Acta Math., 177 (1996), 55–73


# Improved upper bounds for approximation by zonotopes

by

JIŘÍ MATOUŠEK

*Charles University*
*Prague, Czech Republic*

## 1. Introduction

A *zonotope* in $\mathbf{R}^n$ is a special type of a convex polytope; it is defined as a Minkowski sum of finitely many segments. That is, a zonotope is a set in $\mathbf{R}^n$ of the form $\{x_1+x_2+\ldots+x_m: x_1\in I_1,\ldots,x_m\in I_m\}$, where $I_1,\ldots,I_m$ are segments in $\mathbf{R}^n$. A convex body that can be approximated by zonotopes arbitrarily closely is called a *zonoid*. Several authors have recently studied the following question: what is the minimum number, $N$, of summands of a zonotope needed to approximate a given zonoid $Z$ in $\mathbf{R}^n$ with error at most $\varepsilon$ (this means that $Z\subseteq A\subseteq(1+\varepsilon)Z$, where $A$ is the approximating zonotope, and we assume that the center of symmetry of $Z$ is the origin). Here we consider the dimension $n$ fixed, and we investigate the dependence of $N$ on $\varepsilon$ (we assume that $n\geqslant 3$, as the case $n=2$ is simple—see [4]).

*Previous work.* Most of previous work has been devoted to the special case $Z=B^n$, i.e. to the approximation of the Euclidean unit ball by a zonotope. This question has an equivalent formulation as a "tomography" problem (see Betke and McMullen [3]): find the minimum number $N$ of directions $y_1,\ldots,y_N\in S^{n-1}$ (where $S^{n-1}$ is the unit sphere in $\mathbf{R}^n$) such that the surface area of any convex body $K$ in $\mathbf{R}^n$ can be determined, up to a relative error of $\varepsilon$, by the knowledge of the volumes of the $(n-1)$-dimensional projections of $K$ on the hyperplanes orthogonal to the $y_i$. Bourgain, Lindenstrauss and Milman [6] proved that any zonotope approximating $B^n$ with error at most $\varepsilon$ has at least

$$c(n)\varepsilon^{-2+6/(n+2)}$$

summands, where $c(n)>0$ is a constant depending on the dimension. Bourgain and Lindenstrauss [4] showed that this bound is tight up to a logarithmic factor, namely,

Research supported by Grants GAČR 201/95/2167 and 0194/1996, and Charles University Grants 351, 361/1995 and 193, 194/1996.

that for any $\varepsilon \in (0, \frac{1}{2})$ there exists a zonotope approximating $B^n$ with error at most $\varepsilon$ and with the number of summands

$$N = O(\varepsilon^{-2+6/(n+2)}(\log 1/\varepsilon)^{1-3/(n+2)}). \tag{1}$$

(See also Linhart [12] for earlier, weaker bounds.) For approximating general zonoids, they obtained the same asymptotic upper bound in dimension $n=3$, a bound with a slightly worse logarithmic factor in dimension $n=4$, and for $n \geqslant 5$ the bound of $O(\varepsilon^{-2+4/n}(\log 1/\varepsilon)^{1-2/n})$, whose exponent is worse than in the bound for $Z=B^n$. The approximating zonotopes in these results are sums of segments of generally distinct lengths. Wagner [18] showed that for $n \leqslant 6$, the upper bound (1) for approximating $B^n$ can be achieved by zonotopes all of whose summands have equal lengths. This result has been extended to an arbitrary fixed dimension $n$ by Bourgain and Lindenstrauss [5].

*New results.* Here we improve and generalize the above-mentioned upper bounds in two respects. First, for dimensions $n \geqslant 5$, we prove that an arbitrary zonoid can be approximated up to error $\varepsilon$ by a zonotope whose number of summands matches, up to a multiplicative constant, the above-mentioned lower bound, and whose summands are of equal length. For dimensions $n=3$ and $n=4$ the method currently doesn't seem to yield improvements over known results.

Second, we prove a another estimate for approximating general zonoids by zonotopes with summands of generally distinct lengths. Compared to the first result, this one gives a slightly worse bound (by a logarithmic factor), but it has two advantages: it works for dimensions $n=3,4$ as well, and it is constructive, in the sense that if the zonoid is given in a suitable "effective" manner, the approximating zonotope can be found by a polynomial-time deterministic algorithm (while the first result is nonconstructive).

To formulate the results precisely and to prove them, we pass to a dual setting. Here we deal with the following problem (see [4]): given a probability measure $\tau$ on the unit sphere $S^d$ (from now on, we put $d=n-1$ for a more convenient notation), find a probability measure $\tau'$ with an $N$-point support, with $N=N(\varepsilon)$ as small as possible, such that for any $x \in S^d$ we have

$$\left| \int_{S^d} |\langle x, y \rangle| \, d\tau(y) - \int_{S^d} |\langle x, y \rangle| \, d\tau'(y) \right| \leqslant \varepsilon$$

(where $\langle \cdot, \cdot \rangle$ denotes the usual scalar product in $\mathbf{R}^n$). Let us denote the left-hand side of this formula by $E(x, \tau, \tau')$. The requirement for the approximating zonotope to have all summands of equal length translates into requiring the measure $\tau'$ to be uniform, i.e. all points of its $N$-point support have measure $1/N$.

The first of the above-mentioned results can be formulated as follows:

THEOREM 1. *Let $d\geqslant 4$. For any probability measure $\tau$ on $S^d$ and any $\varepsilon\in\left(0,\frac{1}{2}\right)$ there exists an $N$-point set $Q\subset S^d$, with $N\leqslant C\varepsilon^{-2+6/(d+3)}$ (where $C=C(d)$ is a constant), such that for each $x\in S^d$ we have $E(x,\tau,\tau')\leqslant\varepsilon$, where $\tau'$ denotes the uniform probability measure on $Q$.*

The second result is

THEOREM 2. *For any probability measure $\tau$ on $S^d$ and any $\varepsilon\in\left(0,\frac{1}{2}\right)$ there exists a probability measure $\tau'$ on $S^d$ concentrated on $N$ points, with*

$$N\leqslant C\varepsilon^{-2+6/(d+3)}(\log 1/\varepsilon)^{1-3/(d+3)}$$

*(where $C=C(d)$ is a constant), such that for each $x\in S^d$ we have $E(x,\tau,\tau')\leqslant\varepsilon$.*

*If $\tau$ is concentrated on $N_0$ points and is given by a list of weights of these points, then $\tau'$ as above can be computed (deterministically) in time polynomial in $N_0$ (assuming $d$ is fixed). If $\tau=\mu$ is the rotation-invariant measure on $S^d$, a suitable $\tau'$ can be computed in deterministic time polynomial in $N$.*

The proofs of both theorems use methods from geometric discrepancy theory (also called "theory of irregularities of distribution"). For Theorem 2, we use the basic idea of Bourgain and Lindenstrauss [4], but we transfer it to a discrete setting (which, among other things, allows us to make it effective), and we also employ results on partitioning point sets introduced by Chazelle and Welzl [10] and further developed by the author [15]. This approach relies on the fact that the function $y\mapsto|\langle x,y\rangle|$ is linear on both hemispheres (separated by the "equator" $\langle x,y\rangle=0$), and essentially it is a "dual shatter function" method (see [14] for explanation of this terminology).

Theorem 1 is proved by a considerably different method, originating in Beck [2] and further elaborated by Spencer [17] and by the author [14]. Here, instead of linearity, we use the fact that for close points $x,x'\in S^d$, the function $y\mapsto|\langle x,y\rangle|-|\langle x',y\rangle|$ has a small Lipschitz constant on most of $S^d$. The method can be classified as a "primal shatter function" one.

Theorem 2 is proved in §3. In order that the presentation of the proof is not burdened by algorithmic details, we postpone these into separate parts ("algorithmic remarks") in §§ 2 and 3. Theorem 1 is proved in §4.

*Remarks.* In the notation $f=O(g)$ for asymptotic comparisons of functions, the constant of proportionality may depend on the dimension (and possibly other parameters declared as constants). The notation $f\sim g$ means $f=O(g)$ and $g=O(f)$ at the same time.

Algorithms are considered in the so-called *Real RAM* model of computation, where arbitrary real numbers can be stored in memory and the usual arithmetic operations

with real numbers can be performed exactly in a single step (see e.g. [11]). The results remain valid, however, if we consider algorithms in the Turing machine model (or bit model).

## 2. Preliminaries and auxiliary results

In this section we introduce some terminology and notation, and we establish two lemmas for later use (Lemma 5 and Lemma 6). These are both obtained by simple extensions of known methods.

A *great circle* is the intersection of $S^d$ with a hyperplane passing through the center of $S^d$. For a point $x \in S^d$, let $x^*$ denote the great circle $\{y \in S^d : \langle x, y\rangle = 0\}$. Let $\mu$ denote the rotation-invariant probability measure on $S^d$ (i.e. the usual surface measure suitably normalized). We also define a measure $\mu^*$ on great circles by setting

$$\mu^*(C) = \mu(\{x \in S^d : x^* \in C\})$$

for a set $C$ of great circles.

We say that a great circle $c$ *crosses* a set $P \subseteq S^d$ if the points of $P$ lie in both the open hemispheres determined by $c$. Let $p, q \in S^d$ be two points; by $C(p,q)$ we denote the set of great circles crossing $\{p,q\}$, and we set

$$C^*(p,q) = \{x \in S^d : x^* \in C(p,q)\} = \{x \in S^d : \operatorname{sgn}(\langle x,p\rangle)\operatorname{sgn}(\langle x,q\rangle) = -1\}.$$

The set $C^*(p,q)$ is bounded by the great circles $p^*$ and $q^*$, and we call it the *small slices of $p$ and $q$*. Its $\mu$-measure is proportional to the angular distance between $p$ and $q$ (if the angle is measured in radians, the constant of proportionality is $1/\pi$), which in turn is within a constant factor from $\|p-q\|$, the Euclidean distance of $p$ and $q$.

First we need a "cutting lemma" for great circles on the sphere:

LEMMA 3 (cutting lemma). *Let $C$ be a finite set of great circles in $S^d$, $w$ a probability measure on $C$, and $r \geqslant 1$ a parameter. Then $S^d$ can be covered by $m = O(r^d)$ sets $\Delta_1, \ldots, \Delta_m$ such that each $\Delta_i$ is the intersection of $d+1$ closed hemispheres, and the $w$-measure of the set of great circles of $C$ intersecting the interior of $\Delta_i$ is at most $1/r$, for each $i$.*

*Proof.* This follows from a result of Chazelle and Friedman [9], who proved the following analogous result with $\mathbf{R}^d$ instead of $S^d$ (another proof was later given by Chazelle [7]): *Given a finite set $H$ of hyperplanes in $\mathbf{R}^d$, a probability measure $w$ on $H$, and a parameter $r > 1$, the space $\mathbf{R}^d$ can be covered by $m = O(r^d)$ sets $\Delta_1, \ldots, \Delta_m$ such*

*that each $\Delta_i$ is a simplex (possibly with some vertices at infinity), and the $w$-measure of the set of hyperplanes of $H$ intersecting the interior of $\Delta_i$ is at most $1/r$, for each $i$.* (To be precise: Chazelle and Friedman proved this result for the case when $w$ is the uniform measure; the (simple) passage to a general $w$ was noted in [13].)

To derive Lemma 3, we consider $S^d$ embedded in $\mathbf{R}^{d+1}$ with center at the origin, and we embed $\mathbf{R}^d$ into $\mathbf{R}^{d+1}$ as the hyperplane $x_1=1$. The central projection of $S^d$ to the hyperplane $x_1=1$ maps a given set $C$ of great circles to a set $H$ of hyperplanes in $\mathbf{R}^d$. For this $H$, we apply the result of Chazelle and Friedman, obtaining $O(r^d)$-sets $\Delta_1,...,\Delta_m$ covering $\mathbf{R}^d$. The closure of the preimage of each $\Delta_i$ under the central projection is a union of two sets of the form required in Lemma 3. Taking these two pieces of the preimage for each $\Delta_i$ yields the desired covering of $S^d$. □

Next, we need a simple result about "uniformly distributed" sets of great circles.

LEMMA 4. *Let $d$ be fixed and let $N\geqslant 1$ be an integer. There exists a set $T_2$ of great circles in $S^d$, whose size is bounded by a fixed polynomial in $N$, and such that the following holds for any $\delta\geqslant N^{-1/d}$: Whenever $p,q\in S^d$ are two points at distance at least $\delta$, then the set $\{p,q\}$ is crossed by at least $\frac{1}{5}\delta|T_2|$ great circles of $T_2$. (The constant $\frac{1}{5}$ is not important; any sufficiently small positive constant would do.)*

*Proof.* Such a set $T_2$ can be produced in various ways (the best size one can achieve by current methods is about $N^{1/d}\log N$, but the size is not important for us as long as it is polynomially bounded). Here is one possible method, which has the advantage of providing a simple deterministic algorithm.

First we construct a uniformly distributed point set $U$. Starting with the whole $S^d$ as a single piece, we repeatedly slice each of the current pieces into two new pieces of equal measure by a hyperplane perpendicular to one of the coordinate axes (so that at any moment the pieces are intersections of rectangular boxes with the sphere). If the axes are alternated regularly, the diameter of the pieces goes to 0. Having obtained sufficiently small pieces of equal measure, we pick one point of $U$ arbitrarily from each piece.

It is easy to see that if $\beta$ is the maximum diameter of the pieces used for this construction of the set $U\subset S^d$, then for any $p,q\in S^d$ we have

$$\left|\frac{1}{|U|}|U\cap C^*(p,q)|-\mu(C^*(p,q))\right|=O(\beta)$$

(this means that the set $U$ has a small discrepancy with respect to small slices of the form $C^*(p,q)$). If we set $\beta=cN^{-1/d}$ with a sufficiently small constant $c>0$, we get that any small slice $C^*(p,q)$ with $\|p-q\|=\delta\geqslant N^{-1/d}$ contains at least $\frac{1}{5}|U|\delta$ points of $U$. For

the desired $T_2$, we may thus take the set $\{u^*: u \in U\}$. (This method has the advantage of providing a simple deterministic algorithm for finding $T_2$.) □

The following lemma (the first of the two main results of this section) is a slight modification of a theorem of [15], which in turn is a generalization of a result of Chazelle and Welzl [10].

LEMMA 5 (partition lemma). *Let $P$ be an $N$-point set in $S^d$, and $s \geqslant 2$ an integer constant. Then there exist disjoint $s$-point subsets $P_1, P_2, \ldots, P_t \subset P$, which together contain at least $\frac{1}{2}N$ points of $P$, and with the following properties:*

(i) *Each great circle $c \subset S^d$ crosses at most $O(N^{1-1/d})$ sets among the $P_i$.*

(ii) *Each $P_i$ has diameter at most $O(N^{-1/d})$.*

*Proof.* The proof follows [15] closely (an extra ingredient compared to that proof is that we have to watch the diameter of the $P_i$'s). For the reader's convenience, we give a self-contained proof (thus repeating parts of arguments from previous papers almost literally).

First we choose two "test sets" of great circles.

Let us say that two great circles are *equivalent* if they cross the same set of pairs of points of $P$. It is easily seen that there are $O(N^d)$ equivalence classes. Choose one great circle from each equivalence class, obtaining a set $T_1$ of great circles.

Next, we choose a set $T_2$ of great circles as in Lemma 4. Moreover, we may assume that $T_1 \cap T_2 = \varnothing$.

We now describe the construction of the sets $P_1, \ldots, P_t$. The idea is to fix these sets one by one. In each step we want to take an $s$-point subset of the remaining points which is crossed by possibly few great circles of the "test set" $T_1 \cup T_2$. Moreover, the great circles of $T_1$ which already cross many of the sets constructed so far should be considered more important (because they have already used up a great part of their quota for crossed sets). To capture this, we assign a weight to each great circle of $T_1$, which penalizes the crossing of the previously constructed $P_i$.

The algorithm is as follows. Suppose that $P_1, \ldots, P_i$ have already been constructed, and that the set $\widetilde{P}_i = P \setminus (P_1 \cup \ldots \cup P_i)$ still has at least $\frac{1}{2}N$ points. For a great circle $c \in T_1$, let $\varkappa_i(c)$ be the number of sets among $P_1, \ldots, P_i$ crossed by $c$, and set $\bar{w}_i(c) = 2^{\varkappa_i(c)}$ (this is the weight expressing the penalization idea). Further, let $\overline{W}_i = \sum_{c \in T_1} \bar{w}_i(c)$. Then we set $T = T_1 \cup T_2$, and for $c \in T$ we define

$$w_i(c) = \begin{cases} \bar{w}_i(c)/2|\overline{W}_i| & \text{for } c \in T_1, \\ 1/2|T_2| & \text{for } c \in T_2. \end{cases}$$

We apply the cutting lemma (Lemma 3) for the collection $T$ and probability measure $w_i$, with the parameter $r \sim N^{1/d}$, where the constant of proportionality is chosen in such a

way that the value of $m$ in Lemma 3 (the number of the sets $\Delta_i$) is at most $N/2s$. Since we have more than $\frac{1}{2}N$ remaining points in $\widetilde{P}_i$ and at most $N/2s$ sets $\Delta_i$, there exists some $\Delta_i$ containing at least $s$ points of $\widetilde{P}_i$. We take some $s$ such points belonging to a single set $\Delta_i$ as the set $P_{i+1}$. This finishes the description of the construction of the sets $P_i$.

The interior of each $\Delta_i$ is, in particular, intersected by at most $2|T_2|/r=O(|T_2|/N^{1/d})$ great circles of $T_2$. By the choice of $T_2$, this implies that the diameter of $P_{i+1}$ is $O(N^{-1/d})$. This shows property (ii).

Property (i) is obtained by estimating the total weight

$$\overline{W}_t=\sum_{c\in T_1} 2^{\varkappa_t(c)}$$

after the final step. For each $c\in T$ we have $\varkappa_t(c)\leqslant\log_2 \overline{W}_t$; hence, part (ii) will be proved if we show

$$\log_2 \overline{W}_t=O(N^{1-1/d}). \tag{2}$$

Since $|T_1|$ is polynomial in $N$, we get $\log_2 \overline{W}_0=O(\log N)$. Next, we estimate the ratio $\overline{W}_i/\overline{W}_{i-1}$. By passing from $\bar{w}_{i-1}$ to $\bar{w}_i$, the weight of the great circles crossing the set $P_i$ is doubled, while the weight of the other great circles remains unchanged. The total $\bar{w}_i$-weight of the great circles of $T_1$ crossing $P_i$ is $O(\overline{W}_{i-1}/N^{1/d})$ by the construction, and hence we get

$$\overline{W}_i\leqslant\overline{W}_{i-1}+O\left(\frac{\overline{W}_{i-1}}{N^{1/d}}\right)=\overline{W}_{i-1}\left(1+\frac{O(1)}{N^{1/d}}\right).$$

From this we have

$$\overline{W}_t\leqslant\overline{W}_0\left(1+\frac{O(1)}{N^{1/d}}\right)^t,$$

and a routine calculation yields the estimate (2). □

*Algorithmic remark.* In the sequel, we will need an algorithmic version of Lemma 5, namely that given an $N$-point set $P\subset S^d$, the subsets $P_1,\dots,P_t$ as in Lemma 5 can be computed in deterministic polynomial time. For Lemma 3, a deterministic polynomial-time algorithm for computing the sets $\Delta_i$ was given by Chazelle and Friedman [9] (for a faster algorithm see Chazelle [7]). The set $T_1$ can be found by standard computational geometry techniques (constructing the arrangement of the great circles $p^*$, $p\in P$), see e.g. [11]. The set $T_2$ can be obtained by the procedure outlined in the proof of Lemma 4. The construction of the $P_i$ according to the above proof can clearly be accomplished in polynomial time.

Next, we prove a lemma on the existence of suitable "dense enough" sets in the sphere.

LEMMA 6. *Let $P\subset S^d$ be an $N$-point set, and let $\delta\in(0,1)$ be given. Then there exists a set $\mathcal{N}\subset S^d$ of size $O(\delta^{-d})$ such that for any point $x\in S^d$ there exists a $q\in\mathcal{N}$ which is "close" to $x$ in the following sense*:

(i) $\|x-q\|\leqslant\delta$ *and*

(ii) $|P\cap C^*(x,q)|\leqslant\delta N$, *that is, the small slices of $x$ and $q$ contain at most $\delta N$ points of $P$.*

*Proof.* Let $T_1=P^*$ be the set of great circles determined by the points of $P$. Choose another set $T_2$ of great circles as in Lemma 4. Define a probability measure $w$ on $T=T_1\dot\cup T_2$ by

$$w(c)=\begin{cases}1/6|T_1| & \text{for } c\in T_1,\\ 5/6|T_2| & \text{for } c\in T_2.\end{cases}$$

Use the cutting lemma (Lemma 3) for the collection $T$ and the measure $w$, with $r=1/6\delta$. This yields a covering of $S^d$ by $O(\delta^{-d})$ spherically convex sets $\Delta_1,\dots,\Delta_m$ such that the interior of each $\Delta_i$ is intersected by at most $\delta|T_1|$ great circles of $T_1$ and by at most $\frac{1}{5}\delta|T_2|$ great circles of $T_2$. Form the set $\mathcal{N}$ by choosing one point in the interior of each $\Delta_i$. It is easy to check that such an $\mathcal{N}$ has the required properties. □

## 3. Proof of Theorem 2

In Theorem 2, we may assume that the given measure $\tau$ is concentrated on finitely many, $N_0$, points (in particular, for the case $\tau=\mu$, we can produce a suitable discrete approximation of $\mu$ with error at most $\varepsilon$ in time polynomial in $\varepsilon^{-1}$ easily). Theorem 2 is then proved from the following proposition:

PROPOSITION 7. *Let $P\subset S^d$ be an $N$-point set, and let $\tau$ be a probability measure on $P$. Then there exist a subset $P'\subseteq P$ of at most $\frac{7}{8}N$ points and a probability measure $\tau'$ on $P'$ such that for any $x\in S^d$ we have*

$$\left|\int_P|\langle x,y\rangle|\,d\tau(y)-\int_{P'}|\langle x,y\rangle|\,d\tau'(y)\right|=O\big(N^{-1/2-3/2d}\sqrt{\log N}\,\big). \tag{3}$$

*A suitable $\tau'$ can be found deterministically in time polynomial in $N$.*

Given a $\tau$ with an $N_0$-point support as in Theorem 2, we apply Proposition 7 repeatedly, obtaining measures concentrated on $\frac{7}{8}N_0,\big(\frac{7}{8}\big)^2N_0,\dots$ points, and we continue until a number of points $\leqslant N$ is reached. It is easy to see that the errors of these successive approximations form a geometric progression, with the last term being the dominating one, and Theorem 2 follows.

For the proof of Proposition 7 we need the following lemma, which is a "finite version" of considerations of Bourgain and Lindenstrauss [4].

LEMMA 8. *Let $Q \subset \mathbf{R}^n$ be a set of $s \geqslant n+1$ points, and let $\sigma$ be a given probability measure on $Q$. Then there exist probability measures $\sigma_1, ..., \sigma_{s'}$ on $Q$ and probabilities $p_1, ..., p_{s'}$ summing up to 1, where $s' \leqslant s-n$, such that the following holds:*

(i) *Each $\sigma_i$ is concentrated on at most $n+1$ points of $Q$.*

(ii) (*Linear functions are integrated exactly.*) *For any linear function $h: \mathbf{R}^n \to \mathbf{R}$, and for any $\sigma_i$, we have*

$$\int_Q h \, d\sigma = \int_Q h \, d\sigma_i.$$

(iii) (*For arbitrary functions, the integral has the right expectation.*) *If $i$ is a randomly chosen index in $\{1, 2, ..., s'\}$, each $i$ being chosen with probability $p_i$, then for any function $f: Q \to \mathbf{R}$ the expectation (with respect to the random choice of $i$) of $\int_Q f \, d\sigma_i$ is equal to $\int_Q f \, d\sigma$.*

*Proof.* One proof can be given using the method of [4] (for that method to work, one needs to replace $n+1$ by $n+2$ in (i), but for our application of the lemma this difference does not matter). Here is another, perhaps more natural proof. Let $\Sigma$ be the set of all probability measures $\xi$ satisfying conditions (i) and (ii), that is, $\xi$ is concentrated on at most $n+1$ points of $Q$ and $\int_Q h \, d\xi = \int_Q h \, d\sigma$ holds for any linear function $h$. The latter condition is equivalent to $\xi$ having the same center of gravity as $\sigma$; in other words, if $c = \sum_{q \in Q} \sigma(q) q$ denotes the center of gravity of $\sigma$ and $c_j$ denotes its $j$th coordinate, $\xi$ has to satisfy the $n$ linear conditions of the form $\sum_{q \in Q} \xi(q) q_j = c_j$ for $j = 1, 2, ..., n$.

We want to prove that $\sigma$ can be expressed as a convex combination of at most $s-n$ elements of $\Sigma$, i.e. there exist $\sigma_1, ..., \sigma_{s'} \in \Sigma$ and nonnegative real numbers $p_1, ..., p_{s'}$ summing up to 1, $s' \leqslant s-n$, such that $\sigma = \sum_{j=1}^{s'} p_j \sigma_j$ (it is easy to see that such $\sigma_j$'s and $p_j$'s satisfy the condition (iii) of the lemma). We prove the following statement by induction on $k$, the number of nonzero components of $\sigma$: *If $\sigma$ is supported at $k$ points of $Q$, $k \geqslant n+1$, then there exist $\sigma_1, ..., \sigma_{k-n} \in \Sigma$ and nonnegative real numbers $p_1, ..., p_{k-n}$ summing up to 1 such that $\sigma = \sum_{j=1}^{k-n} p_j \sigma_j$.* The case $k = n+1$ is clear, so let $k > n+1$ and let $Q' = \{q \in Q : \sigma(q) > 0\}$ be the $k$-point support of $\sigma$. For each point $q \in Q'$, introduce a variable $x_q$, and consider the following system of $n+1$ linear equations:

$$\sum_{q \in Q'} x_q = 1,$$

$$\sum_{q \in Q'} x_q q_j = c_j, \quad j = 1, 2, ..., n.$$

Any nonnegative solution to this system can be interpreted as a probability measure on $Q'$ satisfying the condition (ii) of the lemma. The measure $\sigma$ determines one nonnegative solution to this system. By basic results of the theory of linear inequalities, this system

also has a *basic* nonnegative solution, in which the number of nonzero components is no larger than the number of equations, i.e. at most $n+1$. Let $\sigma^* \in \Sigma$ be such a basic solution, and define $p^* = \max\{p \geqslant 0 : p\sigma^*(q) \leqslant \sigma(q)\ \forall q \in Q'\}$. Put $\sigma' = (\sigma - p^*\sigma^*)/(1-p^*)$ (this is well-defined since $p^* < 1$). This $\sigma'$ is a probability measure on $Q'$ with the same center of gravity as $\sigma$ and with at most $(k-1)$-point support. By induction, we can express it as a convex combination $\sigma' = \sum_{j=1}^{k-n-1} p'_j \sigma_j$, $\sigma_j \in \Sigma$, and then we get the expression $\sigma = \sum_{j=1}^{k-n} p_j \sigma_j$, with $p_j = (1-p^*)p'_j$ for $j = 1, 2, \ldots, n-k-1$ and $p_{n-k} = p^*$, $\sigma_{n-k} = \sigma^*$. □

*Proof of Proposition* 7. First we give a rough outline of the proof. Our goal is to take about a quarter of the points of $P$ and replace them by fewer points of the same total weight. So we partition about $\frac{1}{4}N$ points of $P$ into groups $P_1, \ldots, P_t$ by $s = 2(d+2)$ points. Each $P_i$ is then replaced by some of its $(d+2)$-point subsets with some appropriate point weights. For each $P_i$, we have several "candidate" $(d+2)$-point subsets, together with certain measures $\sigma_j^{(i)}$ on them. Each such candidate $\sigma_j^{(i)}$ has a certain probability $p_j^{(i)}$ assigned, and the actual replacement for $P_i$ is chosen at random according to these probabilities (with independent choices for different groups $P_i$). The candidates $\sigma_j^{(i)}$ are constructed according to Lemma 8, hence each of them integrates any *linear* function in exactly the same way as the original measure on $P_i$ did. For a nonlinear function, the integral by $\sigma_j^{(i)}$ generally differs from the integral by the original measure, but the expectation of the deviation, for a random choice of the candidate, is zero. If we fix some $x \in S^d$ and consider the total error made in the integral of the function $y \mapsto |\langle x, y\rangle|$, nonzero contributions come only from the $P_i$'s such that the function $y \mapsto |\langle x, y\rangle|$ is not linear on them, and these can be only the $P_i$'s crossed by the great circle $x^*$. By a careful choice of the groups $P_i$, we achieve that for each $x$, only relatively few $P_i$'s are crossed (this is the main new feature in our proof, which allows us to deal with arbitrarily distributed measures). The contribution of the crossed sets to the error is a sum of independent random variables with zero expectation. A tail estimate (Bernstein's inequality) then shows that too large an error for any fixed $x$ has exponentially small probability. Since it clearly suffices to consider only polynomially many "test" points $x$, the overall bound follows.

We now give a quantitative and more formal proof. Given an $N$-point set $P \subset S^d$ and a probability measure $\tau$ on $P$, we first select a subset $\widetilde{P} \subseteq P$ of at least $\frac{1}{2}N$ points such that any point $p \in \widetilde{P}$ satisfies $\tau(p) \leqslant 2/N$ (this is possible by Markov's inequality). Then we apply Lemma 5 for $\widetilde{P}$, with $s = 2(d+2)$. We obtain a collection of disjoint $s$-point subsets $P_1, P_2, \ldots, P_t \subset \widetilde{P}$ covering at least $\frac{1}{4}N$ points of $P$, with diameter $O(N^{-1/d})$, and such that any great circle crosses at most $O(N^{1-1/d})$ of the $P_i$'s.

For each $P_i$, apply Lemma 8 with $P_i$ in the role of $Q$ and with $\tau$ restricted to $P_i$ and appropriately normalized (divided by the factor $\tau(P_i)$) in the role of $\sigma$. Let $\sigma_1^{(i)}, \ldots, \sigma_{s'}^{(i)}$

and $p_1^{(i)}, \ldots, p_{s'}^{(i)}$ be as in Lemma 8 and pick a random index $j_i \in \{1, 2, \ldots, s'\}$ taking each $j$ with probability $p_j^{(i)}$. Make such a random choice independently for each $i=1, 2, \ldots, t$, and define the probability measure $\tau'$ on $P$ as follows:

$$\tau'(q) = \begin{cases} \sigma_{j_i}^{(i)}(q)\tau(P_i) & \text{for } q \in P_i, \\ \tau(q) & \text{for } q \text{ lying in no } P_i. \end{cases}$$

This yields a probability measure on $P$ whose support has no more than $\frac{7}{8}N$ points.

Next, we want to estimate the left-hand side of (3). Set $\varepsilon = N^{-3}$ (say) and fix a set $\mathcal{N} \subset S^d$ of size polynomial in $N$, which is $\varepsilon$-dense in $S^d$, i.e. such that for any $x \in S^d$ there exists an $x' \in S^d$ with $\|x - x'\| \leqslant \varepsilon$ (the existence of such an $\mathcal{N}$ of size $O(\varepsilon^{-d})$ is well-known, and it also follows from Lemma 6). If $x, x' \in S^d$ are two points at distance $\leqslant \varepsilon$, the functions $y \mapsto |\langle x, y\rangle|$ and $y \mapsto |\langle x', y\rangle|$ differ by at most $\varepsilon$ at any point. Hence it suffices to show the error estimate (3) for all $x \in \mathcal{N}$.

Fix one $x \in \mathcal{N}$. Let $I = I(x)$ denote the set of indices $i \in \{1, 2, \ldots, t\}$ such that the great circle $x^*$ crosses the set $P_i$. The function $y \mapsto |\langle x, y\rangle|$ is linear on each $P_i$ with $i \notin I$, and so we have $\int_{P_i} |\langle x, y\rangle| \, d\tau(y) = \int_{P_i} |\langle x, y\rangle| \, d\tau'(y)$ for such $i \notin I$ by (ii) of Lemma 8. On the other hand, for $i \in I$, the difference $X_i = X_i(x) = \int_{P_i} |\langle x, y\rangle| \, d\tau(y) - \int_{P_i} |\langle x, y\rangle| \, d\tau'(y)$ is a random variable. Its expectation is 0 (by (iii) in Lemma 8). The diameter of $P_i$ is $O(N^{-1/d})$, the function $y \mapsto \langle x, y\rangle$ (with $\|x\| = 1$) is 1-Lipschitz, and we have $\tau(P_i) \leqslant 2s/N = O(N^{-1})$, so we get $|X_i| = O(N^{-1-1/d})$.

We have

$$E_x = \int_P |\langle x, y\rangle| \, d\tau(y) - \int_P |\langle x, y\rangle| \, d\tau'(y) = \sum_{i \in I} X_i.$$

The $X_i$ are independent random variables with zero expectation, uniformly bounded by $B = O(N^{-1-1/d})$, and their number is $|I| \leqslant m = O(N^{1-1/d})$. Bernstein's inequality in such a situation gives the tail estimate

$$\text{Prob}[|E_x| > \lambda B\sqrt{m}] < 2e^{-\lambda^2/2}.$$

Choosing $\lambda$ such that the right-hand side is smaller than $1/|\mathcal{N}|$, i.e. $\lambda \sim \sqrt{\log N}$, gives that with a positive probability, no $x \in \mathcal{N}$ has error $E_x$ larger in absolute value than $O(\lambda B\sqrt{m}) = O(N^{-1/2-3/2d}\sqrt{\log N})$. □

*Algorithmic remarks.* We want to show that $P'$ and $\tau'$ as in Proposition 7 can be computed in polynomial time. We have already seen that the sets $P_i$ can be found in polynomial time. The measures $\sigma_j$ and the probabilities $p_j$ as in Lemma 8 can be computed in polynomial time as well—the proof shown yields an efficient procedure. The $\varepsilon$-dense set $\mathcal{N}$ can also be found in polynomial time; one easy explicit construction (giving a suboptimal size) has been described in algorithmic remarks in §2.

Finally we need a suitable choice of the index $j_i$ for each $P_i$. A polynomial-time randomized algorithm is immediate (make a random choice and check if it works for all $x\in\mathcal{N}$). This can be derandomized using a generalization of the *unbiased greedy algorithm* of Chazelle [8] (which can be seen as an instance of Raghavan's and Spencer's *method of pessimistic estimators*; see [1]). In the algorithm, the indices $j_i\in\{1,\dots,s'\}$ as in the proof are chosen one by one. Assuming that $j_1,\dots,j_k$ have already been fixed to values $\bar{\jmath}_1,\dots,\bar{\jmath}_k$, respectively, $j_{k+1}$ is set to a value $\bar{\jmath}_{k+1}$ minimizing the expression $F(\bar{\jmath}_1,\dots,\bar{\jmath}_k,j_{k+1})$, where

$$F(j_1,\dots,j_k)=\sum_{x\in\mathcal{N}}\Big[\prod_{\substack{i\leqslant k\\ i\in I(x)}}(1+\alpha X_i(x,j_i))+\prod_{\substack{i\leqslant k\\ i\in I(x)}}(1-\alpha X_i(x,j_i))\Big].$$

Here $I(x)$ is the set of indices $i$ for which $x^*$ crosses the set $P_i$,

$$X_i(x,j)=\int_{P_i}|\langle x,y\rangle|\,d\tau(y)-\tau(P_i)\int_{P_i}|\langle x,y\rangle|\,d\sigma_j^{(i)}(y)$$

and

$$\alpha=\frac{\sqrt{\ln(2|\mathcal{N}|)}}{B\sqrt{m}},$$

with $B=O(N^{-1-1/d})$ being the uniform bound for all the $X_i(x,j)$ and $m=O(N^{1-1/d})$ bounding the maximum cardinality of $I(x)$.

It is clear that the functions $F(j_1,\dots,j_k)$ can be evaluated in polynomial time; we need $s$ evaluations for the choice of one index $j_i$. It remains to show that the indices found by this algorithm actually guarantee the error bound as in Proposition 7.

If $\bar{\jmath}_1,\dots,\bar{\jmath}_k$ are arbitrary and $j_{k+1}$ is chosen at random (according to the distribution given by $p_1^{(k+1)},\dots,p_s^{(k+1)}$), then for each $x\in\mathcal{N}$ the expectation of $X_{k+1}(x,j_{k+1})$ is 0, and hence the expectation of $F(\bar{\jmath}_1,\dots,\bar{\jmath}_k,j_{k+1})$ is $F(\bar{\jmath}_1,\dots,\bar{\jmath}_k)$. Therefore a choice of $\bar{\jmath}_{k+1}$ with $F(\bar{\jmath}_1,\dots,\bar{\jmath}_{k+1})\leqslant F(\bar{\jmath}_1,\dots,\bar{\jmath}_k)$ always exists, and thus the algorithm guarantees $F(\bar{\jmath}_1,\dots,\bar{\jmath}_t)\leqslant F(\bar{\jmath}_1,\dots,\bar{\jmath}_{t-1})\leqslant\dots\leqslant F(\bar{\jmath}_1)\leqslant F(\,)=2|\mathcal{N}|$.

Let $x\in\mathcal{N}$ and let us write $E_x=\sum_{i\in I(x)}X_i(x,\bar{\jmath}_i)$. We derive an upper bound on $E_x$ (a lower bound follows symmetrically). We have $F(\bar{\jmath}_1,\dots,\bar{\jmath}_t)\geqslant\prod_{i\in I(x)}(1+\alpha X_i(x,\bar{\jmath}_i))$. As one may check by elementary calculus, the inequality $1+z\geqslant e^{z-z^2}$ holds for all $z\in\left[-\frac{1}{2},\frac{1}{2}\right]$. We use it with $z=\alpha X_i(x,\bar{\jmath}_i)$ for each factor in the product (we always have $|\alpha X_i(x,\bar{\jmath}_i)|\leqslant\frac{1}{2}$). In this way we get

$$\begin{aligned}2|\mathcal{N}|\geqslant F(\bar{\jmath}_1,\dots,\bar{\jmath}_t)&\geqslant\prod_{i\in I(x)}(1+\alpha X_i(x,\bar{\jmath}_i))\geqslant\exp\Big(\alpha E_x-\alpha^2\sum_{i\in I(x)}X_i(x,\bar{\jmath}_i)^2\Big)\\&\geqslant\exp(\alpha E_x-\alpha^2 mB^2)\geqslant\exp(\alpha E_x-\ln(2|\mathcal{N}|)).\end{aligned}$$

From this, we obtain $E_x \leqslant 2B\sqrt{m\ln(2|\mathcal{N}|)} = O\big(N^{-1/2-3/2d}\sqrt{\log N}\big)$ by calculation. The lower bound for $E_x$ follows symmetrically. This proves the algorithmic part of Theorem 2 (note that we have essentially re-proved the simple form of Bernstein's inequality we needed in the existence proof). □

## 4. Proof of Theorem 1

The proof has a quite similar structure as the proof in [14]. Theorem 1 is derived from the following proposition.

PROPOSITION 9. *Let $d \geqslant 2$ and let $P \subset S^d$ be an $N$-point set, with $N$ sufficiently large (larger than a prescribed constant). Then there exist a subset $P^* \subseteq P$ of $N^* \geqslant \frac{1}{8}N$ points, with $N^*$ even, and a subset $Q \subset P^*$ of size $\frac{1}{2}N^*$, such that for any $x \in S^d$ we have*

$$\left| \sum_{y \in P^*} |\langle x, y\rangle| - 2 \sum_{y \in Q} |\langle x, y\rangle| \right| = O(N^{1/2-3/2d}).$$

*Proof of Theorem* 1. We prove the following "halving" claim from Proposition 9.

CLAIM. *Let $P \subset S^d$ be an $N$-point set, $d \geqslant 4$, $N$ even. Then there exists a set $P' \subset P$ of size $\frac{1}{2}N$ such that*

$$\left| \sum_{y \in P} |\langle x, y\rangle| - 2 \sum_{y \in P'} |\langle x, y\rangle| \right| = O(N^{1/2-3/2d}).$$

Once this claim is proved, Theorem 1 follows easily. We may assume that the measure $\tau$ given in Theorem 1 is the uniform measure on a finite set $P^{(0)}$, where $|P^{(0)}| = N^{(0)}$ is a power of 2. We apply the claim with $P = P^{(0)}$, producing a set $P^{(1)}$ of size $N^{(1)} = \frac{1}{2}N^{(0)}$, then we again apply the claim with $P = P^{(1)}$, etc., until we reach a set of a suitable size $N$. Similarly as in the proof of Theorem 2, the errors of these successive approximations form a geometric progression, with the error committed in the last halving being the dominating one, and this yields Theorem 1 (note that the error in Proposition 9 and in the claim is rescaled by a factor of $N$ compared to Theorem 1).

The claim is proved by an iterated application of Proposition 9. We start with the set $P_0 = P$. Proposition 9 yields a set $P_0^*$ of at least $\frac{1}{8}N$ points of $P_0$ and its subset $Q_0$ of exactly half the size of $P_0^*$. We set $P_1 = P_0 \setminus P_0^*$, and we apply Proposition 9 on $P_1$, etc. We continue until a set $P_k$ of size smaller than a suitable constant is reached, and at this moment we let $P_k^* = P_k$, and $Q_k$ is chosen as an arbitrary subset of $P_k$ of size $\frac{1}{2}|P_k|$. The set $P'$ as in the claim is then $P' = Q_0 \cup Q_1 \cup \ldots \cup Q_k$. For the error we get

$$\left| \sum_{y \in P} |\langle x, y\rangle| - 2 \sum_{y \in P'} |\langle x, y\rangle| \right| \leqslant \sum_{i=0}^{k} \left| \sum_{y \in P_i^*} |\langle x, y\rangle| - 2 \sum_{y \in Q_i} |\langle x, y\rangle| \right| = \sum_{i=0}^{k} O(|P_i|^{1/2-3/2d}).$$

Since $|P_i| \leqslant (\frac{7}{8})^i N$, and since we assume that $d \geqslant 4$, the sum in the last expression is dominated by the first term, and we obtain the claim. In this way, Theorem 1 is implied by Proposition 9. □

*Remark.* As we saw, the assumption $d \geqslant 4$ (or $n \geqslant 5$) in Theorem 1 was needed to derive the "halving claim" from Proposition 9, namely, we needed that the error bound in Theorem 1 multiplied by $N$ (i.e. the error for the case when the points have unit weights) is a sufficiently fast increasing function of $N$. Such an assumption is not a pure artifact of our proof: the "halving claim" is not true for dimension $d=3$, say. Indeed, if $P$ consists of $N-1$ points clustered in a very small region of $S^3$ and one point at angular distance $\frac{1}{2}\pi$ away from the others, then the error made by selecting half of the points and doubling their weights will be at least half of a point weight, and this is much more than what the bound we are aiming at allows. Therefore, to apply a similar approach as ours, one would need to assume at least some uniform distribution condition for $P$.

*Test functions.* We start proving Proposition 9. We need to assure a bound holding for all points $x \in S^d$ simultaneously. Similarly as in the proof of Theorem 2, we introduce a suitable finite collection of the $x$'s, such that it will be sufficient to bound the error for these. Here we need a more complicated hierarchical structure, however.

For $i=1,2,\ldots,k$, where $2^k \sim N^2$ (say), we set $\delta_i = 2^{-i}$. We apply Lemma 6 for $P$ and $\delta_i$, obtaining a "$\delta_i$-dense" set $\mathcal{N}_i$ as in the lemma, with $|\mathcal{N}_i| = O(2^{di})$. Moreover, we introduce mappings $\pi_1, \pi_2, \ldots, \pi_k : S^d \to \mathcal{N}_i$. Informally, $\pi_i(x)$ is the nearest point of $\mathcal{N}_i$ to $x$. More precisely, we require that $q = \pi_i(x) \in \mathcal{N}_i$ is a point of $\mathcal{N}_i$ satisfying conditions (i) and (ii) in Lemma 6 (we have $\|x-q\| \leqslant \delta_i$ and the small slices of $x$ and $q$ contain at most $\delta_i N$ points of $P$).

We also introduce systems $\mathcal{F}_1, \ldots, \mathcal{F}_k$ of functions. We let $\mathcal{F}_i = \{\varphi_{i,q} : q \in \mathcal{N}_i\}$, where $\varphi_{i,q} : S^d \to \mathbf{R}$ is defined by

$$\varphi_{i,q}(y) = \begin{cases} |\langle q, y\rangle| & \text{for } i = 1, \\ |\langle q, y\rangle| - |\langle \pi_{i-1}(q), y\rangle| & \text{for } i > 1. \end{cases}$$

The following properties of the functions $\varphi_{i,q}$ are easy to check from the definition.

OBSERVATION 10. (i) $|\varphi_{i,q}(y)| = O(2^{-i})$ *for all* $y \in S^d$.

(ii) *Let* $q \in \mathcal{N}_i$, *and let* $L^+_{i,q}, L^-_{i,q}$ *be the two "large slices" of the points* $q$ *and* $\pi_{i-1}(q)$, *i.e.*

$$L^+_{i,q} = \{y \in S^d : \langle q, y\rangle \geqslant 0 \text{ and } \langle \pi_{i-1}(q), y\rangle \geqslant 0\},$$
$$L^-_{i,q} = \{y \in S^d : \langle q, y\rangle \leqslant 0 \text{ and } \langle \pi_{i-1}(q), y\rangle \leqslant 0\}.$$

*The function* $\varphi_{i,q}$ *is* $C$*-Lipschitz on* $L^+_{i,q}$ *and on* $L^-_{i,q}$ *with* $C = O(2^{-i})$.

(iii) *For any* $x \in S^d$ *we have*

$$|\langle x, y\rangle| = \sum_{i=1}^{k} \varphi_{i,q_i}(y) + r_x(y) \tag{4}$$

*for all* $y \in S^d$, *where* $q_k = \pi_k(x)$ *and* $q_{i-1} = \pi_{i-1}(q_i)$, *and* $|r_x(y)| = O(N^{-2})$. □

Let us set $u = \log_2(N^{1/d})$ and

$$\Delta_i = \frac{K}{1+(u-i)^2} N^{1/2-3/2d},$$

where $K$ is a suitable (sufficiently large) constant. Our goal is to select sets $P^* \subset P$, $P^* \geqslant \frac{1}{8}N$, and $Q \subset P^*$ as in Proposition 9 in such a way that for each $i, q$ the error

$$E_{i,q} = \sum_{y \in P^*} \varphi_{i,q}(y) - 2 \sum_{y \in Q} \varphi_{i,q}(y)$$

is at most $\Delta_i$ in absolute value. Having guaranteed this, the expansion (4) and the fact that $\sum_{i=1}^{k} \Delta_i = O(N^{1/2-3/2d})$ imply that $P^*$ and $Q$ are as required in the proposition.

*Colorings and partial colorings.* In order to produce $P^*$ and $Q$, we first apply Lemma 5 for $P$ with $s=2$. In this way, we get disjoint pairs $P_1, P_2, \ldots, P_t$ of points of $P$, with $\overline{P} = P_1 \cup \ldots \cup P_t$ having at least $\frac{1}{2}N$ points, such that each pair $P_j$ has diameter $O(N^{-1/d})$ and each great circle crosses at most $O(N^{1-1/d})$ pairs (this is a *matching with a low crossing number* in the terminology of [10]). Let us choose one of the two points of $P_j$ arbitrarily and denote it by $u_j$, and denote the remaining point by $v_j$.

Let $\chi: \{1, 2, \ldots, t\} \to \{+1, -1\}$ be a mapping (called a *coloring*). Such a $\chi$ encodes a choice of one point from each of the pairs $P_j$: if $\chi(i) = +1$, select $u_j$, and if $\chi(i) = -1$, select $v_j$. Let $Q(\chi)$ denote the subset of $\overline{P} = P_1 \cup \ldots \cup P_t$ selected in this way. We define errors for $\chi$ as follows:

$$E_{i,q}(\chi) = \sum_{y \in \overline{P}} \varphi_{i,q}(y) - 2 \sum_{y \in Q(\chi)} \varphi_{i,q}(y) = \sum_{j=1}^{t} \chi(j)[\varphi_{i,q}(v_j) - \varphi_{i,q}(u_j)].$$

If $\chi$ is chosen at random, say, these errors will typically be much too large, so such a random choice is not good enough. We use a more subtle strategy (apparently invented by Beck [2]). We show that there exist *two* mappings $\chi_1, \chi_2$, which differ on sufficiently many components, but for which

$$|E_{i,q}(\chi_1) - E_{i,q}(\chi_2)| \leqslant 2\Delta_i \tag{5}$$

holds (for all $i$ and $q$ simultaneously). Then we define a new mapping $\bar{\chi}\colon\{1,2,\dots,t\}\to\{+1,-1,0\}$ by setting $\bar{\chi}=\frac{1}{2}(\chi_1-\chi_2)$ (such a $\bar{\chi}$ is called a *partial coloring*). We let $D$ be the set of indices $j\in\{1,\dots,t\}$ for which $\bar{\chi}(j)\neq 0$ (i.e. where $\chi_1$ and $\chi_2$ differ). We put $P^*=\bigcup_{j\in D}P_j$ and we select $Q\subset P^*$ according to the mapping $\bar{\chi}$ (taking $u_j$ if $\bar{\chi}(j)=1$ and $v_j$ if $\bar{\chi}(j)=-1$). For each $i$ and $q$ we have

$$\begin{aligned}E_{i,q}&=\sum_{j\in D}\bar{\chi}(j)[\varphi_{i,q}(v_j)-\varphi_{i,q}(u_j)]\\&=\sum_{j\in D}\tfrac{1}{2}(\chi_1(j)-\chi_2(j))[\varphi_{i,q}(v_j)-\varphi_{i,q}(u_j)]\\&=\tfrac{1}{2}\sum_{j=1}^{t}\chi_1(j)[\varphi_{i,q}(v_j)-\varphi_{i,q}(u_j)]-\tfrac{1}{2}\sum_{j=1}^{t}\chi_2(j)[\varphi_{i,q}(v_j)-\varphi_{i,q}(u_j)]\\&=\tfrac{1}{2}(E_{i,q}(\chi_1)-E_{i,q}(\chi_2)).\end{aligned}$$

Therefore, if (5) can be guaranteed for $\chi_1,\chi_2$, we get $|E_{i,q}|\leqslant\Delta_i$ for all $i,q$. Thus, for proving Proposition 9, it is enough to find $\chi_1,\chi_2$ for which $D\geqslant\frac{1}{4}t\geqslant\frac{1}{16}N$ and for which (5) holds.

*The distribution of the errors.* Suppose that the coloring $\chi\colon\{1,2,\dots,t\}\to\{+1,-1\}$ is chosen at random (all $2^t$ possible colorings have the same probability). We are now interested in distribution of the errors $E_{i,q}(\chi)$. Let us call a pair $P_j$ *good* for $i,q$, if $P_j\subset L^+_{i,q}$ or $P_j\subset L^-_{i,q}$, where $L^+_{i,q},L^-_{i,q}$ are the large slices as in Observation 10 (ii). Otherwise $P_j$ is *bad*. We let $J_{i,q}$ be the set of indices $j$ of all bad pairs.

We have $|J_{i,q}|=O(N^{1-1/d}+2^{-i}N)$. Indeed, each bad pair is either crossed by the great circle $q^*$ (and there are $O(N^{1-1/d})$ such pairs by Lemma 5 (i)), or has at least one point inside the small slices of the points $q$ and $\pi_{i-1}(q)$, and there are $O(2^{-i}N)$ points there by the choice of the $\mathcal{N}_i$ (using Lemma 6 (ii)).

Define random variables $X_{i,q,j}=\chi(j)\,[\varphi_{i,q}(v_j)-\varphi_{i,q}(u_j)]$. For a bad pair $P_j$ we have $|X_{i,q,j}|=O(2^{-i})$ by Observation 10 (i). For a good pair $P_j$ we get $|X_{i,q,j}|=O(2^{-i}N^{-1/d})$ by Observation 10 (ii). All the $X_{i,q,j}$ have zero expectations.

We obtain a tail estimate for the random variable $E_{i,q}(\chi)$ using Bernstein's inequality. First we split $E_{i,q}(\chi)$ into the contribution of the good pairs and of the bad pairs, i.e. $E_{i,q}(\chi)=E^G_{i,q}(\chi)+E^B_{i,q}(\chi)$, with $E^B_{i,q}(\chi)=\sum_{j\in J_{i,q}}X_{i,q,j}$ and $E^G_{i,q}(\chi)=\sum_{j\notin J_{i,q}}X_{i,q,j}$. For the good pairs we have at most $N$ independent random variables, each bounded by $B^G_i=O(2^{-i}N^{-1/d})$, so Bernstein's inequality gives

$$\operatorname{Prob}\bigl[E^G_{i,q}(\chi)\geqslant\alpha B^G_i\sqrt{N}\,\bigr]\leqslant e^{-\alpha^2/2}$$

(and symmetrically for the negative deviation of $E^G_{i,q}(\chi)$). Similarly for bad pairs, we have at most $m_i=O(N^{1-1/d}+2^{-i}N)$ independent random variables, each bounded by

$B_i^B = O(2^{-i})$, so we get

$$\text{Prob}[E_{i,q}^B(\chi) \geqslant \alpha B_i^B \sqrt{m_i}] \leqslant e^{-\alpha^2/2}.$$

Setting $M_i = B_i^G \sqrt{N} + B_i^B \sqrt{m_i} = O(2^{-i} N^{1/2-1/2d} + 2^{-3i/2} N^{1/2})$, altogether we get

$$\text{Prob}[E_{i,q}(\chi) \geqslant \alpha M_i] \leqslant e^{-\alpha^2/2} \quad \text{and} \quad \text{Prob}[E_{i,q}(\chi) \leqslant -\alpha M_i] \leqslant e^{-\alpha^2/2}. \tag{6}$$

*Estimating the entropy.* Let us summarize the current situation. We have a random mapping $\chi: \{1, 2, ..., t\} \to \{+1, -1\}$ and random variables $E_{i,q}(\chi)$ which are functions of $\chi$ and satisfy the tail estimates (6). We want to find values $\chi_1, \chi_2$ of $\chi$ which differ at many (at least $\frac{1}{4}t$) places, but for which $|E_{i,q}(\chi_1) - E_{i,q}(\chi_2)| \leqslant 2\Delta_i$ for all $i, q$. We define auxiliary functions $b_{i,q} = b_{i,q}(\chi)$ by letting $b_{i,q}(\chi)$ be the nearest integer to the number $E_{i,q}(\chi)/2\Delta_i$ (ties are broken by rounding up, say), and we let $b(\chi)$ be the vector $(b_{i,q}(\chi)$, $i = 1, 2, ..., k$, $q \in \mathcal{N}_i)$. With this notation, it is enough to require that $b(\chi_1) = b(\chi_2)$ for some $\chi_1, \chi_2$ differing in at least $\frac{1}{4}t$ components. To this end, it suffices to show that there is a value $\bar{b}$ of $b(\chi)$ with $\text{Prob}(b(\chi) = \bar{b})$ sufficiently large; then many different values of $\chi$ are assigned the same $b(\chi)$, and there are two values differing in sufficiently many components among them.

For quantitative bounds, we use an approach via entropy estimates. We only sketch the main points; details can be found in [1] or [16]. We recall that the *entropy* $H(X)$ of a discretely valued random variable $X$ is

$$H(X) = \sum_v -p_v \log_2(p_v),$$

where $p_v = \text{Prob}(X = v)$ and the summation is over all values $v$ possibly attained by $X$. Entropy is subadditive, that is, if $X = (X_1, ..., X_m)$ then $H(X) \leqslant \sum_{i=1}^m H(X_i)$.

The application of entropy for obtaining suitable $\chi_1, \chi_2$ in our situation is based on the following lemma.

LEMMA 11. *Let $\chi: \{1, 2, ..., t\} \to \{+1, -1\}$ be a random coloring, let $b(\chi)$ be a function of $\chi$, and suppose that $H(b(\chi)) \leqslant \frac{1}{5}t$. Then there exist colorings $\chi_1, \chi_2$, differing in at least $\frac{1}{4}t$ components, for which $b(\chi_1) = b(\chi_2)$.*

With the explicit constants given here, this appears in [16], but very similar ideas and calculations can be found in [1] as well.

By this lemma, it is enough to show $H(b(\chi)) \leqslant \frac{1}{5}t$ for the vector function $b(\chi)$ defined above. We have $H(b(\chi)) \leqslant \sum_{i,q} H(b_{i,q}(\chi))$. For estimating the entropy of the $b_{i,q}$, we may use the following (crude) bounds, calculated in [16]:

LEMMA 12. *Let $E$ be a real random variable satisfying the tail estimates*

$$\mathrm{Prob}[E \geqslant \alpha M] \leqslant e^{-\alpha^2/2}, \quad \mathrm{Prob}[E \leqslant -\alpha M] \leqslant e^{-\alpha^2/2},$$

*for some parameter $M>0$ and all $\alpha \geqslant 0$. Let $b=b(E)$ be defined as the nearest integer to $E/(2\lambda M)$, where $\lambda>0$ is another parameter. Then $H(b) \leqslant G(\lambda)$, where we define*

$$G(\lambda) = \begin{cases} C_0 e^{-\lambda^2/9} & \text{if } \lambda \geqslant 10, \\ C_0 & \text{if } 0.1 \leqslant \lambda \leqslant 10, \\ C_0 \ln(\lambda^{-1}) & \text{if } \lambda < 0.1, \end{cases}$$

*with $C_0$ being a sufficiently large absolute constant.*

We want to apply this lemma to estimate the entropy of $b_{i,q}(\chi)$, with $E_{i,q}(\chi)$ in the role of $E$. By (6) we can choose

$$M = M_i = O(2^{-i} N^{1/2-1/2d} + 2^{-3i/2} N^{1/2}).$$

Further we have $\Delta_i$ in the definition of $b_{i,q}(\chi)$ in the role of $\lambda M$, from which we calculate

$$\lambda = \lambda_i = \frac{\Delta_i}{M_i} \geqslant \frac{C_1}{1+(u-i)^2} \min\left(\frac{2^i}{N^{1/d}}, \frac{2^{3i/2}}{N^{3/2d}}\right),$$

with $C_1$ a constant which can be made as large as we wish by choosing the constant $K$ in the definition of $\Delta_i$ sufficiently large. Therefore, we have

$$H(b(\chi)) \leqslant \sum_{i=1}^{k} \sum_{q \in \mathcal{N}_i} H(b_{i,q}) \leqslant \sum_{i=1}^{k} |\mathcal{N}_i| G(\lambda_i) = \sum_{i=1}^{k} O(2^{di}) G(\lambda_i).$$

A routine calculation, which we omit, shows that if $K$ is chosen large enough, the last expression can be bounded by $\frac{1}{20}N \leqslant \frac{1}{5}t$ as required. This concludes the proof of Proposition 9. □

*Acknowledgment.* I would like to thank Professor Joram Lindenstrauss for bringing the problem to my attention.

## References


[1] ALON, N. & SPENCER, J., *The Probabilistic Method.* John Wiley & Sons, New York, 1992.

[2] BECK, J., Some upper bounds in the theory of irregularities of distribution. *Acta Arith.*, 43 (1984), 115–130.

[3] BETKE, U. & MCMULLEN, P., Estimating the sizes of convex bodies by projections. *J. London Math. Soc.*, 27 (1983), 525–538.

[4] BOURGAIN, J. & LINDENSTRAUSS, J., Distribution of points on the sphere and approximation by zonotopes. *Israel J. Math.*, 64 (1988), 25–31.

[5] — Approximating the ball by a Minkowski sum of segments with equal length. *Discrete Comput. Geom.*, 9 (1993), 131–144.

[6] BOURGAIN, J., LINDENSTRAUSS, J. & MILMAN, V., Approximation of zonoids by zonotopes. *Acta Math.*, 162 (1989), 73–141.

[7] CHAZELLE, B., Cutting hyperplanes for divide-and-conquer. *Discrete Comput. Geom.*, 9 (1993), 145–158.

[8] — Lecture notes on discrepancy and derandomization. Unpublished.

[9] CHAZELLE, B. & FRIEDMAN, J., A deterministic view of random sampling and its use in geometry. *Combinatorica*, 10 (1990), 229–249.

[10] CHAZELLE, B. & WELZL, E., Quasi-optimal range searching in spaces of finite VC-dimension. *Discrete Comput. Geom.*, 4 (1989), 467–489.

[11] EDELSBRUNNER, H., *Algorithms in Combinatorial Geometry.* EATCS Monogr. Theoret. Comput. Sci., 10. Springer-Verlag, Berlin–New York, 1987.

[12] LINHART, J., Approximation of a ball by zonotopes using uniform distribution on the sphere. *Arch. Math.*, 53 (1989), 82–86.

[13] MATOUŠEK, J., Cutting hyperplane arrangements. *Discrete Comput. Geom.*, 6 (1991), 385–406.

[14] — Tight upper bounds for the discrepancy of halfspaces. *Discrete Comput. Geom.*, 13 (1995), 593–601.

[15] — Efficient partition trees. *Discrete Comput. Geom.*, 8 (1992), 315–334.

[16] MATOUŠEK, J. & SPENCER, J., Discrepancy in arithmetic progressions. *J. Amer. Math. Soc.*, 9 (1996), 195–204.

[17] SPENCER, J., Six standard deviations suffice. *Trans. Amer. Math. Soc.*, 289 (1985), 679–706.

[18] WAGNER, G., On a new method for constructing good point sets on spheres. *Discrete Comput. Geom.*, 9 (1993), 111–129.



JIŘÍ MATOUŠEK
Department of Applied Mathematics
Charles University
Malostranské nám. 25
11800 Prague 1
Czech Republic
matousek@kam.ms.mff.cuni.cz


*Received February 27, 1996*