem 6.0. Instead of embedding a section of the body, we embed the entire body between the Euclidean ball and a cube of larger dimension. More precisely, we have the following

THEOREM 6.1: *Let X be an n-dimensional Banach space. For every $\varepsilon > 0$ there exist $m \leq C(\varepsilon) \cdot n \cdot \log^3 n$ and an orthogonal projection $P\colon \mathbb{R}^m \to \mathbb{R}^m$ of rank n having the following factorization through the space X: $P = T \circ S$, where*

$$\|T\colon X \to \ell_\infty^m\| \cdot \|S\colon \ell_2^m \to X\| \leq (1+\varepsilon) \cdot \|P\colon \ell_2^m \to \ell_\infty^m\|. \tag{6.1}$$

Proof: Let B be the unit ball of the space X^*. Then the John ellipsoid of B is B_2^n. Applying Theorem 1.1 to the body B, and using Remark 4.1, we construct a convex symmetric body K whose John ellipsoid is B_2^n and for which (1.3), (1.4) hold. Let Y be a Banach space whose unit ball is K. We construct first the factorization (6.1) for the space Y^*.

Define an operator $\tilde{T}\colon Y^* \to \mathbb{R}^m$ by

$$\tilde{T}y^* = \left(\sqrt{a_1} \cdot \langle y^*, u_1\rangle, \ldots, \sqrt{a_m} \cdot \langle y^*, u_m\rangle\right), \qquad y^* \in Y^*.$$

Note that if the Euclidean structure in Y^* is defined by the John ellipsoid of K^o then $\tilde{T}\colon \ell_2^n \to \ell_2^m$ is an isometric embedding. Since $u_1, \ldots, u_m$ are contact points of K,

$$\left\|\tilde{T}\colon Y^* \to \ell_\infty^m\right\| = \max_{j=1,\ldots,m} \sqrt{a_j}.$$

Define now an operator $\tilde{S}\colon \mathbb{R}^m \to Y^*$ by

$$\tilde{S}z = \sum_{i=1}^m a_i \langle z, \tilde{T}u_i\rangle u_i$$

and let $P = \tilde{T} \circ \tilde{S}$. Then $P|_{(\tilde{T}Y^*)^\perp} = 0$ and for every $z = \tilde{T}y^*$ we get

$$Pz = \sum_{i=1}^m a_i \langle \tilde{T}y^*, \tilde{T}u_i\rangle \tilde{T}u_i = \sum_{i=1}^m a_i \langle y^*, u_i\rangle \tilde{T}u_i = \tilde{T}y^* = z.$$

So P is an orthogonal projection onto the space $\tilde{T}Y^*$. Since $\tilde{S}\colon \ell_2^m \cap \tilde{T}Y^* \to \ell_2^n$ is an isometry,

$$\|P\colon \ell_2^m \to \ell_\infty^m\| = \left\|P\colon \ell_2^m \cap \tilde{T}Y^* \to \ell_\infty^m\right\| = \left\|\tilde{T}\colon Y^* \to \ell_\infty^m\right\|.$$

By Remark 4.1 there exists an operator $R_0 X \to Y^*$ so that

$$\|R_0\colon X \to Y^*\| \cdot \left\|R_0^{-1}\colon Y^* \to X\right\| \le (1+\varepsilon)^2.$$

To end the proof, set $T = \tilde{T} \circ R_0$ and $S = R_0^{-1} \circ \tilde{S}$. ∎

Remark: Note that for the projection P constructed in the proposition we have $\|P\colon \ell_2^m \to \ell_\infty^m\| = \max_{j=1,\dots,m} \sqrt{a_j} \le \sqrt{(1+\varepsilon)n/m}$, while the minimal norm of $P\colon \ell_2^m \to \ell_\infty^m$ over all orthogonal projections of rank n is not smaller than $\sqrt{n/m}$.

Applying Theorem 1.1 and Remark 4.1 to the calculation of the π_2 norm of the identity operator from a Banach space X to the Euclidean space, whose norm is defined by the John ellipsoid of B_X, we obtain the following refinement of Theorem 3.2.5 of [T-J]:

THEOREM 6.2: *Let X be an n-dimensional Banach space and let B_2^n be the ellipsoid of maximal volume contained in its unit ball B_X. Then for every $\varepsilon > 0$ there exists the following factorization of the identity operator from X to ℓ_2^n:*

$$\text{(6.1)} \qquad \begin{array}{ccc} X & \xrightarrow{\ \mathrm{id}\ } & \ell_2^n \\ {\scriptstyle U}\big\downarrow & & \big\uparrow{\scriptstyle V} \\ \ell_\infty^m & \xrightarrow{\ \sqrt{n/m}\cdot \mathrm{id}\ } & \ell_2^m \end{array}$$

Here $\|U\|, \|V\| \le 1+\varepsilon$ and $m \le C(\varepsilon) \cdot n \cdot \log^3 n$.

Proof: Let B be the unit ball of the space X^*. Then the John ellipsoid of B is B_2^n. Applying Theorem 1.1 to the body B, and using Remark 4.1, we construct a convex symmetric body K whose John ellipsoid is B_2^n and for which (1.3), (1.4) hold. Let Y be a Banach space whose unit ball is K. We construct first the factorization (6.1) for the space Y^*. Define an operator $\tilde{U}\colon \mathbb{R}^n \to \mathbb{R}^m$ by

$$\tilde{U}y^* = \left(\frac{m}{n}a_1 \cdot \langle y^*, u_1\rangle, \dots, \frac{m}{n}a_m \cdot \langle y^*, u_m\rangle\right), \qquad y^* \in Y^*.$$

Since $u_1, \dots, u_m$ are the contact points of K and $\frac{m}{n} a_i \leq 1+\varepsilon$ for $i = 1 \dots m$, $\left\| \tilde{U} \colon Y^* \to \ell_\infty^m \right\| \leq 1+\varepsilon$. Let $e_1, \dots, e_m$ be the standard basis of ℓ_2^m. Define now an operator $\tilde{V} \colon \mathbb{R}^m \to \mathbb{R}^n$ by

$$\tilde{V} = \sqrt{\frac{n}{m}} \sum_{i=1}^{m} e_i \otimes u_i.$$

Then

$$\begin{aligned} \left\| \tilde{V} \right\| &= \sqrt{\frac{n}{m}} \cdot \max \left\{ \sum_{i=1}^{m} \langle x, e_i \rangle \langle y, u_i \rangle \;\middle|\; x \in B_2^m, y \in B_2^n \right\} \\ &\leq \sqrt{\frac{n}{m}} \cdot \max \left\{ \left(\sum_{i=1}^{m} \langle x, e_i \rangle^2 \right)^{1/2} \left(\sum_{i=1}^{m} \langle y, u_i \rangle^2 \right)^{1/2} \;\middle|\; x \in B_2^m, y \in B_2^n \right\} \\ &\leq \max \left\{ \left(\sum_{i=1}^{m} a_i \cdot \langle y, u_i \rangle^2 \right)^{1/2} \;\middle|\; y \in B_2^n \right\} \max_{i=1 \dots m} \sqrt{\frac{n}{m} a_i^{-1}} \leq (1+\varepsilon)^{-1/2}. \end{aligned}$$

It follows from (1.4) that

$$\tilde{V} \circ \sqrt{\frac{n}{m}} \mathrm{id}_{\mathbb{R}^m} \circ \tilde{U} = \mathrm{id}_{\mathbb{R}^n}.$$

We remind the reader now that by Remark 4.1,

$$\|R_0^* \colon X \to Y^*\| \leq 1 + 2\varepsilon \quad \text{and} \quad \left\| (R_0^*)^{-1} \colon \ell_2^n \to \ell_2^n \right\| \leq 1+\varepsilon.$$

To end the proof set

$$U = \tilde{U} \circ R_0^*, \qquad V = (R_0^*)^{-1} \circ \tilde{V}. \qquad \blacksquare$$

Using the results of Section 5 we obtain a lower bound for the norm of the factorization of Theorem 6.0.

THEOREM 6.3: *For every $\varepsilon > 0$ and $n > n(\varepsilon)$ there exists an n-dimensional Banach space X so that every factorization $\mathrm{id} = \alpha \circ \beta$ of the identity operator from ℓ_2^m to ℓ_∞^m with $m \geq (1-\varepsilon)n$ satisfies*

$$\|\alpha \colon \ell_2^m \to X\| \cdot \|\beta \colon X \to \ell_\infty^m\| \geq \frac{C}{\sqrt{\varepsilon}}.$$

Here C is an absolute constant.

Proof: Let X be a Banach space whose unit ball is the polar of the body $\Gamma(\omega)$ constructed in Section 5:

$$B_X = \Gamma(\omega)^o = \{x \in \mathbb{R}^n \mid |\langle x, g_1(\omega)\rangle| \le 1, \dots, |\langle x, g_{2n}(\omega)\rangle| \le 1\}.$$

Here $g_1(\omega), \dots, g_{2n}(\omega) \in \mathbb{R}^n$ are independent Gaussian vectors. We show that for some ω the space X has the property claimed in Theorem 6.3.

Suppose that $\mathrm{id} = \alpha \circ \beta$ is a factorization, so that

$$\|\alpha\colon B_2^m \to B_X\| \le s, \qquad \|\beta\colon B_X \to B_\infty^m\| \le 1.$$

Recall that we use the notation $\|T\colon K \to D\|$ for the norm of the operator T between Banach spaces, whose unit balls are K and D. Put $Z = \alpha(\mathbb{R}^m)$, $K = \Gamma(\omega) \cap Z$. Denote by ν the operator α, considered as an operator from $\mathbb{R}^m$ to X, and by η the operator β restricted to Z. Then $\nu^{-1} = \eta$. Passing to the adjoint operators, we get

$$\|\nu^*\colon K^o \to B_2^m\| \le s.$$

Note that $K^o = P_0\Gamma(\omega)$ for some orthogonal projection P_0 for which $\dim\ker P_0 \le \varepsilon n$. We have the following diagram:

$$\begin{array}{ccccc} B_1^m & \xrightarrow{\eta^*} & K^o & \xrightarrow{\nu^*} & s \cdot B_2^m \\ & & {\scriptstyle P_0}\big\uparrow & & \\ B_1^{2n} & \xrightarrow{G(\omega)} & \Gamma(\omega) & & \end{array}$$

where $G(\omega) = (g_1(\omega), \dots, g_{2n}(\omega))$ is an $n \times 2n$ Gaussian matrix. By the lifting property of ℓ_1^m, there exists an operator $A\colon \mathbb{R}^m \to \mathbb{R}^{2n}$, so that

$$P_0 G(\omega) A = \eta^*$$

and $\|A\colon B_1^m \to B_1^{2n}\| \le 1$. Since $\nu^* K^o \subset s \cdot B_2^m$, we have

$$P_0\Gamma(\omega) = K^o \subset s \cdot \eta^* B_2^m = s \cdot P_0 G(\omega) A B_2^m.$$

Applying Lemma 5.2 with $t = (c_0/\varepsilon)^{1/2}$, we obtain that

$$s = \|\alpha\colon B_2^m \to \Gamma(\omega)^o\| \ge t. \qquad \blacksquare$$

7. Submatrices of an orthogonal matrix

In [K-T] B. Kashin and L. Tzafriri posed the following problem:

Let $\varepsilon > 0$ and let n, M be natural numbers, $n < M$. Given an $n \times M$ matrix A whose rows are orthonormal, find a subset $I \subset \{1, \dots, M\}$ of smallest possible cardinality so that for all $x \in \ell_2^n$

$$(1-\varepsilon) \cdot \|x\| \le \sqrt{\frac{M}{|I|}} \cdot \left\| R_I A^T x \right\| \le (1+\varepsilon) \cdot \|x\| .$$

Here $R_I \colon \mathbb{R}^M \to \mathbb{R}^M$ is the orthogonal projection onto the space $\operatorname{span}\{e_i \mid i \in I\}$, where $\{e_i\}_{i=1}^M$ is the standard basis of $\mathbb{R}^M$.

Under an additional restriction that all the entries of A have the same absolute value $1/\sqrt{M}$, they proved that one can take

$$|I| \le \frac{c}{\varepsilon^4} \cdot n^2 \log n.$$

Let $x_1, \dots, x_M$ be the columns of the matrix A. Since the rows of A are orthonormal, we can decompose the identity operator in $\mathbb{R}^n$ as follows:

$$\mathrm{id} = \sum_{j=1}^{M} x_j \otimes x_j. \tag{7.1}$$

Using the technique of Section 3, we prove the following

THEOREM 7.1: *Let $A = (a_{i,j})$ be an $n \times M$ matrix, whose rows are orthonormal. Suppose that for all j*

$$\sum_{i=1}^{n} a_{i,j}^2 \le \frac{n}{M} \cdot t^2. \tag{7.2}$$

Then for every $\varepsilon > 0$ there exists a set $I \subset \{1, \dots, M\}$ so that

$$|I| \le C(\varepsilon) \cdot t^2 \cdot n \log^3 n \tag{7.3}$$

and for all $x \in \mathbb{R}^n$

$$(1-\varepsilon) \cdot \|x\| \le \sqrt{\frac{M}{|I|}} \cdot \left\| R_I A^T x \right\| \le (1+\varepsilon) \cdot \|x\| . \tag{7.4}$$

Remark 7.1: If all the entries of A have absolute values $1/\sqrt{M}$, then $\sum_{i=1}^{n} a_{i,j}^2 = n/M$ for all j and so one can take

$$|I| \le C(\varepsilon) \cdot n \log^3 n.$$

Remark 7.2: The condition (7.2) may be weakened. However, without any condition the number of elements of I can be of order M. Indeed, consider an $(M+1) \times (n+1)$ matrix

$$A = \begin{pmatrix} 1 & 0 \dots 0 \\ 0 & \\ \vdots & A' \\ 0 & \end{pmatrix},$$

where A' is an $M \times n$ matrix with orthonormal rows, all of whose entries have absolute value $1/\sqrt{M}$. Then, since (7.4) implies that $1 \in I$, we have that $\sqrt{M/|I|} \le 1 + \varepsilon$.

The proof of Theorem 7.1 is similar to that of Lemma 3.1 and actually to that of the main lemma of [R]. Let I_1 be a random subset of $\{1, \dots, M\}$ defined as in the proof of Lemma 3.1. Then

$$\sup_{\|x\|=1} \left(2 \cdot \left\|R_{I_1} A^T x\right\|^2 - 1\right) = \left\| 2 \cdot \sum_{j \in I_1}^{M} x_j \otimes x_j - \mathrm{id} \right\|.$$

By Lemma 3.2 this expression is less than

$$C \cdot \log n \cdot \sqrt{\log M} \cdot \max_{j=1,\dots,M} \|x_j\| \cdot \left\| \sum_{j=1}^{M} x_j \otimes x_j \right\|^{1/2} = C \cdot t \cdot \sqrt{\frac{n}{M}} \log n \sqrt{\log M}$$

for some set I_1 satisfying $|I_1| \le M/2$. To obtain the set I we iterate this step until (7.4) holds.

References

[B1] K. Ball, *Volumes of sections of cubes and related problems*, Lecture Notes in Mathematics **1376**, Springer, Berlin, 1989, pp. 251–260.

[B2] K. Ball, *Volume ratios and a reverse isoperimetric inequality*, Journal of the London Mathematical Society **44** (1991), no. 2, 351–359.

[B-S] J. Bourgain and S. Szarek, *The Banach–Mazur distance to the cube and the Dvoretzky–Rogers factorization*, Israel Journal of Mathematics **62** (1988), 169–180.

[Gi1] A. A. Giannopoulos, *A note on the Banach–Mazur distance to the cube*, Operator Theory Advances and Applications **77** (1995), 67–73.

[Gi2] A. A. Giannopoulos, *A proportional Dvoretzky–Rogers factorization result*, Preprint.

[G1] E. Gluskin, *The diameter of the Minkowski compactum is approximately equal to n*, Functional Analysis and its Applications **15** (1981), 72–73 (in Russian).

[G2] E. Gluskin, *Finite dimensional analogs of spaces without basis*, Doklady Adakemii Nauk SSSR **216** (1981), 1046–1050 (in Russian).

[Gr] M. Gruber, *Minimal ellipsoids and their duals*, Rendiconti del Circolo Matematico di Palermo, Ser. 2 **37** (1988), 35–64.

[J] F. John, *Extremum problems with inequalities as subsidiary conditions*, in *Courant Anniversary Volume*, Interscience, New York, 1948, pp. 187–204.

[K-T] B. Kashin and L. Tzafriri, *Some remarks on the restrictions of operators to coordinate subspaces*, Preprint.

[L-T] M. Ledoux and M. Talagrand, *Probability in Banach spaces*, Ergeb. Math. Grenzgeb., 3 Folge, vol. 23, Springer, Berlin, 1991.

[Pa-T-J] A. Pajor and N. Tomczak-Jaegermann, *Subspaces of small codimension of finite dimensional Banach spaces*, Proceedings of the American Mathematical Society **97** (1986), 637–642.

[P-T-J] A. Pelczynski and N. Tomczak-Jaegermann, *On the length of faithful nuclear representations of finite rank operators*, Mathematika **35** (1988), no. 1, 126–143.

[R] M. Rudelson, *Approximate John's decompositions*, Operator Theory Advances and Applications **77** (1995), 245–249.

[S1] S. Szarek, *The finite dimensional basis problem, with an appendix on nets on Grassman manifold*, Acta Mathematica **151** (1983), 153–179.

[S2] S. Szarek, *Spaces with large distance to ℓ_∞^n and random matrices*, American Journal of Mathematics **112** (1990), 899–942.

[S-T] S. Szarek and M. Talagrand, *An isomorphic version of the Sauer–Shelah lemma and the Banach–Mazur distance to the cube*, Lecture Notes in Mathematics **1376**, Springer-Verlag, Berlin, 1989, pp. 105–112.

[T] M. Talagrand, *Construction of majorizing measures, Bernoulli processes and cotype*, Geometric and Functional Analysis **4** (1994), 660–717.

[T-J] N. Tomczak-Jaegermann, *Banach–Mazur Distances and Finite Dimensional Operator Ideals*, Pitman Monographs, **38**, Longman, 1989.