Ideas for an Old Analytic Enigma about the Sphere that Fail in Intriguing Ways

Frederik von Heymann[*]

November 16, 2012

Abstract

For any given dimension n and unit vector $a \in S^{n-1}$, we investigate the well known question of how many sign vectors in $\{\pm 1\}^n$ can have a scalar product with a between -1 and 1.

We look at reformulations of this, and use simple observations about a geometric version of the question to derive an algorithm that finds unit vectors maximizing this number for given dimension. Our results support the conjectured lower bound of $1/2$ of the sign vectors.

1 Introduction

It was always my impression that in mathematics the strong focus on new results leads to the curious situation that whenever one is confronted with a new problem, almost everyone tries to solve it in the same way many before him or her did.

Let us make this more concrete. Consider the following problem, where, as usual, $S^{n-1} = \left\{a \in \mathbb{R}^n \ : \ \sum_{i=1}^n a_i^2 = 1\right\}$ is the n-dimensional sphere:

Let $a = (a_1, \ldots, a_n)$ be any point in S^{n-1}. Of the 2^n expressions

$$|\varepsilon_1 a_1 + \cdots + \varepsilon_n a_n| \quad \text{with} \quad \varepsilon_i = \pm 1,$$

can there be more with value > 1 than with value ≤ 1? This is the formulation in which Bogusłav Tomaszewski was quoted in [Guy86] in 1986. To give an indication of the general belief of most people who worked on the question, here is a more suggestive formulation:

[*] Faculty Electrical Engineering, Mathematics and Computer Science, Delft University of Technology, E-mail: F.J.vonHeymann@tudelft.nl

Conjecture 1.1 (e.g. [HK92])**.** *For all $a \in S^{n-1}$,*

$$|\{\varepsilon \in \{\pm 1\}^n \ : \ |\varepsilon \cdot a| \leq 1\}|/2^n \geq \frac{1}{2}.$$

Here, and everywhere else in the text, "$\cdot$" denotes the inner product of two vectors.

My first thought in cases like this is: "Can I use induction?", and if that fails, as it inevitably does for me when I read open problems in articles, "What happens if it's not true?"

I strongly suspect that something very similar is true for most mathematicians. And I don't think this is a bad thing. It is, in my opinion, at the very foundation of what we do: We try out our tools, starting with the more basic ones and then increase the level of sophistication, whenever we encounter new mathematical riddles.

Thus, I would like to spend the larger part of the following lines on retelling interesting, but ultimately abandoned attempts to use known tools on this still unsolved problem. I think the connections between different parts of mathematics, which appear around this question, can be appreciated even without the great finale of a definitive solution.

2 Say it again, but differently

After an open problem passed an initial sanity check, i.e., we convinced ourselves that we see no reason why it is obviously right or wrong, probably one of the most common methods is to restate the problem in a different formulation, preferably using terminology from another branch of mathematics. So this is what we will do next.

In [HK92], Ron Holzman and Daniel Kleitman propose the below translations of the Conjecture. They are all equivalent to 1.1, where an indication of the flavor of the reformulation is given at the beginning of each statement.

(i) *Sum partitions.* Let $\sum a_i$ be a finite sum, and assume it is normalized to $\sum a_i^2 = 1$. Then at least half of all partitions of the a_i into two parts lead to partial sums that differ by at most 1.

(ii) *Chebyshev-type inequality.* We can regard $\{\pm 1\}^n$ as a probability space with the discrete uniform distribution, and $X = \varepsilon \cdot a$ as a random variable with $E(X) = 0$ and $Var(X) = \sum a_i^2 = 1$. Then X lies within one standard deviation of its mean with probability $\geq \frac{1}{2}$.

(iii) *Geometric representation.* Consider an n-dimensional Euclidean ball and a smallest n-dimensional cube containing it. Then for any pair of parallel supporting hyperplanes of the ball, at least half the vertices of the cube lie between (or on) the two hyperplanes. See Figure 1.

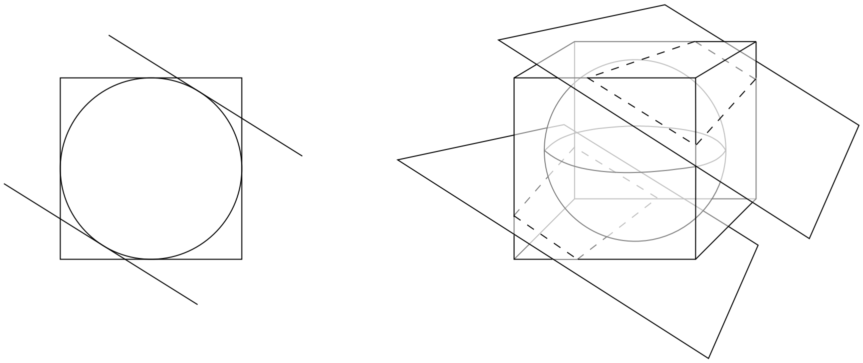


Figure 1: Examples in dimension 2 and 3.

Holzman and Kleitman prove in [HK92] that the left-hand-side in Conjecture 1.1 is at least $\frac{3}{8}$, where they primarily use formulation (ii) above, and in a rather elegant way at that. They also give indications why an approach similar to theirs will most likely not lead to a bound closer to the conjecture.

While formulation (iii) is my personal favorite and will be discussed in greater detail below, I am not aware of anyone trying his luck with (i). But before we proceed to the geometric considerations, let us add another formulation, to which we will come back in section 5:

(iv) *Percolation theory.* Consider the Boolean functions f_a on $\{\pm 1\}^n$, with

$$f_a(v) = \begin{cases} 1 & \text{if } |a \cdot v| > 1, \\ 0 & \text{otherwise.} \end{cases}$$

Then for every $a \in S^{n-1}$ we have $\|f_a\|^2 = \frac{1}{2^n} \sum_{v \in \{\pm 1\}^n} f_a(v)^2 \leq \frac{1}{2}$.

For now, however, we turn to the formulation (iii) above. Although it speaks of arbitrary spheres and fixes no orientation for the cube, it surely doesn't influence the outcome to scale or translate the problem, or to rotate the cube around its center. Thus we will only consider spheres around the origin with radius 1, and we will assume that each facet of the cube around it is orthogonal to one of the coordinate-axes.

For convenience, let us denote the n-dimensional ± 1-hypercube as $C^n = \{x \in \mathbb{R}^n \ : \ -1 \leq x_i \leq 1\}$. Then each $\varepsilon \in \{\pm 1\}^n$ corresponds to a vertex of C^n, which in turn is a smallest cube containing S^{n-1}.

It should be mentioned that Conjecture 1.1 comes up in various settings, in addition to the ones cited before also in, e.g., [Ver08] and [BTNR02]. Strongly related questions can be found in, e.g., [Ole96, Pin07, Pin10] and the references therein.

In fixed dimension, we will exploit formulation (iii) to derive cases that can be solved explicitly. We then use them to sketch an algorithm that can exclude large parts of the possible cases in a fast manner. The remaining cases are checked for counterexamples with quadratic programming. This can be summarized as follows:

Theorem 2.1. *If $n \leq 9$, then for all $a \in S^{n-1}$ we have*

$$|\{\varepsilon \in \{\pm 1\}^n \ : \ |\varepsilon \cdot a| \leq 1\}|/2^n \geq \frac{1}{2}.$$

Why $n \leq 9$? Because due to the rapidly increasing number of sets to check when the dimension increases, the computation was stopped after $n = 9$, which still can be done in reasonable time (see [vH10] for an implementation of the algorithm).

3 Some Geometric Observations

Now let's have a closer look at the geometric interpretation of Conjecture 1.1. There will be some proofs when it seems appropriate, but sometimes it would be, in my opinion, more distracting than illuminating. Nevertheless, it certainly gets more technical from here on out.

From now on, when we talk about a point a on the sphere, you should also think of the supporting hyperplane of the sphere at this point.

Observation 3.1. *By symmetry we can assume $a = (a_1, \ldots, a_n)$ to lie in the positive orthant and also it is no restriction to assume $a_1 \geq a_2 \geq \ldots \geq a_n$.*

Note that this implies that the vertex of C^n with only positive coordinates has the maximal distance to the hyperplane H at a among all separated vertices, because $H = \{x \in \mathbb{R} \ : \ a \cdot x = 1\}$, and thus the distance of any $x \in \mathbb{R}$ to H equals $|a \cdot x - 1|$. Here we call a set A of vertices *separated*, if we find a supporting hyperplane of the sphere that strictly separates A from zero.

With this observation we can rephrase the above conjecture as follows:

Conjecture 3.2. *Let $a \in S^{n-1}$ as in Observation 3.1, then $v \cdot a > 1$ for at most 2^{n-2} vertices $v \in C^n$.*

One question we did not address so far is if this bound can be strengthened. This is not the case, as it is achieved in every dimension by, e.g., $a = (\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}, 0, \dots, 0)$. An interesting result of the computations, however, is that this is the only tight example in all dimensions that were checked, up to small perturbations that cut off the same vertices of C^n, and the above mentioned symmetries.

At this stage it would be nice to have some form of order on the vertices of the cube, depending only on a. Then all we had to do is to find the "last" vertex separated from the sphere by a, and count the partition.

For given a, an obvious candidate to describe this order is the distance between separated vertices and the hyperplane at a. We get a (non-antisymmetric) order on the vertices of C^n:

$$v \preccurlyeq w \quad \Leftrightarrow \quad a \cdot v \leq a \cdot w.$$

Therefore, if a vertex v is separated, so are all larger vertices (or of the same size), and in particular all vertices in the face of minimal dimension containing both v and $(1, \dots, 1)$.

If $v \preccurlyeq w$, then we sometimes say w is *implied* by v, or that w is a *subvertex* of v.

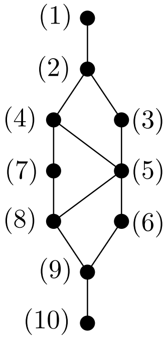
An important observation for our algorithm later on will be that already the assumptions $a_1 \geq \cdots \geq a_n \geq 0$ give us a *partial* order, without the need for any further knowledge about a (see Figure 2 for an example).

Definition 3.3. We call two vertices $v, w \in C^n$ *antipodal*, if $v = -w$. If v and w coincide in exactly one coordinate, we call them *facet-antipodal*.

The second definition is inspired by the fact that any facet of C^n can be characterized by fixing one coordinate. Thus, facet-antipodal vertices are antipodal in the lower-dimensional cube that is the common facet they are in.

Proposition 3.4. *Let $V \subseteq \{\pm 1\}^n$. If $v, w \in V$ are antipodal or facet-antipodal, then $v \cdot a \leq 1$ or $w \cdot a \leq 1$ (or both).*

In both cases, V can not be separated.



(1)	(1,1,1,-1,-1)
(2)	(1,1,-1,1,-1)
(3)	(1,1,-1,-1,1)
(4)	(1,-1,1,1,-1)
(5)	(1,-1,1,-1,1)
(6)	(1,-1,-1,1,1)
(7)	(-1,1,1,1,-1)
(8)	(-1,1,1,-1,1)
(9)	(-1,1,-1,1,1)
(10)	(-1,-1,1,1,1)

Figure 2: The partial order on the vertices of C^5 with two -1's (under the symmetry assumptions from Observation 3.1). The vertex (1) is the most implied in this set.

Proof. If $v, w \in V$ are antipodal or facet-antipodal, then $\|\frac{1}{2}v + \frac{1}{2}w\| \leq 1$ (equal in the facet-antipodal case), and thus this point lies on or in the sphere. Now suppose $v \cdot a > 1$ and $w \cdot a > 1$, then for every convex combination c of v and w we also get $c \cdot a > 1$, in contradiction to the above. □

This very simple observation can be used to prove our first result, which again is not very deep, but powerful enough to solve Conjecture 1.1 for $n \leq 4$.

Theorem 3.5. *Any supporting hyperplane of S^{n-1} can separate at most half the vertices of every facet of the ± 1-cube from the sphere.*

Proof. Fix a facet F. As we just observed, every vertex of F that we separate gives us a facet-antipodal vertex of F that cannot simultaneously be separated. □

Thus, if a hyperplane has empty intersection with the interior of at least one facet of the cube, then the conjecture is true. But against the intuition one might have from dimension 2 and 3, this is not fulfilled for every hyperplane in dimension at least 5:

Proposition 3.6. *In dimension $n \geq 5$ there are supporting hyperplanes of S^{n-1} that intersect all facets of C^n in their interior.*

Proof. Let $n \geq 5$. Consider $a = (\frac{1}{\sqrt{n}}, \ldots, \frac{1}{\sqrt{n}})$ and $v = (v_1, \ldots, v_n) \in \{\pm 1\}^n$. Then

$$a \cdot v > 1 \quad \Leftrightarrow \quad \sum_{i=1}^{n} \tfrac{1}{\sqrt{n}} v_i > 1 \quad \Leftrightarrow \quad \sum_{i=1}^{n} v_i > \sqrt{n},$$

and therefore all vertices with exactly one -1 are separated. But as every facet contains at least one of these (remember that we can characterize them by fixing exactly one coordinate), the hyperplane with touching point a intersects all facets in the interior. $\square$

We can compute that this particular a will not cause any trouble for the conjecture:

We claim that for any $n \in \mathbb{N}$

$$P(|\frac{1}{\sqrt{n}}\sum_{i=1}^{n} v_i| \leq 1) = 1 - P(\frac{1}{\sqrt{n}}\sum_{i=1}^{n} v_i > 1) - P(\frac{1}{\sqrt{n}}\sum_{i=1}^{n} v_i < -1)$$

is bounded from below by $1/2$. Note that the last two terms have the same value because of the symmetric definition of the v_i.

Now we can use the Berry-Esseen inequality

$$\left| P\left(\frac{1}{\sqrt{n}}\sum_{i=1}^{n} X_i \geq x\right) - \overline{\Phi}(x) \right| \leq \frac{C}{\sqrt{n}} E|X_1|^3,$$

where X_i are i.i.d. zero-mean unit-variance random variables, $x \in \mathbb{R}$, $n \in \mathbb{N}$, $\overline{\Phi}$ is the tail of the standard normal distribution, and C is an absolute constant < 0.48 (see [Tyu09, She11]).

In our situation this implies

$$P\left(\frac{1}{\sqrt{n}}\sum_{i=1}^{n} v_i > 1\right) < \overline{\Phi}(1) + \frac{0.48}{\sqrt{n}} < 0.159 + \frac{0.48}{\sqrt{n}}, \tag{1}$$

and the right-hand side is $< \frac{1}{4}$ for $n \geq 28$. The remaining cases $n \leq 27$ are easy to check by computer.

In fact, from Equation (1) we immediately get that the fraction of separated vertices gets smaller and smaller with growing dimension. This is also of interest because a conjecture related to Conjecture 1.1 was recently disproven by Pinelis [Pin12], using a vector similar to this a.

4 The Sketch of an Algorithm

In spite of the negative taste of the above result, we can use it to check small dimensions. The idea for the algorithm is the following: Given a set $V \subseteq \{\pm 1\}^n$ which is closed upwards in our partial order, we want to find properties that imply that V can not be separated. If we cannot separate any V with $|V| > 2^{n-2}$, there is no counterexample to Conjecture 1.1 in dimension n (and below).

Assume for the moment that we found properties of sets V that are easy to check, and each of which implies that V cannot be separated. Then fix an order on the vertices (any order, it does not have to be compatible with our partial order), and try to find a set V as large as possible while avoiding the properties, where we potentially go through the whole binary decision-tree.

Our goal now is of course to cut as many branches off as possible. There are only some details given below, but if you are intrigued beyond the scope of this text, I will be happy to provide more details in personal communication.

One observation we can handily utilize to restrict our search is the following: If V does not contain all vertices of C^n with exactly one -1, then V cannot be a counterexample to the conjecture, as it lies completely in one facet. Thus, we only have to check closed subsets containing all vertices with one -1.

Another practical fact is a generalization of the idea of facet-antipodal vertices. In Theorem 3.5 we showed that a set V containing antipodal or facet-antipodal vertices cannot be separated.

In a similar fashion, we can deduce the following sufficient condition:

Observation 4.1. *If $V \subseteq \{\pm 1\}^n$ contains k vertices $v_1, \ldots, v_k$ with*

$$\left\| \sum_{j=1}^{k} \frac{1}{k} v_j(i) \right\| \leq 1,$$

then V cannot be separated. Such a group of vertices will be called a non-separable k-set.

The case $k = 4$ is especially convenient, as we can construct a simple test from a subset of this to exclude many sets of vertices as possible counterexamples: Given v, we look for one other vertex w, such that each of them implies one more vertex, and all four together build a non-separable 4-set. This case has the advantage over higher k, that between all possible w, there is one that is implied by the others.

The reader is cordially invited to try his/her basic tools on this claim.

Now suppose we have constructed some set $V = \{v_1, \dots, v_m\}$ with $m > 2^{n-2}$. We have to unambiguously decide whether it can be separated or not. This can be done by computing the minimal norm of vectors in the convex hull of V, as we can separate V if and only if this norm is strictly larger than 1. That is, we compute

$$\min \left\{ \|x\| \;:\; x = \sum_{i=1}^{m} \lambda_i v_i,\ \lambda_i \geq 0,\ \sum \lambda_i = 1 \right\},$$

or equivalently

$$\min \left\{ t \in \mathbb{R} \;:\; Ay = b,\ y = (\lambda_1, \dots, \lambda_m, t, x^T)^T,\ \lambda_i \geq 0,\ (t, x^T) \in Q_{\text{cone}} \right\}$$

with

$$A = \begin{pmatrix} & & & 0 & -1 & & 0 \\ v_1 & \cdots & v_m & \vdots & & \ddots & \\ & & & 0 & 0 & & -1 \\ 1 & \cdots & 1 & 0 & 0 & \cdots & 0 \end{pmatrix}, \quad b = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}, \quad \text{and}$$

$Q_{\text{cone}} = \{(s, z) \in \mathbb{R} \times \mathbb{R}^n \;:\; s \geq \|z\|\}$, which is known as the quadratic cone, second order cone, or Lorentz cone (see, e.g., [LVBL98]).

Note that the zero-column in A is necessary, because t is a slack-variable to bound the norm of x.

Of course, one could attempt to use this strategy even earlier in the construction to reject sets sooner, but it turns out that the price in computation time one has to pay for this is much higher (at least for small dimensions) than the gain one has by checking less sets.

5 Percolations

To conclude, let us have another look at reformulation (iv) of Conjecture 1.1, as it was stated at the beginning. This is purely an expansion on the claim that it is indeed a reformulation, plus some basic facts of this field and how they relate to the conjecture.

Most of the general constructions are taken from the excellent paper [KS06]; For a milder introduction to the material see, e.g., [TP08].

Observe that if we are handed a set V of vertices of C^n that is equal to the set of vertices separated by the supporting hyperplane through some $a \in S^{n-1}$,

$a_i \geq 0$, then V can be expressed by the Boolean function $f_a : \{\pm 1\}^n \to \{0,1\}$, with

$$f_a(v) = \begin{cases} 1 & \text{if } a \cdot v > 1, \\ 0 & \text{otherwise.} \end{cases}$$

Also, we can equip the space of real functions on $\{\pm 1\}^n$ with the inner product

$$\langle f, g \rangle = \sum_{v \in \{\pm 1\}^n} 2^{-n} f(v) g(v),$$

which gives us the norm $\|f\|^2 = \langle f, f \rangle$. This space is denoted by $L_2(\{\pm 1\}^n)$.

The reason why we want to do this is that if f is a Boolean function, then the squared norm is the probability that $f = 1$ (with respect to the uniform distribution on $\{\pm 1\}^n$), denoted by $\mu(f)$. For the f_a this is precisely the fraction of separated vertices. Thus, if every f_a as above has norm at most $\frac{1}{2}$, Conjecture 1.1 is true.

But maybe it is too ambitious to aim directly for settling the conjecture. Maybe one should first try to find better bounds: For a subset $S \subset [n]$ consider the function

$$u_S(v) = (-1)^{|\{i \in S \,:\, v_i = 1\}|}.$$

The set of all such functions form an orthonormal basis in $L_2(\{\pm 1\}^n)$.

Given a function $f \in L_2(\{\pm 1\}^n)$, the *Fourier-Walsh coefficient* $\hat{f}(S)$ of f is

$$\hat{f}(S) = \langle f, u_S \rangle$$

(where we note that $\hat{f}(\varnothing) = \|f\|^2$), and since the functions u_S form an orthogonal basis, it follows that

$$\langle f, g \rangle = \sum_{S \subset [n]} \hat{f}(S) \hat{g}(S).$$

In particular, we get *Parseval's Formula*

$$\|f\|^2 = \sum_{S \subset [n]} \hat{f}^2(S).$$

To search for upper bounds for $\mu(f_a)$, we introduce the *influence* of a coordinate k on a function f, denoted by $I_k(f)$, as the probability that flipping the value of the k-th coordinate changes the value of f. Formally, define $\sigma_k(v_1, \ldots, v_n) = (v_1, \ldots, v_{k-1}, -v_k, v_{k+1}, \ldots, v_n)$, and the influence of k on a Boolean function f as

$$I_k(f) = 2^{-n} \cdot |\{v \in \{\pm 1\}^n \ : \ f(v) \neq f(\sigma_k(v))\}|,$$

which is also referred to as the Banzhaf power index of voter k. The total influence of f is $I(f) = \sum_{k=1}^{n} I_k(f)$.

The edge-isoperimetric inequality, going back to the works of Whitney and Loomis, Harper, Bernstein, Hart, and others, asserts that for every Boolean function f,

$$I(f) \geq 2\mu(f)\log_2(1/\mu(f)).$$

This certainly implies an upper bound for $\mu(f_a)$, but can only be made explicit if we find a way to quantify how close $I(f_a)$ is to 1.

6 Summary

Starting with a (rather) analytic problem, we saw four reformulations into different dialects of mathematics. While we ignored the first one and only referred to [HK92] for the second, we tried to use the third for a better understanding of the problem. We used properties of the geometric formulation to find a reasonably fast algorithm for fixed dimension.

One could certainly pursue this further and, with a more sophisticated implementation and more computing power, obtain results for slightly higher dimensions. However, this only seems to be a reasonable effort if one hopes to find a counterexample in some not too high dimension.

But nothing in the computational studies indicates that such a counterexample should exist. On the contrary, in all we have seen the cases close to the conjectured bound are the ones that are well understood. The difficulty lies in showing that the other cases will not start to cause trouble in high dimensions.

For this, some new idea or technique is needed, and as history tells us it is likely to be one that already exists in another part of mathematics. As an appetizer of how different from the original such reformulations can look like, we inspected the problem in the setting of Boolean functions.

References

[BTNR02] A. Ben-Tal, A. Nemirovski, and C. Roos, *Robust solutions of uncertain quadratic and conic quadratic problems*, SIAM Journal on Optimization **13** (2002), no. 2, 535–560 (electronic).

[Guy86] Richard K. Guy, *Any answers anent these analytical enigmas?*, The American Mathematical Monthly **93** (1986), no. 4, 279–281.

[HK92] Ron Holzman and Daniel J. Kleitman, *On the product of sign vectors and unit vectors*, Combinatorica **12** (1992), no. 3, 303–316.

[KS06] Gil Kalai and Shmuel Safra, *Threshold phenomena and influence: perspectives from mathematics, computer science, and economics*, Computational complexity and statistical physics, Santa Fe Institute Studies in the Sciences of Complexity, Oxford University Press, New York, 2006, pp. 25–60.

[LVBL98] Miguel Sousa Lobo, Lieven Vandenberghe, Stephen Boyd, and Hervé Lebret, *Applications of second-order cone programming*, Linear Algebra and its Applications **284** (1998), no. 1-3, 193–228.

[Ole96] Krzysztof Oleszkiewicz, *On the Stein property of Rademacher sequences*, Probability and Mathematical Statistics **16** (1996), no. 1, 127–130.

[Pin07] Iosif Pinelis, *Toward the best constant factor for the Rademacher-Gaussian tail comparison*, ESAIM. Probability and Statistics **11** (2007), 412–426 (electronic).

[Pin10] ______, *An asymptotically Gaussian bound on the Rademacher tails*, arXiv:1007.2137v2 (2010).

[Pin12] ______, *On the supremum of the tails of normalized sums of independent Rademacher random variables*, preprint, arXiv:1204.1761 (2012).

[She11] I. Shevtsova, *On the absolute constants in the Berry-Esseen type inequalities for identically distributed summands*, preprint, arXiv:1111.6554 (2011).

[TP08] Alan Taylor and Allison M. Pacelli, *Mathematics and politics: Strategy, voting, power, and proof*, Springer, 2008.

[Tyu09] I. Tyurin, *New estimates of the convergence rate in the Lyapunov theorem*, preprint, arXiv:0912.0726 (2009).

[Ver08] Mark Veraar, *A note on optimal probability lower bounds for centered random variables*, Colloquium Mathematicum **113** (2008), no. 2, 231–240.

[vH10] Frederik von Heymann, *Matlab implementation of the algorithm sketched in the text*, `http://ta.twi.tudelft.nl/wst/users/heymann/CubeCode.html`, June 2010.