COMPUTING THE VOLUME OF CONVEX BODIES: A CASE WHERE RANDOMNESS PROVABLY HELPS

by

Martin Dyer
School of Computer Studies
Univearsity of Leeds
Leeds, U.K.

and

Alan Frieze
Department of Mathematics
Carnegie Mellon University
Pittsburgh, PA 15213

Research Report No. 91-104

February 1991

COMPUTING THE VOLUME OF CONVEX BODIES: A CASE WHERE RANDOMNESS PROVABLY HELPS

Martin Dyer*
School of Computer Studies, University of Leeds,
Leeds, U.K.

and

Alan Frieze†
Department of Mathematics, Carnegie-Mellon University,
Pittsburgh, U.S.A.

4 January, 1991

Abstract

We discuss the problem of computing the volume of a convex body K in $\mathbf{R}^n$. We review worst-case results which show that it is hard to deterministically approximate $\mathrm{vol}_n K$ and randomised approximation algorithms which show that with randomisation one can approximate very nicely. We then provide some applications of this latter result.

*Supported by NATO grant RG0088/89
†Supported by NSF grant CCR-8900112 and NATO grant RG0088/89

1 Introduction

The mathematical study of areas and volumes is as old as civilization itself, and has been conducted for both intellectual and practical reasons. As far back as 2000 B.C., the Egyptians[1] had methods for approximating the areas of fields (for taxation purposes) and the volumes of granaries. The exact study of areas and volumes began with Euclid[2] and was carried to a high art form by Archimedes[3]. The modern study of this subject began with the great astronomer Johann Kepler's treatise[4] *Nova stereometria doliorum vinariorum*, which was written to help wine merchants measure the capacity of their barrels. Computational efficiency has always been important in these studies but a formalisation of this concept has only occurred recently. In particular the notion of what is computationally efficient has been identified with that of polynomial time solvability.

We are concerned here with the problem of computing the volume of a convex body in $\mathbf{R}^n$, where n is assumed to be relatively large. We present results on the computational complexity of this problem which have been obtained over the past few years. Many of our results pertain to a general oracle-based model of computation for problems concerning sets developed by Grötschel, Lovász and Schrijver [13]. This model is discussed in Section 2. We note here that classical approaches, using calculus, appear tractable only for bodies with a high degree of symmetry (or which can be affinely mapped to such a body). We can for example show by these means that the volume of the unit ball $B(0,1)$ in $\mathbf{R}^n$ is $\pi^{n/2}/\Gamma(1+n/2)$, or that the volume of a simplex Δ with with vertices $p_0, p_1, \ldots, p_n$ is given by the "determinant formula"

$$\mathrm{vol}_n(\Delta) = \left| \begin{array}{cccc} 1 & 1 & \ldots & 1 \\ p_0 & p_1 & \cdots & p_n \end{array} \right|. \tag{1}$$

However, for unsymmetric bodies, the complexity of the integrations grows rapidly with dimension, and quickly becomes intractable. In Section 3, we formalise this observation, and discuss negative results which show that it is provably hard for a completely deterministic polynomial time algorithm to calculate, or even closely approximate, the volume of a convex body.

In stark contrast to these negative results, in Section 4 we describe the randomized polynomial time algorithm of Dyer, Frieze and Kannan [10], with improvements due to Lovász and Simonovits [24], Applegate and Kannan [2]. We give some new improvements in this paper. This algorithm allows one, with high probability, to approximate the volume of a convex body to any required relative error. This algorithm has a number of applications, and some of these are described in Section 5. Section 6 then examines "how much randomness" is needed for this algorithm to succeed.

2 The oracle model

A convex body $K \subseteq \mathbf{R}^n$ could be be given in a number of ways. For example K could be a polyhedron and we are given a list of its faces, as we would be in the domain of Linear Programming. We could also be given a set of points in $\mathbf{R}^n$ and told that K is its convex hull. We consider this "polyhedral" situation briefly in Section 3.2.

In general, however, K may not be a polyhedron, and it might be difficult (or even impossible) to give a compact description of it. For example, if $K = \{(y,z) \in \mathbf{R}^{m+1} : v(y) \geq z\}$, where $v(y) = \max\{cx : Ax = y, x \geq 0\}$ is the value function of a linear program (A is an $m \times n$ matrix.)

[1] The Rhind Papyrus (copied ca. 1650 BC by a scribe who claimed it derives from the "middle kingdom" about 2000 - 1800 BC) consists of a list of problems and solutions, 20 of which relate to areas of fields and volumes of granaries.

[2] The exact study of volumes of pyramids, cones, spheres and regular solids may be found in Euclid's Elements (ca. 300 BC).

[3] Archimedes (ca. 240 BC) developed the method of exhaustion (found in Euclid) into a powerful technique for comparing volumes and areas of solids and surfaces. Manuscripts:

1. Measurement of the Circle. (Proves $3\frac{10}{71} < \pi < 3\frac{1}{7}$).
2. Quadrature of the Parabola
3. On the Sphere and Cylinder
4. On Spirals
5. On Conoids and Spheroids

[4] The application of modern infinitesimal ideas begins with Kepler's *Nova stereometria doliorum vinariorum* (New solid geometry of wine barrels), 1615.

We want a way of defining convex sets which can handle all these cases. This can be achieved by taking an "operational" approach to defining K i.e. we assume that information about K can be found by asking an oracle. This approach is studied in detail by Grötschel, Lovász and Schrijver [13]. Our model of computation for convex bodies is taken from [13]. In order to be able to discuss algorithms which are efficient on a large class of convex bodies, we do not assume any one particular formalism for defining them. For example, we do not want to restrict ourselves to convex polyhedra given by their faces. However, if the body is not described in detail, we must still have a way of gaining information about it. This is done by assuming that one has access to an "oracle". For example we may have access to a *strong membership* oracle. Given $x \in \mathbf{R}^n$ we can "ask" the oracle whether or not $x \in K$. The oracle is assumed to answer immediately. Thus the work that the oracle does is hidden from us, but in most cases of interest it would be a polynomial time computation. For example, if K is a polyhedron given by its facets, all the oracle needs to do is check whether or not x is on the right side of each defining hyperplane. The advantage of working with oracles is that the algorithms so defined can be applied in a variety of settings. Changing the class of convex body being dealt with, only requires changing the oracle (i.e. a procedure in the algorithm,) and not the algorithm itself. Moreover, an oracle such as this, plus a little more information, is sufficient to solve a variety of computational problems on K.

With such an oracle, we will need to be given a litle more information. We must assume that there exist positive $r, R \in \mathbf{R}$ and $a \in \mathbf{R}^n$ such that

$$B(a, r) \subseteq K \subseteq B(a, R) \tag{2}$$

where $B(x, \rho)$ denotes the ball centred at x with radius ρ. In this case we say that the oracle is *well-guaranteed*, with a, r, R being the guarantee.

Without such a guarantee, one could not be certain of finding even a single point of K in finite time. So, from now on, we assume that the guarantee is given along with the oracle. We do not lose any important generality if we assume that $r, R \in \mathbf{Q}$ and $a \in \mathbf{Q}^n$. Using $\langle\ \rangle$ to denote the number of bits needed to write down a rational object, we let $L' = \langle r, R, a\rangle$ and $L = L' + n$. This will be taken as the size $\langle K\rangle$ of our input oracle. A polynomial time algorithm is then one which runs in time which is polynomial in $\langle K\rangle$. Hence we are allowed a number of calls on our oracle which is polynomial $\langle K\rangle$. In the cases of interest, it is also true that each such call can be answered in time which is polynomial in $\langle K\rangle$, and hence we have a polynomial time algorithm overall. (See [13] for further details.)

If K is a polyhedron given by its faces, then it is more usual to let the input length be the number of bits needed to write down the coefficients of these faces. The reader should be able to convince him/herself that if K is non-empty then in polynomial time one can compute a, r, R as above and the two notions of input length are polynomially related. Now let us be precise about the other oracles considered in this paper. First there is the *weak* membership oracle. Given $x \in \mathbf{Q}^n$ and positive $\epsilon \in \mathbf{Q}$ this oracle will answer in one of the following ways:

$$x \in S(K, \epsilon) = \{y \in \mathbf{R}^n : y \in B(z, \epsilon) \text{ for some } z \in K\}$$

or

$$x \notin S(K, -\epsilon) = \{y \in \mathbf{R}^n : B(y, \epsilon) \subseteq K\}.$$

Again each call to the oracle is normally assumed to take time which is polynomial in $\langle K\rangle$ and $\langle\epsilon\rangle$.

We will also have need of a *weak separation* oracle. Here, given $x \in \mathbf{Q}^n$ and positive $\epsilon \in \mathbf{Q}$ this oracle will answer in one of the following ways:

$$x \in S(K, \epsilon) = \{y \in \mathbf{R}^n : y \in B(z, \epsilon) \text{ for some } z \in K\}$$

or

$$c \cdot y \leq c \cdot x + \epsilon \text{ for all } y \in S(K, -\epsilon)$$

where $\|c\|_\infty = 1$ and $c \in \mathbf{Q}^n$ is output by the oracle.

One pleasant consequence of the ellipsoid method is that a weak separation oracle can be obtained from a weak membership oracle in polynomial time (see [13]) and so it is not strictly necessary to consider anything other than weak membership oracles.

The positive results of this paper will be couched in terms of weak oracles. Thus given a weak membership oracle for a bounded convex body K we will see that we can approximate its volume to within arbitrary accuracy in random polynomial time using the algorithm of Dyer, Frieze and Kannan [10].

However some of the negative results can be couched in terms of strong oracles. Thus we must also mention the *strong* separation oracle. Here, given $x \in \mathbb{Q}^n$ the oracle will answer in one of the following ways:

$$x \in K \quad \text{or} \quad c \cdot y < c \cdot x \text{ for all } y \in K$$

where $\|c\|_\infty = 1$ and $c \in \mathbb{Q}^n$ is output by the oracle. It turns out that even with a strong separation oracle, it is not possible to deterministically approximate the volume of a convex body "very well" in polynomial time.

3 Hardness proofs

In this section we review some results which imply that computing the volume of a convex body, or even an approximation to it, is intractable if we restrict ourselves to deterministic computations.

3.1 Oracle model

We say that $\hat{V}$ is an *ϵ-approximation* to $\mathrm{vol}_n(K)$ if $1/(1+\epsilon) \leq \mathrm{vol}_n(K)/\hat{V} \leq (1+\epsilon)$, and that volume is ϵ-approximable if there is a deterministic polynomial time (oracle) algorithm which will produce an ϵ-approximation for any convex set K.

We begin, historically, with the positive result. Assume that K is well-guaranteed (see Section 2). Grötschel, Lovász and Schrijver [13] showed that there is a polynomial time computable affine transformation $f : x \mapsto Ax+b$ in $\mathbf{R}^n$ such that $B(0,1) \subseteq f(K) \subseteq n\sqrt{n+1}B(0,1)$. (The "rounding" operation.) Since the Jacobian of f is simply $\det(A)$, this implies that we can calculate (in deterministic polynomial time) numbers α, β such that $\alpha \leq \mathrm{vol}_n(K) \leq \beta$, with $\beta = O(n^{3n/2}\alpha)$. The reader may easily check that the best we can do in these circumstances is to put $\hat{V} = \sqrt{\alpha\beta}$, giving an $(\sqrt{\beta/\alpha} - 1)$-approximation. It follows that volume is $O(n^{3n/4})$-approximable. This may seem rather bad, but Elekes [11] showed that we cannot expect to do much better. His argument is based on the following

Theorem 1 (Elekes) *Let $p_1, p_2, \ldots, p_m$ be points in the ball $B = B(0,1)$ in $\mathbf{R}^n$, and $P = \mathrm{conv}\{p_1, p_2, \ldots, p_m\}$. Then $\mathrm{vol}_n(P)/\mathrm{vol}_n(B) \leq m/2^n$.*

Proof Let B_i be the ball centre $\frac{1}{2}p_i$, radius $\frac{1}{2}$. Note $\mathrm{vol}_n(B_i) = \mathrm{vol}_n(B)/2^n$. Suppose $y \notin \bigcup_{i=1}^n B_i$. Then $(y - \frac{1}{2}p_i)^2 > \frac{1}{4}$ for $i = 1, 2, \ldots, m$. Since $p_i^2 \leq 1$, we have $p_i y < y^2$ for $i = 1, 2, \ldots, m$. Thus all p_i lie in the half-space $H : yx < y^2$. So $P \subset H$, but clearly $y \notin H$, so $y \notin P$. Thus $P \subseteq \bigcup_{i=1}^n B_i$, and therefore $\mathrm{vol}_n(P) \leq \sum_{i=1}^m \mathrm{vol}_n(B_i) = m\mathrm{vol}_n(B)/2^n$. □

Keeping the above notation, it follows that, with any sub-exponential number $m(n)$ of calls to a strong membership oracle, a deterministic algorithm $\mathcal{A}$ will be unable to obtain good approximations. For, suppose $K = K(\mathcal{A}) \subseteq B$ is such that the oracle replies that the first $m(n)$ points queried lie in K. Then any K such that $P \subseteq K \subseteq B$ is consistent with the oracle, and hence we cannot do better than $\Omega(2^n/\sqrt{m})$-approximation. If $m(n)$ is polynomially bounded, it follows, in particular, that volume is not $2^{n/2-\omega\log n}$-approximable for any $\omega = \omega(n) \to \infty$.

Note that it is crucial to this argument that $\mathcal{A}$ is deterministic, since K must be a fixed body. For, suppose $\mathcal{A}$ is *nondeterministic*, and can potentially produce $M(n)$ different query points, if allowed $m(n)$ queries on a given input. Then it only follows that we cannot do better than $\Omega(2^n/M)$-approximation. If M is a fast growing function of n, this bound may be weak. We return to this point in Section 6 below, in the context of *randomized* computation.

Elekes' result was strengthened by Bárány and Füredi [3], who showed that (even with a strong separation oracle) volume is not n^{cn}-approximable, for any constant $c < \frac{1}{2}$. This result implies that the method of [13] described above is, in a weak sense, an "almost best possible" deterministic algorithm for this problem. However, recently, Applegate and Kannan [2] have adapted an idea of Lenstra [22] to produce an algorithm which works even better. This idea will also be exploited in the algorithm of Section 4. The idea is to start with any right simplex S in the body, and gradually "expand" it. Using the guarantee, we can initially find such a simplex with vertices $\{0, re_i \ (i \in [n])\}$. (We will use e_i for the ith unit vector and e for the vector of all 1's throughout.) If we

scale so that S is the *standard simplex* with vertices $\{0, e_i\ (i \in [n])\}$, K is contained in $B(0, R/r)$. Thus, by simple estimations, $\mathrm{vol}_n(K)/\mathrm{vol}_n(S) < (2nR/r)^n$. Now, for each $i = 1, 2, \ldots, n$, we check whether the region $\{x \in K : |x_i| \geq 1 + 1/n^2\}$ is empty. This can be done in polynomial time [13] to the required precision. Suppose not, then for some i, we can find a point y_i in this region. Replace e_i by y_i as a vertex of S. Clearly the ratio $\mathrm{vol}_n(K)/\mathrm{vol}_n(S)$ decreases by a factor at least $(1 + 1/n^2)$. We now transform S back to the standard simplex. This leaves the volume ratio unaffected. Clearly this must terminate before k iterations, for any $(1 + 1/n^2)^k \geq (2nR/r)^n$. Thus $k = \lceil 2n^3 \ln(2nR/r) \rceil$ iterations will suffice, i.e. "polynomially" many. However, at termination K is clearly contained in a cube $A(0, 1 + 1/n^2)$, where $A(a, b)$ is the cube centred at a with side $2b$. Thus

$$\mathrm{vol}_n(K)/\mathrm{vol}_n(S) \leq n!\{2(1 + 1/n^2)\}^n = O(n!2^n) = n^{(1-o(1))n}.$$

We then approximate $\mathrm{vol}_n(K)$ in the obvious way, producing an $n^{(\frac{1}{2}-o(1))n}$ approximation. It now follows from [3] that this procedure is (in a certain sense) an "optimal" deterministic approximator. Moreover, since S contains the cube $A(e/(2n), 1/(2n))$ so does K. Thus, relocating the origin at $e/(2n)$ and scaling by a factor $2n$ on all axes, we see that K will contain $A(0, 1)$ and be (strictly) contained in $A(0, 2(n+1))$ for any $n \geq 2$. We make use of this in Section 4 below, following Applegate and Kannan [2].

3.2 Polyhedra

Suppose a polyhedron $P \subseteq \mathbf{R}^n$ is defined as the solution set of a linear inequality system $Ax \leq b$. The size of the input (as remarked in Section 2) is defined by $\langle A \rangle + \langle b \rangle$. Here we might hope that the situation regarding volume computation would be better, but this does not seem to be the case (at least as far as "exact" computation is concerned). The following was first shown by Dyer and Frieze [9]. Let us use C_n to denote the unit n-cube $[0, 1]^n = \{0 \leq x \leq e\}$, and $H \subseteq \mathbf{R}^n$ the half-space $\{ax \leq b\}$, where a, b are integral. Consider the polytope $K = C_n \cap H$. Then it is #P-hard to determine the volume of K. The proof is based on the following identity, which is easily proved using inclusion-exclusion. Let $V = \{0, 1\}^n = \mathrm{vert}\, C_n$ and, for $v \in V$, write $|v| = ev$. Then

$$\mathrm{vol}_n(K) = \sum_{v \in V} (-1)^{|v|} \mathrm{vol}_n(\Delta_v), \tag{3}$$

where $\Delta_v = \{x \geq v\} \cap H$. Now if Δ_v is nonempty, it is a simplex with vertices

$$v,\ v + (b - av)e_i/a_i \qquad (i = 1, 2, \ldots n), \tag{4}$$

and hence by the determinant formula (1) for the volume of a simplex, $(n! \prod_{i=1}^n a_i)\mathrm{vol}_n(\Delta_v) = \max(0, b - av)^n$. Thus, from (3),

$$(n! \prod_{i=1}^n a_i)\mathrm{vol}_n(K) = \sum_{v \in V} (-1)^{|v|} \max(0, b - av)^n. \tag{5}$$

Now the right side of (5) may be regarded as a polynomial in b, for all b such that $V \cap H$ remains the same. (This will true be for b in successive intervals of width at least 1.) The coefficient of b^n in the polynomial is $\sum_{v \in H} (-1)^{|v|}$. Now, supposing we can compute volume, we can determine this coefficient in polynomial time by interpolation, using $(n + 1)$ suitable values of b. Now let $N_k = |\{v \in H : |v| = k\}|$, $a' = a + Me, b' = b + Mk$ where $M > ae > b > 0$. Consider the inequality $H' = \{a'x \leq b'\}$. It follows easily that $v \in H'$ iff either $|v| < k$, or $|v| = k$ and $v \in H$. Thus, from (5), b'^n will have coefficient $\sum_{i=1}^{k-1} (-1)^i \binom{n}{i} + (-1)^k N_k$. ¿From this we could compute all N_k $(k = 1, 2, \ldots, n)$. However, $\sum_{k=1}^n N_k = |V \cap H|$ is a well-known #P-hard quantity, i.e. the number of solutions to a zero-one knapsack problem. It follows that volume computation must also be #P-hard.

Since a in the above must contain large integers, this still left open the question of strong #P-hardness of the problem of computing the volume of a polyhedron. This was first shown to be strongly NP-hard by Khachiyan [20], using the intersection of "order polytopes" with suitable halfspaces. The order polytope is defined as follows. Let $\prec$ be a partial order on the set $[n] = \{1, 2, \ldots, n\}$, then the order polytope

$$P(\prec) = \{x \in C_n : x_i \leq x_j \text{ if } i \prec j\}.$$

A permutation of $[n]$ is a *linear extension* of $\prec$ if $\pi(i) \prec \pi(i + 1)$ for $i = 1, 2, \ldots, n - 1$. Given $\prec$, let

$$E(\prec) = \{\pi : \pi \text{ is a linear extension of } \prec\},$$

and let $e(\prec) = |E(\prec)|$. Linial [23] (and others) observed that, in fact, $n!\mathrm{vol}_n(P(\prec)) = e(\prec)$. To see this let

$$S_\pi = \{x \in C_n : x_{\pi(1)} \leq x_{\pi(2)} \leq \ldots \leq x_{\pi(n)}\}.$$

Then one observes that the the S_π intersect in zero volume, and that $P(\prec) = \bigcup_{\pi \in E(\prec)} S_\pi$. An application of (1) shows easily that $\mathrm{vol}_n(S_\pi) = 1/n!$ always, so $\mathrm{vol}_n(P(\prec)) = e(\prec)/n!$, as required. It was conjectured that $e(\prec)$ was #P-hard, but this issue, though of considerable interest, remained open for some years. Recently, however, Brightwell and Winkler [6] have finally settled this conjecture in the affirmative. Their proof is a little too complicated to sketch here, but their result implies, in particular, that polyhedral volume computation is strongly #P-hard, even for this natural application. We will return to this application in Section 5.2 below.

It is also shown in [9] that the volume of a polyhedron can be computed, to any polynomial number of bits, using a #P oracle. The construction uses a "dissection into cubes" similar to that used in Section 4 below. A pre-selected polynomial bound on the number of bits is in fact necessary, as the following considerations imply. By decomposing into simplices, we can easily show that the volume of a rational polyhedron is a rational p/q for $p, q \in \mathbf{Z}$. This argument also shows that p and q require only exponentially many bits, but it was asked in [9] whether polynomially many bits will suffice. The answer to this is negative, and the situation is almost as bad the above indicates. This may be shown using a simple, but ingenious, construction due to Lawrence [21]. Consider the situation of (3), (4) above, with $a = (2^{n-1}, 2^{n-2}, \ldots, 2, 1)$ and $b > ae = 2^n - 1$. Now $K = C_n$ and $V \subset H$. Observe that av is the number whose binary representation is v, so as v runs through V, $(1 + av)$ runs through the integers from 1 to 2^n. Suppose now we make the projective transformation $f : x \mapsto x/(1 + ax)$ in $\mathbf{R}^n$. Since projective transformations preserve hyperplanes, the identity corresponding to (3), i.e.

$$\mathrm{vol}_n(f(C_n)) = \sum_{v \in V} (-1)^{|v|} \mathrm{vol}_n(f(\Delta_v)), \tag{6}$$

is still valid. Note that $f(C_n)$ is the polyhedron $\tilde{C}_n = \{0 \leq x \leq (1 - ax)e\}$. But, from (4), $\tilde{\Delta}_v = f(\Delta_v)$ has vertices

$$v/(1 + av), \ (v + (b - av)e_i/a_i)/(b + 1) \qquad (i = 1, 2, \ldots n). \tag{7}$$

Letting $b \to \infty$, (7) simplifies to

$$v/(1 + av), \ e_i/a_i \qquad (i = 1, 2, \ldots n). \tag{8}$$

Applying the determinant formula (1) to (8), we find $(n! \prod_{i=1}^n a_i)\mathrm{vol}_n(\tilde{\Delta}_v) = 1/(1 + av)$. Hence, from (3), inserting the values of the a_i,

$$\rho = (n! 2^{n(n-1)/2})\mathrm{vol}_n(\tilde{C}_n) = \sum_{j=1}^{2^n} \pm 1/j, \tag{9}$$

where the sign is + iff the binary number j contains an odd number of one-bits. It is not difficult to see that the rational number ρ has an immense denominator. Consider the primes between 2^{n-1} and 2^n. The Prime Number Theorem implies that, for large n, there are at least $2^{n-1}/(n-1)$ such primes. Each of these primes occurs exactly once as a factor of any j in the expression for ρ. It follows easily that every such prime divides the denominator of ρ. Thus ρ's denominator is at least their product, i.e. more than $2^{2^{n-1}}$.

A polyhedron may be defined dually as the convex hull of a set of m points $p_1, p_2, \ldots, p_m$ in $\mathbf{R}^n$. This problem is, however, no easier. It is shown in [9] that computing volume in this situation is also #P-hard. The examples used are the "duals" of the polyhedra K described above. It remains open whether this problem is strongly #P-hard. However, it is true (and easy to prove) that, in this presentation, the volume is a rational of size polynomial in the input. (See [9] for details.)

4 Randomized volume approximation

In spite of the negative results of Section 3, Dyer, Frieze and Kannan [10] succeeded in devising a randomized algorithm which can, with high probability, approximate the volume of a convex body as closely as desired in polynomial time. (This will be made precise later.) The algorithm itself is a fairly simple random walk. The difficulties lie in the analysis. The analysis of [10] used the idea of "rapidly mixing Markov chains", and exploited a powerful isoperimetric inequality on the boundary of convex sets due to Bérard, Besson and Gallot [5] in order

to prove a crucial property of the random walk. A different isoperimetric inequality was also conjectured in [10], concerning the "exposed" surface area of volumes in the interior of convex sets, which would improve the time bound of the algorithm.

Aldous and Diaconis (see, for example, [1]) seem to have originated the investigation of Markov chains which "mix rapidly" to their limit distribution. A major step forward in their applicability to the analysis of randomized algorithms came when Sinclair and Jerrum [30] proved a very useful criterion for rapid mixing, based on *conductance*. They have applied this, for example, in [15]. Intuitively, conductance is a measure of "probability flow" in the chain. More formally, it measures the isoperimetry of a natural weighted digraph underlying the chain. Good conductance implies rapid mixing. It was precisely to prove good conductance that the inequality of [5] was required in [10].

Recently, Lovász and Simonovits [24] generalized the notion of conductance, and gave a sharper proof that this implies rapid mixing (although in a weaker sense than Sinclair and Jerrum [30]). They also proved the above conjecture of [10]. (See also Karzanov and Khachiyan [19].) With these improvements, they improved the analysis of the algorithm and its polynomial time bound. They also simplified the algorithm itself somewhat. In order to obtain rapid mixing, Dyer, Frieze and Kannan were obliged to smooth the boundary of the convex set by "inflating" it slightly. Lovász and Simonovits dispensed with this assumption by showing that the "sharp corners" of the body cannot do too much harm, provided the walk is started uniformly on some "large enough" set.

Applegate and Kannan [2] have recently obtained significant improvements in execution time with a different approach. The main new ingredients are a biassed random walk, and the use of the infinity-norm in the isoperimetry. Somewhat surprisingly, this overcomes the problem of "sharp corners" in a relatively efficient manner by allowing the walk to "step outside" the body if it enters such a region. They use this walk to sample from a non-uniform distribution over a convex body K – see Section 5, and to integrate log-concave functions over K. They estimate the volume of K by combining these two algorithms. In this paper we see how this biassed random walk works naturally with the original approach of [10]. We also manage to reduce the running time by a better method of statistical estimation, and by using uniformity to reduce the walking times.

We will first describe the algorithm, and subsequently develop the various components of its analysis. A key step in all of the algorithms that have been applied to this problem is that of computing a *nearly* uniform random point from a convex body. In Section 4.6 we prove a new result, which is a (sharpened) converse to this. We show that a polynomial number of calls to any good volume approximator suffices to generate (with high probability) a uniform point in any convex body.

We may observe that the only polynomial time (randomized) algorithms for the volume approximation problem seem to be based on the Dyer, Frieze and Kannan approach. For a slightly different approach in a special case, see [26].

It is of interest to display here the time bounds on the various volume algorithms so that we can see the progress that is being made on the problem. Let K be our convex body in $\mathbf{R}^n$ ($n \geq 2$), given by a weak membership oracle. (See Section 2.) Given ϵ and ξ, with probability $(1-\xi)$ we wish to find an ϵ-approximation to $\mathrm{vol}_n(K)$. To avoid unnecessary complication, let us asume $\epsilon \leq 1$. We require the algorithm to run in time polynomial in $\langle K \rangle$, $1/\epsilon$ and $\log(1/\xi)$, i.e. it must be a *fully polynomial randomized approximation scheme (FPRAS)* [18].

Dyer,Frieze and Kannan [10]

$$O(n^{23}(\log n)^5\epsilon^{-2}(\log\frac{1}{\epsilon})(\log\frac{1}{\xi})) \text{ convex programs.}$$

Lovász and Simonovits [24]

$$O(n^{16}\epsilon^{-4}(\log n)^8(\log\frac{n}{\epsilon})(\log\frac{n}{\xi})) \text{ membership tests.}$$

Applegate and Kannan [2]

$$O(n^{10}\epsilon^{-2}(\log n)^2(\log\frac{1}{\epsilon})^2(\log\frac{1}{\xi}))(\log\log\frac{1}{\xi})) \text{ membership tests.}$$

This paper

$$O(n^8\epsilon^{-2}(\log\frac{n}{\epsilon})(\log\frac{1}{\xi}))\ \text{ membership tests.}$$

4.1 The volume algorithm

As discussed in Section 3, K can be "rounded" so that it contains the cube $A(0,1)$ and is contained in the cube $A(0,2(n+1))$. (The work required to carry out this rounding is dominated by the rest of the algorithm, so we will choose to ignore it.) Now let $\delta = 1/(2n)$, and let $\mathcal{L} = \delta(\frac{1}{2}e + \mathbf{Z}^n)$ be an array of points, regularly spaced at distance δ, in $\mathbf{R}^n$. We think of each point of $\mathcal{L}$ as being at the centre of a small *cube* of volume δ^n (we refer to these as δ-cubes.) As in [10], we use the δ-cubes to approximate K closely enough that random sampling within cubes suffices to obtain "nearly random" points within K. Our algorithm is a modification of that of [10], using the ideas of Applegate and Kannan [2].

Let $\rho = 2^{1/n}$, $k = \lceil n \lg 2(n+1) \rceil$ and $d_i = \delta\lfloor \rho^i/\delta \rfloor$ $(i = 0,\ldots,k)$ (so we are "rounding down to whole δ-cubes"). Now consider the sequence of cubes $A_i = A(0,d_i)$ $(i = 0,2\ldots,k)$. (Thus A_i is the ℓ_∞ "ball" of radius d_i around 0.) It follows that $A_0 \subseteq K \subseteq A_k$. So consider the convex bodies $K_i = A_i \cap K$ $(i = 0,1,2,\ldots,k)$. Clearly $K_0 = A(0,1)$ and $K_k = K$. Also $K_i \subseteq \rho K_{i-1}$. Thus

$$\alpha_i = \mathrm{vol}_n(K_{i-1})/\mathrm{vol}_n(K_i) \geq \rho^{-n} = \tfrac{1}{2} \quad (i \in [k]). \tag{10}$$

Also it is easy to see that

$$\mathrm{vol}_n(K) = \mathrm{vol}_n(A(0,1))/(\prod_{i=1}^{k}\alpha_i), \tag{11}$$

where $\mathrm{vol}_n(A(0,1)) = 2^n$. It will therefore suffice to estimate the α_i closely enough.

Suppose we can generate a point $\zeta \in K_i$ such that, for all $S \subseteq K_i$ with (say) $\mathrm{vol}_n(S) > \frac{1}{3}\mathrm{vol}_n(K_i)$, we have $\Pr(\zeta \in S)$ very close to $\mathrm{vol}_n(S)/\mathrm{vol}_n(K_i)$. Then, by repeated sampling, we can estimate α_i closely, and hence $\mathrm{vol}_n(K)$. For this, from purely statistical considerations, we need to assume that α_i is bounded away from zero. This is justified by (10).

To estimate the volume, we perform a sequence of random walks on $\mathcal{L}$, divided into *phases*. For $i = 1,2,\ldots,k$, phase i consists of a number of random walks, which we will call *trials*, on $\mathcal{L} \cap A_i$. Trial j of phase i starts at a point $X_{i,j}$ of A_i and ends at the point $X_{i,j+1}$. If $X_{i,j+1}$ signals the end of phase i (see below), then we enter phase $(i+1)$ with $X_{i+1,1} = X_{i,j}$ (unless $i = k$, in which case we stop). The point $X_{1,1}$ is chosen uniformly on $\mathcal{L} \cap A_0$. Its coordinates may be generated straightforwardly using n (independent) integers uniform on $[4n]$. Starting at $X_{i,j}$, trial j of phase i is a random walk which "moves" at each step from one point of $\mathcal{L}$ to an adjacent point (i.e. one which differs by δ in exactly one coordinate). The exact details are now spelled out.

Associated with each $y \in \mathcal{L}$, we have an integer

$$\phi(y) = \min\{s \in \mathbf{Z} : s \geq 0 \text{ and } y/(1+\delta(s+\tfrac{1}{2})) \in K\}. \tag{12}$$

We keep track of this quantity. Since $X_{1,1} \in K$, $\phi(X_{1,1}) = 0$. We will show in Section 4.2 below that, if y_1, y_2 are adjacent in $\mathcal{L}$ (i.e. $y_2 - y_1 = \pm\delta e_r$ for some $r \in [n]$) then $|\phi(y_2) - \phi(y_1)| \leq 1$, so at most two membership tests suffice to determine $\phi(y_2)$ given $\phi(y_1)$.

The jth trial of phase i then proceeds as follows. Suppose at step t, the walk is at point $X_{t-1} \in \mathcal{L}$. We set $X_0 = X_{i,j}$ and the following operations comprise step t. With probability $\frac{1}{2}$ "do nothing", i.e. put $X_t = X_{t-1}$, $t \leftarrow (t+1)$ and end step t. (This is a technical requirement, see Section 4.4.) Otherwise, select a coordinate direction $\sigma \in \{\pm e_r\}$, all equally likely with probability $1/(2n)$. Let $X'_t = X_{t-1} + \delta\sigma$. Test if $X'_t \in A_i$. If not, do nothing. Otherwise determine $\phi(X'_t)$. If $\phi(X'_t) > \phi(X_{t-1})$, with probability $\frac{1}{2}$ do nothing. Otherwise put $X_t = X'_t$ and end step t, setting $\phi(X_t) = \phi(X'_t)$. (Note that we require only weak membership tests here, with tolerance some small fraction of δ. There is sufficient "slack" in our estimates below to allow for this source of small errors, but we omit further discussion of this issue. See [10] for the details.) We observe that what we have here is an example of the Metropolis algorithm – see the paper by Diaconis in this volume.

We continue the walk until $t = \tau$, where

$$\tau = \tau_i = \lceil 2^9 n^4 d_i^2 \ln(2^{27} n^3 \epsilon^{-4}) \rceil = O(n^4 \log(n/\epsilon) d_i^2),$$

then end trial j of phase i. We now continue with trial $(j+1)$ (or commence phase $(i+1)$) but, before doing so, we accumulate data for the volume estimate, as follows.

We show later (in Sections 4.4 and 4.5) that

$$\Pr(X_\tau = x) \approx c_0 2^{-\phi(x)} \quad (x \in \mathcal{L} \cap A_i),$$

where c_0 normalises the probabilities over $\mathcal{L} \cap A_i$. This distributional information about X_τ is used to find a point $\zeta_{i,j}$, approximately uniform on K_i, in the following way.

Let C be the δ-cube with centre X_τ, and let $s = \phi(X_\tau)$. If $s > 0$, do nothing. We declare trial j to be an *improper trial* and continue with trial $(j+1)$. We show in Section 4.2 that $s > 0$ implies $C \cap K_i = \emptyset$. Otherwise, if $s = 0$, C may meet K_i and we choose $\zeta = \zeta_{i,j}$ uniformly from C. If $\zeta \notin K_i$, we again declare trial j improper. Otherwise we have a *proper trial*, and we claim that ζ is approximately uniformly distributed on K_i. We will justify this claim in Section 4.5 below. Now, if also $\zeta \in K_{i-1}$ we declare the (proper) trial j to be a *success*. We continue phase i until a total of

$$m_i = \lceil 2^9 n^2/(\epsilon^2 d_i) \rceil = O(n^2/(\epsilon^2 d_i))$$

proper trials have been observed, and we accumulate the number ν_i of successes observed in these trials. Then we commence phase $(i+1)$, unless $i = k$, in which case we terminate and use the accumulated data to calculate our estimate of $\mathrm{vol}_n(K)$.

Let $\beta = 2^{-18}\epsilon^4 n^{-3}$. If $\hat{\alpha}_{i,j} = \Pr(\zeta_{i,j} \in K_{i-1} \mid \zeta_{i,j} \in K_i)$, we will show in Section 4.5 that for each (proper) trial in phase i,

$$|\alpha_i - \hat{\alpha}_{i,j}| \leq \sqrt{\beta} = 2^{-9}\epsilon^2 n^{-3/2}, \tag{13}$$

conditional on the previous trial ending *well* in a sense made precise in Section 4.5. We show that no trial ends badly with probability at least $\frac{9}{10}$.

We will also show in Section 4.5 that each trial is proper with probability at least $\frac{1}{5}$ provided no trial ends badly. Thus, under these conditions, the expected number of trials in each phase is less than $5m_i$ (and it is easy to show that the actual number will be less than, say, $10m_i$ with very high probability. If after $10m_i$ trials we have too few proper trials then we start again from the beginning.) Let

$$\hat{\alpha}_i = \frac{1}{m_i} \sum_{j=1}^{m_i} \hat{\alpha}_{i,j}.$$

If

$$P = \prod_{i=1}^{k} \alpha_i \quad \text{and} \quad \hat{P} = \prod_{i=1}^{k} \hat{\alpha}_i,$$

then, since $\alpha_i \geq \frac{1}{2}$, it is straightforward to show that

$$\left| \frac{\hat{P}}{P} - 1 \right| \leq 2^{-8}\epsilon. \tag{14}$$

Now let us form the estimates

$$Z_i = \frac{\nu_i}{m_i} \text{ for } i = 1, 2, \ldots, k$$

and

$$Z = \prod_{i=1}^{k} Z_i.$$

We will use the Chebycheff inequality to show that, if all trials end well,

$$\Pr\left(\left| \frac{Z}{\hat{P}} - 1 \right| > \frac{3}{10}\epsilon \right) \leq \frac{1}{4}. \tag{15}$$

Combining this with (14), and using the fact that the probability that there is a trial which ends badly is at most $\frac{1}{10}$, we obtain

$$\Pr\left(\left|\frac{Z}{P}-1\right|>\tfrac{1}{2}\epsilon\right)\leq\frac{1}{3}.$$

So if we take the median, W, of

$$\Delta=\lceil 12\lg(2/\xi)\rceil=O(\log(1/\xi)),$$

repetitions of the algorithm, then by standard methods (see [16]), we may estimate

$$\Pr\left(\left|\frac{W}{P}-1\right|>\epsilon\right)\leq\xi,$$

as required for use in (11).

Combining our running time estimates, the expected time to compute W is

$$\begin{aligned}O(\Delta\sum_{i=1}^{k}m_i\tau_i) &= O(n^6\epsilon^{-2}\log(n/\epsilon))\log(1/\xi)\sum_{i=1}^{k}d_i)\\ &= O(n^8\epsilon^{-2}\log(n/\epsilon)\log(1/\xi)),\end{aligned}$$

as claimed. Here we have used

$$\sum_{i=1}^{k}d_i\leq\sum_{i=1}^{k}\rho^i<9n^2=O(n^2),$$

since $\rho^k\leq 4n$ and (as is easily shown) $\rho-1>1/(2n)$.

To prove (15) we observe that

$$\begin{aligned}\mathbf{E}(Z) &= \hat{P}\\ \mathbf{Var}(Z) &= \prod_{i=1}^{k}\left(\frac{1}{{m_i}^2}\sum_{j\neq j'}\hat{\alpha}_{ij}\hat{\alpha}_{ij'}+\frac{\hat{\alpha}_i}{m_i}\right)-\prod_{i=1}^{k}\hat{\alpha}_i^2.\end{aligned}\tag{16}$$

The pairwise independence needed to justify (16) will be established in Section 4.5. Then

$$\begin{aligned}\mathbf{Var}(Z) &\leq \prod_{i=1}^{k}\left(\frac{{m_i}^2-m_i}{{m_i}^2}\hat{\alpha}_i^2(1+\sqrt{\beta})^2+\frac{\hat{\alpha}_i}{m_i}\right)-\prod_{i=1}^{k}\hat{\alpha}_i^2\\ &= \hat{P}^2\left(\prod_{i=1}^{k}\left(\left(1-\frac{1}{m_i}\right)(1+\sqrt{\beta})^2+\frac{1}{m_i\hat{\alpha}_i}\right)-1\right)\\ &\leq \hat{P}^2\left(\prod_{i=1}^{k}\left(1+\left(2\sqrt{\beta}+\beta+\frac{2}{m_i}\right)\right)-1\right)\\ &\leq \hat{P}^2\left(\exp\left\{(2\sqrt{\beta}+\beta)k+\sum_{i=1}^{k}\frac{2}{m_i}\right\}-1\right)\\ &\leq \hat{P}^2\left(\exp\left\{\frac{\epsilon^2}{2^7}+\frac{\epsilon^2}{2^9n^2}\sum_{i=1}^{k}d_i\right\}-1\right)\\ &\leq \hat{P}^2(\exp\{(2^{-7}+9\times 2^{-9})\epsilon^2\}-1)\\ &\leq 0.02\epsilon^2\hat{P}^2\end{aligned}$$

and (15) follows from the Chebycheff inequality and $\mathbf{E}(Z)=\hat{P}$.

To justify the algorithm, we must prove the various assertions made above. We do this in the following sections. We first establish some essential theoretical results.

4.2 Convex sets and norms

In this section we prove some preliminary technical results which will be used later. We assume we have any fixed (symmetric) norm $||x||$ for $x \in \mathbf{R}^n$. See [29] for general properties. In particular, we denote the ℓ_p norm by $||x||_p$ for $1 \leq p \leq \infty$. We will denote the "ball" $\{x : ||x - y|| \leq \alpha\}$ by $A(y, \alpha)$. Since any two norms are equivalent, we note that for any other norm $||\cdot||'$, there is a constant $M' > 1$ such that $1/M' < ||x||/||x||' < M'$. For any $S \subseteq \mathbf{R}^n$, $\operatorname{diam}(S)$ will denote the diameter of S in the norm $||\cdot||$ and, for S_1, S_2, $\operatorname{dist}(S_1, S_2)$ the (infimal) distance between the sets S_1, S_2.

It is well known that corresponding to $||\cdot||$, there is a *dual* norm $||\cdot||^*$, such that $||\cdot||^{**} = ||\cdot||$, defined by

$$||x||^* = \max ax/||a|| = \max\{ax : ||a|| = 1\}. \tag{17}$$

Now, for any $a \in \mathbf{R}^n$, consider the set of hyperlanes $H(s) = \{ax = s||a||^*\}$ orthogonal to a, and half-spaces $H^+(s) = \{ax \leq s||a||^*\}$, $H^-(s) = \{ax \geq s||a||^*\}$ they define. If K is any convex body, let $K(s) = K \cap H(s)$, $K^+(s) = K \cap H^+(s)$, $K^-(s) = K \cap H^-(s)$. (We call $K(s)$ a "cross section" of K in "direction" a.) Let $s_1 = \inf_s\{K(s) \neq \emptyset\}$, $s_2 = \sup_s\{K(s) \neq \emptyset\}$. Then $w = s_2 - s_1$ is the *width* of K in direction a, and we will write $w = W(K, a)$. Note that

Lemma 1 $\operatorname{diam} K = \max_a W(K, a)$.

Proof

$$\begin{aligned} \operatorname{diam} K &= \max\{||x - y|| : x, y \in K\} = \max\{||z|| : z \in K - K\} \\ &= \max_z \max_a az/||a||^* = \max_a \max_z az/||a||^* \\ &= \max_a W(K, a). \end{aligned}$$

□

We will also need the following technical result.

Lemma 2 *Let $a_1, a_2, \ldots, a_{n-1}$ be mutually orthogonal. Then for some constant $c > 0$, depending only on n and $||.||$, $\operatorname{diam} K(s) < c \max_i W(K, a_i)$ for all s.*

Proof If a is in the subspace generated by the a_i,

$$W(K(s), a) \leq W(K, a) = (||a||_2/||a||^*)W_2(K, a) < M^* W_2(K, a),$$

where W_2 denotes width in the Euclidean norm and M^* is the constant relating $||\cdot||^*, ||\cdot||_2$. But $W_2(K, a) \leq \sqrt{n-1} \max_i W_2(K, a_i)$, since K can clearly be contained in an (infinite) cubical cylinder of side $\max_i W_2(K, a_i)$. Taking $c = M^*\sqrt{n-1}$ and using Lemma 1 now gives the conclusion. □

If K is any convex body in $\mathbf{R}^n$, then we can define a convex function

$$r(x) = \inf\{\lambda \in \mathbf{R} : \lambda > 0 \text{ and } x/\lambda \in K\},$$

the *gauge function* associated with K. This has all the properties of a norm except symmetry. (See [29].) We have

Lemma 3 *If K contains the unit ball $A(0, 1)$ then, for any $x, y \in \mathbf{R}^n$,*

$$|r(x) - r(y)| \leq ||x - y||.$$

Proof Suppose, without loss, $r(x) \geq r(y)$. Then $y \in r(y)K$ and

$$x - y \in ||x - y||A(0, 1) \subseteq ||x - y||K.$$

Thus $x \in (r(y) + ||x - y||)K$, i.e. $r(x) \leq r(y) + ||x - y||$. □

Corollary 1 *If $A(0,1) \subseteq K$, then $r(y) > 1 + \alpha$ implies $A(y,\alpha) \cap K = \emptyset$.*

Proof If $x \in A(y,\alpha) \cap K$, then $\|x - y\| \leq \alpha$ and $r(x) \leq 1$. Hence $r(y) - r(x) > \alpha$ giving $\|x - y\| > \alpha$, a contradiction. □

We use these results above with the ℓ_∞ norm. If $x \in \mathcal{L}$, then the δ-cube $C(x) = A(x, \frac{1}{2}\delta)$ in this norm. Also it is not difficult to see that $\phi(x)$, as defined by (12), satisfies

$$\phi(x) = \lceil (r(x) - 1)/\delta - \tfrac{1}{2} \rceil.$$

From this we see $1+\delta(\phi(x)+\frac{1}{2}) \leq r(x) < 1+\delta(\phi(x)+\frac{3}{2})$. Any two adjacent points x, y, of $\mathcal{L}$ satisfy $\|x-y\|_\infty = \delta$. From Lemma 3 it now follows that $|r(x) - r(y)| \leq \delta$, since $A(0,1) \subseteq K$. Thus we have

$$\delta \geq r(x) - r(y) > \delta(\phi(x) - \phi(y) - 1),$$

giving $\phi(x) \leq \phi(y) + 1$. By symmetry we therefore have $|\phi(x) - \phi(y)| \leq 1$, as claimed in Section 4.1. Also, if $\phi(y) \geq 1$ for $y \in \mathcal{L}$, we have $r(y) \geq 1 + \frac{3}{2}\delta$. Thus from Corollary 1 we have $C(y) \cap K = \emptyset$, as claimed in Section 4.1.

We will extend the domain of the function $\phi(y)$ from $\mathcal{L}$ to $\mathbf{R}^n$ by letting $\phi(x)$ be the (obvious) upper semicontinuous function which satisfies $\phi(x) = \phi(y)$ for $x \in \operatorname{int} C(y)$, $y \in \mathcal{L}$. Thus, in particular, $\phi(x) = \max\{\phi(y_1), \phi(y_2)\}$ if y_1, y_2 are adjacent in $\mathcal{L}$ and x lies on the $(n-1)$-dimensional face $\operatorname{int}\{C(y_1) \cap C(y_2)\}$. We bound this (extended) function $\phi(x)$ below by the convex function $\hat{\phi}(x) = (r(x) - 1)/\delta - 1$. If $x \in C(y)$, we have

$$\begin{aligned}
\phi(x) - \hat{\phi}(x) &\geq (r(y) - 1)/\delta - \tfrac{1}{2} - (r(x) - 1)/\delta + 1 \\
&= (r(y) - r(x))/\delta + \tfrac{1}{2} \geq 0, \\
\phi(x) - \hat{\phi}(x) &\leq (r(y) - 1)/\delta + \tfrac{1}{2} - (r(x) - 1)/\delta + 1 \\
&= (r(y) - r(x))/\delta + \tfrac{3}{2} \leq 2,
\end{aligned}$$

so $\hat{\phi}(x) \leq \phi(x) \leq \hat{\phi}(x) + 2$.

4.3 The isoperimetric inequality

Here we derive an isoperimetric inequality about convex sets and functions which is the key to proving rapid convergence of the random walks. Our treatment follows that of Applegate and Kannan [2], and Lovász and Simonovits [24], but we give an improvement and generalization of their theorems. We retain the notation of Section 4.2.

Let $A(s) = \operatorname{vol}_{n-1}(K(s))$ and $V(s) = \operatorname{vol}_n(K^+(s))$, and temporarily assume, without loss, that $s_1 = 0$ and $s_2 = w$. Note then $V(w) = \operatorname{vol}_n(K)$. It is a consequence of the Brunn-Minkowski theorem [7], that $A(s)^{1/(n-1)}$ is a concave function of s in $[0, w]$. Then we have

Lemma 4 $(s/w)^n \leq V(s)/V(w) \leq ns/w$.

Proof Since the inequality is independent of the norm used, we will assume the Euclidean norm for convenience. First we show that if $0 < s < u$, $A(s)/A(u) \geq (s/u)^{n-1}$. This follows since if $s = \lambda 0 + (1 - \lambda)u$, then Brunn-Minkowski implies

$$\begin{aligned}
A(s)^{1/(n-1)} &\geq \lambda A(0)^{1/(n-1)} + (1 - \lambda)A(u)^{1/(n-1)} \\
&\geq (1 - \lambda)A(u)^{1/(n-1)} = (s/u)A(u)^{1/(n-1)}.
\end{aligned}$$

Thus

$$V(s) \geq \int_0^s (u/s)^{n-1} A(s)\, du = (s/n)A(s), \tag{18}$$

$$V(w) - V(s) \leq \int_s^w (u/s)^{n-1} A(s)\, du = (w^n - s^n)/(ns^{n-1})A(s). \tag{19}$$

Dividing (19) by (18) gives $V(w)/V(s) \leq (w/s)^n$, which is the left hand inequality. By symmetry, this inequality in turn implies

$$(V(w) - V(s))/V(w) \geq ((w-s)/w)^n = (1 - s/w)^n \geq 1 - ns/w,$$

since $(1-x)^n \geq 1 - nx$ for $x \in [0,1]$. This gives the right hand inequality. □

We say that a real-valued function $F(x)$ defined on the convex set $K \subseteq \mathbf{R}^n$ is *log-concave* if $\ln F(x)$ is concave on K. This clearly entails $F(x) > 0$ on K. With such an F, we will associate a measure μ on the measurable subsets S of K by $\mu(S) = \int_S F(x)\,dx$. We will need the following simple lemma asserting the existence of a hyperplane simultaneously "bisecting the measure" of two arbitrary sets.

Lemma 5 *Let $S_1, S_2 \subseteq \mathbf{R}^n$, measurable, and Λ a two-dimensional linear subspace of $\mathbf{R}^n$. Then there exists a hyperplane H, with normal $a \in \Lambda$, such that the half-spaces H^+, H^- determined by H satisfy $\mu(S_i \cap H^+) = \mu(S_i \cap H^-)$ for $i = 1, 2$.*

Proof Let α_1, α_2 be a basis for Λ. For each $\theta \in [-1, +1]$, let $b_i(\theta)$ be such that the hyperplane $(\theta\alpha_1 + (1 - |\theta|)\alpha_2)x = b_i(\theta)$ bisects the measure of S_i for $i = 1, 2$. (If S_i is disconnected in such a way that the possible b_i form an interval, $b_i(\theta)$ will be its midpoint.) It clearly suffices to show that $b_1(\theta_0) = b_2(\theta_0)$ for some θ_0. If $b_1(-1) = b_2(-1)$ we are done, so suppose without loss $b_1(-1) > b_2(-1)$. We clearly have $b_i(1) = -b_i(-1)$ for $i = 1, 2$, so $b_1(1) < b_2(1)$. But since μ is a continuous measure, it follows easily that $b_i(\theta)$ is a continuous function of θ. The existence of $\theta_0 \in (-1, 1)$ now follows. □

Remark 1 This is a rather simple case of the so-called "Ham Sandwich Theorem". (See Stone and Tukey [31].) The proof here is a straightforward generalization of one in [8, p. 318].

We now give the first version of the isoperimetric inequality. Without the constant $\frac{1}{2}$, the following was proved, for the case $F(x) = 1$ with Euclidean norm, by Lovász and Simonovits [24], and, for the case of general F and the ℓ_∞ norm, by Applegate and Kannan [2]. We give a further generalization and improvement of their theorems.

Theorem 2 *Let $K \subseteq \mathbf{R}^n$ be a convex body and F a log-concave function defined on $\operatorname{int} K$. Let $S_1, S_2 \subseteq K$, and $t \leq \operatorname{dist}(S_1, S_2)$ and $d \geq \operatorname{diam}(K)$. If $B = K \setminus (S_1 \cup S_2)$, then*

$$\min\{\mu(S_1), \mu(S_2)\} \leq \tfrac{1}{2}(d/t)\mu(B).$$

Proof By considering, if necessary, an increasing sequence of convex bodies tending to K, it is clear that we may assume without loss $F(x) > 0$ on K. Thus, for some $M_1 > 1$ we have $1/M_1 < F(x) < M_1$ for all $x \in K$. Also since F is positive log-concave, $\ln F(y) \leq \ln F(x) + \gamma(x)(y - x)$, where $\gamma(x)$ is any subgradient at x. It follows that there exists a number $M_2 \geq 1$ such that $\ln(F(y)/F(x)) < M_2\|y - x\|$ for all $x, y \in K$. Let $M = \max\{M_1, M_2\}$.

Now note that, if $\mu(B) \geq \frac{1}{2}\mu(K)$ the theorem holds trivially, since $d \geq t$. We therefore assume otherwise.

We consider first the case where K is "needle-like", i.e. there exists a direction a such that all cross sections of K are "small". Specifically, for given $0 < \epsilon < t$, we require $\operatorname{diam} K(s) < \epsilon$ for all s. If L is the line segment joining any point of $K(s_1)$ to any point of $K(s_2)$, let $f(s) = F(y)$ for $y \in K(s) \cap L$. Now $f(s)$ is log-concave in s, and we clearly have $|\ln(F(x)/f(s))| < M\epsilon$ for any $x \in K(s)$.

Now for $i = 1, 2$ replace S_i by $\hat{S}_i = \bigcup_s \{K(s) : S_i \cap K(s) \neq \emptyset\}$, and B by $\hat{B} = K \setminus (\hat{S}_1 \cup \hat{S}_2)$. Since $\epsilon < t$, this operation is well defined and $\operatorname{dist}(\hat{S}_1, \hat{S}_2) \geq \hat{t} = t - \epsilon$. Clearly $\mu(\hat{S}_i) \geq \mu(S_i)$ $(i = 1, 2)$, and $\mu(\hat{B}) \leq \mu(B)$. Let us now drop the "hats", bearing in mind that t must eventually be replaced by $t - \epsilon$. The components of S_1, S_2, B now correspond to intervals of s. We may assume without loss that the components of S_1 and S_2 alternate in the increasing s direction, since otherwise we could increase $\mu(S_1)$ and/or $\mu(S_2)$ and decrease $\mu(B)$ without decreasing $\operatorname{dist}(S_1, S_2)$.

We show first that it is sufficient to consider the case when each of S_1, S_2 contains a single component. By symmetry, let us assume that $S_1 = K^+(u_1)$ and $S_2 = K^-(u_2)$ where $(u_2 - u_1) \geq t$. Call this the "connected case", and suppose we are not in this case. Consider any component S_1' of S_1, covering the interval $[s', s'']$. This meets two (possibly empty) components of B which meet no other S_1 component. Let $S_2' = K^+(s' - t)$, $S_2'' = K^-(s'' + t)$. Note that $S_2 \subseteq S_2' \cup S_2''$. Suppose $\mu(S_1') \leq \mu(S_2')$. Assuming the theorem holds for the connected case, let us apply it to $K' = K^+(s'')$ with S_1', S_2' and $B' = K' \setminus (S_1' \cup S_2')$. This implies $\mu(S_1') \leq \frac{1}{2}(d/t)\mu(B')$,

where B' is a component of B which meets no other component of S_1. Similarly if $\mu(S_1') \leq \mu(S_2'')$. If one or other of these holds for every component of S_1, adding all the resulting inequalities implies $\mu(S_1) \leq \frac{1}{2}(d/t)\mu(B)$. Thus suppose there is a component with both $\mu(S_2') \leq \mu(S_1')$ and $\mu(S_2'') \leq \mu(S_1')$. Then we can show, similarly to the above, that $\mu(S_2') \leq \frac{1}{2}(d/t)\mu(B')$ and $\mu(S_2'') \leq \frac{1}{2}(d/t)\mu(B'')$, where B', B'' are different components of B. Adding these now implies $\mu(S_2) \leq \frac{1}{2}(d/t)\mu(B)$.

Thus it suffices to consider the connected case. If $A^*(s) = (\|a\|_2/\|a\|^*)A(s)$, is the "scaled area" of $K(s)$, we have

$$e^{2M\epsilon}\mu(B) \geq e^{M\epsilon}\int_{u_1}^{u_2} f(s)A^*(s)\,ds = (u_2-u_1)e^{M\epsilon}f(\zeta)A^*(\zeta) \geq te^{M\epsilon}f(\zeta)A^*(\zeta), \tag{20}$$

for some $\zeta \in [u_1, u_2]$, by the first mean value theorem for integrals. We will assume without loss that $\zeta = 0$, $s_1 = -\kappa$, $s_2 = \lambda$, so $w = W(K,a) = (\kappa+\lambda)$. By scaling orthogonal to a, we will also assume without loss that $e^{M\epsilon}f(\zeta)A^*(\zeta) = 1$. Now $\ln f(s)$ is concave by assumption, and $\ln A^*(s)$ is log-concave since $A^*(s)^{1/(n-1)}$ is concave. Thus $G(s) = M\epsilon + \ln f(s) + \ln A^*(s)$ is concave with $G(0) = 0$. Let γ be any subgradient of G at $s = 0$. If $\gamma = 0$, then $G(s) \leq 0$ for all s. But then it follows that $\mu(S_1) \leq \kappa$ and $\mu(S_2) \leq \lambda$. Letting $\tilde{\mu} = \min\{\mu(S_1), \mu(S_2)\}$, we therefore have

$$\tilde{\mu} \leq \tfrac{1}{2}(\kappa+\lambda) \leq \tfrac{1}{2}e^{2M\epsilon}(w/t)\mu(B) \tag{21}$$

using (20). If $\gamma \neq 0$, assume $\gamma > 0$, since otherwise we can re-label S_1, S_2 and use the direction $-a$. By scaling in the a direction, we may assume $\gamma = 1$. Then $G(s) \leq s$ for all s, hence $e^{M\epsilon}f(s)A^*(s) \leq e^s$ for all s, giving

$$\begin{aligned}\mu(S_1) &\leq \int_{-\kappa}^{0} e^s\,ds = (1-e^{-\kappa}),\\ \mu(S_2) &\leq \int_{0}^{\lambda} e^s\,ds = (e^{\lambda}-1).\end{aligned}$$

so $\tilde{\mu} \leq \min\{(1-e^{-\kappa}), (e^{\lambda}-1)\}$. This implies $\kappa \geq -\ln(1-\tilde{\mu})$ and $\lambda \geq \ln(1+\tilde{\mu})$. Thus

$$\tfrac{1}{2}w = \tfrac{1}{2}(\kappa+\lambda) \geq \tfrac{1}{2}(\ln(1+\tilde{\mu}) - \ln(1-\tilde{\mu})) > \tilde{\mu},$$

where the final inequality may be obtained by series expansion of both terms in the penultimate expression. Thus (21) holds again, with strict inequality. Recalling that we must replace t by $(t-\epsilon)$, and that by Lemma 1 $w \leq d$ we have proved that in the needle-like case,

$$\min\{\mu(S_1), \mu(S_2)\} \leq \tfrac{1}{2}e^{M\epsilon}\mu(B)d/(t-\epsilon). \tag{22}$$

We move to the general case. Suppose there is a convex body K with sets S_1, S_2 such that the theorem fails. Then, for some $\epsilon > 0$, (22) fails. Suppose that there exist mutually orthogonal directions $a_1, \ldots, a_j$ such that $\max_{1\leq i\leq j} W(K, a_i) < \epsilon/c$ where c is the constant of Lemma 2. If $j \geq n-1$, by Lemma 2 the needle-like case applies and we have a contradiction. Thus suppose $j \leq n-2$ is maximal such that a counter-example can be found. Let Λ be a two-dimensional linear subspace orthogonal to the a_j. By Lemma 4 there is a hyperplane H with normal $a \in \Lambda$, $\|a\|^* = 1$, which bisects the measure of both S_1, S_2. We choose H^+ to be the half-space such that $\mu(B \cap H^+)$ is smaller.

Let us write K' for $K \cap H^+$ etc. If the theorem fails for K, S_1, S_2, then it follows that it must also fail for K', S_1', S_2'. (The diameter can only decrease, and the distance increase, so the same d, t, ϵ will apply.) Note that, since $\mu(B) < \frac{1}{2}\mu(K)$, H cuts K into two parts K', K'' with $\mu(K') \leq \mu(K'') \leq 3\mu(K')$. Since $1/M < F(x) < M$ on K, for any measurable S we have $\mathrm{vol}_n(S)/M < \mu(S) < M\mathrm{vol}_n(S)$. Hence $\mathrm{vol}_n(K')/M^2 \leq \mathrm{vol}_n(K'') \leq 3M^2\mathrm{vol}_n(K')$, and it follows that $\mathrm{vol}_n(K')\} \geq \mathrm{vol}_n(K)/(1+3M^2)$. Thus, by Lemma 4, $W(K', a) \leq \rho W(K, a)$ for some constant $\rho < 1$ depending only on M, n.

Suppose we iterate this bisection, obtaining a sequence of bodies

$$K = K^{(1)} \supset K^{(2)} \supset \cdots K^{(m)} \supset \cdots,$$

where $K^{(m)} = H^{(m)} \cap K^{(m-1)}$, containing sets for which the theorem fails. Now $K^{(m)}$ clearly converges to a compact convex set K^*. If $a^{(m)}$ is the normal to $H^{(m)}$, by compactness $a^{(m)}$ has a cluster point $a^* \in \Lambda$. By continuity, taking the limit in $0 \leq W(K^{(m+1)}, a^{(m)}) \leq \rho W(K^{(m)}, a^{(m)})$ gives $0 \leq W(K^*, a^*) \leq \rho W(K^*, a^*)$. Thus $W(K^*, a^*) = 0$, and hence for some m, $W(K^{(m)}, a^{(m)}) < \epsilon/c$. However, taking $a_{j+1} = a^{(m)}$, the fact that $K^{(m)}$ is a counter-example to the theorem now gives a contradiction. □

Remark 2 The method of proof by repeated bisection is due in this context to Lovász and Simonovits [24], but is similar to that employed by Payne and Weinberger [28] to bound the second largest eigenvalue of the "free membrane" problem for a convex domain in $\mathbf{R}^n$. Eigenvalues are, in fact, closely related to conductance. The approach of Sinclair and Jerrum [30] was based on bounding the second eigenvalue of the transition matrix.

We use this to prove the following isoperimetric inequality.

Theorem 3 *Let $K \subseteq \mathbf{R}^n$ be a convex body, and F log-concave on $\operatorname{int} K$. Let $S \subseteq K$, with $\mu(S) \leq \frac{1}{2}\mu(K)$, be such that $\partial S \setminus \partial K$ is a piecewise smooth surface σ, with $u(x)$ the Euclidean unit normal to σ at $x \in \sigma$. If $\mu'(S) = \int_\sigma F(x)\|u(x)\|^* dx$, then $\mu(S)/\mu'(S) \leq \frac{1}{2}\operatorname{diam}(K)$.*

Proof By considering the limit of an appropriate sequence of simplicial approximations, it clearly suffices to prove the theorem for σ a "simplicial surface", i.e. one whose "pieces" are $(n-1)$-dimensional simplices. For small $t > 0$, let B be the closed $\frac{1}{2}t$-neighbourhood of such a surface σ. Consider a simplicial piece $\sigma' \subseteq \sigma$, with normal u and surface integral $\alpha = \int_{\sigma'} F(x)\,dx$. The measure of B around σ' is then approximately $h\alpha$, where

$$h = \max\{uz : \|z\| = t\} = \|u\|^* t.$$

Thus the measure of this portion of B is $t\alpha\|u\|^* + o(t)$ and hence, since u is constant on each such σ', $\mu(B) = t\mu'(S) + o(t)$. Now, from Theorem 2 with $S_1 = S$, and $S_2 = K \setminus (B \cup S)$, we have $\mu(S) \leq \frac{1}{2}(\operatorname{diam}(K)/t)\mu(B)$, and the theorem follows by letting $t \to 0$. □

Remark 3 The inequality in Theorem 3 is "tight". To see this, let K be any circular cylinder with radius very small relative to it length, $F(x) = 1$, and S be the region on one side of the mid-section of K.

Corollary 2 *Let $F(x)$ be an arbitrary positive function defined on $\operatorname{int} K$, and $\hat{F}(x)$ be any log-concave function such that $\hat{F}(x) \geq F(x)$ for all $x \in K$. If $\Psi = \max_x \hat{F}(x)/F(x)$ then, in the notation of Theorem 3, $\mu(S)/\mu'(S) \leq \frac{1}{2}\Psi\operatorname{diam}(K)$.*

Proof Use the result of Theorem 3 for $\hat{F}$ and the inequalities $F(x) \leq \hat{F}(x) \leq \Psi F(x)$. □

Remark 4 Applegate and Kannan [2] have proved a further weakening of Theorem 3, in terms the maximum ratio of the function to a bounding concave function on each line in K. (The bounding function may vary from line to line.) In [2] this is proved by the bisection argument assuming that F satisfies a Lipschitz condition. However, the condition appears unnecessarily strong to prove an analogue of Theorem 3. Continuity of F is certainly sufficient, and even this can be dispensed with by employing an approximating sequence of continuous functions and dominated convergence of the integrals.

4.4 Rapidly mixing Markov chains

In this section we prove some basic results about the convergence of Markov chains. Our treatment is based on Lovász and Simonovits' [24] improvement of a theorem of Sinclair and Jerrum [30]. Let C_N denote the unit cube, with vertex set V, as in Section 3. We regard $v \in V$ as a (column) N-vector. Then $v = \{i : v_i = 1\}$ gives the usual bijection between V and all subsets of $[N]$. By abuse of language, we will refer to S_v simply as v, the meaning always being obvious from the context. Thus for example, $|v|$ is the cardinality, and $\bar{v} = (e - v)$ the complement, of v in its "set context".

Suppose P is the transition matrix of a finite Markov chain X_t on state space $[N]$, whose distribution at time $t = 0, 1, 2, \ldots$ is described by the (row) N-vector $p^{(t)}$. Thus

$$Pe = e, \quad p^{(t)}e = 1, \quad p^{(t)} = p^{(t-1)}P. \tag{23}$$

(We use only basic facts concerning Markov chains but, if necessary, see [12] for an introduction.)

In our application, observe that the points of $\mathcal{L} \cap K_i$ correspond to the states. Thus any *subset of cubes* in the random walk is actually being identified with a *vertex* of C_N here.

We suppose that we are interested in the "steady state" distribution $q = \lim_{t\to\infty} p^{(t)}$ of X_t, given that this exists. We will write the corresponding random variable as X_∞. It is easy to see that q must be a solution of

$$qP = q, \quad qe = 1. \tag{24}$$

Our objective is to sample approximately from the distribution q. We do this by choosing X_0 from some initial distribution $p^{(0)}$, and determining X_t iteratively in accordance with the transition matrix P (using a source of random bits). We do this for some predetermined finite time τ until X_τ closely enough approximates X_∞. By this we mean that we require the *variation distance* be small, i.e. for some $0 < \eta \ll 1$,

$$|p^{(\tau)} - q| = \tfrac{1}{2}\sum_{1=1}^{N} |p_i^{(\tau)} - q_i| < \eta. \tag{25}$$

We call τ the *mixing time* of X_t for η. We will assume that P is such that $p_{ii} \geq \frac{1}{2}$ $(i \in [N])$. For our purposes, this assumption is unrestrictive, since it is easy to verify that the chain X_t' with transition matrix $P' = \frac{1}{2}(I + P)$ also has limiting distribution q. (I is the $N \times N$ identity matrix.) Also X_t' has mixing time only (roughly) twice that of X_t, since it amounts to choosing at each step, with probability $\frac{1}{2}$, either to do nothing or else to carry out a step of X_t.

Let G be the "underlying digraph" of X_t with vertex set N and edge set $E = \{(i,j) : p_{ij} > 0\}$. As X_t "moves" probabilistically around G we imagine its probability distribution $p^{(t)}$ as a *dynamic flow* through G in accordance with (23). Thus, in the time interval $(t-1, t)$, probability $f_{ij}^{(t)} = p_i^{(t-1)} p_{ij}$ flows from state i to state j. At (epoch) t, the probability $p_j^{(t)}$ at j is, by (23), the total flow $\sum_{i=1}^{N} f_{ij}^{(t)}$ into it during $(t-1, t)$. Thus $\sum_{i=1}^{N} f_{ij}^{(t)} = \sum_{i=1}^{N} f_{ji}^{(t+1)}$ expresses dynamic conservation of flow. Let $f_{ij} = \lim_{t\to\infty} f_{ij}^{(t)} = q_i p_{ij}$. Then clearly we have $\sum_{i=1}^{N} f_{ij} = \sum_{i=1}^{N} f_{ji}$, i.e. static conservation of flow. This is the content of the first equation of (24). In order that probability can flow through the whole of G, we must assume that it is connected (i.e. that X_t is *irreducible*). In applications, the validity of this hypothesis must be examined for the X_t concerned. Under these assumptions, however, we are guaranteed that q exists and is the unique solution of (24). The chain is then said to be *ergodic*. (See [12].)

From (25) it follows easily that

$$|p^{(t)} - q| = \tfrac{1}{2}\max_{v\in V}(p^{(t)} - q)(2v - e) = \max_{v\in V}(p^{(t)} - q)v. \tag{26}$$

Note that $(p^{(t)} - q)v = \Pr(X_t \in v) - \Pr(X_\infty \in v)$. We will examine the behaviour of $\max_{v\in V}(p^{(t)} - q)v$ as a function of the limiting probability qv of the sets. The aim will be to show that this function is (approximately) pointwise decreasing with t, at a rate influenced by the asymptotic speed of probability flow into, and out of, each set v. To make this idea precise, we digress for a moment.

Sinclair and Jerrum [30] defined the *ergodic flow* $f(v)$ from v to be the asymptotic total flow out of v. (Equivalently, this is the limiting value of the probability $\Pr(X_{t-1} \in v \text{ and } X_t \notin v)$.) Thus, from the definition,

$$\begin{aligned}
f(v) &= \sum_{i\in v}\sum_{j\notin v} q_i p_{ij} \\
&= \sum_{i\in v}\sum_{j\notin v} f_{ij} \\
&= \sum_{i\in v}\sum_{j=1}^{N} f_{ij} - \sum_{i\in v}\sum_{j\in v} f_{ij} \\
&= \sum_{i\in v}\sum_{j=1}^{N} f_{ji} - \sum_{i\in v}\sum_{j\in v} f_{ij} \\
&= \sum_{j=1}^{N}\sum_{i\in v} f_{ji} - \sum_{j\in v}\sum_{i\in v} f_{ji} \\
&= \sum_{j\notin v}\sum_{i\in v} f_{ji} \\
&= f(\bar{v}),
\end{aligned}$$

using conservation of flow. Thus the ergodic flow from v is the same as that from its complement $\bar{v}$. (This is, of course, a property of *any* closed system having conservation of flow.) Sinclair and Jerrum [30] now defined the *conductance* of X_t as $\Phi = \min_{v \in V}\{f(v)/qv : qv \leq \frac{1}{2}\}$. This quantity is clearly the limit of $\min_{v \in V} \Pr(X_t \notin v \mid X_{t-1} \in v)$ for sets of "small" limiting probability. (We call these "small sets".) Intuitively then, if the conductance Φ is (relatively) large the flows will be high, and X_t cannot remain "trapped" in any small set v for too long.

Lovász and Simonovits [24] generalized this definition to μ-conductance, which ignores "very small" sets. They defined

$$\Phi_\mu = \min_{v \in V}\{f(v)/(qv - \mu) : \mu < qv \leq \tfrac{1}{2}\}. \tag{27}$$

Remark 5 In [30], conductance is only defined for X_t "time reversible". Our definition of μ-conductance does not agree precisely with that in [24], but is clearly equivalent since $f(v) = f(\bar{v})$.

The intuition now is that, if the distribution of X_0 is already close to that of X_∞ on all very small sets, we know that this will remain true for all X_t. (This will be shown below). Thus X_t cannot be trapped in any very small set, and we need only worry about the larger ones. We will use only the notion of conductance (i.e. 0-conductance) here, but we prove the results in this section in the more general setting of μ-conductance.

To avoid a complication in the proof, we will modify the definition (27) slightly. Let $q_{\max} = \max_i q_i$, and define

$$\Phi_\mu = \min_{v \in V}\{f(v)/(qv - \mu) : \mu < qv \leq \tfrac{1}{2}(1 + q_{\max})\}. \tag{28}$$

The Φ_μ given by (28) is easily seen to be at least $(1 - 2\mu - q_{\max})/(1 - 2\mu + q_{\max})$ times that given by (27). Thus, provided, μ is bounded away from $\frac{1}{2}$ and $q_{\max} = o(1)$, the value from (28) is asymptotic to that from (27). (In our application here, these assumptions are overwhelmingly true.) Now let us return to our main argument. For $0 \leq x \leq 1$, we wish to examine the function

$$z_t(x) = \max_{v \in V}\{p^{(t)}v - x : qv = x\}. \tag{29}$$

Thus z_t is the value function of an equality knapsack problem. This is difficult to analyse, since it is only defined for a finite number of x's, and has few useful properties. Thus we choose to majorize z_t by the "linear programming relaxation" of (29). Therefore define

$$h_t(x) = \max_{w \in C_N}\{p^{(t)}w - x : qw = x\}. \tag{30}$$

We observe that, trivially,

$$h_t(x) \leq 1 - x \quad \text{for all } x \in [0, 1]. \tag{31}$$

Clearly $z_t(x) \leq h_t(x)$ at all x for which z_t is defined. Also, it is not difficult to see that $\max_{0 \leq x \leq 1} h_t(x) = \max_{0 \leq x \leq 1} z_t(x) = |p^{(t)} - q|$, so the relaxation does not do too much harm. Its benefit is that $h_t(x)$ is the value function of a (maximizing) linear program, and hence is (as is easy to prove) a concave function of x on $[0, 1]$. We have $h_t(0) = h_t(1) = 0$.

Now, for given x and t, let $\hat{w}$ be the maximizer in (30). By elementary linear programming theory, $\hat{w}$ is at a vertex of the polyhedron $C_N \cap \{qw = x\}$. Therefore it lies at the intersection of an edge of C_N with the hyperplane $qw = x$. Thus there exists $\lambda \in [0, 1)$ and vertices $v^{(1)}, v^{(2)} \in V$, with $v^{(2)} = v^{(1)} + e_k$ for some $k \in [N]$, such that $\hat{w} = (1 - \lambda)v^{(1)} + \lambda v^{(2)}$. So $\hat{w}$ has only one fractional coordinate $\hat{w}_k$. Moreover, we must have $h_t(qv^{(i)}) = p^{(t)}v^{(i)} - qv^{(i)}$, $(i = 1, 2)$. Otherwise, suppose $w^{(i)} \in C_N$ is such that $qw^{(i)} = qv^{(i)}$, $p^{(t)}v^{(i)} < p^{(t)}w^{(i)}$. Then we can replace $v^{(i)}$ in the expression for $\hat{w}$ by $w^{(i)}$ to obtain a feasible solution to the linear program in (30) with objective function better that $p^{(t)}\hat{w} - x$, a contradiction. Thus $h_t(x) = (1 - \lambda)h_t(qv^{(1)}) + \lambda h_t(qv^{(2)})$. So h_t is piecewise linear with successive "breakpoints" $x = qv^{(1)}, qv^{(2)}$, such that $v^{(1)} \subseteq v^{(2)}$ are sets differing in exactly one element. It follows that there are $N - 1$ such breakpoints in the interior of $[0, 1]$, with successive x values separated by a (unique) q_i.

Note that $h_t(x) = p^{(t-1)}(P\hat{w}) - x$, $P\hat{w} \in C_N$ and $q(P\hat{w}) = q\hat{w} = x$, using (24). Thus $P\hat{w}$ is feasible in the linear program (30) for $h_{t-1}(x)$, giving immediately $h_t(x) \leq h_{t-1}(x)$. Thus h_t certainly decreases with t, but we wish to quantify the rate at which this occurs. We do this by expressing the flow into $\hat{w}$ during $(t - 1, t)$, $p^{(t)}\hat{w}$, as

a convex combination of the flows out of "sets" (points in C_N) w', w'', with $qw' = x' < x < x'' = qw''$. This enables us to bound $h_t(x)$ as a convex combination of $h_{t-1}(x')$ and $h_{t-1}(x'')$. This is made precise in Lemma 6 below. Then, provided x', x'' are "far enough away" from x, $h_t(x)$ decays exponentially (in a certain sense) with t. This will be the content of Theorem 4.

Lemma 6 (Lovász-Simonovits) *Let $y(x) = \min(x, 1-x)$. Then, for $x \in [\mu, 1-\mu]$,*

$$h_t(x) \leq \tfrac{1}{2}h_{t-1}(x - 2\Phi_\mu(y(x) - \mu)) + \tfrac{1}{2}h_{t-1}(x + 2\Phi_\mu(y(x) - \mu)).$$

Proof The function on the right side in the lemma is evidently concave in both intervals $[\mu, \frac{1}{2}]$ and $[\frac{1}{2}, 1-\mu]$. Thus, since h_t is also concave, it suffices to prove the inequality at the breakpoints of h_t and the point $x = \frac{1}{2}$. Thus, consider a breakpoint $\mu < x = qv \leq \frac{1}{2}$, with $h_t(x) = p^{(t)}v - x$. (Breakpoints in $[\frac{1}{2}, 1-\mu]$ are dealt with by a similar argument.) Intuitively, we wish to express the flow $p^{(t)}v$ into v as a convex combination of flows from "small subsets" and "large supersets" of v. Note that we have $0 \leq 2Pv - v \leq e$, since $0 \leq v \leq e$ and $(2P - I)$ is a non-negative matrix since all $p_{ii} \geq \frac{1}{2}$. Hence define

$$\begin{aligned} v'_i &= 2(Pv)_i - v_i, & v''_i &= v_i, & &\text{if } v_i = 1, \\ v'_i &= v_i, & v''_i &= 2(Pv)_i - v_i, & &\text{if } v_i = 0. \end{aligned} \tag{32}$$

Thus $v', v'' \in C_N$ and $Pv = \frac{1}{2}(v' + v'')$. Clearly, v', v'' are convex combinations of sets respectively contained in, or containing, v. Thus, since from (24)

$$p^{(t)}v = p^{(t-1)}(Pv) = \tfrac{1}{2}p^{(t-1)}v' + \tfrac{1}{2}p^{(t-1)}v'',$$

we have achieved our objective of expressing the flow into v as a convex combination of flows from subsets and supersets $\tilde{v}$ of v. It remains to prove that the $\tilde{v}$ in this representation are large enough, or small enough, in comparison with v. From (32), since $(Pv)_i = \sum_{j \in v} p_{ij}$, we have

$$q(v'' - v) = 2\sum_{i \notin v} \sum_{j \in v} q_i p_{ij} = 2f(\bar{v}) = 2f(v). \tag{33}$$

Also, using (24) and $Pv = \frac{1}{2}(v' + v'')$,

$$q(v - v') = q(Pv - v') = q(v'' - Pv) = q(v'' - v) = 2f(v). \tag{34}$$

Let $x' = qv', x'' = qv''$. Then (34) gives $(x - x') = (x'' - x) = 2f(v)$. Thus, from (27), and (34), since $x \leq \frac{1}{2}$,

$$(x - x') = (x'' - x) \geq 2\Phi_\mu(x - \mu). \tag{35}$$

Also, since v is a maximizer for $h_t(x)$ and $Pv = \frac{1}{2}(v' + v'')$,

$$\begin{aligned} h_t(x) &= (p^{(t-1)} - q)Pv = \tfrac{1}{2}(p^{(t-1)} - q)(v' + v'') \\ &\leq \tfrac{1}{2}h_{t-1}(qv') + \tfrac{1}{2}h_{t-1}(qv'') \\ &= \tfrac{1}{2}h_{t-1}(x') + \tfrac{1}{2}h_{t-1}(x'') \end{aligned}$$

Let $x_1 = x - 2\Phi_\mu(x - \mu)$, $x_2 = x + 2\Phi_\mu(x - \mu)$. Then we have $x = \frac{1}{2}(x' + x'') = \frac{1}{2}(x_1 + x_2)$, and (35) implies $x' \leq x_1 \leq x_2 \leq x''$. For these four x's, denote $h_{t-1}(x')$ by h' etc. Since h_{t-1} is concave, the whole of the line segment $[(x_1, h_1), (x_2, h_2)]$ lies above $[(x', h'), (x'', h'')]$. Hence, in particular,

$$h_t(x) \leq \tfrac{1}{2}h_{t-1}(x') + \tfrac{1}{2}h_{t-1}(x'') \leq \tfrac{1}{2}h_{t-1}(x_1) + \tfrac{1}{2}h_{t-1}(x_2). \tag{36}$$

We have still to consider the point $x = \frac{1}{2}$. Observe that there must be a breakpoint of h_t within $\frac{1}{2}q_{\max}$ of $\frac{1}{2}$. Let this be x^+, and suppose that $x^+ \in [\frac{1}{2}, \frac{1}{2}(1 + q_{\max})]$, the other case being symmetric. Let the previous breakpoint be $x^- < \frac{1}{2}$. By our definition (28), the inequality in (35) will still apply at x^+. Thus we can prove (36) for x^+. The linearity of h_t in $[x^-, x^+]$ and the concavity of h_{t-1} now imply that (36) holds throughout $[x^-, x^+]$, and hence at $x = \frac{1}{2}$. □

Clearly Lemma 6 is equivalent to $h_t(x) \le H_t(x)$ $(\mu \le x \le 1-\mu)$, where $H_0(x)$ is any function such that $h_0(x) \le H_0(x)$ for all $x \in [\mu, 1-\mu]$ and

$$H_t(x) = \tfrac{1}{2}H_{t-1}(x - 2\Phi_\mu(y(x)-\mu)) + \tfrac{1}{2}H_{t-1}(x + 2\Phi_\mu(y(x)-\mu)). \tag{37}$$

We have to solve the recurrence (37). Clearly $H_t(x) = C$, for any constant C is a solution. To find others, we use "separation of variables". We look for a solution of the form $H_t(x) = g(t)G(y(x))$ for $x \in [\mu, 1-\mu]$. Then

$$g(t)/g(t-1) = (G(y - 2\Phi_\mu(y-\mu)) + G(y + 2\Phi_\mu(y-\mu)))/2G(y)$$

where $y = y(x) \in [\mu, \frac{1}{2}]$. (Note $y(y(x)) = y(x)$.) Thus, for some γ, we must have $g(t) = \gamma g(t-1)$, i.e. $g(t) = C_1\gamma^t$, for some constant C_1, and

$$2\gamma G(y) = G(y - 2\Phi_\mu(y-\mu)) + G(y + 2\Phi_\mu(y-\mu)) \quad (\mu \le y \le \tfrac{1}{2}).$$

The form of this equation suggests trying $G(y) = C_2(y-\mu)^\alpha$ for some constants α, C_2. This gives

$$2\gamma = (1 - 2\Phi_\mu)^\alpha + (1 + 2\Phi_\mu)^\alpha.$$

Assuming that Φ_μ is small, we have $\gamma \approx 1 + 2\alpha(\alpha-1)\Phi_\mu^2$. We wish to minimize γ in order to force H_t to decrease quickly with t. Thus we should take $\alpha = \frac{1}{2}$, giving

$$\gamma = \tfrac{1}{2}(\sqrt{1-2\Phi_\mu} + \sqrt{1+2\Phi_\mu}) \le 1 - \tfrac{1}{2}\Phi_\mu^2. \tag{38}$$

The inequality in (38) is proved by noting that, for $x \in [0,1]$, $\sqrt{1-x} \le (1 - \frac{1}{2}x)$ and $\frac{1}{2}(\sqrt{1-x} + \sqrt{1+x}) = \sqrt{\frac{1}{2}(1 + \sqrt{1-x^2})}$. Both are easily proved by squaring. Thus the middle term of (38) is

$$\sqrt{\tfrac{1}{2}(1 + \sqrt{1 - 4\Phi_\mu^2})} \le \sqrt{1 - \Phi_\mu^2} \le 1 - \tfrac{1}{2}\Phi_\mu^2.$$

In view of this discussion, we have justified a bound of the form

$$h_t(x) \le C + C'(1 - \tfrac{1}{2}\Phi_\mu^2)^t\sqrt{y(x) - \mu}, \tag{39}$$

for some constants C, C', given only that this inequality holds for $h_0(x)$ $(x \in [\mu, 1-\mu])$. Thus we may prove

Theorem 4 (Lovász-Simonovits) *If* $C = \max\{h_0(x) : x \in [0,\mu] \cup [1-\mu, 1]\}$, *and* $C' = \max_{\mu \le x \le 1-\mu}(h_0(x) - C)/\sqrt{y(x)}$, *then*

$$h_t(x) \le C + C'\exp(-\tfrac{1}{2}\Phi_\mu^2 t) \qquad (x \in [0,1], t \ge 0)$$

Proof The constant C ensures the inequality holds for $t = 0$ and $x \le \mu$ or $x \ge 1-\mu$. Then C' ensures that it holds for $x \in [\mu, 1-\mu]$ and $t = 0$. It then holds for all t, using the solution of the recurrence (39). □

We turn now to the application of Theorem 4 to the volume algorithm. The Markov chain X_t we consider is the phase i, trial j, random walk.

An ergodic Markov chain is *time reversible* if there exist constants $\lambda_i \ge 0$ $(i \in [N])$, not all zero, such that $\lambda_i p_{ij} = \lambda_j p_{ji}$ for all $i, j \in [N]$. (These are called the *detailed balance* equations.) Since

$$\sum_{i=1}^{N} \lambda_i p_{ij} = \lambda_j \qquad (j \in [N]),$$

it follows, by uniqueness, that $q_i = \lambda_i/(\sum_{j=1}^N \lambda_j)$ for all $i \in [N]$. In our random walks, we have (in obvious notation) for all $x, y \in \mathcal{L}$,

$$\begin{array}{rcll} p(x,y) & = & 0 & \text{if } x, y \text{ nonadjacent} \\ & = & \frac{1}{4n} & \text{if } x, y \text{ adjacent and } \phi(y) \le \phi(x) \\ & = & \frac{1}{8n} & \text{if } x, y \text{ adjacent and } \phi(y) > \phi(x) \\ & = & 1 - \sum_{z \ne x} p(x,z) & \text{if } x = y, \end{array}$$

Where $\phi(x)$ is as defined in Section 4.1 and discussed in Section 4.2. If we take $\lambda(x) = 2^{-\phi(x)}$, the only cases to be checked are if x, y are adjacent. It is then easy to verify that

$$\lambda(x)p(x,y) = \lambda(y)p(y,x) = \frac{1}{4n}2^{-\max\{\phi(x),\phi(y)\}} = \frac{1}{4n}2^{-\phi(z)}, \tag{40}$$

for any $z \in \text{int}\,\{C(x) \cap C(y)\}$. The conductance

$$\Phi = \sum_{x\in v}\sum_{y\notin v}\lambda(x)p(x,y)/\sum_{x\in v}\lambda(x),$$

for some $v \in V$. Let $S = \bigcup_{x\in v} C(x)$, with bounding surface σ. Note that σ is a union of $(n-1)$-dimensional δ-cube faces, with $\|u\|_1 = \|u\|_\infty^* = 1$ at all points at which u is defined. If we put $F(x) = \lambda(x) = 2^{-\phi(x)}$, and $\hat{F}(x) = 2^{-\hat{\phi}(x)}$, where $\hat{\phi}(x)$ is as defined in Section 4.2, we have

$$\tfrac{1}{4}\hat{F}(x) \le F(x) \le \hat{F}(x),$$

and $\hat{F}$ is log-concave, since $r(x)$ is convex. Letting μ be the measure induced by F, we apply Corollary 2 with the norm ℓ_∞ and $\Psi = 4$. If Φ_i is the conductance of any phase i random walk, we then have

$$\Phi_i = \frac{f(v)}{q(v)} = \frac{4n\delta^{n-1}f(v)}{\delta^n qv}\cdot\frac{\delta}{4n} = \frac{\mu'(S)}{\mu(S)}\cdot\frac{\delta}{4n},$$

since $\phi(\cdot) = \max\{\phi(x),\phi(y)\}$ on $\text{int}\,\{C(x)\cap C(y)\}$ by definition. Thus

$$\Phi_i \ge \frac{2\delta}{4^2 n d_i} = \frac{1}{2^4 n^2 d_i}, \tag{41}$$

for $i = 1, 2, \ldots, k$.

4.5 The random walk

In this section we conclude the analysis of the random walks employed in the algorithm. For convenience, let us assume that a point ζ is generated in the final δ-cube at the end of every walk, and we always check whether ζ is in K_i. Thus, if the random walk is run "long enough", the (extended) function $F(x) = 2^{-\phi(x)}$ is the (unnormalised) probability density function of ζ . We call $F(x)$ the "weight function".

We observe that each walk has one of three mutually exclusive outcomes :

(E_1) $\zeta \notin K_i$, an improper trial.

(E_2) $\zeta \in K_i \setminus K_{i-1}$, a failure.

(E_3) $\zeta \in K_{i-1}$, a success.

We generate ζ, and observe one of the outcomes $E_j, j = 1,2,3$. Let us denote the observed outcome by E. Denote the final (i.e. $t = \tau$) and limiting distributions of the random walk by p_j and q_j for $j \in [N]$ similarly to Section 4.4, and let

$$z_j = \Pr(\zeta \in E \mid X_t = j) \quad (j \in [N]).$$

(Observe that this is independent of t.) We will use primes to denote the probabilities conditional on E. Thus, if $p_E = \Pr(\zeta \in E) = pz$, and we write $q_E = qz \ge \beta$ for its asymptotic value,

$$p'_j = p_j z_j / p_E, \quad q'_j = q_j z_j / q_E.$$

We say that E is a *good* set and the outcome is good if

$$q_E \ge \beta = \frac{\epsilon^4}{2^{18}n^3}.$$

We now proceed inductively. We assume that the outcome of a trial is good and its final distribution is close to its steady state i.e.

$$h_\tau(x) \le 2^{-6}\sqrt{\beta}\sqrt{\min(x, 1-x)} \quad (x \in [0,1]). \tag{42}$$

This is certainly true initially. Let us show next that, when the walk is close to its asymptotic distribution, the probability of E_1 will not be too high. Now

$$\phi(x) = \lceil (r(y) - 1)/\delta - \tfrac{1}{2} \rceil \ge \lceil (r(x) - 1)/\delta \rceil - 1,$$

for some $y \in \mathcal{L}$, using Lemma 3. Thus $F(x) \le 2^{-j}$ if $r(x) > (1 + \delta j)$. Thus, if $\bar{E}_1 = E_2 \cup E_3$, the definition of $r(x)$ implies

$$\begin{aligned}
\Pr(E_1)/\Pr(\bar{E}_1) &= \Pr(\zeta \notin K_i)/\Pr(\zeta \in K_i), \\
&= \int_{A_i \setminus K_i} F(x)\,dx \Big/ \int_{K_i} F(x)\,dx, \\
&\le \sum_{j=0}^{\infty} \int_{1+j\delta < r(x) \le 1+(j+1)\delta} F(x)\,dx \Big/ \int_{K_i} F(x)\,dx, \\
&< \sum_{j=0}^{\infty} 2^{-j}\{(1 + \delta(j+1))^n - (1+\delta j)^n\}, \\
&= -1 + \sum_{j=1}^{\infty} 2^{-j}(1+\delta j)^n, \\
&< -1 + \sum_{j=1}^{\infty} 2^{-j} e^{\frac{1}{2}j}, \\
&= (\sqrt{e} - 1)/(1 - \tfrac{1}{2}\sqrt{e}) < 3.7,
\end{aligned}$$

giving $\Pr(E_1) < \frac{37}{47}$. So, given (42) the probability of a proper trial is at least $\frac{1}{5}$, as we claimed in Section 4.1.

Now let E_{bad} be the event that any trial ends badly. We will show below that $\Pr(\zeta \in E_j) \le 1.5\beta$ if E_j is bad. Since at most two of the E_j are bad and the expected number of trials is less than $5m_i$,

$$\Pr(E_{bad}) < 15\beta \sum_{i=1}^{k} m_i < \frac{16\epsilon^2}{2^9 n} \sum_{i=1}^{\infty} \rho^{-(i-1)}$$

using $d_i \ge \rho^{-(i-1)}$, as may be easily proved. Thus, since $\rho > 1/(2n)$,

$$\Pr(E_{bad}) < \frac{\epsilon^2}{2^5 n} 2(n+1) < \frac{1}{10}$$

as claimed in Section 4.1.

Note next that since $z_j \in [0,1]$,

$$|p_E - q_E| = |\sum_j (p_j - q_j) z_j| \le h_\tau(q_E) \le 2^{-6}\sqrt{\beta q_E}. \tag{43}$$

Thus if E is a bad set ($q_E < \beta$), we certainly have $p_E < 1.5\beta$, as claimed above. Also for a good set ($q_E \ge \beta$) we have

$$|p_E - q_E| \le \max_x h_\tau(x) < 2^{-15}\epsilon^2 n^{-3/2}.$$

Since $q_{E_1} < \frac{5}{6}$, a straightforward calculation now validates the claim made in (13) in the analysis of Section 4.1, i.e.

$$|\alpha_i - \hat{\alpha}_{i,j}| = |q_{E_3}/(1 - q_{E_1}) - p_{E_3}/(1 - p_{E_1})| < 2^{-9}\epsilon^2 n^{-3/2} = \sqrt{\beta}.$$

Now assuming that E is good let $h'(x)$ be the function defined in (30), but conditional on $\zeta \in E$. Thus

$$\begin{aligned} h'(x) &= \max_w\{p'w : q'w = x\} - x \\ &= \max_w\{\sum_j p_j z_j w_j/p_E : \sum_j q_j z_j w_j/q_E = x\} - x \\ &= \max_w\{\sum_j p_j w_j/p_E : \sum_j q_j w_j/q_E = x\} - x \\ &= \max_w\{\sum_j p_j w_j : \sum_j q_j w_j = q_E x\}/p_E - x \\ &= (h_\tau(q_E x) + q_E x)/p_E - x \\ &\leq 2^{-6}\sqrt{\beta q_E}(\sqrt{x} + x)/p_E, \\ &< 2^{-4}\sqrt{x}, \end{aligned}$$

using (42), (43) and $q_E \geq \beta$.

We now consider $h_0(x)$ in the subsequent trial. Let us denote this by $h^*(x)$, and the asymptotic distribution by q^*. The initial probability distribution is p' on the event E, with asymptotic probability q^*_E. Note that $q^*_E \geq \frac{1}{14}\beta$. This follows as the total weight may increase at most 14 between phases (the weight corresponding to points in K can double at most and $\Pr(E_1) < \frac{5}{6}$ shows there is at most another 12 from points outside K.) In the following $\Omega = [0,1]^N$ and $\tilde{\Omega} = [0,1]^{\tilde{N}}$ where N is the number of states in the phase that has just ended and $\tilde{N} \geq N$ is the number of states in the phase which is just starting. Observe that $p'_j, q'_j = 0$ for $j > N$. Let p'', q'' denote the N-vectors obtained by deleting the last $(\tilde{N} - N)$ components of p', q'. Now

$$\begin{aligned} h^*(x) &= \max_{w\in\tilde{\Omega}}\{p'w : q^*w = x\} - x \\ &= p'\tilde{w} - x, \text{ say} \\ &= p''\hat{w} - x, \text{ say} \\ &\leq \max_{w\in\Omega}\{p''w : q''w = q''\hat{w}\} - x \\ &= \max_{w\in\Omega}\{p''w : q''w = x''\} - x, \end{aligned}$$

where $\hat{w}$ is the truncation of $\tilde{w}$ to its first N components, and

$$x = \sum_{j=1}^{\tilde{N}} q^*_j\tilde{w}_j \geq \sum_{j=1}^{N} q^*_j z_j\hat{w}_j = q^*_E(q''\hat{w}) = q^*_E x''.$$

Thus

$$\begin{aligned} h^*(x) &\leq h'(x'') + x'' - x \\ &< 1.1\sqrt{x''} \\ &\leq 1.1\sqrt{x/q^*_E} \\ &< 5\beta^{-\frac{1}{2}}\sqrt{x}. \end{aligned}$$

The trivial inequality (31), $h^*(x) \leq 1 - x$, now implies that

$$h^*(x) \leq 2\beta^{-\frac{1}{2}}\sqrt{\min(x, 1-x)},$$

and thus we take (with $\mu = 0$) $C = 0, C' = 2\beta^{-\frac{1}{2}}$ in Theorem 4. Thus we need only run the random walk until

$$\begin{aligned} 2\beta^{-\frac{1}{2}}\exp\{-\tfrac{1}{2}\Phi_i^2\tau\} &\leq 2^{-6}\sqrt{\beta}, \\ \text{i.e.} \qquad \tau &\geq 2\Phi_i^{-2}\ln(5\times 2^6/\beta) \\ \text{or} \qquad \tau &\geq 2^9 n^4 d_i^2 \ln(2^{27}n^3\epsilon^{-4}), \end{aligned}$$

using (41). We have included an extra factor of 8/5 to allow for the discrepancy in the definitions of conductance between (27) and (28) in Section 4.4. This is generous, since $q_{\max} \leq 1/(4n)^n \leq 2^{-6}$ (the initial distribution for $n = 2$), and thus the factor

$$(1 + q_{\max})/(1 - q_{\max}) < 1.1 .$$

We can now see that (16) is justified. Basically we need to consider quantities $\Pr(E'|E'')$ where E', E'' are good events and E'' refers to an earlier trial than E'. We can assume that at the trial corresponding to E'' (42) holds. Our inductive argument then implies that assuming E_{bad} does not occur the probability of E' will be within the correct error bounds because of (42).

This concludes the analysis of the algorithm.

4.6 Generating uniform points

We have seen how a generator of "almost uniform" points in an arbitrary convex body can be used to estimate volume. Here we will prove a stronger converse to this, that a volume estimator can be used to determine, with high probability, a uniformly generated point in a convex body. (The probability of failure is directly related to the probability that the volume estimator fails.) The development here has a similar flavour to, though is not derivable from, results of Jerrum, Valiant and Vazirani [16]. We will gloss over most of the issues of accuracy of computation, leaving the interested reader to supply these.

Let $\epsilon = 1/(6n)$ and $m = 60n^2$, say. We consider a general dimension d ($2 \leq d \leq n$). We will use the same terminology and notation as in Section 4.3. Choose the lowest numbered coordinate direction, and determine the Euclidean width w of K in this direction. We assume, for convenience, that the area function $A(s)$ is defined for $s \in [0, w]$.

We know, from Brunn-Minkowski, that $A(s)^{1/(n-1)}$ is a concave function of s in $[0, w]$. Thus, in particular, $A(s)$ is unimodal, i.e. for some s^*, $A(s)$ is nondecreasing in $[0, s^*]$ and nonincreasing in $[s^*, w]$. We will write $A^* = A(s^*)$. We have

Lemma 7 *If* $0 \leq s \leq s^*$, $(s/s^*)^n(A^*s^*/n) \leq V(s) \leq A^*s$.

Proof From the proof of Lemma 4, for $0 < s < u$, we have$A(s)/A(u) \geq (s/u)^{n-1}$. But $V(s) = \int_0^s A(y)\,dy$, so the result follows from this and $A(s) \leq A^*$, on putting $u = s^*$ and integrating between 0 and s. □

Corollary 3 $A^*w/n \leq \mathrm{vol}_n(K) \leq A^*w$.

Proof The right hand inequality is immediate. For the left hand, from Lemma 7, $V(s^*) \geq A^*s^*/n$. By symmetry, $V(w) - V(s^*) \geq A^*(w - s^*)/n$. The result follows by adding. □

Now let us divide the width of the body into m "strips" of size $\delta = w/m$. Write $A_i = A(i\delta)$, $V_i = \int_{(i-1)\delta}^{i\delta} A(s)\,ds$, so $V = \mathrm{vol}_n(K) = \sum_{i=1}^m V_i$.

We begin by obtaining some easy estimates which form the basis of the method. Assume without loss that $s^* \in [(k-1)\delta, k\delta)$ with $k \geq \frac{1}{2}m$. Then the $\{A_i\}$ form a nondecreasing sequence for $0 \leq i \leq (k-1)$, and a nonincreasing sequence for $k \leq i \leq m$. Then, by Corollary 3, $V \geq A^*w/d$. Thus $A^* \leq dV/w = dV/(m\delta)$. Therefore

$$A^*\delta \leq dV/m \leq nV/m = \epsilon V/10 \tag{44}$$

Let $\hat{A}(s)$ be an ϵ-approximation to $A(s)$, with probability at least $(1-\xi)$, i.e. (with this probability) $A(s)/(1+\epsilon) \leq \hat{A}(s) \leq (1+\epsilon)A(s)$. Write $\hat{A}_i = \hat{A}(i\delta)$, and let $H_i = (1+\epsilon)^3 \max\{\hat{A}_{i-1}, \hat{A}_i\}$.

Lemma 8 *If* $s \in [(i-1)\delta, i\delta]$, *then* $\hat{A}(s) \leq H_i$.

Proof If $i \neq k$, then

$$\begin{aligned} \hat{A}(s) \leq (1+\epsilon)A(s) &\leq (1+\epsilon)\max\{A_{i-1}, A_i\} \\ &\leq (1+\epsilon)^2 \max\{\hat{A}_{i-1}, \hat{A}_i\} \\ &= H_i/(1+\epsilon) \leq H_i. \end{aligned}$$

If $s \in [(k-1)\delta, k\delta]$, $\hat{A}(s) \leq (1+\epsilon)A^*$. Also, using Corollary 7

$$\begin{aligned} A_{k-1} &\geq ((k-1)\delta/s^*)^{d-1}A^* \\ &\geq ((k-1)/k)^{d-1}A^* \\ &\geq (1-2/m)^{d-1}A^* \text{ since } k \geq \tfrac{1}{2}m, \\ &\geq (1-1/(30n^2))^n A^* \text{ since } m = 60n^2, \\ &\geq (1-\epsilon/(5n))^n A^* \text{ for } n \geq 1, \\ &\geq A^*/(1+\epsilon) \text{ since } \epsilon < 1. \end{aligned}$$

Thus $A^* \leq (1+\epsilon)A_{k-1}$, and therefore

$$\hat{A}(s) \leq (1+\epsilon)^2 A_{k-1} \leq (1+\epsilon)^3 \hat{A}_{k-1} \leq (1+\epsilon)^3 \max\{\hat{A}_{k-1}, \hat{A}_k\} = H_k.$$

□

Thus, if $V' = \delta \sum_{i=1}^{m} H_i$, we have

$$\begin{aligned} V' &\leq \delta(1+\epsilon)^4 \sum_{i=1}^{m} \max\{A_{i-1}, A_i\} \\ &= \delta(1+\epsilon)^4 (\sum_{i=1}^{k-1} A_i + \sum_{i=k}^{m-1} A_i + \max\{A_{k-1}, A_k\}) \\ &\leq \delta(1+\epsilon)^4 (\sum_{i=0}^{m} A_i + A^*) \end{aligned} \tag{45}$$

Also

$$V' \geq \delta(1+\epsilon)^2 \sum_{i=1}^{m} \max\{A_{i-1}, A_i\} \geq \delta(1+\epsilon)^2 (\sum_{i=0}^{m} A_i - A^*). \tag{46}$$

Using elementary area estimates

$$V \leq \delta(\sum_{i=1}^{k-1} A_i + A^* + \sum_{i=k}^{m-1} A_i) \leq \delta(\sum_{i=0}^{m} A_i + A^*) \tag{47}$$

and

$$\begin{aligned} V &\geq \delta(\sum_{i=1}^{k-2} A_i + \min\{A_k, A_{k-1}\} + \sum_{i=k+1}^{m} A_i) \\ &= \delta(\sum_{i=1}^{k} A_i - \max\{A_k, A_{k-1}\} + \sum_{i=k+1}^{m} A_i) \\ &\geq \delta(\sum_{i=0}^{m} A_i - 2A^*) \end{aligned} \tag{48}$$

From (46) and (47),

$$V \leq V'/(1+\epsilon)^2 + 2\delta A^* \leq V'/(1+\epsilon)^2 + \epsilon V/5,$$

using (44), so $V'/V \geq (1-\epsilon/5)(1+\epsilon)^2 \geq (1+\epsilon)$. From (45) and (48),

$$V' \leq (1+\epsilon)^4 (V + 3\delta A^*) \leq (1+\epsilon)^5 V,$$

using (44), so $V'/V \leq (1+\epsilon)^5$, i.e.

$$(1+\epsilon) \leq V'/V \leq (1+\epsilon)^5. \tag{49}$$

We may now turn to the algorithm itself. We select a strip $i \in [m]$ from the probability distribution $H_i/(\sum_{j=1}^{m} H_j)$. Within the chosen strip we select a point uniformly, i.e. $s \in [(i-1)\delta, i\delta]$ with density $1/\delta$. With probability $\hat{A}(s)/H_i$, we "accept" s and proceed recursively to dimension $(d-1)$ and the cross-section at s. When $d = 1$ we generate uniformly on $[0, w]$. The generated point $(s_1, s_2, \ldots, s_n) \in K$, where we use subscript d to refer to quantities at dimension d, is now accepted with a final probability

$$q = \frac{1}{eV_n'} \prod_{d=1}^{n} \frac{V_d'}{\hat{A}(s_d)}.$$

Note that q can be calculated within the algorithm. Now,

$$\begin{aligned} q &= \frac{1}{eV_n} \frac{V_n}{V_n'} \prod_{d=1}^{n} \frac{V_d'}{V_d} \frac{A(s_d)}{\hat{A}(s_d)} \frac{V_d}{A(s_d)} \\ &\leq \frac{1}{eV_n} \frac{1}{(1+\epsilon)} \prod_{d=1}^{n} (1+\epsilon)^5 (1+\epsilon) \frac{V_d}{A(s_d)} \\ &= \frac{(1+\epsilon)^{6n-1}}{e} \frac{1}{V_n} \prod_{d=1}^{n} \frac{V_d}{V_{d-1}} \\ &= \frac{(1+\epsilon)^{6n-1}}{e} < 1 \text{ since } \epsilon = 1/(6n). \end{aligned}$$

Also

$$\begin{aligned} q &\geq \frac{1}{eV_n} \frac{1}{(1+\epsilon)^5} \prod_{d=1}^{n} (1+\epsilon) \frac{1}{(1+\epsilon)} \frac{V_d}{A(s_d)} \\ &= \frac{1}{e(1+\epsilon)^5} \geq \frac{1}{e(1+1/12)^5} > \frac{1}{5}. \end{aligned}$$

The overall (improper) density of the selected point is

$$\begin{aligned} q \prod_{d=1}^{n} \frac{ds_d}{\delta} \frac{H_{id}}{\sum_{j=1}^{m} H_{jd}} \frac{\hat{A}(s_d)}{H_{id}} &= q \prod_{d=1}^{n} \frac{\hat{A}(s_d)}{V_d'} \prod_{d=1}^{n} ds_d \\ &= q \frac{1}{eV_n'} \prod_{d=1}^{n} ds_d, \end{aligned}$$

i.e. uniform. The overall probability of acceptance is clearly

$$\frac{1}{eV_n'} \int_K \prod_{d=1}^{n} ds_d = \frac{V_n}{eV_n'} \geq \frac{1}{e(1+\epsilon)^5} > \frac{1}{5}.$$

Thus each "trial" of determining a point has a constant probability of success. We can make this as high as we wish by repeating the procedure. We use at most $60n^2 \cdot n = 60n^3$ calls to the volume approximator. Thus the overall error probability will be at most $60n^3\xi$, if the approximator fails with probability ξ.

Finally, we observe that if K is well guaranteed, then all the sections which we might wish to approximate can easily be shown to be well guaranteed also. Thus our approximator can be restricted to work only for well guaranteed bodies, as we would obviously require. Thus this is no real restriction. (Provided, of course, the body K from which we wish to sample is itself well guaranteed.)

5 Applications

5.1 Integration

We describe algorithms for integrating non-negative functions over a well-guaranteed convex body K. We assume non-negativity since we can only approximate and so we cannot deal with integrals which evaluate to zero. It may of course be entirely satisfactory to integrate the positive and negative parts of the function separately.

5.1.1 Concave functions

Integration of a non-negative function $f : \mathbf{R}^n \rightarrow \mathbf{R}$ over a convex body K can be expressed as a volume computation by:

$$\int_{x \in K} f dx = \mathrm{vol}_{n+1}(K_f)$$

where

$$K_f = \{(x, z) \in \mathbf{R}^{n+1} : 0 \leq z \leq f(x)\}.$$

Now if f is concave then K_f is convex and so we can compute $\int_{x \in K} f dx$ as accurately as required by the algorithm of Section 4. The time taken depends on the guarantee that we make for K_f. This will depend on how large f can become on K and also on its average value

$$\bar{f} = \frac{\int_{x \in K} f dx}{\mathrm{vol}_n(K)}. \tag{50}$$

We assume from hereon that

$$f_{max} = \max\{f(x) : x \in K\} \leq \lambda_1 = e^{L_1}$$

and

$$\bar{f} \geq \frac{1}{\lambda_2} = e^{-L_2}.$$

We feel that L_1, L_2 and $\langle K \rangle$ are good measures of the *size* of the problem here. We need a parameter (L_2) which accounts for f being very small on K.

If the guarantees for K are a, r, R then observe that (i) $K_f \subseteq B(a, R + \lambda_1)$ and (ii) $f(x) \geq \rho = r\bar{f}/2(R + r)$ for $x \in B(a, r/2)$ (this follows from $\bar{f} \leq f_{max}$ and the non-negativity of f.) It follows that K_f is well guaranteed by $((a, \rho/2), \rho/2(1+(\frac{\bar{f}}{r+R})^2)^{-1/2}, R+\lambda_1)$. Thus we can compute the integral of f over K in time which is polynomial in $\langle K \rangle, L_1, L_2$.

5.1.2 Mildly varying functions

Here we consider a *pseudo-polynomial* time algorithm i.e. one which is polynomial in the parameters L, λ_1, λ_2 but which is valid for general integrable functions. We see from (50) that it is only necessary to get a good approximation for $\bar{f}$ in order to get a good approximation for the integral. We use the equation

$$\bar{f} = \int_0^{\lambda_1} \Pr(f(x) \geq t) dt \tag{51}$$

where the probability in (51) is for x chosen uniformly from K. Now let

$$N = \left\lceil \frac{(2 + \epsilon)\lambda_1 \lambda_2}{\epsilon} \right\rceil,$$

$$h = \frac{\lambda_1}{N}$$

and

$$\pi_i = \Pr(f(x) \geq ih) \text{ for } i = 0, 1, ..., N.$$

Then we have

$$\bar{f} = \sum_{i=0}^{N-1} I_i$$

where

$$I_i = \int_{ih}^{(i+1)h} \Pr(f(x) \geq t) dt.$$

Furthermore

$$h\pi_{i+1} \leq I_i \leq h\pi_i \text{ for } i = 0, 1, ..., N - 1,$$

and so

$$S_0 \leq \bar{f} \leq S_1$$

where

$$\begin{aligned} S_0 &= h\sum_{i=1}^{N-1} \pi_i, \\ S_1 &= h\sum_{i=0}^{N-1} \pi_i. \end{aligned}$$

Thus

$$\begin{aligned} 1 \leq \frac{S_1}{S_0} &= 1 + \frac{h\pi_0}{S_0} \\ &\leq 1 + \frac{h}{\bar{f} - h} \\ &\leq 1 + \frac{\epsilon}{2}. \end{aligned}$$

We have now reduced our problem to one of finding a good estimate for S_0 and hence for $\pi_i, i = 1, 2, ..., N-1$. Assume that we wish our estimate for S_0 to be within $\epsilon/3$ with probability at least δ. This will yield an ϵ-approximation for $\bar{f}$ when ϵ is small. We let

$$M = \lceil 2160\lambda_1\lambda_2\epsilon^{-3}\ln(\frac{4N}{\delta})\rceil$$

and choose points $x_1, x_2, ..., x_M$ uniformly at random from K. Let $\nu_i = |\{j : f(x_j) \geq ih\}|$ and $\hat{\pi}_i = \frac{\nu_i}{M}$ for $i = 1, 2, ..., N-1$. Observe that the ν_i are binomially distributed and we will use standard tail estimates of the binomial distribution without comment (see e.g. Bollobás [4].) We consider two cases.

Case 1: $\pi_i < \frac{\epsilon}{20\lambda_1\lambda_2}$

For this case we observe that if $\gamma = \frac{\epsilon M}{6\lambda_1\lambda_2}$ then

$$\begin{aligned} \Pr(\nu_i \geq \gamma) &\leq \left(\frac{3e}{10}\right)^{\gamma} \\ &\leq \frac{\delta}{2N}. \end{aligned}$$

This enables us to assume that if $i_0 = \min\{i : \pi_i < \frac{\epsilon}{20\lambda_1\lambda_2}\}$ then

$$\hat{\pi}_i \leq \frac{\epsilon}{6\lambda_1\lambda_2} \text{ for } i \geq i_0.$$

The probability of this not holding being at most $\delta/2$.

Case 2: $\pi_i \geq \frac{\epsilon}{20\lambda_1\lambda_2}$

For this case we observe that

$$\begin{aligned} \Pr(|\hat{\pi}_i - \pi_i| \geq \frac{\epsilon\pi_i}{6}) &\leq 2\exp\left\{-\frac{\epsilon^3 M}{2160\lambda_1\lambda_2}\right\} \\ &\leq \frac{\delta}{2N}. \end{aligned}$$

This enables us to assume that

$$|\hat{\pi}_i - \pi_i| < \frac{\epsilon\pi_i}{6} \text{ for } i < i_0.$$

The probability of this not holding being at most $\delta/2$.

Now our estimate for $\bar{f}$ will be $\hat{S}_0 = h\sum_{i=1}^{N-1}\hat{\pi}_i$. It follows from the above that with probability at least 1-δ

$$\begin{aligned}
|S_0 - \hat{S}_0| &\leq h\sum_{i=1}^{N-1}|\pi_i - \hat{\pi}_i| \\
&\leq h\sum_{i=1}^{i_0-1}\frac{\epsilon\pi_i}{6} + h\sum_{i=i_0}^{N-1}\frac{\epsilon}{6\lambda_1\lambda_2} \\
&\leq \frac{\epsilon S_0}{6} + \frac{\epsilon}{6\lambda_2} \\
&\leq \frac{\epsilon\bar{f}}{3}.
\end{aligned}$$

5.1.3 Quasi-concave functions

It is possible to improve the preceding analysis in the case where f is *quasi-concave* i.e. the sets $\{x : f(x) \geq a\}$ are convex for all $a \in \mathbf{R}$. We will need to assume that f satisfies a (semi-) Lipschitz condition

$$f(y) - f(x) \leq \lambda_3||y - x|| \text{ for } x, y \in K.$$

Our algorithm includes a factor which is polynomial in $L_3 = \ln(\lambda_3)$, which can be taken to be positive. This is reasonable for if f grows extremely rapidly at some point then a small region may contribute *disproportionately* to the integral and so require extra effort. Note that the algorithm will be polynomial in the log of the Lipschitz constant. Next let

$$\begin{aligned}
N &= \lceil\ln(\frac{10}{\epsilon})\rceil + 1, \\
M &= \lceil\frac{10NL}{\epsilon}\rceil.
\end{aligned}$$

Let $L = 1 + \max\{L_1, L_2, L_3\}$ and $\lambda = e^L$.

It will be convenient later to assume that we know $a^* \in K$ such that $f(a^*) = \lambda_1$ and that $L_1 \geq 1$. this can be justified as follows: we use the Ellipsoid algorithm to find $a^* \in K$ such that

$$\frac{\text{vol}_n(\{x \in K : f(x) \geq f(a^*)\})}{\text{vol}_n(K)} \leq \frac{\epsilon}{10}e^{-2L}$$

and then replace $f(x)$ by $\min\{f(x), f(a^*)\}$. The loss in the computation of $\bar{f}$ is at most $\frac{\epsilon}{10}\bar{f}$ and can be absorbed in our approximation error. We can then if necessary scale to make $L_1 \geq 1$.

By making a change of varable $t = e^u$ in (51) we have

$$\begin{aligned}
\bar{f} &= \int_{-\infty}^{L_1}\Pr(f(x) \geq e^u)e^u du, \\
&= I + J.
\end{aligned}$$

Here

$$\begin{aligned}
I &= \int_{-\infty}^{-NL}\Pr(f(x) \geq e^u)e^u du, \\
&\leq \int_{-\infty}^{-NL} e^u du \\
&= e^{-NL} \\
&\leq \frac{\epsilon}{10}\bar{f}.
\end{aligned}$$

Then

$$\begin{aligned} J &= \int_{-NL}^{L_1} \Pr(f(x) \geq e^u) e^u du, \\ &= \sum_{i=0}^{2M-1} J_i, \end{aligned}$$

where

$$J_i = \int_{u_i}^{u_{i+1}} \Pr(f(x) \geq e^u) e^u du,$$

and

$$u_i = \begin{cases} -NL + \frac{iNL}{M} & \text{if } i \leq M \\ \frac{(i-M)L_2}{M} & \text{if } i > M \end{cases}$$

Now define $\pi_i = \Pr(f(x) \geq e^{u_i})$ and $h_i = u_{i+1} - u_i$ for $i = 0, 1, ..., 2M-1$. Then

$$h_i e^{u_i} \pi_{i+1} \leq J_i \leq h_i e^{u_{i+1}} \pi_i.$$

Now let

$$\begin{aligned} S_0 &= \sum_{i=0}^{2M-1} h_i e^{u_i} \pi_{i+1}, \\ S_1 &= \sum_{i=0}^{2M-1} h_i e^{u_{i+1}} \pi_i. \end{aligned}$$

Then clearly

$$S_0 \leq J \leq S_1.$$

But

$$\begin{aligned} S_0 &\geq \exp\{-\frac{LN}{M}\}(S_1 - h_0 e^{u_1} \pi_0) \\ &\geq (1 - \frac{\epsilon}{10})(\bar{f} - \frac{\epsilon}{10}\bar{f} - \frac{\epsilon^2}{90}\bar{f}) \\ &\geq (1 - \frac{\epsilon}{4})\bar{f}. \end{aligned}$$

(The second inequality uses $\pi_0 \leq 1, e^{u_1} \leq \frac{\epsilon}{10}\bar{f}e^{\epsilon/10} \leq \frac{\epsilon}{9}\bar{f}$ and $h_0 \leq \frac{\epsilon}{10}$.)

But $\bar{f} \geq S_0$ and so we need only estimate S_0. Equivalently we need to estimate the π_i. Suppose we can compute $\hat{\pi}_i$ such that

$$|\frac{\hat{\pi}_i}{\pi_i} - 1| \leq \frac{\epsilon}{2} \text{ for } i = 0, 1, ..., 2M-1.$$

(We will see shortly that we have fixed things so that π_{2M-1} is sufficiently large.) Under these circumstances if

$$\hat{S}_0 = \sum_{i=0}^{2M-1} h_i e^{u_i} \hat{\pi}_{i+1}$$

then

$$(1 - \frac{\epsilon}{2})(1 - \frac{\epsilon}{4})\bar{f} \leq \hat{S}_0 \leq (1 + \frac{\epsilon}{2})\bar{f}$$

and we are done. Observe next that

$$\pi_i = \frac{\text{vol}_n(K_i)}{\text{vol}_n(K)} \text{ for } i = 0, 1, ..., 2M-1$$

where

$$K_i = \{x \in K : f(x) \geq e_{u_i}\}.$$

Now the K_i are convex sets and it remains only to discuss their guarantees. Since $K_i \subseteq K$ for each i, we have no worries about the outer ball. It is the inner ball of K_{2M-1} that we need to deal with.

Now letting $a_t = (1-t)a^* + ta$ for $0 \leq t \leq 1$ we find that K contains the ball $B(a_t, \rho_t)$ where $\rho_t = \frac{tr}{R}$. Then if

$$\tau = \frac{R}{r}\exp\{L_1 - L_3 - \frac{L_2}{M}\}$$

(we can make L_3 large enough so that $0 < \tau < 1$)

then $x \in B(a_\tau, \rho_\tau)$ implies

$$\begin{aligned} f(a^*) - f(x) &\leq e^{L_3}\frac{\tau r}{R} \\ &= f(a^*)\exp\{-\frac{L_2}{M}\} \end{aligned}$$

and so $K_{2M-1} \supseteq B(a_\tau, \rho_\tau)$ and we have a guarantee of $(a_\tau, \rho_\tau, 2R)$ for each K_i. Thus we can approximate $\bar{f}$ in time polynomial in L and $\frac{1}{\epsilon}$.

It should be observed that Applegate and Kannan [2] have a more efficient integration algorithm for log-concave functions.

5.2 Counting linear extensions

We noted in Section 3.2 that determining the number of linear extensions of a partial order can be reduced to volume computation (and so it can be approximated by the methods of Section 4). The volume approximation algorithm of Dyer, Frieze and Kannan applied (in the notation of Section 3.2) to $P(\prec)$ gave the first (random) polynomial time approximation algorithm for estimating $e(\prec)$. However, Karzanov and Khachiyan [19] have recently given an improvement to the algorithm for this application which is more natural, and which we will now outline. Observe first that it suffices to be able to generate an (almost) random linear extension of $\prec$. For an incomparable pair i, j under $\prec$, let ρ_{ij} denote the proportion of linear extensions π with $\pi^{-1}(i) < \pi^{-1}(j)$. It is known, Kahn and Saks [17], that for some i, j we have $\min\{\rho_{i,j}, \rho_{j,i}\} \geq \frac{3}{11}$. Thus by repeated sampling we will be able to determine, for some i, j, a close approximation to the proportion of linear extensions with $\pi^{-1}(i) < \pi^{-1}(j)$ – choose the i, j for which the estimate gives the largest minimum. We then add $i \prec j$ to the partial order and proceed inductively until the order becomes a permutation and then our estimate is the product of the inverses of the proportions that we have found. This requires us to generate $O(n \log n)$ linear extensions.

To generate a random linear extension we do a random walk on $E(\prec)$. At a given extension π we do nothing with probability $\frac{1}{2}$, otherwise we choose a random integer i between 1 and $(n-1)$. If $\pi(i) \not\prec \pi(i+1)$ then we get a new permutation π' by interchanging $\pi(i)$ and $\pi(i+1)$. Let us say that in these circumstances π, π' are adjacent. The steady state of this walk is uniform over linear extensions and so the main interest now is in the conductance Φ of this chain which is

$$\min\left\{\frac{b(X)}{(2n-2)|X|} : |X| \leq \tfrac{1}{2}e(\prec)\right\}$$

where

$$b(X) = |\{(\pi, \pi') : \pi \in X, \pi' \notin X \text{ are adjacent}\}|.$$

So let $X \subseteq E(\prec)$ satisfy $|X| \leq e(\prec)/2$. Let $S_X = \bigcup_{\pi \in X} S_\pi$ and A_X be the $(n-1)$-dimensional volume of the common boundary of S_X and $S_{E(\prec)/X}$. Now a straightforward calculation (using a two-dimensional rotation followed by an application of (1)) shows that each simplicial face of this boundary has $(n-1)$-dimensional volume $\sqrt{2}/(n-1)!$. In the notation of Theorem 3, with $F(x) = 1$ and the ℓ_∞ norm, we see that the unit normal u to any face of the common boundary has $\|u\|^* = \sqrt{2}$. Thus $\mu'(S_X) = \sqrt{2}A_X$. Applying the theorem we obtain

$$\sqrt{2}A_X \geq \frac{2|X|}{n!}$$

since diam(K)=1 here.Thus

$$b(X) = A_X\frac{(n-1)!}{\sqrt{2}} \geq \frac{|X|}{n}.$$

and so

$$\Phi \geq \frac{1}{2n(n-1)}.$$

and we can generate a random linear extension in polynomial time. Note that this estimate is better by a factor of $\sqrt{n}$ than that given in [19]. (This order of improvement was, in fact, conjectured in [19].) Applying similar arguments to those in Section 4 we see that we can estimate $e(\prec)$ to within ϵ, with probability at least $(1-\xi)$ in $O(n^6\epsilon^{-2}(\log n)^2 \log(n/\epsilon)\log(1/\xi))$ time.

5.3 Mathematical Programming

We can use our algorithm to provide random polynomial time algorithms for approximating the expected value of some stochastic programming problems. Consider first computing the expected value of $v(b)$ when $b = (b_1, b_2, \ldots b_m)$ is chosen uniformly from a convex body $K \subseteq \mathbf{R}^m$ and

$$\begin{aligned} v(b) = \max \quad & f(x) \\ \text{subject to} \quad & g_i(x) \leq b_i \qquad (i = 1, 2, \ldots, m) \end{aligned}$$

To estimate $\mathbf{E}v(b)$ we need to estimate $\int_{b \in K} v$ and divide it by an estimate of the volume of K. We thus have to consider under what circumstances the results of Section 4 can be applied. If f is concave and $g_1, g_2, \ldots, g_m$ are all convex then v is concave and we can estimate $\mathbf{E}v$ efficiently if we know that v is uniformly bounded below for $b \in K$.

Observe also that we will be able to estimate $\Pr(v(b) \geq t)$ by randomly sampling b and computing $v(b)$, provided this probability is large enough.

Of particular interest is the case of PERT networks where the b_i represent (random) durations of the various activities and f represents the completion time of the project. The results here represent a significant improvement, at least in theory, over the traditional heuristic method of assuming one critical path and applying a normal approximation. As another application consider computing the expected value of $\phi(c)$ when $c = (c_1, c_2, \ldots c_n)$ is chosen uniformly from some convex body $K \subseteq \mathbf{R}^n$ and

$$\begin{aligned} \phi(c) = \quad & \min \ cx \\ \text{subject to} \quad & g_i(x) \leq b_i \qquad (i = 1, 2, \ldots, m) \end{aligned}$$

Now $\phi(c)$, being the supremum of linear functions, is concave and we will be able to estimate the expectation of ϕ when ϕ can be computed efficiently. The same remark holds for computing $\Pr(\phi(c) \geq t)$.

As a final example here, suppose that we have a linear program

$$\begin{aligned} \min \quad & cx & & \\ \text{subject to} \quad & Ax & = & \ b \\ & x & \geq & \ 0. \end{aligned}$$

Suppose that (b, c) is chosen uniformly from some convex body in $\mathbf{R}^{m+n}$. Suppose that B is a basis matrix (i.e. an $m \times m$ non-singular submatrix of A). Sensitivity analysis might require us to estimate the probability that B is the optimal basis. This can be done efficiently since it amounts to computing $\mathrm{vol}_{m+n}(K_{opt})/\mathrm{vol}_{m+n}(K)$ where K_{opt} is the convex set

$$K \cap \{c_j \geq c_B B^{-1} a_j : j = 1, 2, \ldots, n\} \cap \{B^{-1}b \geq 0\}.$$

(Here we are using common notation: a_j is column j of A and c_B is the vector of basic costs.)

5.4 Learning a halfspace

This problem was brought to our attention by Manfred Warmuth who suggested that volume computatation might be useful in solving the problem. The method described here is due to the authors and Ravi Kannan. We

describe here the application of good volume estimation to a problem in learning theory. Student X is trying to learn an inequality

$$\sum_{j=1}^{n} \pi_j x_j \geq \pi_0.$$

The unknowns are $\pi_j \geq 0$, $(j = 0, 1, \ldots, n)$ and X's aim is to be able to answer questions of the form "What is the sign of $x \in \mathbf{R}^n$ relative to this inequality ?" Here $\text{sign}(x, \pi) = +$ if $\sum_{j=1}^{n} \pi_j x_j \geq \pi_0$, and $-$ otherwise. There is a teacher Y who provides X with an infinite sequence of examples $z^{(t)}, t = 1, 2, \ldots$. Given an example $z^{(t)}$, X must make a guess at $\text{sign}(z^{(t)}, \pi)$ and then Y will reveal whether or not X's guess is correct or not.

We assume that there is an $L \geq 2$ such that $z^{(t)} \in \Omega = \{0, 1, \ldots, L-1\}^n$. Integrality is not a major assumption and non-negativity can be assumed, at the cost of doubling the number of varables, if X treats arbitrary components as the difference of two non-negative components. The problem we have to solve is to design a strategy for X which minimises the total number of errors made. If there is no bound on component size then, even for n=2, Y can construct a hyperplane in response to any answers which is consistent with X being wrong every time.

We define an equivalence relation $\sim$ on $\mathbf{R}^{n+1}$ by

$$\pi^{(1)} \sim \pi^{(2)} \text{ if } \text{sign}(x, \pi^{(1)}) = \text{sign}(x, \pi^{(2)}) \text{ for all } x \in \Omega.$$

X cannot hope to compute π exactly and instead aims to find $\pi' \sim \pi$. Moreover we will see that it is advantageous for X to assume π satisfies

$$\sum_{j=1}^{n} \pi'_j x_j \neq \pi'_0 \text{ for all } x \in \Omega. \tag{52}$$

There is always a small perturbation $\hat{\pi}$ of π, $\hat{\pi} \sim \pi$, that satisfies (52). We can also assume that $0 \leq \pi_j \leq 1, j = 0, 1, \ldots, n$ since scaling does not affect signs. For $x \in \Omega$ let $a_x = (x, -1)$ and H_x be the hyperplane (in π space) $\{\pi \in \mathbf{R}^{n+1} : a_x \cdot \pi = 0\}$. These hyperplanes partition $\mathbf{R}^{n+1}$ into an arrangement of open cones. Consider the partition $S_1, S_2, \ldots$ that these cones induce of $C_{n+1} = [0, 1]^{n+1}$. Note that if two vectors π, π' lie in the same S_i then $\pi \sim \pi'$. If π satisfies (52) then it lies in an S_i of dimension $n + 1$ and volume at least $\nu = (nL)^{-n^2}$.

It follows from these remarks that the following algorithm never makes more than $O(n^2(\log n + \log L))$ mistakes:

Keep a polytope P within whose interior π is known to lie; initially $P = C_{n+1}$;
for $t = 1, 2, \ldots$ **do**
begin
    let $P_+ = \{\pi : \pi \cdot z \geq 0\}$ and $P_- = \{\pi : \pi \cdot z \leq 0\}$;
    compute $\text{vol}_n(P_+)$, $\text{vol}_n(P_-)$;
    answer $\pi \in P_+$ if this larger volume, otherwise P_-;
    if you are wrong, having chosen P_+ say, then $P := P_-$
end

Each mistake halves the volume of P, which starts at 1. On the other hand, $\text{vol}_{n+1}(P) \geq \nu$ and the result follows. Although we cannot compute volumes exactly, a $\frac{1}{10}$-approximation will guarantee that the volume of P reduces by $\frac{3}{4}$, say, which suffices. Also we have a probabilistic error in our computation. To keep the overall probability of error down to ξ say, we need only keep the error probability for each computation down to $\xi / \log_{4/3}(1/\nu)$.

This analysis improves the the number of errors required by a factor of n from the method proposed by Maass and Turán [25].

6 The number of random bits

We have already seen in Section 3.1 that a deterministic algorithm cannot guarantee a good approximation to volume in the oracle model. We return now to our remarks about nondeterministic computation, using the notation of Section 3.1. We assume we are interested in ϵ-approximation, with $\epsilon = \Theta(n^\alpha)$ for some $\alpha \in \mathbf{R}$, i.e. *polynomial* approximation. As usual, we have a convex body $K \subseteq \mathbf{R}^n$ described by an oracle as in Section 2.

Suppose that we have a randomised algorithm which makes at most $m(n)$ calls on the oracle for a polynomial m, and that it uses at most $b = n - \omega \log_2 n$ random bits, where $\omega = \omega(n) \to \infty$. Then $M(n) \leq 2^b m(n)$. Thus the relative error of approximations from this algorithm cannot be guaranteed to be better than $(2^{n-b}/m(n))^{1/2} \geq n^{\omega/4}$ for large n. So we cannot polynomially approximate with much less than n (truly) random bits.

On the other hand, a result of Nisan [27] shows that only $O(n(\log n)^2)$ truly random bits are actually necessary. This is rather surprising, but it follows from the fact we need only $O(n \log n)$ space to maintain the random walk and accumulate the required information to make our estimate. (We need not, of course, worry about the space needed by the oracle.) Nisan's result states that, in an algorithm using space S and R random bits, the random bits can be supplied by a pseudorandom generator which uses only $O(S \log(R/S)$ truly random bits. One then observes from Section 4 that in our case, for polynomial approximations, R is polynomially bounded in n.

Acknowledgements

We thank Ross Willard for providing us with the first paragraph of historical information and David Applegate, Ravi Kannan and Umesh Vazirani for general comments. We thank Nick Polson for his observation on the estimation of P in Section 4.1 which saved us from a much more complicated argument. We thank Russell Impagliazzo for bringing Nisan's paper to our attention.

References

[1] D. Aldous and P. Diaconis, Shuffling cards and stopping times, *American Mathematical Monthly* **93** (1986), 333–348.

[2] D. Applegate and R. Kannan, Sampling and integration of near log-concave functions, Computer Science Department Report, Carnegie-Mellon University, 1990.

[3] I. Bárány and Z. Füredi, Computing the volume is difficult, *Proc. 18th Annual ACM Symposium on Theory of Computing* (1986), 442–447.

[4] B.Bollobás, Random Graphs, Academic Press, 1985.

[5] P. Bérard, G. Besson and A. S. Gallot, Sur une inégalité isopérimétrique qui géneralise celle de Paul Levy-Gromov, *Inventiones Mathematicae* **80** (1985), 295–308.

[6] G. Brightwell and P. Winkler, Counting linear extensions is #P-complete, DIMACS Technical Report 90-49, 1990.

[7] Yu. D. Burago and V. A. Zalgaller, *Geometric inequalities*, Springer-Verlag, Berlin, 1988.

[8] R. Courant and H. Robbins, *What is mathematics ?*, Oxford University Press, London, 1941.

[9] M. E. Dyer and A. M. Frieze, On the complexity of computing the volume of a polyhedron, *SIAM J. Comput.* **17** (1988), 967–974.

[10] M. E. Dyer, A. M. Frieze and R. Kannan, A random polynomial time algorithm for approximating the volume of convex bodies, *Proc. 21st Annual ACM Symposium on Theory of Computing* (1989) 375-381 (full paper will appear in *J. ACM.*)

[11] G. Elekes, A geometric inequality and the complexity of computing volume, *Disc. Comp. Geom.* **1** (1986), 289–292.

[12] W. Feller, *Introduction to the theory of probability and its applications Vol. I*, Wiley, New York, 1968.

[13] M. Grötschel, L. Lovász and A. Schrijver, *Geometric algorithms and combinatorial optimization*, Springer-Verlag, 1988.

[14] W. Hoeffding, Probability inequalities for sums of bounded random variables, *J. Amer. Stat. Assoc.* **58** (1963) 13-30.

[15] M. R. Jerrum and A. J. Sinclair, Approximating the permanent, *SIAM J. Comput.* **18** (1989) 1149-1178.

[16] M. R. Jerrum, L. G. Valiant and V. V. Vazirani, Random generation of combinatorial structures from a uniform distribution, *Theoretical Computer Science* **43** (1986), 169–188.

[17] J.Kahn and M.Saks,Every poset has a good comparison, *Proc. 16th Annual IEEE Symposium on Foundations of Computer Science* (1984) 299-301.

[18] R. M. Karp and M. Luby, Monte-Carlo algorithms for enumeration and reliability problems, *Proc. 24th Annual IEEE Symposium on Foundations of Computer Science* (1983) 56-64.

[19] A. Karzanov and L. G. Khachiyan, On the conductance of order Markov chains, Technical Report DCS TR 268, Rutgers University, 1990.

[20] L. G. Khachiyan, On the complexity of computing the volume of a polytope, *Izvestia Akad. Nauk SSSR, Engineering Cybernetics* **3** (1988), 216–217 (in Russian).

[21] J. Lawrence, Polytope volume computation, Preprint NISTIR 89-4123, U.S. Dept. of Commerce, National Institute of Standards and Technology, Center for Computing and Applied Mathematics, Galthersburg, 1989.

[22] H. W. Lenstra, Integer programming with a fixed number of variables, *Math. Oper. Res.* **8** (1983), 538–548.

[23] N. Linial, Hard enumeration problems in geometry and combinatorics, *SIAM J. Alg. Disc. Meth.* **7** (1986), 331–335.

[24] L. Lovász and M.Simonovits, The mixing rate of Markov chains, an isoperimetric inequality, and computing the volume, Preprint 27/1990, Mathematical Institute of the Hungarian Academy of Sciences, 1990.

[25] W. Maass and G.Turán, On the complexity of learning from counterexamples, *Proc. 30th Annual IEEE Symposium on Foundations of Computer Science* (1989) 262-267.

[26] P. Matthews, Generating a random linear extension of a partial order, University of Maryland (Baltimore County) Technical Report, 1989.

[27] N. Nisan, Pseudorandom generators for space-bounded computation, *Proc. 22nd Annual ACM Symposium on Theory of Computing* (1990) 204-212.

[28] L. E. Payne and H. F. Weinberger, An optimal Poincaré inequality for convex domains, *Arch. Rat. Mech. Anal.* **5** (1960), 286–292.

[29] R. T. Rockafellar, *Convex analysis*, Princeton University Press, Princeton, New Jersey, 1970.

[30] A. J. Sinclair and M. R. Jerrum, Approximate counting, generation and rapidly mixing Markov chains, *Information and Computation* **82** (1989), 93–133.

[31] A. H. Stone and J. W. Tukey, Generalized "sandwich" theorems, *Duke Math. J.* **9** (1942), 356–359.