Math. Program., Ser. B 97: 337–374 (2003)

Digital Object Identifier (DOI) 10.1007/s10107-003-0447-x

Miklós Simonovits

# How to compute the volume in high dimension?

Received: January 28, 2003 / Accepted: April 29, 2003
Published online: May 28, 2003 – © Springer-Verlag 2003

**Abstract.** In some areas of theoretical computer science we *feel* that randomized algorithms are better and in some others *we can prove* that they are more efficient than the deterministic ones.

Approximating the volume of a convex $n$-dimensional body, given by an oracle is one of the areas where this difference can be proved. In general, if we use a deterministic algorithm to approximate the volume, it requires *exponentially many oracle questions* in terms of $n$ as $n \to \infty$. Dyer, Frieze and Kannan gave a randomized *polynomial* approximation algorithm for the volume of a convex body $K \subseteq \mathbb{R}^n$, given by a membership oracle.

The DKF algorithm was improved in a sequence of papers. The area is full of deep and interesting problems and results. This paper is an introduction to this field and also a survey.

## 1. Introduction

We shall consider $n$-dimensional convex bodies $K \subseteq \mathbb{R}^n$ and will try to calculate various geometric parameters of these bodies. The most important ones are the volume, diameter and width.

Computing the volume of a "given" 3-dimensional body is not too difficult. We may assume that the convex body $K$ is enclosed in a box $B = \mathsf{X}_{i\le 3}[a_i, b_i]$. We can simply subdivide the intervals up to a given precision $\varepsilon > 0$ and then count how many of the obtained small cubes have nonempty intersection with $K$. This number, properly normalized, will give a sufficiently good approximation of the volume, $\mathbf{vol}(K)$.

The above method could be considered efficient in every *fixed dimension*, if polynomiality is measured in $1/\varepsilon$ but not if we measure it in $n$ and $n \to \infty$: practically the above method becomes useless.

Here we are looking for geometric algorithms that are polynomial in $n$, the *dimension* of the considered body. So we cannot use the above method of "fine subdivision" for $\mathbb{R}^n$. Further, even the above simplistic approach rises a sequence of problems, theoretical difficulties. Among others, we should ask:

**Q1.** What does it mean that a body $K$ is given? In which form is it given? We shall consider bodies given primarily by oracles (see §2).

**Q2.** How can we decide if a box has a nonempty intersection with $K$?

**Q3.** When do we regard an algorithm efficient? We are looking for geometric algorithms polynomial in the dimension. We wish either the exact value of the quantity, or an approximation of small **relative error** $\varepsilon > 0$. In this later case we also often require the algorithm to be polynomial in $\frac{1}{\varepsilon}$. [1]

M. Simonovits: Alfréd Rényi Mathematical Institute, Budapest, e-mail: miki@renyi.hu

[1] Since the input size describes $\varepsilon$ using only $\log(1/\varepsilon)$ bits, this is a "relaxation" deserving some attention.

Our aim is to give an introduction to a relatively new part of theoretical computer science, namely, the

**Application of Multiphase Monte Carlo Markov Chain methods to randomized volume computation.**

Soon we shall explain in details, what do we call (Direct) Monte Carlo, what is "Monte Carlo Markov Chain", why do we need "Multi-Phase" and why do some simpler approaches break down.

This is a very interesting theoretical field on the borderline of applicability. Yet, the papers in the field are rather lengthy and technical and make it difficult for the interested reader to get a good insight.

*Remark 1 (Randomization-derandomization).* Speaking of randomized algorithms, we assume that we have a *source of random bits* or of random real numbers from [0, 1]: the algorithms we shall speak of cannot be derandomized, as we shall see. Therefore – theoretically – the usage of *pseudorandom* numbers cannot replace using really random resources.[2]

The field is connected to various deep mathematical principles and the algorithms are often beautiful. Perhaps the most important areas used in the field are the method of Markov Chains (Metropolis algorithm) to generate given distributions, the eigenvalue technique used to analyze the speed of convergence of these Markov Chains to their Stationary distribution, Rapid Mixing, Harmonic Functions, connection to the Heat Kernel, isoperimetric inequalities, discrete forms of Cheeger inequality, and many more.

Knowing the **"Multiphase Monte Carlo Markov Chain"** Methods (and the Product Estimators, see Section 4), perhaps it is easy to construct algorithms seeming to work fine in various circumstances. However, they are often extremely difficult to analyze rigorously. In many important cases years pass by from the time of invention of some algorithms to their precise analysis. In other cases we simply do not have rigorous estimates. This is not so surprising: many of the algorithms have backgrounds in Physics. Similar is the situation, e.g., in connection with the Simulated Annealing, (see, e.g., Grötschel and Lovász, [47].)

One further difficulty and at the same time, beauty of the field is that the experience and intuition obtained in low dimensions are often misleading (see §2.3). (These differences are explained from a slightly different point of view in V. Milman's papers, e.g., in [88].)

Here I decided to write an introductory paper that *mostly* concentrates on the non-technical steps and on the questions: why do we do this or that in the considered papers. *At the end of the paper I will give a short bibliography.*

I will almost entirely restrict myself to *geometric algorithms*: I will mention only the Broder-Sinclair-Jerrum permanent algorithm from the randomized combinatorial algorithms, this being a direct predecessor of the randomized geometric algorithms forming the main subject of this paper.

[2] This may seem a contradiction, since the computers do not use truly random sources. Yet, the – very few – implementations we know of seem to work.

### *1.1. The structure of the survey*

This paper consists of four parts and an Appendix.

In the first part we shall introduce the *basic notions* and outline the basic problems we are dealing with. We shall introduce the Oracle representation, the well guaranteed convex bodies, the sandwiching ratio of convex bodies and will try to convince the reader of the importance of the whole topic.

In the second part we shall describe the difficulties, negative results: the "impossibility" to find exact algorithms, or deterministic approximation algorithms for volume computation, sampling and integration over a high dimensional convex body given by an oracle.

This survey is centered around the algorithms and other results of Kannan, Lovász and the author in [60]. So Part III describes the basic algorithm through which I will approach the whole area. I decided to start with two central theorems and *only then* explain the notions occurring in these theorems and their importance. At this point the reader may but does not have to understand all the notions and motivations. To define these notions and provide motivation is the task of the next parts.

**Theorem 1 (Volume [60]).** *Given a convex body $K \subseteq \mathbb{R}^n$ by a separation oracle, there is a (randomized) algorithm that, given $\varepsilon, \eta > 0$, returns a real number $\zeta$ for which*

$$(1-\varepsilon)\zeta < \mathbf{vol}(K) < (1+\varepsilon)\zeta$$

*with probability at least $1-\eta$. The algorithm uses*

$$O\left(\frac{n^5}{\varepsilon^2}\left(\ln\frac{1}{\varepsilon}\right)^3\left(\ln\frac{1}{\eta}\right)\ln^5 n\right) = O^*(n^5) \tag{1}$$

*oracle calls.*

Here the notation $O^*(n^h)$ in (1) means that we neglect the $\log^c n$ factors and the constants depending on $\varepsilon$ and $\eta$. Actually, we are always interested *primarily* in the exponent of $n$. [3]

**The failure probability** $\eta$ does not really influence the speed these algorithms: proving our results with a fixed $\eta$, e.g., with $\eta = \frac{1}{4}$ implies the general case. As Karp and Luby [61] and Jerrum, Valiant and Vazirani observed [55], if we can achieve $\varepsilon$ relative error with failure probability $\leq \frac{1}{4}$ in some number of steps, then we can repeat the same procedure *independently* $T$ times and then take the *median* of the results. That will be an $\varepsilon$-approximation with failure probability $\leq e^{-cT}$. Therefore switching from failure probability $\eta = \frac{1}{4}$ to a small $\eta$ increases the number of steps only by a factor $\log\frac{1}{\eta}$.

All the algorithms we consider are based on **sampling:** generating random (independent) points in some domain, according to a given, (mostly, but not always uniform) distribution. Moreover, in some sense sampling, volume approximation and integration of certain functions are equivalent, see e.g., [35]. Therefore it is natural that the above theorem is strongly connected to the following "sampling" theorem: Denote by $\mathbb{B}(\mathbf{x}, R)$ the ($n$-dimensional) ball of radius $R$ and center $\mathbf{x} \in \mathbb{R}^n$.

[3] Some people use $\tilde{O}(.)$ instead of $O^*(.)$. We could also be interested in the dependence on $\varepsilon$ that is *mostly* a multiplicative factor of the form $\frac{1}{\varepsilon^2}\log^\gamma\frac{1}{\varepsilon}$.

**Theorem 2 (Sampling, [60]).** *Given a convex body $K \subseteq \mathbb{R}^n$, (by a separation oracle), satisfying $\mathbb{B}(\mathbf{0}, 1) \subseteq K \subseteq \mathbb{B}(\mathbf{0}, d)$, a positive integer $N$ and an $\varepsilon > 0$, we can generate a set of $N$ random points $\{v_1, \dots, v_N\}$ in $K$ that are*

(a) **almost uniform** *in the sense that the distribution of each one is at most $\varepsilon$ away from the uniform in total variation distance, and*
(b) **almost pairwise independent** *in the sense that for every $1 \le i < j \le N$ and any two measurable subsets $A$ and $B$ of $K$,*

$$\left|\mathbf{prob}(v_i \in A, v_j \in B) - \mathbf{prob}(v_i \in A)\mathbf{prob}(v_j \in B)\right| \le \varepsilon.$$

*The algorithm uses only $O^*\left(n^3d^2 + Nn^2d^2\right)$ calls on the oracle.*

*Remark 2.* By generating a random point $\mathbf{x} \in K$ we mean a randomized algorithm, that uses random bits (coin-flipping) and also random, uniformly distributed independent vectors from $\mathbb{B}(\mathbf{0}, 1) \subseteq \mathbb{R}^n$. So we could say that assuming that we can generate randomness in simple situations we try to generate uniform distribution on complicated domains and that is highly non-trivial.

*Remark 3.* At this point we should emphasize that the last formula of Theorem 2 reflects a very important feature of our algorithms: it takes many more questions, $O^*(n^3d^2)$, to generate the first point than the subsequent ones, (which require $O^*(n^2d^2)$). The reason for this is that we shall use random walks to generate these points, and in principle we may start from a "bad corner" of $K$. "Unfortunately", it takes time to get out of that corner. Afterwards it is much easier to generate a random point. [4]

Part IV describes the *impossibility* of efficient randomized algorithms to find the diameter and width of a convex body. Speaking of the impossibility of some deterministic algorithm we always assume that $\mathcal{P} \neq \mathcal{NP}$, or at least, $\mathcal{P} \neq \#\mathcal{P}$. The Appendix contains a short description of some attached research, and also of some technical difficulties.

**Repetitions.** The structure of the field is rather involved. Therefore I will repeat the most important notions and connections in some places. I hope this will help and not bother the reader.

*Added in proof.* Between sending this paper to the editor and getting it back a "radical improvement" was obtained by: Lovász and Vempala [84]. They devised and verified an algorithm that calculates the volume in $O^*(n^4)$ oracle steps, instead of $O^*(n^5)$. In some sense this is not so surprising: our algorithm [60] was improved step by step in several aspects, by Kannan and Lovász [57], Kannan, Lovász and Montenegro, [58] and lately, by Lovász and Vempala, [81], [82], [83]. So one could wonder, why cannot the whole algorithm be turned into an $O^*(n^4)$ algorithm. Finally, Lovász and Vempala did it. I have decided not to rewrite the paper very much but change in a few places, very moderately. I do not feel that the parts described here became (very) obsolate. I feel that this survey describes the general problems, difficulties and methods. To understand the beautiful new results one has to understand the previous ones as well.

(See also "Added in Proof II" in Appendix II.) □

[4] A "corner" here is not connected to smoothness, see Definition 3.

# I. Convex bodies and Oracles

## 2. Oracles

In this survey paper we shall mostly restrict ourselves to convex, compact, "well guaranteed" bodies in $\mathbb{R}^n$, given by oracles.

In this section we explain three things: oracles, guarantees and the sandwiching ratio.

**Definition 1.** *A body $K$ is well guaranteed if we know that it contains some ball $\mathbb{B}(\mathbf{0}, r)$ and is contained in some ball $\mathbb{B}(\mathbf{0}, R)$.*

One reason why we need $K \subseteq \mathbb{R}^n$ to be well guaranteed is that we shall ask questions of the type "is $\mathbf{x} \in K$?" and without a guarantee nothing protects us from asking arbitrarily many questions and receiving only NO answers. That way we will be unable to assert anything about $\mathbf{vol}(K)$. Generally we regard this notion a "technical nuisance".

The usage of *oracles* can be found all over the mathematical literature, in mathematical logic, in computer science, etc. In computer science it is equivalent with speaking of a subroutine or a black box.

A **body** $K$ **is given by an oracle**, if we do not have any direct information about it, *except that it is well guaranteed* with $r$, $R$, but we may ask questions about $K$, and we get answers to our questions.

Depending on the kind of questions and answers, we distinguish several types of *oracles*. Here we shall use only two types: *weak separation oracles* and *strong membership oracles*, and a third one, connecting them, the strong separation oracle. The expressions "weak" and "strong" indicate whether the oracle makes rounding errors or not.

Strong Membership Oracle

A convex body $K \subseteq \mathbb{R}^n$ is fixed and we can ask questions of the type:

is $\mathbf{x} \in K$ or not?

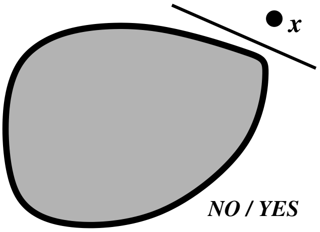
To define the weak separation oracle, first we define the strong version of it. We know that if an $\mathbf{x} \notin K$, then, by the convexity, we can find a hyperplane $S$ separating $\mathbf{x}$ from $K$.

Strong Separation Oracle

A convex body $K \subseteq \mathbb{R}^n$ is fixed and we can ask questions of the type:

is $\mathbf{x} \in K$ or not?

The answer is YES, or NO, and, if the answer is NO, we also get a hyperplane $S$ separating $\mathbf{x}$ from $K$.



Separation Oracle

The separating hyperplane is given by a *vector* $\mathbf{s}$, and the separation means that $\mathbf{s} \cdot \mathbf{x} > 1$, while $\mathbf{s} \cdot \mathbf{y} \leq 1$, whenever $\mathbf{y} \in K$.

In practice we always have some rounding errors in our calculations, and this is reflected in the following definition:

Denote by $d(\mathbf{x}, A)$ the distance of the point $\mathbf{x}$ from the set $A$.

Weak Separation Oracle

A convex body $K \subseteq \mathbb{R}^n$ is fixed and we can fix an $\varepsilon > 0$ and ask:

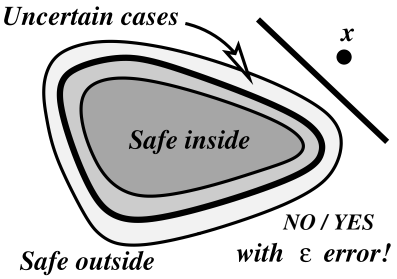
is $\mathbf{x} \in K$ or not?

The answer is YES, or NO, and if the answer is NO, we also get a hyperplane $S$ separating $\mathbf{x}$ from $K$, but the precision of the answer is only $\varepsilon$ in the following sense:

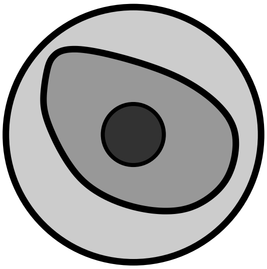
(a) If $d(\mathbf{x}, \partial K) < \varepsilon$, where $\partial K$ is the boundary of $K$, then we can get any answer, i.e., the answer is not necessarily correct.

(b) If $\mathbb{B}(\mathbf{x}, \varepsilon) \subseteq K$, then we always get the correct YES.

(c) If $d(\mathbf{x}, K) \geq \varepsilon$, then we get the correct NO, and a vector $\mathbf{s}$ normalized by $||\mathbf{s}||_1 = 1$, for which $\mathbf{s} \cdot \mathbf{y} < \mathbf{s} \cdot \mathbf{x} + \varepsilon \quad$ for every $\quad \mathbf{y} \in K$.



Weak separation oracle



Well guaranteed $K$

Often we shall also be interested in the so called "sandwiching ratio", $d := R/r$. We shall see that the sandwiching ratio and some generalizations of it influence the speed of the algorithms very much.

Since applying a linear transformation to a $K \subseteq \mathbb{R}^n$ will be used in many crucial places, we define the sandwiching ratio more generally:

If $E_1 \subseteq K \subseteq E_2$ where $E_1$ and $E_2$ are homothetic ellipsoids around $\mathbf{0}$ and $E_1$ is obtained from $E_2$ by shrinking by a factor of $d$, then we shall say that we have a sandwiching of $K$ with **sandwiching ratio** $d$.

**Definition 2 (Sandwiching).** *Given a $K \subseteq \mathbb{R}^n$, we shall often look for a linear transformation $A$ such that $AK$ contains the unit ball $\mathbb{B}(\mathbf{0}, 1)$ and is contained in $\mathbb{B}(\mathbf{0}, d)$ and then we say that we sandwiched $K$ with sandwiching ratio $d$.*

Sandwiching is natural in volume-computation, since the volumes change according to the determinant of $A$, but it cannot be used in approximating the diameter.

Speaking of polynomial approximation algorithms, we should specify the **input-size** as well. In our cases the input contains $n$, $\varepsilon > 0$ and also the two numbers of the guarantee, $r$ and $R$. We wish polynomiality in $n$ and $1/\varepsilon$, in all the practical cases we can forget the other parameters. Yet, to be precise, we almost always assume that $r = 1$ and the input-size contains $\log R$ additional bits to describe $R$.

*Remark 4.* It is trivial that if we have weak membership oracles for $K$ and $K'$, then we also have the same for $K \cap K'$, for free. Similarly, if we have separation oracles for $K$ and $K'$, then we have also for $K \cap K'$: among others, we have a separation oracle for $K_r := K \cap \mathbb{B}(\mathbf{0}, r)$ as well.[5]

**Pre-sandwiching.** In principle, it can happen that we have a "very pencil-like" $K \subseteq \mathbb{R}^n$: one for which the inscribed ball is much-much smaller than the circumscribed one. Therefore we always start with a preliminary sandwiching, which achieves that $K$ be well guaranteed with $r = 1$ and $R = n^{3/2}$. This can be achieved in $O^*(n^4)$ steps, see [49].

### *2.1. Why to use oracles?*

The oracles we consider are used in several fairly different settings:

(a) we use them for the "original purpose", to describe convex bodies, in our geometric algorithms;
(b) and also we may use them to solve some combinatorial problems;
(c) sometimes using oracles helps to understand deeper theoretical questions.
(d) Finally, the usage of oracles can also be considered as a very useful tool to simplify the language to describe some equivalence/reduction results of the form "If we can solve Problem $\mathcal{A}$ polynomially, then we can also solve Problem $\mathcal{B}$ polynomially".

Below we make some remarks on (b) and (c).

*Remark 5.* For a long period it was not clear if Linear Programming can be solved in polynomial time. In the 1979 Garey-Johnson book [45], on p155, three problems are listed that would be *natural* candidates for being strictly in between $\mathcal{P}$ and $\mathcal{NP}$: one of them is Linear Programming. Then Khachiyan [65] applied Shor's algorithm [95] to linear programming, proving that linear programming is polynomially solvable. Next Grötschel, Lovász and Schrijver [48, 49] Padberg and Rao [92] and Karp and Papadimitriou [62] started applying Khachiyan's method to Polyhedral Combinatorics. They noticed that

> in applying the Khachiyan algorithm to linear programming one does not have to have all the inequalities describing a convex $K$ in advance:

it is enough if for any given vector $\mathbf{x} \notin K$ one can always generate an inequality, separating $\mathbf{x}$ from $K$.[6] This is a very important feature, because in many situations where, e.g.,

[5] If we have optimizing oracles for two convex bodies then we have an optimizing oracle for the intersection as well, but this is not trivial.

[6] The more efficient Karmarkar algorithm does not have this feature.

we have a graph of order $n$ and an attached polytope, over which we should optimize, the number of inequalities we should list is exponentially large.

This is the case for example, when we consider a graph $G_n$ on $n$ vertices, its matchings, and the polytope spanned by the characteristic vectors of its matchings: $G_n$ is described roughly by a vector of length $\binom{n}{2}$ but there are exponentially many inequalities describing its "matching polytope".

This triggered a whole new area of research. The reader is recommended to read the books of Grötschel, Lovász and Schrijver [49] or of Lovász [74] describing the equivalence of several oracle types, their application to Combinatorial Optimization, the connection to Geometric Number Theory, etc.

The most important combinatorial applications include polynomial algorithms for vertex packing in perfect graphs, for the matching and matroid intersection problems, for optimum covering of directed cuts of a digraph, and to minimize value of a submodular set function.

*Remark 6.* We have mentioned that sometimes the usage of oracles helps to understand deeper relations. One example of this is the theorem of Baker, Gill and Solovay [9] according to which, if we replace $\mathcal{P}$ and $\mathcal{NP}$ by their Oracle versions, $\mathcal{P}_{\mathcal{O}}$ and $\mathcal{NP}_{\mathcal{O}}$, then one can find oracles $\mathcal{O}$ for which $\mathcal{P}_{\mathcal{O}} = \mathcal{NP}_{\mathcal{O}}$ and other oracles where $\mathcal{P}_{\mathcal{O}} \neq \mathcal{NP}_{\mathcal{O}}$. This shows that to decide if $\mathcal{P} = \mathcal{NP}$ one has to use that the classes are given concretely, not by oracles.

### *2.2. How to count the steps?*

Generally we have several types of steps to count:

- Number of oracle queries (questions asked from the oracle)
- (generating) random bites
- arithmetic steps and "if" decisions;

*We shall count only the number of oracle queries*, because theoretically there is not much difference between the two ways to count the steps, and usually the oracle questions are the "more expensive" ones.

## II. Negative results

### *2.3. Strange phenomena in $\mathbb{R}^n$?*

Below I list three facts about high dimensional convex bodies showing that the phenomena are different in high and low dimensional cases. First we introduce a standard notation: for a fixed real $\alpha$

$$\alpha K := \{\alpha \mathbf{x} : \mathbf{x} \in K\}.$$

(a) In low dimensions a thin layer around the surface of $K$ is negligible in volume. On the other hand, since $(1 - \frac{1}{n})^n \to \frac{1}{e}$, in $\mathbb{R}^n$ "almost all points" of $K$ are near the surface $\partial K$, as $n \to \infty$, in the following sense:

$$\mathbf{vol}\left(K \setminus \left(1 - \frac{\omega_n}{n}\right) K\right) \approx \mathbf{vol}(K), \quad \text{if} \quad \omega_n \to \infty \quad \text{as} \quad n \to \infty.$$

(b) Let $\omega = \omega_n \to \infty$. Take a hyperplane through the origin and take all those parts of $\mathbb{B}(\mathbf{0}, 1)$ which are further away from this hyperplane than $\frac{\omega}{\sqrt{n}}$. Again, this part of the ball is negligible: almost all points are near to the hyperplane.

This is expressed in the following important lemma:

**Lemma 1 (Spherical cap).** *Let $H$ be a halfspace in $\mathbb{R}^n$ and $\mathbb{B} := \mathbb{B}(\mathbf{x}, 1)$, whose center $\mathbf{x}$ is at a distance $t$ from $H$. (So we speak of the halfspace not containing the center.) Then*

(i) *if $t \le 1/\sqrt{n}$, then*

$$\mathbf{vol}(H \cap \mathbb{B}) > \left(\frac{1}{2} - \frac{t\sqrt{n}}{2}\right)\mathbf{vol}(\mathbb{B});$$

(ii) *if $t > 1/\sqrt{n}$ then*

$$\frac{1}{10t\sqrt{n}}(1-t^2)^{(n+1)/2}\mathbf{vol}(\mathbb{B}) \ < \ \mathbf{vol}(H \cap \mathbb{B}) \ < \ \frac{1}{t\sqrt{n}}(1-t^2)^{(n+1)/2}\mathbf{vol}(\mathbb{B}).$$

*Remark 7.* Here $(1-t^2)^{\frac{(n+1)}{2}} \approx e^{-\frac{1}{2}(n+1)t^2}$. One could ask, why is most of the volume of a ball near its equator? For me this means that the section-sizes follow a normal distribution: I connect this phenomenon mostly to the Central Limit Theorem, and the $\frac{1}{\sqrt{n}}$ above to the standard deviation. Another explanation could be found in the "Saddle Point Method". See also [89].

(c) Dvoretzky's theorem [33] asserts that all the high-dimensional convex bodies have sections (of sufficiently lower dimensions) which are nearly spheres. For related results we refer the reader to Milman's paper [88].

Implicitly we shall use one further surprizing fact, showing that the convexity is important in our cases:

(d) Let, for a unit vector $\mathbf{x}$, $\mathbb{D}^*(0, \mathbf{x}) := \mathbb{B}(\mathbf{0}, 1) \cup \mathbb{B}(\mathbf{x}, 1) \subset \mathbb{R}^n$. This body can be cut into two equal parts by an $n-1$-dimensional disk of radius $\frac{\sqrt{3}}{2}$: this has an exponentially small *relative* surface.[7] (For the importance if this, see Section 7.)

### 2.4. *Can we calculate the volume exactly?*

The first question is if we can calculate the volume exactly, in polynomial time. As we agreed, here we shall always assume that $\mathcal{P} \neq \#\mathcal{P}$. Then the answer is negative: *No, we cannot in polynomially many steps!* Finding the volume was proved to be $\#\mathcal{P}$-hard, by Dyer and Frieze [34] and Khachiyan [66, 67], even for explicitly given polytopes. A nice survey of L. Khachiyan [68] covers many important aspects of this field. We explain here only two facts.

(a) Computing the volume would solve a $\#\mathcal{P}$-hard problem:

Take an arbitrary partial order $\mathbb{P}$, say on the elements $a_1, \dots, a_n$ and try to count exactly its linear extensions. Consider that part of the unit cube which is determined by the inequalities

$$0 \le x_i \le 1 \quad (i = 1, \dots, n) \quad \text{and} \quad x_i \le x_j \quad \text{whenever} \quad a_i \le a_j. \qquad (2)$$

[7] i.e., its area divided by the total surface of the sphere is exponentially small.

The number of linear extensions is $n! \cdot \mathbf{vol}(Poly(\mathbb{P}))$, where $Poly(\mathbb{P})$ is a *polyhedron attached by (2) to the partial order*. By a result of Brightwell and Winkler [24], counting the linear extensions of $\mathbb{P}$ is $\#\mathcal{P}$-hard. So, if $\mathcal{P} \neq \#\mathcal{P}$, then computing the volume is impossible in polynomially many steps.

The reduction of the volume problem to the linear-extension problem itself is almost trivial, since *each* linear extension provides a simplex of volume $1/n!$ in the unit cube $[0, 1]^n$, and different extensions correspond to different simplices.

(b) There is another, very interesting approach to this question, (Lawrence [71], see also Khachiyan [68]). One can construct a simple convex polytope $\mathbb{P}$ with inequalities over the rationals, for which, if we could find $\frac{a}{b} := \mathbf{vol}(\mathbb{P})$, then $b$ would be so large that even to write it down would take exponentially many digits.

### *2.5. Can we approximate the volume? the basic questions*

We have seen that the exact computation of volume is impossible. From now on we are interested only in the approximate calculations.

Speaking of convex bodies we always speak of compact bodies, with positive volume, though being closed is not really important.

In this survey we are interested in the following problems.

- Given a high-dimensional body $K$, can we approximate its volume?
- Can we generate uniform distribution on $K$?
- Can we integrate functions on $K$?
- Can we approximate the diameter or the width of a body?
- What can be done with deterministic algorithms?
- What can be done with randomized ones?
- How fast are our algorithms?

The answers to these questions are highly non-trivial. In a nutshell, we shall restrict ourselves to the "input form" where *the convex bodies are given by oracles*, and all the three problems: uniform sampling, estimating the volume and integrating over $K$ are *unsolvable by deterministic algorithms* in polynomially many steps. (In some sense these questions are equivalent).

However, if we assume that $K$ is convex, then there exist some *randomized* algorithms that give sufficiently good approximation of the volume or provide sufficiently good approximation of the uniform distribution.

When we wish to integrate a function $f$ on a convex $K$, then again, we cannot integrate all the functions, only a very important but very narrow subclass of them, the so called *log-concave* functions. (A function $f(\mathbf{x}) \geq 0$ is log-concave if $\log f(\mathbf{x})$ is concave. Positive concave functions are log-concave.) Very many important (distribution) functions are log-concave, e.g., the multidimensional normal distribution, or $e^{-x}$, and several further density functions in statistics/probability theory.

*Remark 8.* Integrating a concave function, of course is the same as taking the volume of a convex body in $\mathbb{R}^{n+1}$. The problem of integrating concave functions or almost concave functions was mentioned by Dyer, Frieze and Kannan already in [36]. The integration of log-concave functions was "solved" by Applegate and Kannan [8]. See also [79].

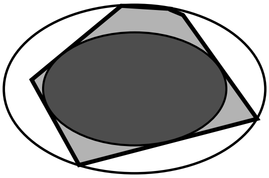
### 2.6. *"Brute force methods fail"*

**"Fine grid method".** The simplest attempt to estimate the volume is to enclose $K$ in a box and then – subdividing the axes – put a fine grid on $K$, finally counting the grid points in $K$. As we saw, this method works in bounded dimension,[8] however, in $K \subseteq \mathbb{R}^n$ it is doomed to fail because of the exponentially many points. One can slightly improve this method by using the theory of uniformly distributed points, but as the dimension increases, one has to give up using the improved methods as well. As we shall see, *we have to give up all the deterministic methods.*

**Löwner-John ellipsoid.** We shall need the following:

**Theorem 3 (F. John [50]).** *If $K \subseteq \mathbb{R}^n$ is a convex body and $E$ is an ellipsoid containing $K$ and having minimum volume, then shrinking $E$ around its center by a factor $n$ we get another ellipsoid, $E' \subseteq K$.*

We shall call this pair of ellipsoids the Löwner-John ellipsoid. They are uniquely determined. The Löwner-John ellipsoid and its variants are important in several geometric algorithms. The reader wishing to learn about it more is referred to [49], Section 4.6.



Löwner-John ellipsoid

One way to approximate the volume of a convex body $K$ is to find its approximate Löwner-John ellipsoid. Assume for a second that we could find the Löwner-John ellipsoid of a convex body by a polynomial algorithm. Then, of course, we could estimate the volume of $K$ from below by the volume of the inscribed ellipsoid and from above by the circumscribed ellipsoid. The ratio of the two estimates is $\leq n^n$. There are two problems with this approach:

(a) we cannot find the Löwner-John ellipsoids for a convex body, not even approximately, in polynomial time. [9]

The solution is that we can find in polynomial time two ellipsoids where the ratio of shrinking is $(n+1)\sqrt{n}$.

(b) The result is very weak: we would like to have, e.g., in dimension 10, a relative error, say 1/10, or, 1/1000, and here we get $10^{10}$. Who cares for such a weak result? In the next two sections we shall see that deterministically this is the best one can get.

### 2.7. *Elekes' theorem*

The results of Elekes [39] and the improvements of Bárány-Füredi [11], Carl [27] and Carl-Pajor [28] show that restricting ourselves to deterministic algorithms, we cannot really hope for reasonably good results.

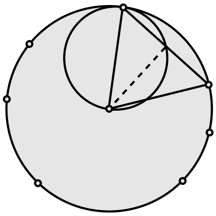
**Theorem 4 (Elekes [39]).** *Every deterministic algorithm (to estimate the volume of an arbitrary $K \subseteq \mathbb{R}^n$ and using $q$ oracle question, makes a relative error $\geq \sqrt{2^n/q}$ for some convex $n$-dimensional bodies given by well guaranteed separation oracles.*

[8] It gives a polynomial (in $1/\varepsilon$) algorithm but the degree grows with $n$.

[9] We shall return to this question and revise what we just have said, in Section 5.4.

*Proof.* Assume that an algorithm $\mathcal{A}$ to approximate the volume is given and we wish to prove that – having asked $q$ questions – it cannot approximate the volume of *all* convex bodies better than with $\sqrt{2^n/q}$ relative error. *The fact that the algorithm is deterministic* means that for a given $K$ and $\varepsilon > 0$, if we run it twice, it asks the same points $\mathbf{x}_1, \dots, \mathbf{x}_q$ and gives the same result. (This is not so with the randomized algorithms.) Further, if we have two convex bodies, $K_1$ and $K_2$ and run the algorithms, and the algorithm asks the sequence $(\mathbf{x}_i)$ for $K_1$ and $(\mathbf{y}_i)$ for $K_2$, then the first place where the two sequences may differ, $\mathbf{x}_i \neq \mathbf{y}_i$ follows a point $\mathbf{x}_{i-1} = \mathbf{y}_{i-1}$ belonging to the symmetric difference $K_1 \Delta K_2$.

We fix $\varepsilon := 2^n$ (!!!) and apply the algorithm with this $\varepsilon$. If for $K_1$ the algorithm provides in $q$ steps the sequence $\mathbf{x}_1, \dots, \mathbf{x}_q$, and $K_2$ is the convex hull of these points, then for $K_2$ the algorithm $\mathcal{A}$ would ask the same points, $\mathbf{x}_1, \dots, \mathbf{x}_q$ (and provide the same estimate $\zeta$). If the volume of $K_1$ and $K_2$ are very far from each other, then the algorithm must be bad at least for one of them.



The "$\frac{1}{2}$"-balls cover the convex hull

Apply this to $K_1 := \mathbb{B}(\mathbf{0}, 1)$ and the convex hull $K_2$ of the corresponding $q$ points $\mathbf{x}_1, \dots, \mathbf{x}_q$. Elekes observed that if $\mathbb{B}_i$ are the "Thales" balls of $(\mathbf{0}, \mathbf{x}_i)$: $\mathbb{B}_i := \mathbb{B}(\frac{1}{2}\mathbf{x}_i, \frac{1}{2})$, then

$$K_2 \subseteq \bigcup_{\substack{i \le q \\ \mathbf{x}_i \in \mathbb{B}}} \mathbb{B}_i. \quad ^{10}$$

Clearly, $\mathbf{vol}(B_i) = 2^{-n}\mathbf{vol}(\mathbb{B}(\mathbf{0}, 1))$, implying that

$$\frac{\mathbf{vol}(K_2)}{\mathbf{vol}(\mathbb{B}(\mathbf{0}, 1))} \le \frac{q}{2^n}.$$

Since $\mathcal{A}$ is deterministic, for $K_2$ (defined by the algorithm!) the algorithm asks the same $\mathbf{x}_1, \dots, \mathbf{x}_q$, and gives the same estimate $\zeta$: the algorithm cannot distinguish if we had the unit ball $\mathbb{B}(\mathbf{0}, 1)$ or the convex hull $K_2$ of $\mathbf{x}_1, \dots, \mathbf{x}_q$. So the algorithm will have a relative error at least $\sqrt{2^n/q}$ either for the ball or for the convex hull. □

We conclude that the fact that the volume of $\mathbb{B}(\mathbf{0}, 1)$ cannot be approximated by the volume of convex polyhedra of polynomially many vertices implies that the algorithm has to have large relative error, either for $K_1$ or $K_2$.

*Remark 9.* This is again a case where we see something counterintuitive, or at least something completely different in low and high dimensions. Again, as in the first example of Section 2.3, the fact that $q^n$ is very small for large $n$ is in the background.

### *2.8. The Bárány-Füredi results*

The Bárány-Füredi theorem does roughly the same as the Elekes theorem, in a more complicated but much more precise way.

[10] This is equivalent with that from a point $\mathbf{x} \in K_2$ at least one of the angles $\mathbf{0}\mathbf{x}\mathbf{x}_i$ is obtuse or a right angle. We can see this in the plane and a short calculation proves it for the general case.

**Theorem 5 (Bárány-Füredi [11, 12]).** *There is no polynomial time (deterministic) algorithm that would compute a lower bound $\underline{\mathbf{vol}}(K)$ and an upper bound $\overline{\mathbf{vol}}(K)$ for the volume of every convex $K \subseteq \mathbb{R}^n$, given by some oracle, so that*

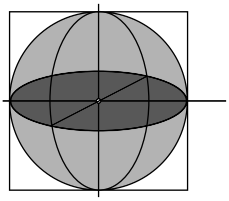
$$\frac{\overline{\mathbf{vol}}(K)}{\underline{\mathbf{vol}}(K)} \le \left(c\frac{n}{\log n}\right)^n .$$

Bárány and Füredi proved three further theorems in their paper, one of which is related to the non-approximability of the diameter and will be formulated in Part IV.

Carl has obtained *implicitly* the same result [27]. For related results see also Carl and Pajor, [28], Bourgain-Milman, [20].

One corollary of these results is that the *randomized* volume approximation algorithms cannot be derandomized to get a polynomial time deterministic algorithm. In fact, as Dyer and Frieze [35] pointed out, in a polynomial randomized algorithm we need at least $cn$ random bits.

### *2.9. Why cannot we use Monte Carlo methods directly?*



The volume of the inscribed ball is exponentially small

The easiest way to estimate the volume of a convex body could be to use a Monte Carlo algorithm: find a rectangular box $Q$ containing $K$, generate uniformly distributed points $x_1 \dots, x_N \in Q$ and count how often $x_i \in K$.

If we get $S$ such points, then $\zeta = S/N$ would be a good approximation of $\mathbf{vol}(K)/\mathbf{vol}(Q)$. The problem with this approach is that many phenomena familiar in low dimension completely change as the dimension increases. Indeed, even in the simplest case, when $K = \mathbb{B}(\mathbf{0}, \frac{1}{2})$ is the ball inscribed in the $n$-dimensional unit cube, the proportion $\mathbf{vol}(K)/\mathbf{vol}(Q) \le q^n$ for some $q < 1$.[11]

Therefore we need $N > q^{-n}$ points to hit $\mathbb{B}(\mathbf{0}, \frac{1}{2})$ at least once. So this algorithm does not work: neither theoretically, nor in practice.

To argue in the *more classical way* we would say: If we wish to approximate an event of probability $p$, its standard deviation is around $\sqrt{pN}$, so we should not use Monte Carlo for events of small probability. ...

## III. The volume algorithms

## 3. Origins: The permanent problem

The methods used to approximate the volume come from the permanent problem. The permanent is that variant of the determinant where all the signs are switched to $+1$. The permanent equals to the number of 1-factors of a corresponding bipartite graph. So,

[11] We know that $\mathbf{vol}(\mathbb{B}(\mathbf{0}, 1)) = \pi^{n/2}/\,\Gamma(1 + n/2)$.

finding the permanent is counting the 1-factors of a bipartite graph. Valiant [100] proved that the problem of finding the permanent deterministically is as difficult as it can be: if one can find the permanent of the 0-1 matrices in polynomially many steps, then one can solve all the problems in a fairly wide class of counting problems. In a more technical term, the permanent problem is $\#\mathcal{P}$-hard. It is commonly believed (and we assumed) that these problems are unsolvable polynomially.

It was A. Broder [25] who suggested to use random walks to estimate the number of 1-factors in *dense* bipartite graphs. The algorithm of Broder used a random walk on the 1-factors and "almost"-1-factors of a graph. Unfortunately, there was an error in the argument of Broder, pointed out by Milena Mihail, [86]. Therefore the first correct proof of that the Broder algorithm approximates the permanent with high probability, in polynomially many steps, was given by M. Jerrum and A. Sinclair [53]. The algorithms of this survey all follow the basic approach of Jerrum and Sinclair, despite that there are many important differences in the details.

As to the permanent problem, for many years the condition that the matrix should be dense could not be removed. Kannan in 1995 [56] listed this problem as one of the important open questions. Recently Jerrum, Sinclair and Vigoda succeeded in eliminating this density condition [54].

### *3.1. How to describe the Multiphase Monte Carlo Markov Chain method in a nutshell?*

The field we try to describe can be characterized as follows:

- We have a (geometric) problem that we cannot solve by deterministic methods. We would like to use Monte Carlo, to estimate an exponentially "small" number $\Lambda$ with small *relative* error. So we cannot apply Monte Carlo methods directly.[12]
- One way to get around the inapplicability of Monte Carlo methods is to write the $\Lambda$ as a product of polynomially many factors: $\Lambda = \prod \Lambda_i$, where the factors $\Lambda_i \in (\frac{1}{3}, 1)$ and can already be approximated by Monte Carlo methods. In these cases we call $\Lambda$ a *product estimator* and the whole procedure we shall call *Multiphase Monte Carlo method.*
- In our cases $\prod \Lambda_i$ will be a "telescopic" product: we shall define $m := cn\log n$ domains $K_1 \subseteq \ldots \subseteq K_m$ and estimate $\Lambda_i := \mathbf{vol}(K_i)/\mathbf{vol}(K_{i-1})$. In our cases (mostly) $K_i$ is the intersection of $K$ with a large ball, say, $K_i := K \cap \mathbb{B}(\mathbf{0}, 2^{i/n})$.
- To use the Monte Carlo method, to get the numbers $\Lambda_i$, we have to generate random (mostly almost uniformly distributed) independent points in the domains $K_i$. To be precise, we shall generate the distributions in $cn\log n$ domains, recursively. We use a random walk for this: we devise a Markov Chain whose stationary (i.e. limit) distribution is uniform (or almost uniform) on $K_i$, run (simulate) this Markov Chain for polynomially many steps, and then take its "state" as a uniformly distributed point in $K_i$.

[12] Speaking of (simple or direct) Monte Carlo methods I mean the simplest version, where a measurable $K$ is embedded into a larger set $\mathcal{D}$, the volume of which is known and we also assume that we can generate uniform distribution in $\mathcal{D}$. Then we generate $N$ points uniformly and independently in $\mathcal{D}$ and count, how many of them belong to $K$. If $S$ of them belong to $\mathcal{D}$ then we use $\mathbf{vol}(K) \approx \frac{S}{N}\mathbf{vol}(\mathcal{D})$.

As to these Markov Chains, in this survey we restrict ourselves to three of them: Random Walk on a Grid, Ball-Step, and Hit-and Run. For us the Random Walk with Ball-steps is the most important one.

The Markov Chains are connected to the convex bodies $K_i$ by the fact that in the $i^{\text{th}}$ phase when we walk in $K_i$, whenever we would leave $K_i$, we skip that move: decide to stay in $K_i$; at the same time, of course, we count, how often are we in $K_{i-1} \subseteq K_i$. (As we shall see, the Hit-and-Run does not even try to leave $K$, by its definition.) In this sense the Random Walk "explores" the unknown convex body.

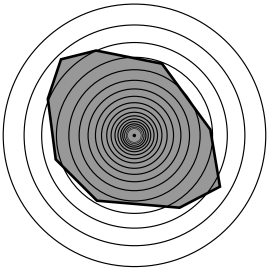
### *3.2. Missing lower bounds, on the number of queries*

Generally it is nice to have matching lower and upper bounds or at least ones that are not too far away from each other. Here the reasonable lower bounds are missing. It would be nice to prove that one needs at least $n\sqrt{n}$ oracle questions to estimate the volume of a convex $K \subseteq \mathbb{R}^n$ given by an oracle, with precision $\varepsilon$ and failure probability $\eta = 0.1$. [13]

## 4. Multiphase Monte Carlo

We have mentioned on p343 that using $O^*(n^4)$ steps we may achieve a sandwiching ratio $d = (n+1)\sqrt{n}$. Let us consider a $K \subseteq \mathbb{R}^n$ containing $\mathbb{B}(\mathbf{0}, 1)$ and contained in $\mathbb{B}(\mathbf{0}, (n+1)\sqrt{n})$. Above, the main obstacle to use Monte Carlo methods was that the ratio to be approximated was exponentially small. One way to get around this problem is to produce this number as the product of some (not too many) numbers each of which is already reasonably large, say is in $(\frac{1}{2}, 1)$. To this end, consider the following sequence of bodies, intersections of $K$ with some balls: Let for $i = 0 \dots m := \lfloor 4n \log n \rfloor$,

$$K_i := K \cap \mathbb{B}(\mathbf{0}, 2^{i/n}).$$



Multiphase Monte Carlo

One can easily see that

$$1 \le \frac{\mathbf{vol}(K_i)}{\mathbf{vol}(K_{i-1})} \le 2.$$

Clearly, $K_0 = \mathbb{B}(\mathbf{0}, 1)$ and $K_m = K$. Therefore, if we could generate uniformly distributed points in each convex body $K_i$ in polynomial time, then we could approximate $\mathbf{vol}(K)$, using

$$\mathbf{vol}(K) = \mathbf{vol}(K_0) \cdot \prod_{i=1}^{m} \frac{\mathbf{vol}(K_i)}{\mathbf{vol}(K_{i-1})}. \tag{3}$$

where $\mathbf{vol}(K_0) = \mathbf{vol}(\mathbb{B}(\mathbf{0}, 1)) = \pi^{n/2}/\Gamma(1 + n/2)$.

[13] We do not even know that one needs say, at least $n(\log n)^{10}$ oracle question.

Here comes a serious difficulty: we can easily generate uniform distributions on $n$-dimensional cubes, simplices, ellipsoids, but we cannot easily generate on $K_i$. We shall generate uniformly distributed points recursively, using random walks: assuming that we have already generated a $\mathbf{v}_i$ (almost) uniformly distributed on $K_{i-1}$, we start a random walk on $K_i$, simulate it for polynomially many steps and then stop. If we do this the right way, we get a uniformly distributed $\mathbf{v}_i \in K_i$.

Here we have some luck: reaching the last convex body, $K_m$, we do not have to go back to $K_0$, to generate the next random point in $K$: having an (almost) uniformly distributed $\mathbf{y}_\ell \in K$ we may start from this $\mathbf{y}_\ell$ to get the next point, $\mathbf{y}_{\ell+1} \in K$, (almost) uniformly distributed and (almost) independent from $\mathbf{y}_\ell$.

### *4.1. The breakthrough*

As we have already indicated, in the volume computation the breakthrough came in the papers of Dyer, Frieze, and Kannan [36, 37].

They showed that the volume of a convex body $K \subseteq \mathbb{R}^n$, given by a separation oracle, can be estimated with arbitrary precision, in polynomially many steps. Their paper was a real breakthrough in the field, despite the fact that it had to solve $O^*(n^{23})$ convex programming problems and therefore was very far from anything practical. (Remember that the $O^*$-notation is a soft version of the $O$-notation, that suppresses powers of $\log n$ (and some functions of $\varepsilon$ and $\eta$, see p339.))

The DFK algorithm was improved in a sequence of papers. Below we list some of the important steps:[14]

- First Lovász and Simonovits [78] improved it to $O^*(n^{16})$, by proving an appropriate *isoperimetric inequality* and simplifying, improving the original algorithm in several places. The introduction of the $\mu$-conductance was an important improvement, finding a good isoperimetric inequality and the better analysis were other ones. (See Theorem 9.)
- Applegate and Kannan [8] introduced several new ingredients, among others, the Metropolis algorithm and the Integration of log-concave functions. They obtained an $O^*(n^{10})$ algorithm. (See Section 4.7.)
- Next Lovász introduced the ball-steps [76], obtaining an $O^*(n^{10})$ algorithm. This was the first switching to continuous random walks.[15]
- Dyer and Frieze [35] obtained an $O^*(n^8)$ algorithm (still using a random walk on the grid).
- In [80] we obtained an $O^*(n^7)$ algorithm, using ball-steps and Metropolis algorithm. (See Section 4.7.)
- The next step depended primarily on improving the sandwiching: Kannan, Lovász, and I constructed an algorithm with $O^*(n^5)$ oracle queries. We used the isotropic position for sandwiching. (See Section 5.2.)
- Bubley, Dyer, and Jerrum [26] gave an analysis of the Ball-Walk algorithm using a "coupling argument".

[14] A more detailed description of the story is given in [56].

[15] Another continuous random walk was the Hit-and-Run but that was analyzed only much later.

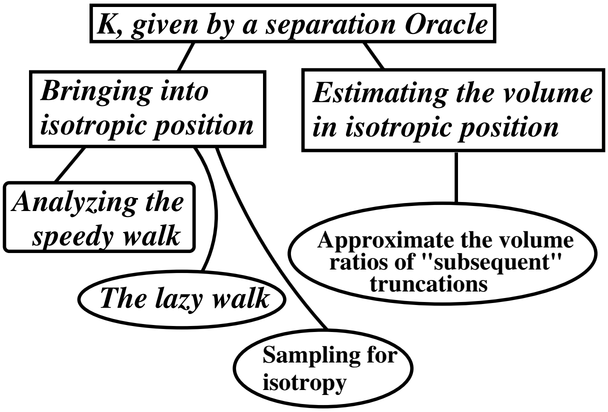
- Lovász [77] proved that after certain preprocessing the Hit-and-Run method mixes fast. (See Theorem 13.)
- Recently Kannan, Lovász, and Montenegro [58] gave a better analysis of the ball-walk.
- Lovász and Vempala extended the hit-and-run results to sampling according a log-concave distribution [82].

We return to this "story" in a slightly different form of a table, in §6.

### *4.2. The two phases: sandwiching and Multiphase Monte Carlo*

We defined sandwiching in Definition 2. Generally we speak of rounding or sandwiching a convex body but for us this means the same.

In all the algorithms of which we are speaking here, first we use a sandwiching for $K$, and then we apply a multiphase Monte Carlo algorithm to the sandwiched body.


K, given by a separation Oracle
Bringing into isotropic position
Estimating the volume in isotropic position
Analyzing the speedy walk
The lazy walk
Sampling for isotropy
Approximate the volume ratios of "subsequent" truncations

Simplified outline of the $O^*(n^5)$ algorithm
(The structure of the algorithm is not a tree!)

The sandwiching is very important because our algorithms would not work for "pencil-like" bodies, i.e., bodies which are too long in one direction compared to their other dimensions. Later we shall return to this question.

**Random walks.** The theory of random walks is very rapidly growing and increasing in its importance. Random walks are attached to random coin-tosses, to Brownian motions, to many algorithms in computer science, to optimization, ...[16]

All the random walks we consider here are "time-reversible" which is kind of a symmetry condition, but we shall not define this here. Also, in case of the grid-walk we are walking in a finite state-space, therefore it is easy to attach a matrix $A$ (of the transition probabilities) to our random walks and use the matrix-theoretical properties

[16] One of the first applications in the related field was to generate a sequence of rules which helps one to walk around in an unknown "maze" [5].

of $A$. This can be done because the $t$-step transition probabilities are represented by $A^t$, and this is also the reason why the spectral properties of $A$ are very useful for us. For the continuous situation we have to invest a little extra work.

Basically we could distinguish between random walks in discrete spaces and random walks in arbitrary metric spaces. Strangely enough, in the field we are trying to describe, namely in geometric algorithms, first the discrete versions were applied (random walks on the grid) but now the emphasis is shifted to random walks in continuous spaces. Parallel to this, many interesting and important results were obtained in other applications of random walks, e.g., on card shuffling, generating a random element of a group, etc. and also a whole new body of research developed related to random walks on arbitrarily given finite graphs. And there is also another theory for *infinite* graphs.

Here we shall restrict ourselves to the minimum one should know about these random walks, but the reader is referred to the books [43] ... works of Diaconis [31], Aldous and Fill [3], papers of Lovász and Winkler [85] just to mention a few ones.

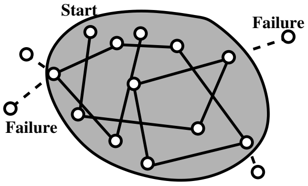
The theory of ergodic billiards is also related to this theory.

We are interested only in the geometric cases, when a convex body is given in $\mathbb{R}^n$ and we produce a random walk inside this body.

### 4.3. *Random walks in a convex body*

*4.3.1. How to use random walks to generate random points?* As we have already mentioned, in each of the considered algorithms one "invents" a random walk whose stationary distribution is either uniform on $K$ or has some other nice properties.

Then one simulates this random walk for polynomially many steps and outputs its endstate. The crucial question is if we can prove that in not too many steps we get a point whose distribution is nearly stationary. Our random walks have exponentially many states (or "even worse", sometimes they are continuous walks). We call such a random walk *rapidly mixing* if it gets near to its stationary distribution in polynomially many steps.[17]



The random walk produces the stationary distribution

*4.3.2. Lazy random walk* Whichever random walk we use for generating random points, we mostly assume that at each step we flip a coin, and (with probability $\frac{1}{2}$), i.e., for "tail" we *stay* where we were ("laziness") and for "head" we *plan* a random step: choose a random direction $\mathbf{v}$ and if $\mathbf{a}+\mathbf{v} \in K$, then we move to $\mathbf{a}+\mathbf{v}$, ("success") otherwise we (still) stay put ("failure").[18] If we have this original random "laziness", we call the random walk "lazy".

[17] Observe that this definition in this form is slightly loose.

[18] More precisely, sometimes we deviate from this basic scheme: e.g., for the Hit-and Run walk we do not have to check if we drop out of $K$ and in [80] we walk/integrate on the whole space, see Section 4.7.

Because of the original coin-flipping we move on average half slower than we could. So one would think that this "laziness" is completely unnecessary. But this is not so. If we walk around on a grid, then parity problems can prevent us from getting uniformly distributed points on the grid-points in $K$: however, this is not the real point. In the finite case, e.g., a random walk is described by a matrix. We use the laziness because it turns our matrices describing the random walk into *positive semidefinite* matrices. The analysis of our algorithm becomes much easier.[19]

do we need it too?

*Remark 10.* We use in our algorithms two kinds of sources for randomness: a "coin"-flipping, i.e., a sequence of independent random bits, and a sequence of independent random vectors, defining our steps and depending on the actual types of the walk.

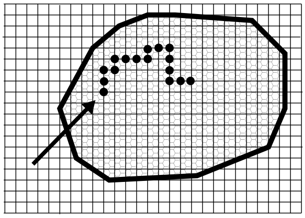
**Real exact arithmetics.** When counting the arithmetic steps, we have an additional "problem": the precision of "our arithmetics". Namely, we may choose two different models: in the first one we use *Real, exact arithmetics*, while in the second one we take into count the rounding errors as well. This second model may seem to be more realistic, however, in our cases the difference between the two models is negligible.

By continuity, if we use high enough precision and simulate a random walk using the two different arithmetics, the orbits would be roughly the same, with one exception: the *rounding error* would lead only to one serious change: when we are simulating a random walk in some (truncated) convex body $K_i$, at each step we have to decide if we are in the convex body or not. If with real arithmetics we decide that we are inside but the rounding error would result in getting out from $K_i$, then this would really change the realization of the considered random orbit. Yet, it is not too difficult to choose a high enough precision where the probability of such errors is negligible. For details see, e.g., [80].

!!

A convex body $K \subseteq \mathbb{R}^n$ is given and we consider three types of random walks on it.

### 4.4. Walking on the truncated grid



Walking on the truncated grid

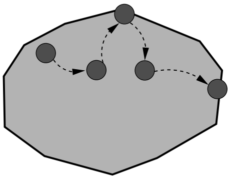
We define a sufficiently fine grid (of $\delta$-steps) and denote by $\mathbb{L}_\delta$ this grid. At each step we are at a point $\mathbf{x}_j$ (=vector) of the grid, and flip a coin and stay at $\mathbf{x}_j$ if the result of the flipping is "tail". Otherwise we choose a random direction $\mathbf{v}$ out of the $2n$ grid directions (uniformly, independently) and try to move to the neighbor $\mathbf{x}_j + \mathbf{v}$. If $\mathbf{x}_j + \mathbf{v} \notin K$, we stay put. If $\mathbf{x}_j + \mathbf{v} \in K$ then we move to $\mathbf{x}_{j+1} := \mathbf{x}_j + \mathbf{v}$.

In the original paper of Dyer, Frieze and Kannan [36] they use a grid with step-size $\delta = n^{-5/2}$. In [78] we changed several points and therefore could use larger steps, $\delta = n^{-3/2}$. This was one of the sources why our algorithm was faster.

[19] The situation is somewhat analogous to the one in Fejér's theorem: in case of the lazy walk we take some weighted averages of the probabilities of the ordinary walk. The averages of the Fourier sums of a function $f$ often converge even if the Fourier expansion does not.

### 4.5. Ball-steps

We choose a step-size, say $\delta > 0$ which is in the KLS Algorithm around $1/\sqrt{n}$. Then we use a "lazy" random walk, but when we try to move, we choose a random $\mathbf{v} \in \mathbb{B}(\mathbf{0}, \delta)$. Being in $\mathbf{x}_j$ we try to move into $\mathbf{x}_{j+1} := \mathbf{x}_j + \mathbf{v}$. However, if $\mathbf{x}_j + \mathbf{v} \notin K$ then we declare "failure" and do not move.



Random walk
with ball-steps

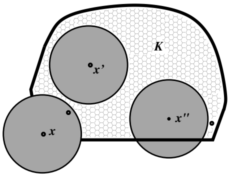
One problem is – with all our walks – that they may get stuck near corners of $K$. (Think of a point very close to a vertex of an $n$-dimensional cube: the probability of escape in a single step is close to $2^{-n}$.) This "getting stuck in a corner" has two versions: in the beginning, when we do not know where to start from, and in the middle of the algorithm.

Heuristically we feel that the problem is not so serious *during the algorithm* because the probability of getting into such a corner is also very small. Yet, somehow we have to handle this problem. To measure the seriousness of this "catch" we introduce the

**Definition 3 (Local conductance).** *The local conductance $\ell(x)$ is the probability of staying inside $K$:*

$$\ell(\mathbf{x}) = \ell_\delta(\mathbf{x}) := \frac{\mathbf{vol}(K \cap \mathbb{B}(\mathbf{x}, \delta))}{\mathbf{vol}(\mathbb{B}(\mathbf{x}, \delta))}. \tag{4}$$

On the figure we see three positions of $\mathbf{x}$, where in one case the $\delta$-ball is completely in $K$, $\ell(\mathbf{x}) = 1$, in the other a small part of the ball is outside, say, $\ell := 0.8$[20] and in the third case $\mathbf{x}$ is near the corner and staying inside has exponentially small chance.



Dangerous corners

Some results show that if the local conductance is large enough then the convergence is fast. One question often occuring is: if we know only that the *average local conductance* is large, can we still assure rapid mixing? The answer is YES and this is important in [60].

We have three important input parameters, $n$, $\varepsilon$ and $\eta$, and two "technical ones": $R$, $r$ of the oracle guarantee. After the sandwiching these are replaced by $d$ (the sandwiching ratio) and 1.

We also have to choose a step-size $\delta > 0$ in our algorithms using the grid-walk or the ball-walk, (but not in the Hit-and-Run [77]). The choice of $\delta$ is very important, see the next section.

In our KLS algorithm [60] we used the isotropic position for sandwiching (see §5.2) so we also needed two further parameters connected to the sandwiching: $\vartheta$, characterizing the quality of the approximate isotropic position, and the *average local conductance*

[20] There the figure may be misleading in high dimension.

$$\lambda := \frac{1}{\mathbf{vol}(K)} \int_K \ell(\mathbf{x})\, d\mathbf{x}, \tag{5}$$

defined using (4).

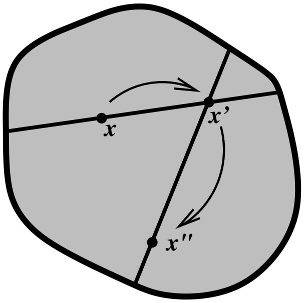
**How to choose the stepsize?** In many of these random walks we may choose the stepsize $\delta$ and if $\delta$ is small, then our rambling around will not be fast enough and we lose on that. On the other hand, if we choose a too large $\delta$, then we shall "jump out of $K$" too often, wasting many steps. So we should choose $\delta$ so that the probability of "jumping out" be on average a constant, say, $\approx 1/2$.

**Problem.** We could change the stepsize during the random walk by decreasing $\delta$ if we jump out too often and increasing it if we jump out too rarely. Can this help in our algorithms? Namely,

(a) Can we choose such rules to get good implementations?
(b) Can we analyze the obtained "generalized" random walks?

The difficulty with this is that using such rules we do not always get Markov Chains. An additional problem can be that the stationary distribution does not always exist for this general setting, or it may exist but it may differ from the desired distribution.

### *4.6. Hit-and-Run*



Hit and Run

Given a $K \subseteq \mathbb{R}^n$, we define the Hit-and-Run step for an $\mathbf{x} \in K$ as follows: we generate a random uniform vector $\mathbf{v} \in \mathbb{S}(\mathbf{0}, 1)$, (where $\mathbb{S}(\mathbf{x}, r)$ denotes the sphere of radius $r$ around $\mathbf{x}$) and then determine (using a halving method) the intersection segment of the line $\mathbf{x} + t\mathbf{v}$ and $K$. Next we take a random uniformly distributed $\mathbf{x}'$ on this segment and move there. This is called the "Hit-and-Run" random walk, introduced by Smith [96].

Some people felt that this random walk mixes very fast. This was verified (in some sense) by Lovász [77], see in the Appendix.

lazy???

*Remark 11 (Warm start).* Hit-and run is analyzed in several papers, from practical and theoretical points of view (Practical: [96], [15], theoretical: [77], [82], etc.). Right now the theoretical approach does not extend to the sandwiching part: uses so called *warm start*. **Warm start means** that in analyzing an algorithm we immediately jump to the second part of the algorithms: to the volume estimate of a sufficiently round (i.e., well sandwiched) convex body. So we assume that $K$ is sufficiently round. We use one more extra assumption: that we have a sufficiently good initial distribution on the convex body.

### *4.7. Metropolis algorithms?*

As we pointed out in the introduction, the field contains – beside many technical difficulties and tedious calculations – many elegant ideas.

If we can generate uniform distribution on $K$ then we can generate many other distributions as well, in many different ways. One standard approach is the following one:

**Metropolis Algorithm.** Assume that we have a function $f(\mathbf{x})$ on $K$ and a random walk, say any of the above ones: grid-walk, ball-walk, hit-and-run. We can modify easily our random walk using the same laziness as above, but even when we wish to move (because of getting "head") we

- check if $f(\mathbf{x}) \geq f(\mathbf{x}+\mathbf{v})$, and if YES, we move to $\mathbf{x}+\mathbf{v}$,
- if NO, then we produce a random event $\mathcal{C}$ (=generalized coin flipping) of probability $\frac{f(\mathbf{x}+\mathbf{v})}{f(\mathbf{x})}$. If we have a success with $\mathcal{C}$, we move to $\mathbf{x}+\mathbf{v}$, otherwise we stay in $\mathbf{x}$.

If $\int f < \infty$ then this will produce a distribution proportional to $f(\mathbf{x})$. For the details see [8, 80].

Applegate and Kannan [8] were the first to use Metropolis algorithm [87] in this field. This means that instead of generating uniform distribution we generate some other one. In our paper with Lovász [80], yielding an $O^*(n^7)$ algorithm we also used Metropolis algorithm and the following

**Lemma 2.** *Let $K$ be a convex body containing the origin in the interior and $x \in \mathbb{R}^n$. Denote by $\phi(x) = \phi_K(x)$ the least non-negative number $t$ for which $x \in tK$. Then*

$$\mathbf{vol}(K) = \frac{1}{n!} \int\limits_{\mathbb{R}^n} e^{-\phi(x)} dx.$$

The formula easily follows from that $\int_0^\infty t^{n-1} e^{-t}\, dt = (n-1)!$. Its application – in some sense – replaces the sandwiching: the parts of the integral corresponding to the distant parts of the space decay exponentially.

One advantage of this formula is that it is an integral over the whole space: the problems connected with the boundary of $K$ disappear. To use this formula we need to generate points according to a distribution proportional to $f(\mathbf{x}) := e^{-\phi(\mathbf{x})}$, which is easy, using the Metropolis algorithm.

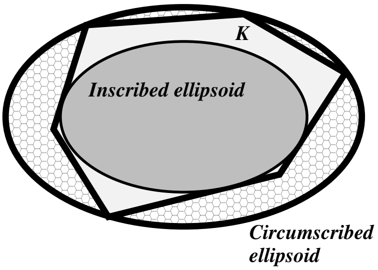
### *4.8. Local conductance and speedy walk*

Another place where we used random ball walks to generate non-uniform distributions was our paper [60]. We used a random walk that – as a lazy random walk – converged to uniform distribution on $K$, but when – for technical reasons – we "observed" it only when it really moved, then we got a non-uniform distribution. If we do not count the steps when we jump out, then the probability of those points where we jump out with high probability will be very small. Indeed, we can see that we get a distribution proportional to the local conductance $\ell(\mathbf{x})$, defined in (4). This walk is called the "speedy walk". Its analysis is simpler, since it does not get stuck in corners, but we have to compensate this by some extra work at the end: we are interested in the number of steps of the Lazy Random walk and are not allowed to forget the wasted steps. So we have to show that on the average we do not lose to many steps. The details are omitted.

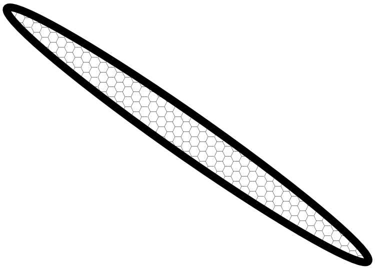
## 5. Sandwiching a convex body

### 5.1. Sandwiching and its importance

Sandwiching was defined in Definition 2. The sandwiching means that we try to find a linear transformation $A$ such that for $AK$ the ratio of the radii of circumscribed and inscribed balls is small: $n^c$. We use both sandwiching and approximate sandwiching, as explained below.



Sandwiching



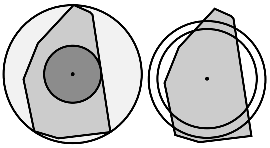
Why do we use sandwiching?

The sandwiching ratio strongly influences the speed of our algorithms. The thumb-rule is that if we gain a factor $\lambda$ in sandwiching, we gain $\lambda^2$ in the speed: for $K$ with a sandwiching ratio $d$, all the considered algorithms will have upper estimates for the number of oracle queries, proportional to $d^2$. Therefore having a sandwiching ratio $d \sim n\sqrt{n}$, in the Dyer-Frieze-Kannan algorithm instead of the Löwner-John ratio $n$ means losing a factor of $n$. In [80] we used randomized approximate sandwiching. By randomization we pushed down the sandwiching ratio to $n$, thus gaining a $\sqrt{n}$. This gains in "speed" a factor of $n$. We could also throw away an $\varepsilon$ portion of $\mathbf{vol}(K)$, bringing down the sandwiching ratio of the truncated body to $\sqrt{n}$. This resulted in another improvement of a factor of $n$.

This yields in [80] an $O^*(n^7)$ algorithm, but for centrally symmetric $K$ we can gain in the "approximate sandwiching" factor a further $\sqrt{n}$, thus reducing the number of queries to $O^*(n^6)$, If we consider a polyhedron defined by polynomially many inequalities, then we can gain a further $\sqrt{n}$ on sandwiching, thus bringing down the number of oracle queries to $O^*(n^5)$.

The ratio of approximate sandwiching may be $n$, or even better, $\sqrt{n}$. Perhaps it is possible to achieve a sandwiching ratio that is a log-power.

**Approximate sandwiching.**



Sandwiching is difficult. In the early papers we used so many steps to approximate the volume of a sandwiched convex body that the sandwiching seemed cheap. As the algorithms improved the sandwiching became more involved, slightly more expensive and the approximation of the sandwiched body cheaper and cheaper. So in [60] we used $O^*(n^5)$ oracle queries for both sandwiching and approximating in the second phase.

From that on, if one wishes to get a faster algorithm, one has to improve the sandwiching as well.

To be precise, we used exact sandwiching and approximate sandwiching as well. Approximate sandwiching means that the ellipsoid $E_2$ by and large should be inside $K$ while the ellipsoid $E_1$ should by and large contain $K$. [21]

To speed up the sandwiching means that one has to find a sandwiching which gives at least $\sqrt{n}$ approximate sandwiching ratio, but does it in, say, $O^*(n^4)$ steps.

We conclude this part with a problem connected to sandwiching:

**Problem.** (Lovász)[22] Given a convex $K \subseteq \mathbb{R}^n$ and an $\varepsilon > 0$, can one always find two concentric homothetic ellipsoids, $E_1, E_2$ so that their ratio is $\le (\log n)^c$ and $\mathbf{vol}(K \setminus E_2) < \varepsilon\mathbf{vol}(K)$ and $\mathbf{vol}(E_1 \setminus K) < \varepsilon\mathbf{vol}(K)$?

The conjecture is YES. The conjecture can easily be checked for a simplex or a cube. Observe that this problem is purely geometric, not algorithmic.

### *5.2. The isotropic position*

The shape of a general convex body may be very complicated and there are several ellipsoids attached to a $K \subseteq \mathbb{R}^n$ to describe its shape more or less accurately. We have already seen the Löwner-John ellipsoids. Earlier by sandwiching we meant – among others – to change the shape of $K$ by a linear transformation so that its Löwner ellipsoid became a ball. Now we describe another similar but perhaps more efficient method.

Two further ellipsoids attached to $K$ are the Legendre and the Binet ellipsoids. Assume that the center of gravity is $\mathbf{0}$. Given a unit vector $\mathbf{s}$, that defines a hyperplane $H_{\mathbf{s}}$ through the origin, and we may calculate the quadratic inertia of $K$ to this $H_{\mathbf{s}}$:

$$I(\mathbf{s}) := \int_K (\mathbf{x} \cdot \mathbf{s})^2 \, d\mathbf{x},$$

where $\mathbf{x} \cdot \mathbf{s}$ is the ordinary scalar product. There exists a unique ellipsoid $E_K$ with the property that their inertia is the same in every direction:

$$\int_K (\mathbf{x} \cdot \mathbf{s})^2 \, d\mathbf{x} = \int_{E_K} (\mathbf{x} \cdot \mathbf{s})^2 \, d\mathbf{x}, \quad \text{for every} \quad \mathbf{s} \in \mathbb{R}^n.$$

This $E_K$ is called the Legendre ellipsoid of $K$. If this ellipsoid is a unit ball, then, (after a proper normalization) we say that $K$ is in isotropic position. The Binet ellipsoid is dual to the Legendre ellipsoid.[23] For a more detailed description see, e.g., [90, 89]. If $E_K$ is not a ball, then applying a linear transformation $A$ to $K$ we may achieve that the ellipsoid becomes a unit ball. This convex body $K_I := AK$ is called the isotropic position of $K$.

More formally,

**Definition 4 (Isotropic position).** *$K \subseteq \mathbb{R}^n$ is in isotropic position, if the center of gravity of $K$ is the origin:*

$$\mathbf{b}(K) := \int_K \mathbf{x} \, d\mathbf{x} = 0.$$

[21] In [80] we "paid" $O^*(n^7)$ for both approximate sandwiching and approximating the volume of the sandwiched body!

[22] I have heard this conjecture in this form from Lovász but it goes back to some works of V. Milman.

[23] at least, for centrally symmetric bodies.

*and, using the notation* $\mathbf{x} = (x_1, \dots, x_n)$*, for every* $1 \le i \le j \le n$,

$$\frac{1}{\mathbf{vol}(K)} \int_K x_i x_j = \begin{cases} 1, & \text{if } i = j, \\ 0, & \text{if } i \neq j. \end{cases}$$ [24]

The above definition implies that

$$\frac{1}{\mathbf{vol}(K)} \int_K \|\mathbf{x}\|^2 \, d\mathbf{x} = n,$$

and therefore the largest part, all but an $\varepsilon$ portion of $K$ belongs to $\mathbb{B}(\mathbf{0}, \sqrt{\frac{n}{\varepsilon}})$.

*Remark 12.* Here we underemphasized two topics: the log-concavity and the Brunn-Minkowski type theorems. A theorem of Borell [18] asserts that the measure of the spherical sections of a convex body is a log-concave function. This implies that $\mathbf{vol}(K \setminus B(\mathbf{0}, T)) < e^{-cT}$, providing better results.

### 5.3. Almost isotropic position

Because of computational errors (and weak separation) we cannot hope for an exact isotropic position: we have to introduce its approximate versions.

**Definition 5.** *K is in* $\vartheta$*-almost-isotropic position if (for some* $\vartheta \in (0, 1)$*),*

$$\|\mathbf{b}(K)\| \le \vartheta,$$

*and, for every* $\mathbf{v} \in \mathbb{R}^n$*, we have*

$$(1 - \vartheta)\|\mathbf{v}\|^2 \le \frac{1}{\mathbf{vol}(K)} \int_{K - \mathbf{b}(K)} (\mathbf{v}^{\mathsf{T}}\mathbf{x})^2 \, d\mathbf{x} \le (1 + \vartheta)\|\mathbf{v}\|^2. \qquad (6)$$ [25]

In our algorithms we use a quantitative version of the following

**Lemma 3.** *Given a convex* $K \subseteq \mathbb{R}^n$ *(by a weak separation oracle), for every* $\vartheta, \eta > 0$*, there exist an* $N = N(n, \vartheta, \eta)$[26] *for which if we select N points in K uniformly, independently, attach to each of them weights* $\frac{1}{N}$ *and find a linear transformation A that brings this point-set into isotropic position, then* $AK$ *will be in* $\vartheta$*-almost isotropic position, with probability* $> 1 - \eta$.

We cannot use this lemma in *this* form, since it is not quantitative. So we proved that $N := c_{\eta,\vartheta} n^2$ will do [60]. Our results were improved to $cn \log^3 n$ by Bourgain [19] and to $cn \log^2 n$ by Rudelson [94]. We used

**Theorem 6.** *For given* $0 < \eta, \vartheta < 1$*, there exists a randomized algorithm, that finds an affine transformation A such that* $AK$ *is* $\vartheta$*-almost isotropic, with probability at least* $1 - \eta$*.*

*The number of oracle calls is* $O(n^5 |\ln(\vartheta\eta)| \ln n)$.

*Further, with probability at least* $1 - \eta$,

$$\mathbf{vol}(AK \setminus 2\sqrt{2n} \log(1/\varepsilon)\mathbf{B}) < \varepsilon \mathbf{vol}(AK).$$ [27]

[24] Milman and Pajor (1987) used a slightly different normalization.

[25] Such a lemma can be found, e.g., in [89]

[26] Here we assumed a preliminary sandwiching, otherwise the $R$, $r$ in well-guaranteeing $K$ should also be mentioned.

[27] This last statement is a version of Remark 12.

### *5.4. The approximate Löwner-John ellipsoids?*

As we mentioned, we cannot really find the smallest (in volume) circumscribed, or the largest inscribed ellipsoids for a given well-guaranteed $K \subseteq \mathbb{R}^n$. Not even with a randomized algorithm. At the same time, we have a randomized algorithm [60] that finds in $O^*(n^5)$ steps a linear transformation $A$ such that

$$\mathbb{B}(\mathbf{0}, 1-\varepsilon) \subseteq AK \subseteq \mathbb{B}(\mathbf{0}, n+\varepsilon).$$

More precisely, we have an algorithm which finds approximately the isotropic position of $K$ and also, we have the following theorem.

**Theorem 7.** *If $AK$ is in isotropic position of $K$ then*

$$\sqrt{\frac{n+2}{n}}B \subseteq AK \subseteq \sqrt{n(n+2)}B.$$

Observe that the ratio of the upper and lower bounds is $n$. Again, if $AK$ is the regular simplex, then this is sharp. So the preimage of these balls can replace the LJ-ellipsoids in many cases.

(A similar result was independently proved by Gy. Sonnevend [97].)

*Remark 13.* (a) We have to be careful: our algorithm gives only the *approximate* isotropic position, but it is not too hard to show that that gives a good approximation in Theorem 7. (b) One reason why we would not call what we got an approximate LJ-ellipsoid is that the LJ ellipsoid was defined as the minimum volume ellipsoid containing $K$.

### *5.5. Volume of a "well sandwiched" K*

Assume that $K$ is brought into near isotropic position, using $O^*(n^5)$ oracle calls. After this, we omit the parts of $K$ outside the ball of radius $2\sqrt{2n}\log(1/\varepsilon)$. We lose at most a fraction of $\varepsilon$ of its volume (see Remark 12). Thus we reduced the problem to the case when $\mathbb{B}(\mathbf{0}, 1) \subseteq K \subseteq \sqrt{8n}\log(1/\varepsilon)\mathbb{B}(\mathbf{0}, 1)$, in time $O^*(n^5)$. More generally, one can compute the volume of a convex body $K$ satisfying $B \subseteq K \subseteq dB$ in time $O^*(n^4 d^2)$.

Put $K_i := K \cap \mathbb{B}(\mathbf{0}, 2^{i/n})$ $(i = 0, \dots, m = \lceil n \log_2 d \rceil)$. $K_0 = \mathbb{B}(\mathbf{0}, 1)$ and $K_m = K$. Roughly speaking, using random walks, we generate $p = 400\varepsilon^{-2} n \log n = O^*(n)$ random points in each $K_i$ and count how many of them fall in $K_{i-1}$; this gives an estimate of the ratio $\mathbf{vol}(K_{i-1})/\mathbf{vol}(K_i)$. Then the telescopic product (3) yields the approximation of $\mathbf{vol}(K)$.

However, to improve the algorithm a little bit, i.e., for some technical reasons, we replace these volumes by the integrals of the local conductance functions, $\ell_i$ defined by the truncated bodies $K_i$. Then we take the corresponding telescopic product to estimate the volume. At this point we stop giving the details but remark that the actual algorithm becomes more complicated because of several technical reasons.

**Theorem 8.** *Assume that $K$ satisfies $B \subseteq K \subseteq dB$. Then the probability that the value $\zeta$ returned by the algorithm is between* $(1-\varepsilon)\mathbf{vol}(K)$ *and* $(1+\varepsilon)\mathbf{vol}(K)$ *is at least* $3/4$. *With probability at least* $9/10$*, the total number of oracle calls is*

$$O\left(\frac{n^4d^2}{\varepsilon^2}\ln n \ln d (\ln \frac{n}{\varepsilon})^2\right).$$

With the isotropic sandwiching we can use $d = \sqrt{\frac{n}{\log(1/\varepsilon)}}$. Thus, by and large, we get back Theorem 1: the estimates are slightly weaker there because the sandwiching is more expensive than the estimates for the sandwiched body. We emphasize that here one has to be very cautious, otherwise one can get into circular arguments: to bring $K$ into sandwiched situation we already do almost everything we need to get its volume: we generate recursively uniformly distributed points in $K_i$.

## 6. Comparison of algorithms

First I will count the number of oracle queries in our $O^*(n^5)$ KLS algorithm [60], then provide a table that compares some features of the algorithms considered until now.

*How many steps?*

1. Preliminary sandwiching needs $O^*(n^4)$ Oracle queries.
2. Improving the average local conductance ... are technical steps which we skip here.
3. Bringing into isotropic position has two subcases: the very elongated body and the not too elongated one:
   - For $K$ with $B \subseteq K \subseteq 10nB$: Theorem 2 with $N := \frac{80n^2}{\vartheta\eta}$ random points uses $O(n^3d^2 + Nn^2d^2)$ oracle queries, which would be $O^*(n^5)$ if we could achieve $d := O(\sqrt{n})$. We achieve this by an involved interlacing method but an alternative way is to achieve only $d = O(n)$ in a much simpler way and use the Bourgain-Rudelson results, mentioned on p361.
   - For the general case we notice that if $K$ is very badly sandwiched and we bring into isoperimetric position only the "near part": $K \cap (10n\mathbb{B}(\mathbf{0}, 1))$ then the diameter decreases by a constant factor and we may iterate this: this happens only $O(\log n)$ times.
4. When $K$ is in isotropic position, we delete those parts which are outside of the ball $\mathbb{B}(\mathbf{0}, \sqrt{\frac{8n}{\log(1/\varepsilon)}})$. This causes a relative error $\leq \varepsilon$ and provides a good sandwiching. For each $K_i$ we use $p := \frac{400n\log n}{\varepsilon^2}$ random points, altogether, $O(\frac{n^2\log^2 n}{\varepsilon^2})$. points. For that we need $O^*(n^5)$ oracle queries.

*The comparison table.* To avoid getting an overcrowded table, I left some boxes empty. Each algorithm below, except the second one, runs on time proportional to $\frac{1}{\varepsilon^2}$ $\log^k \frac{1}{\varepsilon} \log \frac{1}{\eta}$, in the second algorithm we have $\frac{1}{\varepsilon^4}$ instead of $\frac{1}{\varepsilon^2}$.

Each algorithm has a pre-sandwiching phase, to get to $d_0 := n\sqrt{n}$, which is deterministic and costs $O(n^4\log(R/r))$ questions.

| Authors | Walk Type | Sandwiching method | Sampling | Remark | #S |
|---|---|---|---|---|---|
| Dyer-Frieze -Kannan [36] | grid | $d = n\sqrt{n}$ +Minkowski sum | | Break-through | $n^{23}$ |
| Lovász- -Sim.[78] | grid | | | Localization Lemma | $n^{16}$ |
| Applegate -Kannan [8] | grid | two cubes $d = n$ | | Metropolis | $n^{10}$ |
| Lovász [76] | Ball walk | | | | $n^8$ |
| Dyer-Frieze [35] | grid | two cubes | | | $n^8$ |
| Lovász -Sim.[80] | ball walk | randomized, $d = cn$ $\int_{\mathbb{R}^n} e^{-\Phi}$, Cost: $n^7$ | | Metropolis | $n^{10}$ |
| Kannan-Lovász -Sim. [60] | ball walk | Isotropic, interlaced Cost: $n^5$ | $c_1 n^3 d^2 +$ $c_2 N n^2 d^2$ | Theorems 1 2 | $n^5$ |
| Lovász [77] | Hit-and -Run | Warm start see Remark 11 | Warm start | | $n^5$ |
| Lovász -Vempala [84] | "Simulated Annealing" | | | See Appendix II | $n^4$ |

## 7. Eigenvalues, conductance, Isoperimetric Inequalities and Rapid Mixing

### *7.1. Why are the isoperimetric inequalities important?*

In these algorithms it is very important to understand, why the isoperimetric inequalities are important.

Isoperimetric inequalities belong to the classical part of mathematics. In analyzing Rapid Mixing of Markov Chains they are important for the following reason:

Consider the example of two intersecting balls in Section 2.3. There we have defined a non-convex body: the union of two unit balls, $\mathbb{D}^*(\mathbf{0}, \mathbf{x})$. Choose $\mathbf{x}$ at random from the unit sphere. If we start a random walk say from the origin, then we have only exponentially small chance to reach the center of the other ball, because they can be separated from each other by an exponentially small surface: there is a *bottleneck* between the two balls and we have no chance to find this bottleneck.

So to hope for rapid mixing we need lower bounds for the sizes of separating surfaces, and these are the Isoperimetric Inequalities. We cannot hope for such inequalities in all the cases but we can if $K$ is convex.

### *7.2. Localization Lemma*

In [78] we established a method which made easier to prove various isoperimetric inequalities.

Dyer, Frieze and Kannan conjectured an isoperimetric inequality which we proved in a stronger form [78]:

**Theorem 9 (An isoperimetric inequality).** *Let $K \subseteq \mathbb{R}^n$ be convex, with diameter $d$. Assume that a surface with $(n-1)$-dimensional measure $f$ splits $K$ into two sets $K^*$*

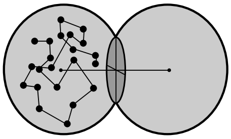
*and* $K^{**}$. *Then*

$$\min\{\mathbf{vol}(K^*), \mathbf{vol}(K^{**})\} < fd. \tag{7}$$

If we take the hyperplane sections of $K$ orthogonal to a direction $\mathbf{s}$, then their measure gives a log-concave function, (mostly) with one maximum and *decreasing* in one of the two directions. So, (7) is trivial for hyperplane sections. Theorem 9 asserts that for *any* surface (7) still holds.

Theorem 9 is was slightly sharpened and strongly generalized in several steps, see [59]. The proof was based on a *"Localization Lemma"* that reduces the high-dimensional cases to 1-dimensional cases. (An alternative approach to prove such inequalities was given by Khachiyan and Karzanov [64] and a similar approach was used by Payne and Weinberger [93].)

*7.2.1. Conductance*



The bottleneck prevents rapid mixing

Instead of Isoperimetric Inequalities we often use a version of theirs: the *conductance* (introduced by Sinclair and Jerrum [53]). The conductance itself has several versions, e.g., edge-conductance, vertex conductance, $\mu$-conductance. For a random walk on a not necessarily convex $K \subseteq \mathbb{R}^n$ one way to define the "edge-conductance" is by

$$\Phi(K) = \min_{\substack{S \subseteq K \\ \mathbb{P}(S) \le 1/2}} \frac{\mathbb{P}(x_{i+1} \in \overline{S} \mid x_i \in S)}{\mathbb{P}(S)}. \tag{8}$$

The connection of the conductance to the isoperimetry can be understood easily: If we can cut $K$ into two large parts $S$ and $K \setminus S$ by a small surface $F$, then the probability of jumping from one side to the other corresponds to the $\delta$-neighbourhood of $F$: so that is small: the conductance is small ...

Why is this notion important? We generate a given distribution on a convex body $K \subseteq \mathbb{R}^n$ by using an appropriate Markov Chain. Here "appropriate" means two things:

(a) that its limit distribution is the required one (independently from the initial distribution) and

(b) that the distribution converges to its limit distribution relatively fast.

To formulate more precise statements, mostly we introduce some distances on the distributions, and if $\rho(P, P_i)$ is a distance of the distribution $P$ from $P_i$, then mostly we use results of the following form:

$$\rho(P, P_i) \le \rho(P, P_0) \cdot \left(1 - \frac{\Phi^2}{2}\right)^i, \tag{9}$$

where $P$ is the limit distribution, $P_0$ is the initial distribution, and $\Phi$ is defined by (8), characteristic for $K$, and the random walk. A typical problem occuring in our proofs is that $\rho(P, P_0)$ is often "too large"!

The "distance" of distributions in (9) varies from place to place: sometimes we use $L_2$-norm, or $L_1$-norm, which is equivalent with using *total variation* distance,[28] but,

[28] This is equivalent with the $L_1$-norm if the density functions exist.

e.g., in [60] we used the asymmetric

$$M(P,Q)=\sup_S \frac{|P(S)-Q(S)|}{\sqrt{Q(S)}}.$$

Historically it was clear that the spectral gap[29] is strongly connected to the speed of mixing of a random walk. J. Cheeger [29] proved for compact Riemannian manifolds of dimension $n$ that some isoperimetric properties are directly connected to the spectral gap. This was translated to the discrete case by several people, like Alon, Milman [6] [7], Dodziuk and Kendall [32], Tanner [99]. The connection is not surprising at all.

For graphs, if a graph has good isoperimetric properties, or large conductance, then the random walk on the graph will be rapidly mixing.

# IV. Negative result for the diameter

## 8. Diameter and width algorithms

Below the results for the diameter and width are roughly the same. We do not really have to distinguish them. Speaking of $K$ we always assume that it is convex, bounded and is given by some oracle: by strong membership oracle in the lower bounds and weak separation oracles in the upper bounds. (This way we get stronger results!)

Grötschel, Lovász and Schrijver [49] gave a polynomial time deterministic algorithm that computed an upper bound $\overline{\mathbf{w}}(K)$ and a lower bound $\underline{\mathbf{w}}(K)$ for the width, with $\frac{\overline{\mathbf{w}}(K)}{\underline{\mathbf{w}}(K)}\le\sqrt{n}(n+1)$.

Elekes [39] proved that there is no polynomial algorithm which would compute an upper and a lower bounds for the width of a convex $K$ (given by an oracle) with $\frac{\overline{\mathbf{w}}(K)}{\underline{\mathbf{w}}(K)}\le 2$. Bárány and Füredi improved this [12] by proving

**Theorem 10.** *There is no polynomial time deterministic algorithm that would compute an upper bound $\overline{\mathbf{w}}(K)$ and a lower bound $\underline{\mathbf{w}}(K)$ with*

$$\frac{\overline{\mathbf{w}}(K)}{\underline{\mathbf{w}}(K)}\le\sqrt{\frac{n}{c\log n}}.$$

Much later, Lovász and I proved [79] that

**Theorem 11.** *Every randomized algorithm that computes for every centrally symmetric convex $K\subseteq\mathbb{R}^n$, given by an oracle, a lower bound $\underline{\mathbf{w}}(K)$ for* **width**$(K)$ *with*

$$\underline{\mathbf{w}}(K)\le\mathbf{width}(K)\le n^{1/4}\underline{\mathbf{w}}(K),$$

*has to make at least $2^{n^{1/4}}$ calls on the oracle.*

[29] the difference between the largest in absolute value and the second largest eigenvalue of the Laplacian.

This means that the width cannot be efficiently computed, *not even by randomized algorithms.*

The problem of estimating the diameter or the width of a convex $K \subseteq \mathbb{R}^n$ (given by an oracle) are – at least for centrally symmetric bodies – dual problems and therefore equivalent: all the negative results for centrally symmetric bodies for width and diameter are equivalent.

Theorem 11 was improved by Kannan, Lovász, and Simonovits and Brieden, Gritzmann and Klee [21] [22] and extended to other metrics.

If $K \subseteq \mathbb{R}^n$ is a convex body given by a (well-guaranteed) separation oracle, then it is not too difficult to prove that

**Lemma 4 ([21, 22]).** *We can compute a* $\zeta(K)$ *with a deterministic polynomial time algorithm such that* $\zeta(K) \le \mathbf{diam}(K) \le (1+\varepsilon)\sqrt{n} \cdot \zeta(K)$.

*Proof.* (Sketch) We can find a smallest box $\prod[a_i, b_i]$ containing $K$ with relative error $\varepsilon/3 > 0$. The diameter of this box will be the upper bound, the longest side, $\max[b_i - a_i]$ the lower bound on $\mathbf{diam}(K)$: clearly, their ratio is smaller than $(1+\varepsilon)\sqrt{n}$. □

This can be improved:

**Lemma 5.** *If we have a fixed K and a* random orthogonal coordinate system, *then, with high probability the ratio of the upper and lower bounds will be at most* $O(\sqrt{n/\log n})$. □

Even better, using a construction of M. Kochol, [70] we obtained

**Theorem 12 ([21, 22]).** *For every constant* $c > 0$, *we can compute a* $\zeta(K)$ *with a deterministic polynomial time algorithm such that*

$$\zeta(K) \le \mathbf{diam}(K) \le c\sqrt{\frac{n}{\log n}} \cdot \zeta(K).$$

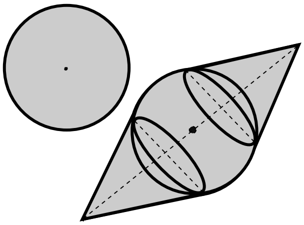
*(The degree of the polynomial depends on c.)*

*On the other hand, if a randomized algorithm* $\mathcal{A}$ *produces for every convex* $K \subseteq \mathbb{R}^n$ *a* $\zeta(K) \le \mathbf{diam}(K)$ *in polynomially many steps, then for some convex* $K_0$ *in the n dimensional Euclidean space* $\mathbb{R}^n$

$$\frac{\mathbf{diam}(K_0)}{\zeta(K_0)} \ge c_{\mathcal{A}} \cdot \sqrt{\frac{n}{\log n}}.$$

This is the most we can get: the lower bound for the randomized approximation algorithms matches the upper bound for a deterministic one.

## 9. Why is the diameter more difficult?



We have seen that for the diameter computation the randomization does not help. The difficulty comes from the fact that if we consider the two bodies on the figure on the left, then the algorithms cannot really distinguish them: The first body is the ball, the second one is the "double coned" ball: we select a random vector $\mathbf{x}$ at distance $|\mathbf{x}| = \sqrt{\frac{n}{\log n}}$ and take the convex hull of the ball, $\mathbf{x}$ and $-\mathbf{x}$.

The arguments of §II/2.7 apply to this situation, showing that the deterministic algorithms must fail. The same time, the volume of the two caps are so small that the probability that a random walk reaches them is also negligible: this is why even the randomized algorithms must fail. We could restrict ourselves to one cap as well, to get the negative result: we used two caps to get centrally symmetric "test" bodies: then the negative result immediately implies the analogous result for the width, and also, in Geometric Functional Analysis the centrally symmetric bodies are used[30].

## 10. Other metrics?

Most of the problems discussed in the last section make sense for other metrics as well. So, e.g., it is natural to ask, what happens if we replace the Euclidean metrics by some $\ell_p$-metrics. Many results generalize to this more general setting. This is not really the place to go into details. The reader is referred to our paper [22], or some earlier results of Gritzmann and Klee [42].

## 11. Another open problem

The problem below refers to the fact that our negative results heavily use that the convex bodies are given by Oracles. In reality one often meets explicitly given convex bodies and one would like to know what is the situation for those cases.

**Problem.** Do we have lower bounds on the number of oracle questions, if $K \subseteq \mathbb{R}^n$ is given in a "concrete form", not by an oracle?

# V. Appendix

## 12. The analysis of the Hit and Run method

The hit-and run method is one of the most interesting steps for random walks in a convex body. We have already defined it in Section 4.6.

Lovász proved [77] that

[30] The equivalence is not really needed: our proofs easily carry over from one of the two cases to the other.

**Theorem 13.** *Let $K$ be a convex body in $\mathbb{R}^n$ with diameter $D$, and suppose that $K$ contains a unit ball. Let $w_0, w_1, \ldots$ be a lazy hit-and-run walk in $K$ with warm start, and let* $0 < \varepsilon < 1$. *Let*

$$N = \left\lceil 10^8 \ln \frac{1}{\varepsilon} \frac{n^2 D^2}{\varepsilon^2} \right\rceil.$$

*Then for every set $S \subset K$, for the limit (=uniform) distribution* $\Pi(.)$,

$$|\mathbb{P}(w_N \in S) - \Pi(S)| \le \varepsilon.$$

To generate a log-concave distribution see Lovász and Vempala [81], [82].

## 13. Connection to harmonic functions

Assume we have a random walk on a graph or in a convex domain.[31] The probability $p^t(\mathbf{x})$ of being in $\mathbf{x}$ at time $t$ is the average of the probabilities of being in the neighboring points. This is exactly the same mechanism we use to describe the heat propagation. Therefore it is not surprising at all that the same techniques, equations, inequalities can be applied to Markov Chains as to describe the heat propagation.

## 14. Other sources

Again, there are several overlapping parts in the four sections below.

**Books:** I have already mentioned the book of Grötschel, Lovász, and Schrijver, [49], as a basic source for the related wider areas. Lovász also wrote a small book [74], describing some application of the ellipsoid method, and connecting this to the Lenstra-Lenstra-Lovász approximate basis reduction algorithm [73], and many other things. One can find downloadable papers on the homepage of Mark Jerrum, now a book [51].

Several analytic aspects of the field, primarily related to the eigenvalue technique are nicely collected in F. Chung's book [30] on the spectral properties of graphs.

**Surveys:** There are many surveys of the field, or research papers with longer introductions, older and newer ones, that I would warmly recommend for reading, just to mention some papers of Lovász [75], Dyer and Frieze [35], Bollobás [13], Kannan [56], Jerrum [51].

Bollobás gave lectures on the topic and wrote them up [13]. It provides a lot of geometric details. Most of which I left out I warmly recommend it to the reader. Perhaps the excellent survey by Ravi Kannan [56] on the applications of Markov Chain Monte Carlo methods is the nearest to my approach. It covers a wider area, describing very many aspect of the field: applications both in combinatorial and in geometric algorithms. Also in applications to statistical problems which are important but I neglected them here.

Most of these surveys basically approach the field in the same way. The differences are in the details: where the emphasis is put and how much knowledge is assumed on the side of the reader.

[31] I mean here the grid walk and the ball walk: forget the Hit-and-Run or he Metropolis,...

I would also recommend the survey of Dominic Welsh [101], with the title "Approximate Counting" as one approaching a wider area and being concise, self-contained and very readable.[32]

The literature the reader may need can be classified as follows:

(i) Surveys following the same line as mine, (or introductions to research papers).
(ii) Introduction to the theory of Markov Chains: this was the field I neglected the most.
(iii) Description of the general Markov Chain Monte Carlo method. Here I warmly recommend to visit Mark Jerrum's Home Page and download some of his papers, book chapters. I recommend among others, [51] [52]. It is also interesting to see how [26] analyzes basically the same algorithm by an important alternative method, via Coupling technique.
(iv) Usage of ingenious formulas in the field.

**Further research papers:** There are several papers of Lovász describing the volume computation and related fields and a paper related to his ICM talk in Kyoto, 1990 [75].

Some papers of Lovász and Winkler describe the general theory of random walks on graphs, and their various applications, [85]. Another approach can be found in Aldous, Lovász, Winkler [4].

The introduction of the paper of Dyer and Frieze [35] is also a very good source of information.

**Internet sources:** The book of Aldous and Fill, the lecture of Bollobás [13], posted on the homepage of MSRI, Berkeley, [3] Zürich lectures of Jerrum [51] ...

## 15. Appendix II: Added in proof II.

I mentioned the important new results of Lovász and Vempala, on p340. The corresponding papers (also listed there) can be found on Vempala's home-page.

Lovász and Vempala "risk" the conjecture [84] that perhaps an $O^*(n^2)$ sampling algorithm could be devised leading to an $O^*(n3)$ volume algorithm. They also hope that their results can be extended to integration.

The reader could ask how their algorithm – described in a relatively short paper but using results from some other of their papers – is related to the algorithms described in this survey. In brief, they use "simulated annealing" and – instead of estimating ratios of volumes – they estimate ratios of integrals. (Using integrals has already been used in previous papers, but in another way.) They use only $O(\sqrt{n})$ bodies $K_i$ and only $O^*(\sqrt{n})$ points in each of them. For the interested reader, I highly recommend reading (at least Sections 1, 2, and 5) of their paper [84].

*Acknowledgements.* I would like to thank to László Lovász his very valuable mathematical and historical remarks, comments, and also to Vera T. Sós for the many helpful suggestions.

[32] Perhaps the proof-sketch described on p299 is misunderstandable: it is restricted – by the last few sentences – to the grid-walk case.

## References

1. Aldous, D., Diaconis, P.: Strong uniform times and finite random walks. Adv. Appl. Math. **8**(1), 69–97 (1987)
2. Aldous, D., Diaconis, P.: Shuffling cards and stopping times. Amer. Math. Monthly **93**(5), 333–348 (1986)
3. Aldous, D., Fill, J.: Reversible Markov Chains and Random walks on graphs. D. Aldous' homepage, http://www.stat.Berkeley.EDU/users/aldous/book.html
4. Aldous, D., Lovász, L., Winkler, P.: Mixing times for uniformly ergodic Markov chains. Stochastic Process. Appl. **71**(2), 165–185 (1997) MR 98i:60062
5. Aleliunas, R., Karp, R.M., Lipton, R.J.: Lovász, L., Rackoff, Ch.: Random walks, universal traversal sequences, and the complexity of maze problems. 20th Annual Symposium on Foundations of Computer Science, IEEE, New York, 1979, pp. 218–223
6. Alon, N.: Eigenvalues and expanders. Combinatorica **6**, 83–96 (1986)
7. Alon, N., Milman, V.D.: $\lambda_1$, isoperimetric inequalities for graphs and superconcentrators. J. Comb. Theory B **38**, 73–88 (1985)
8. Applegate, D., Kannan, R.: Sampling and integration of near log-concave functions. Proc. 23 ACM STOC, 156–163 (1990)
9. Baker, T., Gill, J., Solovay, R.: Relativizations of the $\mathcal{P} =?\mathcal{NP}$ question. SIAM J. Comput. **4**(4), 431–442 (1975)
10. Babai. L.: Automorphism Groups, Isomorphism, Reconstruction, Handbook of Combinatorics (eds Grötschel, Lovász, Schrijver) Springer, 1995, pp. 1447–1540
11. Bárány, I., Füredi, Z.: Computing the volume is difficult. Proc. of the 18th Annual ACM Symp, Theory Comput. 1986, pp. 442–447
12. Bárány, I., Füredi, Z.: Computing the volume is difficult. Disc. Comput. Geom. **2**(4), 319–326 (1987)
13. Bollobás, B.: Volume estimates and rapid mixing. Flavors of geometry. Math. Sci. Res. Inst. Publ. **31**, 151–182 (1997)
14. Bélisle, C.J.P., Romeijn, H.E., Smith, R.L.: Hit-and-run algorithms for generating multivariate distributions. Math. Oper. Res. **18**, 255–266 (1993)
15. Berbee, H.C., Boender, C.G., Rinnooy Kan, A.H.G., Scheffer, C.L., Smith, R.L., Telgen, J.: Hit-and-run algorithms for the identification of nonredundant linear inequalities. Math. Programming **37**, 184–207 (1987)
16. Bokowski, J.: Ungleichungen für des Inhalt von Trennflächen. Arch. Math. **34**, 84–89 (1980)
17. Bokowski, J., Spencer, E. Jr.: Zerlegung Konvexen Körperdurch minimale Trennflächen. J. Reine und Angew. Math. **311-312**, 80–100 (1979)
18. Borell, C.: The Brunn-Minkowski inequality in Gauss spaces. Invent. Math. **30**, 207–216 (1975)
19. Bourgain, J.: Random points in isotropic convex sets. Convex geometric analysis (Berkeley, CA, 1996), Math. Sci. Res. Inst. Publ. **34**, Cambridge Univ. Press, Cambridge, 1999, pp. 53–58
20. Bourgain, J., Milman, V.D.: Sections euclidiennes et volume des corps symétriques convexes dans $R^n$. [Euclidean sections and volume of symmetric convex bodies in $\mathbf{R}^n$] C. R. Acad. Sci. Paris Sér. I Math. **300**(13), 435–438 (1985)
21. Brieden, A., Gritzmann, P., Kannan, R., Klee, V., Lovász, L., Simonovits, M.: Approximation of diameters: randomization doesn't help. Proc. 39th IEEE Symp. Found. Comput. Sci. (FOCS '98), 1998, pp. 244–251
22. Brieden, A., Gritzmann, P., Kannan, R., Klee, V., Lovász, L., Simonovits, M.: Approximation of radii and norm-maxima: randomization does not help Matematika, 2003, in print
23. Brieden, A., Gritzmann, P., Klee, V.: Inapproximability of some geometric and quadratic optimization problems. Approximation and complexity in numerical optimization (Gainesville, FL, 1999), Nonconvex Optim. Appl. **42**, Kluwer Acad. Publ. Dordrecht, 2000, pp. 96–115
24. Brightwell, G., Winkler, P.: Counting linear extensions is $\#P$-complete. Order **8**, 225–242 (1992)
25. Broder, A.: How hard is it to marry at random? (On the approximation of the permanent). Proc. 18th Annual ACM Symp. Theory Comput. 50–58 (1986)
26. Bubley, R., Dyer, M., Jerrum, M.: An elementary analysis of a procedure for sampling points in a convex body. Random Structures Algorithms **12**(3), 213–235 (1998)
27. Carl, B.: On the entropy of absolutely summing operators. Arch. Math. (Basel) **43**(2), 183–186 (1984)
28. Carl, B., Pajor, A.: Gel'fand numbers of operators with values in a Hilbert space. Invent. Math. **94**(3), 479–504 (1988)
29. Cheeger, J.: A lower bound for the smallest eigenvalue of the Laplacian. Problems in analysis (Papers dedicated to Salomon Bochner, 1969), pp. 195–199, Princeton Univ. Press, Princeton, N.J., 1970
30. Chung, F.R.K.: Spectral Graph Theory, CBMS Reg. Conf. Series 92, Amer. Math. Soc. 1997
31. Diaconis, P.: Group representations in probability and Statistics. Institute of Mathematical Statistics, Hayward, CA, 1988

32. Dodziuk, J., Kendall, W.S.: Combinatorial Laplacians and isoperimetric inequality. In: From Local Times to Global Geometry, Control and Physics, (ed. K. D. Ellworthy), Pitman Res. Notes in Math. **150**, 68–74 (1986)
33. Dvoretzky, A.: A theorem on convex bodies and applications to Banach spaces. Proc. Nat. Acad. Sci. U.S.A. **45**(1959), 223–226 (1554)
34. Dyer, M., Frieze, A.: On the complexity of computing the volume of a polytopes. SIAM J. Comp. **17**, 967–974 (1988)
35. Dyer, M., Frieze, A.: Computing the volume of convex bodies: a case where randomness provably helps. In: Probabilistic Combinatorics and Its Applications (ed. Béla Bollobás), Proceedings of Symposia in Applied Mathematics, Vol. **44**, 1992, pp. 123–170
36. Dyer, M., Frieze, A., Kannan, R.: A Random Polynomial Time Algorithm for Approximating the Volume of Convex Bodies, Proc. of the 21st Annual ACM Symposium on Theory of Computing, 1989, pp. 375–381
37. Dyer, M., Frieze, A., Kannan, R.: A random polynomial time algorithm for approximating the volume of convex bodies, J. ACM **38**, 1–17 (1991), MR 91m:68162
38. Dyer, M., Gritzmann, P., Hufnagel, A.: On the complexity of computing mixed volumes. SIAM J. Comput. **27**(2), 356–400 (1998) (electronic)
39. Elekes, G.: A geometric inequality and the complexity of computing volume. Discrete and Computational Geometry **1**, 289–292 (1986)
40. Faigle, U., Kern, W., Streng, M.: Note on the computational complexity of $j$-radii of polytopes in $R^n$. Math. Prog. **73**(1), 1–5 (1996)
41. Faigle, U., Gademann, N., Kern, W.: A random polynomial time algorithm for well-rounding convex bodies. Workshop on Discrete Algorithms (Osnabrück, 1991). Discrete Appl. Math. **58**(2), 117–144 (1995)
42. Gritzmann, P., Klee, V.L.: Math. Programming **59**(2), 163–213 (1993)
43. Feller, W.: An introduction to probability theory and its applications. Vol. **I-II**. Second edition John Wiley & Sons, Inc., New York-London-Sydney 1971
44. Gademan, N.: Linear optimazation in random polynomial time, PhD thesis, ...
45. Garey, M.R., Johnson, D.S.: Computers and intractability. A guide to the theory of NP-completeness. A Series of Books in the Mathematical Sciences. W. H. Freeman and Co., San Francisco, Calif., 1979
46. Goffin, J.-L: Variable metric relaxation methods. II. The ellipsoid method. Math. Programming **30**(2), 147–162 (1984)
47. Grötschel, M., Lovász, L.: Combinatorial Optimization. In Handbook of Combinatorics, pp. 1541–1597
48. Grötschel, M., Lovász, L., Schrijver, A.: The ellipsoid method and its consequences in combinatorial optimization. Combinatorica **1**(2), 169–197 (1981)
49. Grötschel, M., Lovász, L., Schrijver, A.: Geometric Algorithms and Combinatorial Optimization, Springer-Verlag. Second edition. Algorithms and Combinatorics **2**, Springer-Verlag, Berlin, 1993
50. John, F.: Extremum problems with inequalities as subsidian (?) conditions, Studies and Essays presented to R. Courant, New York, 1948, pp. 187–204
51. Jerrum, M.: "Counting, sampling and integrating" (Lectures in Mathematics), Birkhäuser (2003). (See also http://www.dcs.ed.ac.uk/home/mrj/pubs.html.)
52. Jerrum, M.: Mathematical foundations of the Markov chain Monte Carlo method. Probabilistic methods for algorithmic discrete mathematics. Algorithms Combin. **16**, Springer, Berlin, 1998, pp. 116–165
53. Jerrum, M., Sinclair, S.: Conductance and the rapid mixing property for Markov chains: the approximation of the permanent resolved. Proc. 20th ACM STOC, 1988, pp. 235–244
54. Jerrum, M., Sinclair, A., Vigoda, E.: A polynomial-time approximation algorithm for the permanent of a matrix with non-negative entries, Electronic Collo. on Computational Complexity, Report No **79** (2000), see also the STOC version: STOC 2001: pp. 712–721
55. Jerrum, M.R., Valiant, L.G., Vazirani, V.V.: Random generation of combinatorial structures from a uniform distribution. Theoret. Comput. Sci. **43**, 169–188 (1986)
56. Kannan, R.: Markov chains and polynomial time algorithms. 35th Annual Symposium on Foundations of Computer Science (Santa Fe, NM, 1994), IEEE Comput. Soc. Press, Los Alamitos, CA, 1994, pp. 656–671, 68Q25 (68R05)
57. Kannan, R., Lovász, L.: Faster mixing through average conductance, STOC 1999
58. Kannan, R., Lovász, L., Montenegro, R.: Blocking conductance and mixing in random walks, Manuscript (?)
59. Kannan, R., Lovász, L., Simonovits, M.: Isoperimetric problems for convex bodies and a localization lemma. J. Discr. Comput. Geom., special issue dedicated to L. Fejes Tóth (eds I. Bárány and J. Pach) **13**, 541–559 (1996)
60. Kannan, R., Lovász, L., Simonovits, M.: Random walks and an $O^*(n^5)$ volume algorithm. Random Structures and Algorithms **1**, 1–50 (1997)
61. Karp, R.M., Luby, M.: Monte Carlo algorithms for enumeration and reliability problems. In: Proc. of the Twenty-Fourth IEEE Symp. Foundations of Comput. Sci., 1983, pp. 56–64

62. Karp, R.M., Papadimitriou, C.H.: On linear characterizations of combinatorial optimization problems. SIAM J. Comput. **11**(4), 620–632 (1982)
63. Karp, R.M., Papadimitriou, C.H.: On linear characterizations of combinatorial optimization problems. 21st Annual Symposium on Foundations of Computer Science (Syracuse, N.Y., 1980), pp. 1–9, IEEE, New York, 1980
64. Karzanov, A., Khachiyan, L.: On the conductance of order Markov chains. Order **8**, 7–15 (1991)
65. Khachiyan, L.G.: A polynomial algorithm in linear programming. Soviet Math. Doklady **20**, 191–194 (1979) (Originally in Russian, Doklady Akad. Nauk SSSR, **244**, 1093–1096
66. Khachiyan, L.G.: On the complexity of computing the volume of a polytope. Izvestia Akad. Nauk SSSR, Engineering Cybernetics **3**, 216–217 (1988)
67. Khachiyan, L.G.: The problem of computing the volume of polytopes is NP-hard. Uspekhi Mat. Nauk **44**, 199–200 (1989)
68. Khachiyan, L.G.: Complexity of polytope volume computation. In: New Trends in Discrete and Computational Geometry (ed. J. Pach), Springer, 1993, pp. 91–101
69. Khachiyan, L.G., Todd, M.J.: On the complexity of approximating the maximal inscribed ellipsoid for a polytope. Math. Programming **61**(2), 137–159 (1993)
70. Kochol, M.: Constructive approximation of a ball by polytopes. Math. Slovaca **44**(1), 99–105 (1994)
71. Lawrence, J.: Polytope volume computation. Math. Comput. **57**, 259–271 (1991)
72. Lenstra, H.W., Jr.: Integer programming with a fixed number of variables. Oper. Res. **8**, 538–548 (1983)
73. Lenstra, A.K., Lenstra, H.W., Jr., Lovász, L., Jr.: Factoring polynomials with rational coefficients. Math. Ann. **261**(4), 515–534 (1982)
74. Lovász, L.: An algorithmic theory of numbers, graphs and convexity, SIAM, Philadelphia, PA, 1986; MR 87m:68066
75. Lovász, L.: Geometric algorithms and algorithmic geometry. Proc. of Int. Congress of Math., Kyoto, 1990, Springer-Verlag, 1991, pp. 139–154
76. Lovász, L.: How to compute the volume? Jber. d. Dt. Math.-Verein, Jubiläumstagung 1990, B. G. Teubner, Stuttgart, 1992, pp. 138–151
77. Lovász, L.: Hit-and-Run mixes fast. Math. Program **86**(3), 443–461 (1999)
78. Lovász, L., Simonovits, M.: Mixing rate of Markov chains, an isoperimetric inequality, and computing the volume. Proc. 31st Annual Symp. on Found. of Computer Science, IEEE Computer Soc. 1990, pp. 346–355
79. Lovász, L., Simonovits, M.: On the randomized complexity of volume and diameter. Proc. 33rd IEEE FOCS, 1992, pp. 482–491
80. Lovász, L., Simonovits, M.: Random walks in a convex body and an improved volume algorithm. Random Struct. and Algorithms **4**, 359–412 (1993)
81. Lovász, L., Vempala, S.: The Geometry of Logconcave Functions and an $O^*(n^3)$ Sampling Algorithm Manuscript (2003?) Microsoft Research Tech. Report, (http://www-math.mit.edu/˜vempala/papers/logcon-ball.ps)
82. Lovász, L., Vempala, S.: Hit-and-Run is Fast and Fun, Manuscript submitted, 2003 Microsoft Research Tech. Report, (http://www-math.mit.edu/˜vempala/papers/logcon-hitrun.ps)
83. Lovász, L., Vempala, S.: Where to start a geometric random walk, Microsoft Research Tech. Report, (http://www-math.mit.edu/˜vempala/papers/start.ps)
84. Lovász, L., Vempala, S.: Simulated annealing in Convex Bodies and an $O^*(n^4)$ volume algorithm, submitted
85. Lovász, L., Winkler, P.: Mixing times. Microsurveys in discrete probability (Princeton, NJ, 1997), pp. 85–133, DIMACS Ser. Discrete Math. Theoret. Comput. Sci., **41**, Amer. Math. Soc., Providence, RI, 1998
86. Mihail, M.: "The approxmation of the permanent is still open," manuscript, Aiken Computing Laboratory, Harvard Univ. 1987
87. Metropolis, N., Rosenbluth, A.W., Rosenbluth, M.N., Teller, A.H., Teller, E.: Equation of state calculation by fast computing machines. J. Chem. Phys. **21**, 1087–1091 (1953)
88. Milman, V.: Surprising geometric phenomena in high-dimensional convexity theory. European Congress of Mathematics, Vol. **II** (Budapest, 1996), pp. 73–91, Progr. Math. **169**, Birkhäuser, Basel, 1998
89. Milman, V., Pajor, A.: Isotropic position and inertia ellipsoids and zonoids of the unit ball of a normed $n$ dimensional space, GAFA-Seminar 87–88. Springer Lecture Notes in Math. **1376**, 64–104 (1989)
90. Milman, V., Schechtman, G.: Asymptotic Theory of Finite-Dimensional Normed Spaces. Springer Lecture Notes in Math. **1200**, 1986. MR 87m:46038
91. Nesterov, Yu.E., Nemirovskiĭ , A.S.: ["Self-concordant functions and polynomial-time methods in convex programming", Central Econom. Math. Inst., USSR Acad. Sci., Moscow, 1989; per bibl.]
92. Padberg, M.W., Rao, M.R.: Odd minimum cut-sets and $b$-matchings. Math. Oper. Res. **7**(1), 67–80 (1982)
93. Payne, L.E., Weinberger, H.F.: An optimal Poincaré inequality for convex domains. Arch. Rat. mech. Anal. **5**, 286–292 (1960), MR 22 #8198

94. Rudelson, M.: Random vectors in the isotropic position. J. Funct. Anal. **164**(1), 60–72 (1999)
95. Shor, N.Z.: Nonlinear optimization problems. Kibernetika (Kiev) (2), 80–85 (1970); MR 45 #6452
96. Smith, R.L.: Efficient Monte-Carlo procedures for generating points uniformly distributed over bounded regions. Oper. Res. **32**, 1296–1308 (1984)
97. Sonnevend, G.: Applications of analytic centers for the numerical solution of semiinfinite, convex programs arising in control theory, DFG report Nr. 170/1989, Univ. Würzburg, Inst.f. angew. Mathematik
98. Spencer, J.: Random algorithms leave little to chance,... In: What's Happening in the Mathematical Sciences, Vol **2**, 1994 (Amer. Math. Soc.)
99. Tanner, R.M.: Explicit constructions of concentrators from generalized $N$-gons. SIAM J. Algebraic Disc. Methods **5**, 287–293
100. Valiant, L.G.: The complexity of computing the permanent. Theoret. Comput. Sci. **8**(2), 189–201 (1979)
101. Welsh, D.: Approximate Counting, Surveys in Combinatorics, 1997, (British Comb. Conf) London Math. Soc. Cambr. Univ. Press, pp. 287–325