UNIVERSITÄT KAISERSLAUTERN

On the expected number of shadow vertices of the convex hull of random points

Karl-Heinz Küfer

Preprint Nr. 282

ISSN 0943-8874

Juli 1996

FACHBEREICH MATHEMATIK

On the expected number of shadow vertices of the convex hull of random points

K.-H. Küfer
Dept. of Mathematics, University of Kaiserslautern,
Erwin–Schrödinger-Str., 67663 Kaiserslautern, Germany

July 16, 1996

Abstract

Let $a_1, \ldots, a_m$ be independent random points in $\mathbb{R}^n$ that are independent and identically distributed spherically symmetrical in $\mathbb{R}^n$. Moreover, let X be the random polytope generated as the convex hull of $a_1, \ldots, a_m$ and let L_k be an arbitrary k-dimensional subspace of $\mathbb{R}^n$ with $2 \leq k \leq n-1$. Let X_k be the orthogonal projection image of X in L_k. We call those vertices of X, whose projection images in L_k are vertices of X_k as well shadow vertices of X with respect to the subspace L_k. We derive a distribution independent sharp upper bound for the expected number of shadow vertices of X in L_k.

Keywords: Stochastic geometry, random convex hulls, vertex process, shadow vertices
Mathematical subject classification: *Primary:* 60D05 *Secondary:* 52A22

1 Introduction and main results

We consider m independent random points a_i that are identically distributed spherically symmetric in $\mathbb{R}^n$. To be more formal, let

$$a_i = r_i\,\omega_i \tag{1}$$

be the polar representation of a_i with r_i in $\mathbb{R}_0^+$ and $\omega_i \in \mathcal{S}^{n-1}$, where r_i and ω_i are stochastically independent. r_i has the distribution function F, i.e. $F(r) = \Pr(r_i \le r)$ for $r \in [0,\infty)$, while ω_i is uniformly distributed on the unit sphere $\mathcal{S}^{n-1}$ in $\mathbb{R}^n$. Without loss of generality we assume F continuous from the right. In addition, we assume that the distribution of the a_i has no mass in the origin, i.e. $F(0) = 0$. Moreover, let

$$X := \operatorname{conv}(a_1, \ldots, a_m) \tag{2}$$

be the random polytope generated as the convex hull of $a_1, \ldots, a_m$.
For any k–dimensional subspace $L_k \subset \mathbb{R}^n$, $k \in \{2, \ldots, n-1\}$, let P_{L_k} be the ortho-projector onto L_k and let

$$X_k := P_{L_k}(X) = \operatorname{conv}(b_1, \ldots, b_m), \;\; b_i := P_{L_k} a_i, \tag{3}$$

be X's *shadow polytope* in L_k. We call those vertices of X, whose images under P_{L_k} are vertices of X_k as well, *shadow vertices* of X with respect to L_k. We denote the number of shadow vertices of X with respect to L_k with $v_k(X)$. The number of vertices of X_k is denoted by $v(X_k)$. By definition, $v_k(X) = v(X_k)$.

The question we deal with is: How many vertices of X are shadow vertices with respect to L_k? In a deterministic framework, the answer is easy: Let a_i be pairwise different points in $\mathbb{R}^n$. Then, for any $p \in \{1, \ldots m\}$ and any subspace L_k there is an arrangement of the a_i such that $v_k(X) = p$. Thus, worst–case analysis gives no information.
In this paper, we study the expected number $\mathrm{E}(v_k)$ of X's shadow vertices with respect to L_k in the stochastic model described above.
We will prove the following upper bound of $\mathrm{E}(v_k)$ that holds independent from the particular choice of the distribution in our stochastic model:

Theorem 1: *For any $2 \le k \le \lfloor n/2 \rfloor$ and $m \ge n+1$ holds:*

$$\mathrm{E}(v_k) \le C_k(n)\, k^{(n-k)/(n-1)}\, (m+1)^{(k-1)/(n-1)} \tag{4}$$

with

$$C_k(n) := \frac{2}{n-k} \frac{1}{B(\frac{n-k}{2}, \frac{k}{2})} (2\pi\, n)^{\frac{n-k}{2(n-1)}}. \tag{5}$$

Discussion:

1. The upper bound (4) is sharp as one can prove for the particular case of uniformly on the unit sphere $\mathcal{S}^{n-1}$ distributed a_i that for fixed n and k the expectation

$E(v_k)$ satisfies the asymptotic equation $\lim_{m\to\infty} \frac{E(v_k)}{m^{(k-1)/(n-1)}} = k^{(n-k)/(n-1)}\tilde{C}_k(n)$, where $\tilde{C}_k(n) = C_k(n)\left(\frac{(n-1)\mu_{n-1}}{\mu_n\sqrt{2\pi n}}\right)^{(n-k)/(n-1)}$. Here, μ_n is the $(n-1)$-dimensional Lebesgue-measure of $\mathcal{S}^{n-1}$. That means in particular that the bound delivers the smallest possible order of growth in m for fixed n and k. On the other hand, $C_k(n)$ considered as a function in n has the smallest possible order of growth in n for fixed k as $\lim_{n\to\infty} \tilde{C}_k(n)/C_k(n) = 1$.

2. It is possible to estimate $E(v_k)$ for $k \geq \lfloor n/2 \rfloor$ as well. This case is covered by Theorem 2 in Section 2, which gives a more general upper bound.

3. The emphasis of the bound in Theorem 1 is on the *minimal* order of growth in m. It is immediate that the given bound is much better than the trivial upper bound m for fixed n and k and *large* m.

   But what about moderate m? It is not hard to prove that the bound in Theorem 1 is better than the trivial upper bound m if $m \geq k\, C_k(n)^{(n-1)/(n-k)} + 1$. In particular, for $k = 2$ m must be at least $n+1$, for $k = 3$ must hold $m \geq 6n$. This means, the bound is meaningful even for relatively small values of m if k is small. In general, $C_k(n)$ satisfies the inequality $C_k(n) \leq 4\sqrt{\pi}(n/2)^{(k-1)/2}/\Gamma(k/2)$. Thus, m must have at least the order of magnitude $(n/2)^{(k-1)(n-1)/2(n-k)}$ in order to compete with the trivial upper bound. Thus, if $k \sim n^\epsilon$ for $n \to \infty$ and an $\epsilon \in (0,1]$, m must be exponentially large.

   The analysis shows that in case of moderate n and not too small k there is some need for estimates between the bound of Theorem 1 and the trivial upper bound. Theorem 3 delivers a scale of upper bounds depending on a parameter that can be chosen in an optimal way with respect to the particular triple (m, n, k) under consideration.

The question for the number of shadow vertices of X can be discussed in the framework of vertex processes in $\mathbb{R}^k$. As the points a_i are identically and spherically symmetrically distributed in $\mathbb{R}^n$ we may assume without loss of generality that $L_k = \text{lin}(e_1, \ldots, e_k)$, which we identify with $\mathbb{R}^k$. It is a basic observation that we can interpret the points $b_i = P_{L_k} a_i$, $i = 1, \ldots, m$, as independent and identically distributed points spherically symmetrical in $\mathbb{R}^k$ with the radial distribution function

$$F_k(r) := \Pr(\|b_i\|_2 \leq r) = \Pr(\|P_{L_k} a_i\|_2 \leq r), \quad r \in [0, \infty). \tag{6}$$

Thus, the sequence $(v_k)_{m\in\mathbb{N}}$ with $v_k = v(X_k)$ is a vertex process in $\mathbb{R}^k$. It is much known about the asymptotical properties of such vertex processes. For instance, Hueter [5] analyzed the limiting distribution of the normalized vertex process under classes of distributions in $\mathbb{R}^k$ generalizing results of Groeneboom [4]. We state the corresponding result for our particular process (v_k) and for uniformly distributed a_i on the sphere. The limiting distribution of the normalized process

$$\left(\frac{v_k - E(v_k)}{\sigma(v_k)}\right) \tag{7}$$

converges in distribution to the standard normal distribution $\mathcal{N}(0,1)$. This result is essentially due to the fact that the tail of the radial distribution function F_k, cf. (6), is regularly varying at 1 with exponent $(n-k)/2$ if the a_i are uniform on the sphere, as one can easily derive from Lemma 1 given below.
But the emphasis of our work is on *proper estimates* of $\mathrm{E}(v_k)$ and not on its asymptotical properties, which we could have easily obtained as consequences of Hueter's results.
In order to avoid misleading interpretations, we remark that the question we discuss here is no generalization of Borgwardt's analysis of the expected number of shadow vertices of polyheda with respect to a plane in [1,2], as the underlying probabilistic models are different.

2 The estimate of the expectation

Our first result is a formula that relates the tail $\bar{F}_k = 1 - F_k$ of the radial distribution function of the projected process to the tail $\bar{F} = 1 - F$ of the original radial distribution function:

Lemma 1: *For any radial distribution function F and $n > k \geq 2$ holds:*

$$\bar{F}_k(h) = \frac{1}{B(\frac{k}{2},\frac{n-k}{2})} \int_0^1 \bar{F}(\frac{h}{\sqrt{1-x}})(1-x)^{(k-2)/2} x^{(n-k-2)/2} dx, \quad h \in \mathbb{R}_0^+. \tag{8}$$

Proof: Let F be the radial distribution function of the points a_i, $i = 1,\ldots,m$. For the sake of simplicity let us assume for a while that F has a density, i.e. there exists a non-negative function $f : \mathbb{R}^n \to \mathbb{R}_0^+$ with $F(h) = \int_{h\mathcal{B}^n} f(a)da$ for all $r \in \mathbb{R}^+$. Here, $\mathcal{B}^n$ denotes the unit ball in $\mathbb{R}^n$. f is the density function of the spherically symmetrical distribution associated with the radial distribution function F. Moreover, let $\hat{f} : \mathbb{R}_0^+ \to \mathbb{R}_0^+$ be defined by $\hat{f}(r) = f(r\omega)$ for $r \in \mathbb{R}_0^+$ and $\omega \in \mathcal{S}^{n-1}$. We denote μ_d for the $(d-1)$–dimensional Lebesgue-measure of $\mathcal{S}^{d-1}$. F and $\hat{f}$ are related by the formula

$$dF(r) = \mu_n r^{n-1} \hat{f}(r) dr. \tag{9}$$

Thus, $r \longrightarrow \mu_n r^{n-1}\hat{f}(r)$, $r \in R^+$ is the radial density function.
For any point $a = a_i$, $i = 1,\ldots,m$, let $b = P_{L_k}a$ and $\bar{b} = a - b$. Then, by the definition of F_k we have

$$\bar{F}_k(h) = \int_{\mathbb{R}^{n-k}} \int_{\mathbb{R}^k} \chi(\|b\|_2 > h) f(b + \bar{b})\, db d\bar{b}. \tag{10}$$

We represent b and $\bar{b}$ in polar coordinates. Let $b = s\omega$ with $s \in \mathbb{R}_0^+$, $\omega \in \mathcal{S}^{k-1}$, and $\bar{b} = t\bar{\omega}$ with $t \in \mathbb{R}_0^+$ and $\bar{\omega} \in \mathcal{S}^{n-k-1}$. Then, we get after integration on the spheres

$$\bar{F}_k(h) = \mu_k \mu_{n-k} \int_0^\infty \int_h^\infty \hat{f}(\sqrt{s^2+t^2})\, s^{k-1} ds\, t^{n-k-1}\, dt. \tag{11}$$

It is wellknown that $\mu_d = 2\pi^{d/2}/\Gamma(d/2)$ for $d \geq 1$. Thus,

$$\mu_k \mu_{n-k} = \frac{2\mu_n}{B(\frac{k}{2}, \frac{n-k}{2})}. \tag{12}$$

We substitute $s^2 = u^2 - t^2$ in (11) and obtain by use of (9) and (12)

$$\bar{F}_k(h) = \frac{2}{B(\frac{k}{2}, \frac{n-k}{2})} \int_h^\infty \int_0^{\sqrt{u^2-h^2}} \left(1 - \frac{t^2}{u^2}\right)^{(k-2)/2} \left(\frac{t}{u}\right)^{n-k-1} dt \frac{dF(u)}{u}. \tag{13}$$

Now, we substitute $t = u\sqrt{y}$ and $u = h/\sqrt{1-x}$ in (13) and get

$$\bar{F}_k(h) = \frac{1}{B(\frac{k}{2}, \frac{n-k}{2})} \int_0^1 \int_0^x y^{(n-k-2)/2}(1-y)^{(k-2)/2} dy dF(\frac{h}{\sqrt{1-x}}). \tag{14}$$

Finally, we integrate (14) by parts and obtain the desired formula (8). As any radial distribution function F is a pointwise limit of an appropriate sequence of radial distributions with densities, we conclude from Lebesgue's theorem that (8) holds true for all radial distribution functions.

□

It is our next goal to derive a representation for $\mathrm{E}(v_k)$ that is appropriate for estimates. Let the points b_i, $i = 1, \ldots, m$, be independent and identically spherically symmetrically distributed in $\mathbb{R}^k$ with the radial distribution function F_k, whose tail $\bar{F}_k$ is given in Lemma 1. We call an elementary event $\{b_1, \ldots, b_m\}$ *non–degenerate*, if every subset consisting of k points is linearly independent and if every subset consisting of $k+1$ points is in general position. In our model, almost all elementary events are non–degenerate. So, we are allowed to concentrate on this case. If $\{b_1, \ldots, b_m\}$ is non–degenerate the number of vertices $v(X_k)$ is given by

$$v(X_k) = \sum_{i=1}^m \chi(b_i \notin \mathrm{conv}(b_j \mid j \neq i)). \tag{15}$$

Thus, by the identical distribution of the b_i, the expectation $\mathrm{E}(v_k) = \mathrm{E}(v)$ satisfies Efron's identity

$$\mathrm{E}(v_k) = m\,(1 - \Pr(b \in \mathrm{conv}(b_1, \ldots, b_{m-1}))) \tag{16}$$

with $b = b_m$.

Now, we evaluate a representation for $\Pr(b \in \mathrm{conv}(b_1, \ldots, b_{m-1}))$ in the framework of *facet–additive* polytope functionals – a concept introduced by the author [6]. In order to do that, we need some more notation. For any non–degenerate event $\{b_1, \ldots, b_m\}$ let

$$X' := \mathrm{conv}(b_1, \ldots, b_{m-1}) \tag{17}$$

be the polytope generated as convex hull of $b_1, \ldots, b_{m-1}$. For any set $I = \{i_1, \ldots, i_k\}$ of pairwise different indices drawn from $1, \ldots, m-1$ let $S_I := \text{conv}(b_i \mid i \in I)$ be the $(k-1)$–dimensional simplex generated by b_i with $i \in I$ and $\tilde{S}_I := \text{conv}(S_I \cup \{0\})$ be the associated k–dimensional simplex with additional vertex at the origin. Analogously, let $\tilde{X}' := \text{conv}(\{0\} \cup X')$. Each S_I is a candidate for being a boundary simplex of X'. We differentiate between two kinds of boundary simplices: S_I is called a *boundary simplex of the first kind* if S_I is a boundary simplex of X' and of $\tilde{X}'$ simultaneously. If S_I is a boundary simplex of X' but not of $\tilde{X}'$, we call S_I a *boundary simplex of the second kind.* We represent the functional $\Pr(b \in X')$ for fixed $b_1, \ldots, b_{m-1}$ as a sum of functionals of boundary simplices. In order to do that, we define a sign-functional $\sigma = \sigma(X', I)$ for the boundary simplex candidates S_I that is non-zero if and only if S_I is a boundary simplex of X'. If S_I is a boundary simplex of the first kind $\sigma(X', I) = 1$ and if S_I is a boundary simplex of the second kind $\sigma(X', I) = -1$. Elementary geometry delivers that for any non–degenerate $X' = \text{conv}(b_1, \ldots, b_{m-1})$ holds

$$\Pr(b \in X') = \sum_I \sigma(X', I) \Pr(b \in \tilde{S}_I). \tag{18}$$

This means, the mass of $\tilde{S}_I$ is added if S_I is a boundary simplex of the first kind and is subtracted if S_I is a boundary simplex of the second kind. Observing the identical distribution of the b_i, we average on the choice of the b_i and on the choice of b and get

$$\Pr(b \in X') = \binom{m-1}{k} \mathrm{E}(\sigma(X', I) \Pr(b \in \tilde{S}_I)) \tag{19}$$

for any fixed set of indices I.

The representation in (18) is a decomposition of $\Pr(b \in X')$ in functionals of the poytope X_k's boundary simplices. We call such a functional *f-additive*, which refers to facet–additive. Almost all interesting polytope functionals have such a decomposition property, which is very useful for the calculation of expectations and variances of these functionals under spherically symmetrical distributions. For a survey the interested reader is referred to [6].

With exactly the same technique used above for $\Pr(b \in X')$ we can evaluate a representation of the functional $\Pr(\text{cone}(X') = \mathbb{R}^k)$=$\Pr(0 \in \text{int}(X'))$. It holds:

$$\Pr(\text{cone}(X') = \mathbb{R}^k) = \binom{m-1}{k} \mathrm{E}(\sigma(X', I) \Pr(b \in \text{cone}(S_I)). \tag{20}$$

Hence, if we write (16) in the form

$$\mathrm{E}(v_k) = m \left\{ \Pr(\text{cone}(X') \neq \mathbb{R}^k) + \Pr(\text{cone}(X') = \mathbb{R}^k) - \Pr(b \in X') \right\} \tag{21}$$

and use (19) and (20), we obtain

$$\mathrm{E}(v_k) = m \left\{ \Pr(\text{cone}(X') \neq \mathbb{R}^k) + \binom{m-1}{k} \mathrm{E}(\sigma(X', I) \Pr(b \in \text{cone}(S_I) \setminus \tilde{S}_I)) \right\}. \tag{22}$$

By geometrical insight, the left summand on the right of (21) is independent from the specific underlying distribution and was independently calculated by Schlaefli and later on by Wendel:

Lemma 2: (Wendel [11]) *For any spherically symmetrical distribution in* $\mathbb{R}^k$ *and* $m > k \geq 2$ *holds:*

$$\Pr(\operatorname{cone}(X') \neq \mathbb{R}^k) = 2^{-m+2} \sum_{j=0}^{k-1} \binom{m-2}{j}. \tag{23}$$

Inserting (23) into (22), we have proven the following representation of $\mathrm{E}(v_k)$:

Lemma 3: *For any* $m > k \geq 2$, *any spherically symmetrical distribution in* $\mathbb{R}^n$ *and any set of indices* I *holds:*

$$\mathrm{E}(v_k) = m \left\{ 2^{-m+2} \sum_{j=0}^{k-1} \binom{m-2}{j} + \binom{m-1}{k} \mathrm{E}(\sigma(X', I) \Pr(b \in \operatorname{cone}(S_I) \setminus \tilde{S}_I)) \right\}. \tag{24}$$

Next, we try to simplify the expectation on the right of (24). Obviously, the probability $\Pr(b \in \operatorname{cone}(S_I) \setminus \tilde{S}_I)$ depends on b_i, $i \in I$, and b, only. Thus, preparing the evaluation of the expectation in (24) we calculate $\mathrm{E}(\sigma(X', I))$ for fixed b_i, $i \in I$, taking the average on b_j, $j \notin I$.

Let $\mathcal{H}_I$ be the hyperplane supporting S_I, let $\mathcal{H}_I^{(2)}$ be the closed halfspace lying beyond $\mathcal{H}_I$ and $\mathcal{H}_I^{(1)}$ be the closed complement of $\mathcal{H}_I^{(2)}$ in $\mathbb{R}^k$. The probability that a spherically symmetrically distributed vector b with radial distribution function F_k lies in $\mathcal{H}_I^{(i)}$ depends exclusively on the distance h_I of the hyperplane $\mathcal{H}_I$ from the origin. We define

$$G_k(h) := \Pr(b \in \mathcal{H}_I^{(2)} | h_I = h). \tag{25}$$

By spherical symmetry, the probability on the right hand side of (25) is independent from the specific choice of the hyperplane. So, we take $\mathcal{H}_I := he_1 + \operatorname{lin}(e_2, \ldots, e_k)$ and obtain

$$G_k(h) := \Pr(b^{(1)} \geq h), \tag{26}$$

where $b^{(1)}$ is the coordinate of b in the direction of e_1. Our next observation is that G_k does not depend on k. We remember that $b \in \mathbb{R}^k$ can be considered the projection of a random point $a \in \mathbb{R}^n$ that is spherically symmetrically distributed with radial distribution function F. Obviously, for $b = P_{L_k} a$ holds

$$G_k(h) = \Pr(b^{(1)} \geq h) = \Pr(a^{(1)} \geq h) =: G(h), \tag{27}$$

as the first $k \geq 2$ coordinates of a remain unchanged under the projection. As the b_i are independent and identically distributed for $i \notin I$, we have

$$\mathrm{E}(\sigma(X', I) | h_I = h) = (1 - G(h))^{m-1-k} - G(h)^{m-1-k}. \tag{28}$$

The function G is wellknown and was introduced by Rényi and Sulanke [10] for particular distributions. Lemma 4 gives a useful integral representation of G that holds for all spherically symmetrical distributions in $\mathbb{R}^n$:

Lemma 4: (Borgwardt [1,2]) For any radial distribution function F in $\mathbb{R}^n$, $n \geq 2$, holds:

$$G(h) = \frac{\mu_{n-1}}{\mu_n} \int_h^\infty \int_{h/r}^1 (1-x^2)^{(n-3)/2} dx\, dF(r), \quad h \in \mathbb{R}_0^+. \tag{29}$$

From the spherical symmetry of the underlying distribution we conclude that $G(h) \in [0, 1/2]$ and hence, the expectation $\mathrm{E}(\sigma(X', I))$, cf. (28), is non-negative.

It is a hard job to calculate $\Pr(b \in \mathrm{cone}(S_I) \setminus \tilde{S}_I)$ exactly as the geometry is rather complicated. So, we estimate it moderately from above. Before, we introduce a notation for the spherical angle generated by S_I: let

$$V(S_I) := \frac{\lambda_{k-1}(\mathrm{cone}(S_I) \cap \mathcal{S}^{k-1})}{\lambda_{k-1}(\mathcal{S}^{k-1})}, \tag{30}$$

where λ_{k-1} denotes the Lebesgue-measure of dimension $k-1$.

Lemma 5: *For any spherically symmetrical distribution in $\mathbb{R}^k$ with radial distribution function F_k holds:*

$$\Pr(b \in \mathrm{cone}(S_I) \setminus \tilde{S}_I) \leq V(S_I)\, \bar{F}_k(h_I). \tag{31}$$

Proof: For each $b \in \mathrm{cone}(S_I) \setminus \tilde{S}_I$ holds $\|b\|_2 > h_I$. Hence

$$\mathrm{cone}(S_I) \setminus \tilde{S}_I \subset \mathrm{cone}(S_I) \setminus h_I \mathcal{B}^k. \tag{32}$$

Let b have the polar representation $b = s\omega$ with $s \in \mathbb{R}_0^+$ and $\omega \in \mathcal{S}^{k-1}$. Then, by independence of ω and s we obtain

$$\Pr(b \in \mathrm{cone}(S_I) \setminus h_I \mathcal{B}^k) = \Pr(\omega \in \mathrm{cone}(S_I) \cap \mathcal{S}^{k-1}) \Pr(r > h_I). \tag{33}$$

As ω is uniformly distributed on $\mathcal{S}^{k-1}$ we have

$$\Pr(\omega \in \mathrm{cone}(S_I) \cap \mathcal{S}^{k-1}) = V(S_I). \tag{34}$$

By definition, we know that $\bar{F}(h_I) = \Pr(r > h_I)$ and (31) follows. □

The probability function $P(h) := \Pr(h_I \leq h)$ is wellknown to be absolutely continuous for any radial distribution function F_k in $\mathbb{R}^k$, cf. [9]. Henceforth, it has a density function p with $P(h) = \int_0^h p(h')dh'$. So, if we insert the estimate of Lemma 5 and (28) into (24) we can introduce $h = h_I$ as an independent variable. The law of total probability gives

$$\mathrm{E}(\sigma(X', I) \Pr(b \in \mathrm{cone}(S_I) \setminus \tilde{S}_I)) \leq \int_0^\infty ((1-G(h))^{m-1-k} - G(h)^{m-1-k}) \Lambda_V(h)\, \bar{F}_k(h)\, dh \tag{35}$$

with

$$\Lambda_V(h) := \mathrm{E}(V(S_I)|h_I = h)\, p(h). \tag{36}$$

The function Λ has a surprisingly simple representation in terms of $G_k = G$ as was proved by the author. We state it in a form that is reduced to our needs:

Lemma 6: (Küfer [7],[8]) *For any spherically symmetrical distribution in* $\mathbb{R}^k$ *with radial distribution function* F_k, $k \geq 2$, *holds:*

$$\Lambda_V(h) = -k\, G(h)^{k-1} \frac{\partial}{\partial h} G(h), \quad h \in \mathbb{R}_0^+. \tag{37}$$

Now, we substitute $t = G(h)$ in (35) and denote $\tilde{G}$ for the inverse function of G, i.e. $h = \tilde{G}(t)$ and $G(\tilde{G}(t)) = t$ for $t \in [0, 1/2]$. We obtain:

$$\mathrm{E}(\sigma(X', I)\Pr(b \in \mathrm{cone}(S_I) \setminus \tilde{S}_I)) \leq k \int_0^{1/2} ((1-t)^{m-1-k} - t^{m-1-k}) t^{k-1} \bar{F}_k(\tilde{G}(t)) dt. \tag{38}$$

We define

$$H_k(t) := \bar{F}_k(\tilde{G}(t)) \tag{39}$$

for $t \in [0, 1/2]$. H_k is a distribution function on $[0, 1/2]$ as we know that

$$H_k(t) = \Pr_b(\Pr_a(a^{(1)} \geq \|b\|_2) \leq t), \tag{40}$$

where a and b are independent with radial distributions F in $\mathbb{R}^n$ and F_k in $\mathbb{R}^k$ respectively. In (40), the inner probability is calculated with random a and fixed b, whereas the outer probability depends on random b. Using (38) and (39), we obtain immediately from Lemma 3:

Lemma 7: For any spherically symmetrical distribution in $\mathbb{R}^n$ and $m > n > k \geq 2$ holds:

$$\mathrm{E}(v_k) \leq m\, 2^{-m+2} \sum_{j=0}^{k-1} \binom{m-2}{j} + mk \binom{m-1}{k} \int_0^{1/2} ((1-t)^{m-1-k} - t^{m-1-k}) t^{k-1} H_k(t) dt. \tag{41}$$

If we replace $H_k(t)$ by its trivial bound 1 in Lemma 7, the right hand side of (41) equals m. This means that the estimate of Lemma 7 is not too rough.
Now, the only matter left is to estimate the function H_k independent from the underlying distribution.

Lemma 8: *For any spherically symmetrical distribution in* $\mathbb{R}^n$ *and* $2 \leq k \leq n-1$ *holds*

$$H_k(t) \leq C_k(n)\, t^{(n-k)/(n-1)}, \quad t \in [0, 1/2], \tag{42}$$

with $C_k(n)$ *as in (4).*

Proof: We take $\bar{F}_k$ in its representation (14). The kernel of this integral is a reduced beta function with upper bound

$$\int_0^x y^{(n-k-2)/2}(1-y)^{(k-2)/2}dy \leq \frac{2}{n-k}\,x^{(n-k)/2}, \quad x \in [0,1]. \tag{43}$$

We insert this upper bound into (14), substitute $x = 1 - h^2/r^2$ and obtain

$$\bar{F}_k(h) \leq \frac{2}{n-k}\frac{1}{B(\frac{n-k}{2},\frac{k}{2})}\int_h^\infty \left(1-\frac{h^2}{r^2}\right)^{(n-k)/2} dF(r). \tag{44}$$

Now, we estimate the integral on the right of (44) from above with Jensen's inequality and get

$$\int_h^\infty \left(1-\frac{h^2}{r^2}\right)^{(n-k)/2} dF(r) \leq \left(\int_h^\infty \left(1-\frac{h^2}{r^2}\right)^{(n-1)/2} dF(r)\right)^{(n-k)/(n-1)}. \tag{45}$$

On the other hand, we obtain easily from Lemma 4 that

$$G(h) \geq \frac{\mu_{n-1}}{\mu_n(n-1)}\int_h^\infty \left(1-\frac{h^2}{r^2}\right)^{(n-1)/2} dF(r). \tag{46}$$

Moreover, it is not hard to prove that $\frac{\mu_n(n-1)}{\mu_{n-1}} \leq \sqrt{2\pi\,n}$. Thus, we obtain

$$\int_h^\infty \left(1-\frac{h^2}{r^2}\right)^{(n-1)/2} dF(r) \leq \sqrt{2\pi\,n}\,G(h). \tag{47}$$

Finally, we replace the integral on the right hand side of (46) by the upper bound given in (47). By the definition of $C_k(n)$ in (4), this yields

$$\bar{F}_k(h) \leq C_k(n)\,G(h)^{(n-k)/(n-1)} \tag{48}$$

if we insert the estimate (45) into (44). The claim of Lemma 8 follows, if we substitute $h = \tilde{G}(t)$ in (48). □

Now, we are ready to give a distribution independent upper bound for $\mathrm{E}(v_k)$:

Theorem 2: *For any spherically symmetrical distribution of the* a_i *in* $\mathrm{I\!R}^n$ *and* $m > n > k \geq 2$ *holds:*

$$\mathrm{E}(v_k) \leq R_k(m,n) + C_k(n)\,k^{(n-k)/(n-1)}\,(m+1)^{(k-1)/(n-1)} \tag{49}$$

with $C_k(n)$ *as in (5) and*

$$R_k(m,n) := m\, 2^{-m+2} \left\{ \sum_{j=0}^{k-1} \binom{m-2}{j} - \frac{m-1}{m} \binom{m-2}{k-1} C_k(n)\, 2^{-(n-k)/(n-1)} \right\}. \tag{50}$$

Proof: We estimate the integral of the upper bound in Lemma 7 from above, if we replace $H_k(t)$ by its upper bound given by Lemma 8. With

$$I_k(m,n) := \int_0^{1/2} ((1-t)^{m-1-k} - t^{m-1-k})\, t^{k-1+\frac{n-k}{n-1}} dt \tag{51}$$

we have

$$\int_0^{1/2} ((1-t)^{m-1-k} - t^{m-1-k})\, t^{k-1}\, H_k(t) dt \le C_k(n)\, I_k(m,n). \tag{52}$$

It is easily checked that $I_k(m,n)$ satisfies

$$I_k(m,n) = B(m-k, k+\tfrac{n-k}{n-1}) - \int_0^{1/2} t^{m-1-k}[(1-t)^{k-1+\frac{n-k}{n-1}} + t^{k-1+\frac{n-k}{n-1}}] dt \tag{53}$$

$$\le B(m-k, k+\tfrac{n-k}{n-1}) - 2^{-m+2-\frac{n-k}{n-1}}/m,$$

as $1-t \ge t$ for $t \in [0,1/2]$. Hence, we have

$$mk\binom{m-1}{k} I_k(m,n) \le \frac{\Gamma(k+\frac{n-k}{n-1})\Gamma(m+1)}{\Gamma(k)\Gamma(m+\frac{n-k}{n-1})} - (m-1)\binom{m-2}{k-1} 2^{-m+2-\frac{n-k}{n-1}}. \tag{54}$$

As $\Gamma(x+\alpha) \le x^\alpha\, \Gamma(x)$ for $x > 0$ and $\alpha \in [0,1]$, we obtain

$$mk\binom{m-1}{k} I_k(m,n) \le k^{(n-k)/(n-1)}\, (m+1)^{1-\frac{n-k}{n-1}} - (m-1)\binom{m-2}{k-1} 2^{-m+2-\frac{n-k}{n-1}} \tag{55}$$

from which claim (49) follows. □

Corollary 1: *If* $k \le \lfloor n/2 \rfloor$ *in addition to the assumptions of Theorem 2, we have*

$$R_k(n,m) \le 0 \tag{56}$$

and Theorem 1 is completely proven.

Proof: We prove (56) only for $k \ge 4$. The particular cases $k = 2$ and $k = 3$ are easier and can be proved with standard methods.
For the rest of the proof let $m > n \ge 2k \ge 8$. As $\binom{m-2}{j} \le \binom{m-2}{k-1}$ for $j = 0, \ldots, k-1$, we conclude from (50)

$$R_k(m,n) \le km\, 2^{-m+2} \binom{m-2}{k-1} \left(1 - \frac{m-1}{km}\, C_k(n)\, 2^{-(n-k)/(n-1)}\right). \tag{57}$$

We introduce

$$S_k(n) := \frac{n}{n+1} \frac{2}{(n-k)k} \frac{1}{B(\frac{n-k}{2}, \frac{k}{2})} \left(\frac{\pi n}{2}\right)^{\frac{n-k}{2(n-1)}} \tag{58}$$

and obtain

$$R_k(m,n) \leq km\, 2^{-m+2} \binom{m-2}{k-1} (1 - S_k(n)), \tag{59}$$

as $(m-1)/m$ increases for $m > n$. It will be sufficient to prove that $S_k(n) \geq 1$ for $n \geq 2k$. For $\lfloor n/2 \rfloor \geq k \geq 4$ we know that

$$\frac{2}{(n-k)k} \frac{1}{B(\frac{n-k}{2}, \frac{k}{2})} \geq \frac{1}{2(n-4)} \frac{1}{B(\frac{n-4}{2}, 2)} = \frac{n-2}{8}. \tag{60}$$

Thus, we obtain from (59) by use of monotonicity arguments:

$$S_k(n) \geq \frac{k(k-1)}{2(2k+1)} (\pi\, k)^{\frac{k}{2(2k-1)}} \geq \frac{2}{3} (4\pi)^{1/4} > 1 \tag{61}$$

and the proof is complete. □

As we mentioned in the discussion after Theorem 1 the emphasis of our estimate was on optimality of the order of growth in m and we saw that m has to be very large for a competition with the trivial bound m if k is not small enough.
How can we find better estimates for moderate m and bigger k? One method is to weaken the order of growth in m. That means, we seek for bounds of the type

$$\mathrm{E}(v_k) \leq C_k^{(\alpha)}(n)\, k^{\alpha \frac{n-k}{n-1}} \,(m+1)^{1-\alpha+\alpha \frac{k-1}{n-1}} \tag{62}$$

with $\alpha \in [0,1]$, where we choose $C_k^{(\alpha)}(n)$ as small as possible. Obviously, for $\alpha = 1$ we may choose $C_k^{(1)}(n) = C_k(n)$ with $C_k(n)$ from Theorem 1, whereas we can choose $C_k^{(0)}(n) = 1$ for $\alpha = 0$. These choices are asymptotically optimal for $n \to \infty$. Hence, $C_k^{(1)}(n)$ corresponds to the minimal rate of growth in m while $C_k^{(0)}(n)$ corresponds to the trivial bound m with the maximal possible order of growth in m. The following result gives an upper bound for $\mathrm{E}(v_k)$ minimizing on the choice of α:

Theorem 3: *For any spherically symmetrical distribution of the $a_i \in \mathbb{R}^n$ and $m > n > k \geq 2$ holds:*

$$\mathrm{E}(v_k) \leq \min_{\alpha \in [0,1]} \left\{ R_k^{(\alpha)}(m,n) + C_k^{(\alpha)}(n)\, k^{\alpha \frac{n-k}{n-1}} \,(m+1)^{1-\alpha+\alpha \frac{k-1}{n-1}} \right\} \tag{63}$$

with

$$C_k^{(\alpha)}(n) := (1-\alpha)^{-k/2} (2\pi\, n)^{\frac{\alpha}{2} \frac{n-k}{n-1}} \tag{64}$$

for $\alpha \in [0,1)$ and $C_k^{(1)}(n) = C_k(n)$ with $C_k(n)$ as in Theorem 1. $R_k^{(\alpha)}(m,n)$ is given by

$$R_k^{(\alpha)}(m,n) := m\, 2^{-m+2} \left\{ \sum_{j=0}^{k-1} \binom{m-2}{j} - \frac{m-1}{m} \binom{m-2}{k-1} C_k^{(\alpha)}(n)\, 2^{-\alpha \frac{n-k}{n-1}} \right\}. \tag{65}$$

Proof: We prove the Theorem for $\alpha \in [0,1)$ only, as the particular case $\alpha = 1$ is already done. The starting point for the proof is the upper bound from Lemma 7. We split off the argumentation in two stages. First, we establish a scale of upper bounds for the function H_k, cf. (39), second, we imitate essentially the proof of Theorem 2 for those upper bounds.
Stage 1: In order to estimate H_k from above, we start with an upper bound for reduced beta functions, cf. (43). It holds for $p \in [0, n-k)$:

$$\int_0^x y^{(n-k-2)/2}(1-y)^{(k-2)/2}dy \le x^{p/2}B(\tfrac{n-k-p}{2}, \tfrac{k}{2}). \tag{66}$$

Thus, if we insert (66) in (14) and substitute $x^2 = 1 - h^2/r^2$ we get

$$\bar{F}_k(h) \le \frac{B(\frac{n-k-p}{2}, \frac{k}{2})}{B(\frac{n-k}{2}, \frac{k}{2})} \int_h^\infty \left(1 - \frac{h^2}{r^2}\right)^{\frac{p}{2}} dF(r). \tag{67}$$

It is well known, that

$$\frac{B(\frac{n-k-p}{2}, \frac{k}{2})}{B(\frac{n-k}{2}, \frac{k}{2})} \le \left(\frac{n-k}{n-k-p}\right)^{\frac{k}{2}}. \tag{68}$$

We estimate the integral on the right of (67) with Jensen's inequality from above following lines (45)-(47) and get

$$\bar{F}_k(h) \le \left(\frac{n-k}{n-k-p}\right)^{\frac{k}{2}} (\sqrt{2\pi}\, n\, G(h))^{p/(n-1)}. \tag{69}$$

Finally, we substitute $h = \tilde{G}(t)$ and $p = \alpha(n-k)$ and obtain for $\alpha \in [0,1)$

$$H_k(t) \le (1-\alpha)^{-k/2}(\sqrt{2\pi}\, n\, t)^{\alpha\frac{n-k}{n-1}}, \; t \in [0, 1/2]. \tag{70}$$

Stage 2: We insert the upper bound (70) for H_k into the upper bound of $\mathrm{E}(v_k)$ from Lemma 7 and imitate the proof of Theorem 2 replacing all terms $(n-k)/(n-1)$ in lines (51)-(55) by $\alpha(n-k)/(n-1)$ and the proof is complete. □

In order to arrive at estimates of type (62) we try to get rid of the cumbersome terms $R_k^{(\alpha)}(m,n)$. Unfortunately, this is not possible for all triples (m,n,k) and all α, cf. Corollary 1. We have:

Corollary 2: *In addition to the assumptions of Theorem 3 let $n \ge 2k$ and $\alpha \in [\alpha_{\min}, 1]$ with*

$$\alpha_{\min} := 1 - k^{-\frac{2}{k}}. \tag{71}$$

Then, it holds:

$$\mathrm{E}(v_k) \le C_k^{(\alpha)}(n) k^{\alpha\frac{n-k}{n-1}}(m+1)^{1-\alpha+\alpha\frac{k-1}{n-1}} \tag{72}$$

with $C_k^{(\alpha)}(n)$ *as in (64).*

Proof: Like in the proof of Corollary 1 it is enough to show that $R_k^{(\alpha)}(m,n) \leq 0$. We will prove claim (72) for $k \geq 4$, only. The particular cases $k = 2$ and $k = 3$ are omitted here, as they are easily obtained from the definition of $R_k^{(\alpha)}$.
We have for $m > n \geq 2k \geq 8$:

$$R_k^{(\alpha)}(m,n) \leq km2^{-m+2}\binom{m-2}{k-1}(1 - S_k^{(\alpha)}(n)), \tag{73}$$

where $S_k^{(\alpha)}(n)$ is defined by

$$S_k^{(\alpha)}(n) := \frac{n}{(n+1)k}(1-\alpha)^{-k/2}\left(\frac{\pi n}{2}\right)^{\frac{\alpha(n-k)}{2(n-1)}}. \tag{74}$$

We have to prove that $S_k^{(\alpha)}(n) \geq 1$. Using monotonicities we get immediately

$$S_k^{(\alpha)}(n) \geq \frac{2k}{2k+1}(\pi k)^{\alpha_{\min}/4}. \tag{75}$$

On the other hand, for $k \geq 4$ holds

$$(\pi k)^{\alpha_{\min}/4} \geq (\pi k)^{\frac{\ln k}{4k}} \geq \exp\left(\frac{\ln k}{2k}\right) \geq \frac{2k+1}{2k} \tag{76}$$

and we are done. □

Discussion: The starting point for our refined upper bound for $\mathrm{E}(v_k)$ in Theorem 3 was the observation that the bound given in Theorem 1 with the minimal order of growth in m is not meaningful unless $m \geq C\,(n/2)^{(k-1)/2}$ for a certain constant C depending on k. It is not hard to prove that the bound in Theorem 3 is meaningful if $m \geq 1 + e\sqrt{2\pi n k}$. That means for any $m \geq 1 + e\sqrt{2\pi n k}$ that there exists an $\alpha > 0$ such that the bound of Theorem 3 is better than the trivial one. If k is not too big and m is not too small, it is a good choice to take $\alpha = 1/2$. Here, we can derive from Corollary 2 that (72) is meaningful if $m \geq 1 + \sqrt{2\pi n k}2^{k\frac{n-1}{n-k}}$. Here, for fixed k, m grows like $\sqrt{n}$ for fixed k.

Concluding remarks: In this work we have considered expectations of v_k exclusively. It is a natural question to ask whether the expectation $\mathrm{E}(v_k)$ is reliable or – more formally spoken – whether $\Pr(|v_k - \mathrm{E}(v_k)| \geq t\mathrm{E}(v_k))$ is small for some $t > 0$. For fixed n and k and large m the answer is affirmative for particular distributions within the class of spherically symmetrical distributions. For instance, if the distribution is concentrated in the unit ball and if the radial distribution function F is regularly varying near 1, $\mathrm{Var}(v_k)/\mathrm{E}^2(v_k)$ tends to zero as m tends to infinity. This can be shown using methods introduced by Groeneboom [4] and Hueter [5]. Hence, by Chebychev's inequality the expectation $\mathrm{E}(v_k)$ is reliable as the probability of a relative deviation tends to zero for $m \to \infty$.
For moderate m there is no satisfying answer. The only fact known so far is due to Devroye [3], who proved for a class of convex hull variables covering our variables v_k that

the quotient $\mathrm{E}(v_k^p)/\mathrm{E}^p(v_k)$ is bounded from above for any $p \in \mathbb{N}$, where the bound only depends on p. Unfortunately, these bounds are to big for showing reliability in the above described sense. So, the question for good tail bounds for the distribution of $E(v_k)$ is open.
Another interesting open question is the following: The distribution independent upper bound of Theorem 1 is sharp for the uniform distribution on the sphere, cf. the discussion following Theorem 1. We conjecture that the expectation $\mathrm{E}(v_k)$ for any fixed k, n, m attains its maximum value if and only if the a_i are uniformly distributed on a sphere.

References

[1] Borgwardt, K. H.: *The average number of pivot steps required by the simplex–method is polynomial.* ZOR (1981), 157-177.

[2] Borgwardt, K. H.: *The simplex method — a probabilistic analysis.* Springer, New York, Berlin, Heidelberg (1987).

[3] Devroye,L.: *Moment inequalities for random variables in computational geometry.* Computing 30 (1983), 111-119.

[4] Groeneboom, P.: *Limit theorems for convex hulls.* Prob. Theory Rel. Fields 79 (1988), 327-368.

[5] Hueter, I.: *The convex hull of n random points and its vertex process.* Dissertation, Universität Bern (1992).

[6] Küfer, K.-H.: *A unified asymptotic probabilistic analysis of polyhedral functionals: a survey.* J. Comp. and Inf. 4 (1994), 145-161.

[7] Küfer, K.-H.: *Zur Asymptotik in der stochastischen Polyedertheorie.* Diplomarbeit, Universität Kaiserslautern (1988).

[8] Küfer, K.-H.: *An improved asymptotic analysis of the expected number of pivot steps required by the simplex algorithm.* To appear in ZOR (1996).

[9] Küfer, K.-H.: *Asymptotische Varianzanalysen in der stochastischen Polyedertheorie.* Dissertation, Universität Kaiserslautern (1992).

[10] Rényi, A. and Sulanke, R.: *Über die konvexe Hülle von n zufällig gewählten Punkten I.* Z. Wahrscheinlichkeitsth. 2 (1994), 76-84.

[11] Wendel, J.: *A problem in geometric probability.* Math. Scand. 11 (1962), 109-111.