A RANDOM POLYNOMIAL TIME ALGORITHM FOR APPROXIMATING THE VOLUME OF CONVEX BODIES

by

Martin Dyer[1] Alan Frieze[2] Ravi Kannan[3]

(June 15, 1995)

Abstract

We present a randomised polynomial time algorithm for approximating the volume of a convex body K in n-dimensional Euclidean space. The proof of correctness of the algorithm relies on recent theory of rapidly mixing Markov chains and isoperimetric inequalities to show that a certain random walk can be used to sample nearly uniformly from within K.

Introduction

In this paper we give an algorithm for approximating the volume of a convex body in Euclidean space. Our algorithm is a randomised polynomial time bounded algorithm. In other words, suppose we are given a convex body K, determined by a membership oracle (see Grötschel, Lovász and Schrijver [1988]) and a relative error bound ϵ. Then, our algorithm takes time bounded by a polynomial in n, the dimension of the body K and $1/\epsilon$. With probability at least $3/4$, it finds an ϵ approximation to the volume of K. (Here, as usual, we count unit time per call to the oracle. Observe that we can make the failure probability as small as we like by repeatedly running the algorithm and taking the median value as output. See [Karp and Luby 1983]

[1]School of Computer Studies, University of Leeds, Leeds, U.K.

[2]Mathematics Department, Carnegie-Mellon University

[3]Department of Computer Science, Carnegie-Mellon University. Supported by NSF grants ECS-8418392 and CCR-8805199.

and [Jerrum, Valiant and Vazirani 1986].) Our result should be contrasted with results of Elekes [1986], Bárány and Füredi [1986], and Dyer and Frieze [1988]. In particular the first two of these references show that with such an oracle it is not possible to approximate the volume of a convex set within even a polynomial factor in deterministic polynomial time. In fact Bárány and Füredi showed that the best one could do was to get within a factor of the volume which is exponential in n. Grötschel, Lovász and Schrijver [1988] had already given such an approximation algorithm. Furthermore Dyer and Frieze [1988] show that if K is a polyhedron, given either by a list of its facets or its vertices then it is # P-hard to compute the volume of K exactly. By comparing our results with these, we see that here is a case where randomness gives a super-polynomial speed-up in computing power.

We remark that one consequence of our algorithm is that the number of linear extensions of a partial order can be similarly approximated. See, for example, [Lovász, p. 61].

Our algorithm is based on a scheme for sampling nearly uniformly from within K. To do this, we place a grid consisting of cubes of side $O(1/n^{5/2})$ and do a random walk over the cubes in the grid that intersect a slightly smoother enlargement of K. For this random walk, it is not difficult to show that eventually it "settles down" to being nearly uniform. What is much more difficult to show is that the time taken to settle down is polynomial. To do this we use results on the theory of rapidly mixing Markov chains. In particular we employ an extremely useful result of Sinclair and Jerrum [1988] which relates the rapid mixing property to structural properties of the chain which are somewhat easier to establish. We note that Jerrum and Sinclair [1988] have used this result to rigorously verify Broder's algorithm [1986] for approximating dense permanents. These methods are likely to

yield further interesting results. See Aldous [1981] for an expository paper on other methods for establishing the rapid mixing property. The key step in the Sinclair-Jerrum approach is to establish an isoperimetric inequality for the graph underlying the random walk. To do this we use a result from differential geometry, i.e. the isoperimetric inequality of Bérard, Besson and Gallot [1985] which generalises the more classical inequality of Lévy-Gromov (see Milman and Schechtmann [1980]) on the volume of the boundary of subsets of smooth Riemannian manifolds with positive curvature.

In the next few sections we will make these arguments more precise. In §1, we describe the random walk and the algorithm. In §2 we will show that the algorithm has the claimed properties under the assumption that the *conductance* [Sinclair and Jerrum 1988] of our Markov chain is at least $1/q(n)$ where, $q(\cdot)$ is a polynomial. In §3, we will verify this claim. The final section contains some technical Lemmas.

Notation and values used throughout

$n \geq 3$ is the dimension of the body whose volume is to be approximated, and $0 < \epsilon < 1$ is the desired degree of approximation.

$$\delta = \frac{1}{20n^{5/2}}$$

$$\alpha = 12\sqrt{2}n^{3/2}\delta \qquad \alpha' = \delta/(2\sqrt{n}).$$

$$r = \sqrt{n}(n+1)$$

$$\rho = 1 - (1/n) \qquad k = \lceil \log_{1/\rho} r \rceil$$

$$m = \lceil \frac{700k^2}{\epsilon^2} \log 8k \rceil$$

$$\tau = \lceil 10^{17} n^{19} \log(\left(\frac{3r}{\delta}\right)^n \frac{300k}{\epsilon}) \rceil$$

$$\beta = \lceil \log_2(\frac{900k\delta n^{3/2}}{\epsilon}) \rceil \qquad \eta = 2^{-\beta}\delta$$

All logarithms are to the base e unless otherwise specified.

B is the unit ball in $\mathbf{R}^n$ with the origin as center, and σ_n denotes its surface area.

By a "convex body" we mean a closed, bounded convex set of non-zero volume.

For any convex set K and non-negative real number α, we denote by αK the "dilation" of K by a factor of α, i.e. $\alpha K = \{\alpha x : x \in K\}$.

If $T \subseteq S \subseteq \mathbf{R}^m$, we denote the "boundary" of T with respect to S by $\partial_S T$. This is the set of points x in the closure of T such that any ball in $\mathbf{R}^m$ with x as center intersects $S \setminus T$. Usually, the context will make clear what S is, so we will denote $\partial_S T$ as ∂T.

For any set K in $\mathbf{R}^m$ and a non-negative real number λ, we denote by $K(\lambda)$ the set of points at distance at most λ from K. If K is convex, it is easy to see that $K(\lambda)$ is too.

All our convex bodies will be given a so-called "well-guaranteed membership oracles" – i.e. we will be given a sphere containing the body, a sphere contained in the body, both of non-zero radius (this is called the "guarantee" – see Grötschel, Lovàsz and Schrijver [1988] for a discussion of why many problems are meaningless without these guarantees) and a black box, which presented with any point x in space, either replies that x is in the convex body or that it is not. Grötschel, Lovàsz and Schrijver [1988] show that from such an oracle, we may construct (in polynomial time) a so-called weak separation oracle (see their §4.4.) For convex bodies presented by a weak separation oracle, they also show that we can find in polynomial time a (nonsingular) affine transformation so that, on applying the transformation,

the body is "well-rounded", i.e. the body contains the unit ball with the origin as center and is contained in a concentric ball of radius $r = \sqrt{n}(n+1)$ where n is the dimension of the body. (Polyhedra of positive volume fit this category. Polyhedra of zero volume can be detected in polynomial time by the ellipsoid algorithm.)

1. A random walk

Throughout we assume that space ($\mathbf{R}^n$) is divided into cubes of side δ, i.e. cubes of the form $\{x : m_i\delta \leq x_i \leq (m_i+1)\delta \text{ for } i = 1, 2, \ldots, n\}$ where the m_i are integers. Note that the cubes are defined as closed sets.

Suppose K is any well-rounded convex body. Central to our algorithm will be the following random walk through the cubes which intersect $K(\alpha)$. (Reminder : see notation section for the value of α.) The random walk starts at any cube intersecting $K(\alpha)$, for example the cube containing the origin. At each step, it stays in the present cube or it moves from the present cube to one of its adjacent cubes (a cube that shares an $(n-1)$ dimensional face) as follows : it chooses a facet of the present cube each with probability $1/(2n)$. If the cube across the chosen facet intersects $K(\alpha)$, the random walk moves to that cube, else it stays in the present cube. The random walk gives us a Markov chain with the states corresponding to the cubes. The underlying undirected graph (containing edges corresponding to the transitions of non-zero probability) is connected as the following argument shows : if a cube C intersects $K(\alpha)$ and x is in $C \cap K(\alpha)$ the line joining x to the origin of course lies inside $K(\alpha)$. The sequence of cubes intersected by the line gives us a path from our cube to the cube containing the origin : if the line "passes"

from a cube C_1 to a cube C_2 through an $(n-i)$ dimensional face shared by C_1, C_2, then there is obviously a path of length i from C_1 to C_2 in the graph. We will later refer to the random walk described here as the *natural random walk*[4] on K, although we really walk over the cubes that intersect $K(\alpha)$. The reason for walking over the cubes that intersect $K(\alpha)$ rather than the cubes that intersect K is that $K(\alpha)$ is a little "smoother" than K ; in particular, for any point $x \in K(\alpha)$, there is a sphere of radius α which contains x and is contained in $K(\alpha)$. This fact will be used in our proofs. Note also that $K(\alpha)$ is "close" to K, in fact it will be easy to see (cf. Proposition 1 of §4) that $(1+\alpha)K$ contains $K(\alpha)$. Thus, at least intuitively, we see that we may replace K by $K(\alpha)$ for purposes like computing the volume approximately.

We will be given K by an oracle, and this will not let us decide precisely whether a particular cube intersects $K(\alpha)$. We will therefore modify the natural random walk so that the set of cubes over which the random walk is executed includes all of those that intersect $K(\alpha)$ plus some other cubes each of which intersects $K(\alpha+\alpha')$ where $\alpha' = \delta/(2\sqrt{n})$, as defined earlier. The modification is as follows : it is easy to see that for any cube C, there is a membership oracle for $C(\alpha+\alpha')$.[5] Using this, and the separation oracle for K, with the well-known techniques of Grötschel, Lovász and Schrijver [1988] based on the ellipsoid algorithm, we have a deterministic polynomial time algorithm that terminates with either

(i) a point $x \in C(\alpha+\alpha') \cap K$ whence we know that $C \cap K(\alpha+\alpha')$ is nonempty.

or

[4]For technical reasons, we will have to modify the natural random walk.

[5]The nearest point in a cube from an exterior point can be found by "rounding " the coordinates of the point on to the cube.

(ii) an ellipsoid of volume at most $(\alpha')^n \sigma_{n-1} n^{-2} (\frac{2}{\pi})^{n-2} r^{-n+1}$ containing $C(\alpha + \alpha') \cap K$,

whence we will show (cf. Proposition 5, §4) that $C(\alpha) \cap K$ is empty or equivalently $C \cap K(\alpha)$ is empty. (See notation section for σ_{n-1}.)

The random walk will go to cubes for which the alternative (i) occurs and will not go to those for which (ii) occurs. We will show (cf. Proposition 11 (proof), §4) that any cube for which alternative (i) occurs must in fact either itself intersect $K(\alpha)$ or one of its adjacent cubes must, so this walk does not "stray" too far from the original, a fact that will be useful later. If (i) is the result of the algorithm, we say that the cube C *weakly intersects* the convex body $K(\alpha)$. A further technical modification is needed. In order to apply the theorem of Sinclair and Jerrum, we need to be sure that at each step, the walk has probability at least $1/2$ of staying in the same cube. This is achieved as follows : at each step, with probability $1/2$, the walk makes no attempt to change cubes. With probability $1/(4n)$ each it picks one of the facets of the current cube and moves accross to an adjacent cube if it weakly intersects $K(\alpha)$. Thus, in the interior of K, the probability of staying put is precisely $1/2$ and at the boundary, it is at least $1/2$. We call the random walk thus obtained the *technical random walk*.

We wish to show that, after a polynomial number of steps, the steady state probabilities of the (technical) Markov chain will be approximated with an exponentially small error. More precisely, suppose N is the number of states of the Markov chain and let the states be numbered $1, 2, \ldots, N$. Let p_{ij} be the probability of transition from state i to state j. The p_{ij} 's assume values 0 or at least $1/(4n)$. Let P be the matrix with the p_{ij} as entries and for any natural number t, we denote by $p_{ij}^{(t)}$ the entries of the matrix P^t, the t th power of P which represents the t step transition probabilities.

It is easy to see that our Markov chain is "irreducible", i.e. for each pair of states i, j, there is a natural number s such that $p_{ij}^{(s)}$ is nonzero. This follows since the graph of the natural random walk is connected, and each cube in the technical random walk is either included in the natural random walk or is adjacent to such a cube. Also the Markov chain can be seen to be aperiodic, i.e. $\gcd\{s : p_{ij}^{(s)} > 0\} = 1$ for all i, j. This follows from the facts that the graph is connected and each cube has a self-loop. Hence, the chain is "ergodic" [Feller 1968] and there exist "stationary" probabilities $\pi_1, \pi_2, \ldots, \pi_N > 0$ such that

$$\lim_{s \to \infty} p_{ij}^{(s)} = \pi_j \quad \forall i, j.$$

The vector π of π_j 's is the unique solution to the equations $\pi P = \pi$ and $\sum \pi_j = 1$. In our case, since P is symmetric, it is easy to see that all the π_j 's are equal. Thus also, the Markov chain is "time-reversible" : i.e. $p_{ij}\pi_i = p_{ji}\pi_j \quad (\forall i, j)$.

Our approach is as follows : we will use a result from Sinclair and Jerrum [1988] on time-reversible ergodic Markov chains to show that our Markov chain is "rapidly mixing", i.e. we will prove the following :

Theorem 1 For any i, j, and t, we have

$$|p_{ij}^{(t)} - \pi_j| \leq \left(1 - \frac{1}{10^{17} n^{19}}\right)^t.$$

∎

Thus, when t is a sufficiently large, yet polynomial function of n, (namely $t = \tau$ - see notation) the $p_{ij}^{(t)}$ are approximately equal. Roughly speaking, this gives us the ability to pick a random cube intersecting the convex body with uniform distribution in polynomial time. Using this, we will argue in the next section that the following algorithm does the job.

1. Let K be the convex body in $\mathbf{R}^n$ whose volume is to be found. Transform the body so that it is now well-rounded, i.e. now we have $B \subseteq K \subseteq rB$ where $r = \sqrt{n}(n+1)$. The determinant of the linear transformation gives the factor by which the volume is changed. We keep track of this.

2. Let $\rho = 1 - \frac{1}{n}$. Let $k = \lceil \log_{\frac{1}{\rho}} r \rceil$ and for $i = 0, 1, 2, \ldots, k$, let $\rho_i = \max\{\rho^i r, 1\}$. The algorithm will find for $i = 1, 2, \ldots, k$ an approximation to the ratio
$$\frac{\mathrm{Vol}_n(\rho_i K \cap rB)}{\mathrm{Vol}_n(\rho_{i-1} K \cap rB)}.$$
The ratio will be found by a sequence of "trials". In each trial, we first do the technical random walk on $K_{i-1} = \rho_{i-1} K \cap rB$ for τ steps. (The states of the random walk will be the cubes that weakly intersect $K_{i-1}(\alpha)$.) Suppose we are in cube $C = \{x : q_i\delta \leq x_i \leq (q_i+1)\delta\}$ after τ steps. We pick randomly (uniformly and independently) integers $\gamma_1, \gamma_2, \ldots, \gamma_n$ each from $\{0, 1, 2, \ldots, \gamma\}$ where $\gamma = 2^\beta - 1$. Let $x_0 = \left((q_1 + \frac{\gamma_1}{\gamma})\delta, (q_2 + \frac{\gamma_2}{\gamma})\delta, \ldots, (q_n + \frac{\gamma_n}{\gamma})\delta\right)$.

   If $x_0 \in K_{i-1}$ then we declare the trial a *proper* trial and check to see if $x_0 \in K_i$. If it does we declare the trial a *success*. This completes the trial. We repeat until we have made m proper trials and we keep track of the ratio of the number of successes to m. We will later show that with high probability, the ratio will be a good approximation to the ratio of volumes that we want to compute.

   Clearly this together with the fact that $K_k = K$ and the volume of $K_0 = rB$ is known in closed form gives us the volume of K, as required. Note that K_i contains ρK_{i-1}, so each of the ratios to be computed is

at least ρ^n which is known to be at least $1/4$. This fact will be required later.

Remark We conjecture that Theorem 1 can be considerably strengthened – i.e. the polynomial $O(n^{19})$ in that Theorem is not optimal. Whether this is true or not, a heuristic method would be to run the random walk above for many fewer than τ steps. See also Remark 8 of §5.

2. Proof of correctness of the algorithm

Consider the i th step of our algorithm. We first estimate the probability that a trial is declared proper. Let W be the set of cubes that weakly intersect $K_{i-1}(\alpha)$. Observe that $|W| \leq (3r/\delta)^n$. Then

$$\Pr(\text{proper trial}) = \sum_{C \in W} \Pr(\text{proper trial}|\text{walk ends in } C)\ \Pr(\text{walk ends in } C)$$

Consider a fixed $C \in W$ and let $a_C = \text{Vol}_n(C \cap K_{i-1})/\delta^n$. We imagine C divided into subcubes of side $\eta = 2^{-\beta}\delta$ and our sample point x_0 is equally likely to be the corner of any one of these subcubes.

Let now N_C^B be the number of "border" subcubes (i.e. which meet K_{i-1}, but are not fully contained in K_{i-1}) and $N_C = 2^{\beta n}$. Then with

$$\pi_C = \Pr(\text{proper trial}|\text{walk ends in} C),$$

we have

$$|a_C - \pi_C| \ \leq\ \frac{N_C^B}{N_C} \ =\ \zeta_C \text{ (say)}.$$

Now $\zeta = \sum_{C \in W} \zeta_C$ is $(\eta/\delta)^n$ times the total number of subcubes which meet K_{i-1}, but are not fully contained in it. Using Proposition 3 of §4, ζ is at most $3n^{3/2}\eta\,\text{Vol}_n(K_{i-1})/\delta^n$.

Now, using Theorem 1,

$$\begin{aligned}
\Pr(\text{proper trial}) &\leq \sum_{C \in W} (a_C + \zeta_C) \left(\frac{1}{|W|} + \left(1 - \frac{1}{10^{17} n^{19}}\right)^{\tau} \right) \\
&\leq \frac{\mathrm{Vol}_n(K_{i-1})}{\delta^n} (1 + 3n^{3/2}\eta) \left(\frac{1}{|W|} + \frac{\epsilon}{300k} \left(\frac{\delta}{3r} \right)^n \right), \\
&\quad \text{using the fact that } 1 + x \leq e^x \forall \text{ real } x \\
&\leq \frac{\mathrm{Vol}_n(K_{i-1})}{|W|\delta^n} (1 + \frac{\epsilon}{300k})^2 \\
&\leq \frac{\mathrm{Vol}_n(K_{i-1})}{|W|\delta^n} (1 + \frac{\epsilon}{100k}).
\end{aligned}$$

Similarly,

$$\Pr(\text{proper trial}) \geq \frac{\mathrm{Vol}_n(K_{i-1})}{|W|\delta^n} (1 - \frac{\epsilon}{100k}) \geq 0.33,$$

using Proposition 4 and the bounds on ϵ and k.

Observe that this lower bound is independent of the starting point of the random walk and so the number of proper trials occuring in s walks stochastically dominates the Binomial Bin(s, 0.33). Thus, with probability close to one, at least a quarter of any large number of trials will be proper.

We now consider the probability of success. By an identical argument to that above, we obtain

$$\frac{\mathrm{Vol}_n(K_i)}{|W|\delta^n} (1 - \frac{\epsilon}{100k}) \leq \Pr(\text{success}) \leq \frac{\mathrm{Vol}_n(K_i)}{|W|\delta^n} (1 + \frac{\epsilon}{100k}).$$

So, if $p = \Pr(\text{success} \mid \text{proper trial})$ and $\nu = \mathrm{Vol}_n(K_i)/\mathrm{Vol}_n(K_{i-1})$, we have

$$\nu(1 - \frac{\epsilon}{100k})(1 + \frac{\epsilon}{100k})^{-1} \leq p \leq \nu(1 + \frac{\epsilon}{100k})(1 - \frac{\epsilon}{100k})^{-1}$$

which implies $\frac{1}{5} \leq (1 - \frac{\epsilon}{49k})\nu \leq p \leq (1 + \frac{\epsilon}{49k})\nu$.

Let $\hat{m}$ be the number of successes after there have been m proper trials. It is a standard result from probability theory (for example, an easy consequence of Theorem 1 of Hoeffding [1963]), that for any positive $\lambda < 1$,

$$\Pr\left(|\frac{\hat{m}}{m} - p| \geq \lambda p\right) \leq 2e^{-\lambda^2 mp/3}.$$

$$\text{Hence,} \qquad \Pr\left(|\frac{\hat{m}}{m} - \nu| \geq \lambda\nu\right) \qquad \leq \Pr\left(|\frac{\hat{m}}{m} - p| \geq \left(\lambda - \frac{\epsilon}{20k}\right)p\right)$$

So with $\lambda = \frac{\epsilon}{5k}$ we have

$$\Pr\left(|\frac{\hat{m}}{m} - \nu| \geq \frac{\epsilon}{5k}\nu\right) \leq 2e^{-\frac{1}{3}(3\epsilon/20k)^2 mp} \qquad \leq 2e^{-\frac{3}{5}(\epsilon/20k)^2 m}$$

Now we must make k volume estimates and so assuming that we compute $\mathrm{Vol}_n(K_0)$ to within $1\pm\frac{\epsilon}{2}$ we see that the above algorithm computes an estimate v satisfying

$$(1 - \frac{\epsilon}{2})(1 - \frac{\epsilon}{5k})^k \leq \frac{v}{\mathrm{Vol}_n(K)} \leq (1 + \frac{\epsilon}{2})(1 + \frac{\epsilon}{5k})^k$$

with probability at least

$$1 - 2ke^{-\frac{3}{5}(\epsilon/20k)^2 m}$$

The reader may check, with the constants given in the notation section, that v turns out to be within $1\pm\epsilon$ of $\mathrm{Vol}_n(K)$ with probability at least $\frac{3}{4}$ as required.

The running time of the algorithm is that needed to solve

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

3. The Markov chain is rapidly mixing

Let $\mathcal{M}$ be an ergodic Markov chain with states $\{1, 2, \ldots, N\}$, transition probabilities p_{ij} and stationary probabilities $\pi_1, \pi_2, \ldots, \pi_N$. Sinclair and Jerrum define, for any subset S of states, the *capacity* C_S of S to be $\sum_{i \in S} \pi_i$ and the *ergodic flow* out of S to be

$$\sum_{i \in S, j \notin S} p_{ij} \pi_i.$$

They also define the *conductance* Φ_S of S to be the ergodic flow out of S divided by the capacity of S. Finally, they define the conductance of the whole chain to be

$$\Phi = \min_{S: C_S \leq 1/2} \Phi_S.$$

Intuitively, Φ measures the minimum relative connection strength between subsets of the states and we expect that if Φ is relatively high, the random walk will not "get stuck" in some subset S of states, thus it will "mix" rapidly. The following is a direct consequence of their main Theorem.

Theorem 2 (Sinclair and Jerrum) For a time-reversible ergodic Markov chain with all the π_j 's equal, and $p_{ii} \geq 1/2$ for all i,

$$|p_{ij}^{(t)} - \pi_j| \leq \left(1 - \frac{\Phi^2}{2}\right)^t \qquad \forall i, j.$$

∎

We will show that the conductance of our Markov chain cannot be too small. First, we work on the natural Markov chain whose states are precisely the cubes that intersect $K(\alpha)$. (We should of course talk about $K_i(\alpha)$, but we will drop the subscript for clarity). We then extend the result to the technical version whose states are all cubes that weakly intersect $K(\alpha)$.

For any subset S of states (of the technical Markov chain), we denote by $\bar{S}$ the complementary set of states and by $(S, \bar{S})$ the set of edges in the

underlying transition graph from a vertex of S to a vertex of $\bar{S}$. Since all the π_j's are equal, and for any edge (i,j) in the graph, $p_{ij} = 1/(4n)$, we have

$$\Phi_S = \frac{\gamma(S)}{4n} \qquad \text{where} \qquad \gamma(S) = \frac{|(S,\bar{S})|}{|S|}.$$

So a lower bound on Φ will follow from a lower bound on the minimum of $\gamma(S)$. We start first with the natural Markov chain. In Lemma 1 below, $\gamma(S)$ now refers to edges and vertices in the transition graph of the natural Markov chain.

Lemma 1 $\gamma(S) \geq \frac{\delta^2}{2400n^{7/2}}$ for any subset S of states in the natural Markov chain with $C_S \leq \frac{1}{2}$.

Proof : A "cube" means a cube that intersects $K(\alpha)$. A cube is called a "border cube" if it intersects both $K(\alpha)$ and the complement of $K(\alpha)$ and it is called an "inside cube" if it is wholly contained in $K(\alpha)$. We will also look upon a subset S of states as the union of whole cubes corresponding to the states. We let S^B be the border cubes in S and S^I be the inside cubes in S. Now, by Proposition 10, for any subset S of states,

$$|S^B| \leq 2n|(S,\bar{S})| + 18|S^I|.$$

We deduce that

$$\mathrm{Vol}_n(S \cap K(\alpha)) \geq |S^I|\delta^n = (|S| - |S^B|)\delta^n \geq (|S| - 2n|(S,\bar{S})| - 18|S^I|)\delta^n$$

$$\geq (|S| - 2n|(S,\bar{S})|)\delta^n - 18\mathrm{Vol}_n(S \cap K(\alpha)).$$

Hence

$$\mathrm{Vol}_n(S \cap K(\alpha)) \geq \tfrac{1}{19}\delta^n(|S| - 2n|(S,\bar{S})|).$$

Let S be an arbitrary subset of states with $|S| \leq N/2$. This S will be fixed for the rest of this proof. We need the following basic fact from analysis (for

example, see Gilbarg and Trudinger §7.2 [1983]) : every convex body can be approximated arbitrarily closely by a convex body containing it whose surface forms a smooth ($\mathcal{C}^\infty$) Riemannian manifold. Let KK be a convex body such that ∂KK forms a smooth Riemannian manifold, $K(\alpha) \subseteq KK$ and the set of cubes intersected by KK is precisely the set of cubes intersected by $K(\alpha)$. (Since the cubes are defined as closed sets, the last condition can be ensured by a sufficiently close approximation to $K(\alpha)$.)

If $\gamma(S) \geq \frac{1}{4n}$, then the Lemma is proved, so assume that $\gamma(S) \leq \frac{1}{4n}$. Then, letting $T = S \cap KK$ and $\bar{T} = \bar{S} \cap KK$, we have

$$\mathrm{Vol}_n(T) \geq \mathrm{Vol}_n(S \cap K(\alpha)) \geq \frac{\mathrm{Vol}_n(S)}{38}.$$

By the classical isoperimetric inequality, [Milman and Schechtman 1980, page 125][6]

$$\mathrm{Vol}_{n-1}(\partial T) \geq \frac{n\mathrm{Vol}_n(T)(c_n)^{1/n}}{(\mathrm{Vol}_n(T))^{1/n}}.$$

where $c_n = \mathrm{Vol}_n(B)$.

But we know that $\mathrm{Vol}_n(T) \leq \mathrm{Vol}_n(KK) \leq c_n r^n (1+\alpha+\delta\sqrt{n})^n \leq 2.5 c_n r^n$. Substituting this for the denominator for the above expression, we get

$$\mathrm{Vol}_{n-1}(\partial T) \geq \frac{\mathrm{Vol}_n(S)}{100 n^{1/2}}.$$

Consider the set $T_1 = (\partial T \setminus \partial KK)$. This set consists of the union of parts of facets of cubes with the property that on one side of the facet is a cube in S and on the other side is a cube in $\bar{S}$. So we have $|(S, \bar{S})| \geq \mathrm{Vol}_{n-1}(T_1)/\delta^{n-1}$. Thus if the volume of T_1 is at least half the volume of ∂T, by the above inequality on $\mathrm{Vol}_{n-1}(\partial T)$, we have a lower bound on $\gamma(S)$, of $\frac{1}{4000n^3}$. This

[6] This inequality states that the ball has the least surface area to volume ratio among all (reasonable) subsets of $\mathbf{R}^m$.

would give us the Lemma. So assume that the volume of T_1 is at most half the volume of ∂T. Then, letting $T_2 = (\partial T) \cap (\partial KK)$, we have that

$$\mathrm{Vol}_{n-1}(T_2) \geq \frac{\mathrm{Vol}_n(S)}{200n^{1/2}}.$$

For notational consistency, we define $\bar{T}_1 = (\partial \bar{T} \setminus \partial KK)(= T_1)$. If the volume of $\bar{T}_1$ is greater than or equal to $\mathrm{Vol}_n(\bar{S})/(200n^{1/2})$, this would again imply $\gamma(\bar{S}) \geq \frac{1}{4000n^3}$. But $\gamma(S) = \gamma(\bar{S})|\bar{S}|/|S| \geq \gamma(\bar{S})$, and so this would imply that $\gamma(S) \geq \frac{1}{4000n^3}$. This would complete the proof of the Lemma. Assume this fails. Then, letting $\bar{T}_2 = (\partial \bar{T}) \cap (\partial KK)$, we have

$$\mathrm{Vol}_{n-1}(\bar{T}_2) \geq \frac{\mathrm{Vol}_n(\bar{S})}{200n^{1/2}}.$$

Now one of the two sets $T_2, \bar{T}_2$ must have at most half the $(n-1)$-volume of ∂KK. We treat the two cases :

Case 1 : T_2 has at most half the volume of ∂KK. Then by using the inequalities of Bérard, Besson and Gallot [1985], (see Proposition 6), we have that

$$\mathrm{Vol}_{n-2}(\partial T_2) \geq \frac{\mathrm{Vol}_{n-1}(T_2)}{6n^2} \geq \frac{\delta^n |S|}{1200n^{5/2}}.$$

Now each point in ∂T_2 belongs to a facet F with an S cube on one side and an $\bar{S}$ cube on the other. Thus ∂T_2 is the union of $(n-2)$ dimensional pieces of the form $F \cap \partial KK$. By convexity, each such piece has $(n-2)$ volume bounded above by the $(n-2)$ dimensional volume of ∂F which is less than $2n\delta^{n-2}$. Thus the number of such pieces (and therefore $|(S, \bar{S})|$) must be at least $\delta^2|S|/(2400n^{7/2})$, so we have the Lemma in this case.

Case 2 : In this case, arguing symmetrically, we have $\gamma(\bar{S}) \geq \delta^2/(2400n^{7/2})$ and since $\gamma(S) \geq \gamma(\bar{S})$, the proof of Lemma 1 is now complete.

∎

Now we extend the Lemma to the technical Markov chain.

Lemma 2 If S is any subset of states of the technical Markov chain with $C_S \leq \frac{1}{2}$ then we have

$$\gamma(S) \geq \delta^2/(86400n^{7/2}).$$

Proof Let S' be the cubes in S that actually intersect $K(\alpha)$ and let $\bar{S}'$ be the cubes not in S that actually intersect $K(\alpha)$. Now by Proposition 11

$$|S| \leq |(S, \bar{S})| + 18|S'|.$$

If, $|(S, \bar{S})| \geq |S|/2$, then clearly $\gamma(S) \geq \frac{1}{2}$, so assume not. Then we have $|S'| \geq |S|/36$. We may similarly assume, $|\bar{S}'| \geq |\bar{S}|/36$. Lemma 1 yields :

$$|(S, \bar{S})| \geq |(S', \bar{S}')| \geq \delta^2(\min\{|S'|, |\bar{S}'|\})/2400n^{7/2}.$$

Lemma 2 now follows.

∎

Theorem 1 follows now from Lemma 2, Theorem 2 and the fact that $\Phi_S = \gamma(S)/(4n), \quad \forall S.$

4. Technical Results

Proposition 1 Suppose K is a convex body in $\mathbf{R}^n$ such that $B \subseteq K$ and ϵ is a positive real. Then for any y in $\mathbf{R}^n \setminus (1+\epsilon)K$, and z in K, we have $|z - y| > \epsilon$.

Proof : Let the hyperplane $v.x = (1+\epsilon)$ separate y from $(1+\epsilon)K$, i.e. $v \cdot y > (1+\epsilon)$ and for all z in K, $v \cdot (1+\epsilon)z \leq (1+\epsilon)$. From the last inequality it follows that $v \cdot z \leq 1$ and so we have $v \cdot (y-z) > \epsilon$. From the fact that K contains B, we have $|v| \leq 1$ and hence we must have $|y-z| > \epsilon$.

∎

Proposition 2 With the same hypothesis as before and $\epsilon \leq 1$, we have $y \in (1-\epsilon)K$ implies that the distance from y to the boundary of K is at least ϵ.

Proof : If z is on the boundary of K, there exists a vector v such that $v \cdot z = 1$ and $v \cdot x \leq 1$ for all x in K. So we have $v \cdot (z-y) \geq \epsilon$ and again $|v| \leq 1$, so $|z-y| \geq \epsilon$.

∎

Suppose K is a convex body in $\mathbf{R}^n$ such that $B \subseteq K$. Consider a division of $\mathbf{R}^n$ into "cubes" of side η (i.e. cubes of the form $\{x : m_i\eta \leq x_i \leq (m_i+1)\eta$ for $i = 1, 2, \ldots, n\}$ where m_i are integers) where $\eta \leq \frac{1}{900n^{3/2}}$. Let K^I be the set of cubes that are wholly contained in K and K^B the set of cubes that intersect both K and $\mathbf{R}^n \setminus K$. Then,

Proposition 3

$$|K^B| \leq 3n^{3/2}\eta|K^I|.$$

Proof: Any point y in any cube in K^B is at distance at most $\eta\sqrt{n}$ from K, so by Proposition 1, it is contained in $(1+\eta\sqrt{n})K$. Further, y is at distance at most $\eta\sqrt{n}$ from the boundary of K, so it is not in the interior

of $(1-\eta\sqrt{n})K$ from Proposition 2 . These together imply that the cubes in K^B are all wholly contained in the closure of $(1+\eta\sqrt{n})K \setminus (1-\eta\sqrt{n})K$ from which it follows[7] that their total volume is at most $2.5n^{3/2}\eta \mathrm{Vol}_n(K)$ which implies that $|K^B| \leq 2.5n^{3/2}\mathrm{Vol}_n(K)/\eta^{n-1}$. The cubes in K^B, K^I together include K, so we have $|K^B| + |K^I| \geq \mathrm{Vol}_n(K)/\eta^n$ and the Proposition follows.

∎

Proposition 4 If K contains the unit ball, then the number of cubes that weakly intersect $K(\alpha)$ is at most three times the number of cubes that are fully contained in K.

Proof : Using the same argument as in Proposition 3, this follows from the fact that any cube that weakly intersects $K(\alpha)$, but is not contained in K, is wholly contained in the set

$$(1+\alpha+\alpha'+\delta\sqrt{n})K \setminus (1-\delta\sqrt{n})K.$$

∎

Proposition 5 If

$$\mathrm{Vol}_n(C(\alpha+\alpha') \cap K) < (\alpha')^n \sigma_{n-1} n^{-2} (\frac{2}{\pi})^{n-2} r^{-n+1}$$

then $C(\alpha) \cap K = \emptyset$.

Proof Suppose not and $x \in C(\alpha) \cap K$. Let θ be the angle between the line joining x to the origin and any line through x tangent to B. Then $C(\alpha+\alpha') \cap K$ contains the intersection of a ball X of radius α' centered at

[7] Observe that, if $0 \leq y \leq 1 \leq x \leq (1+a/n)$, then $x^n - y^n \leq ne^a(x-y)$.

x and a cone Y of half-angle $\theta > 1/r$ with vertex x whose extreme rays are the tangents from x to B. The volume of $X \cap Y$ is

$$\sigma_{n-1}(\alpha')^n n^{-1} \int_0^\theta (\sin\phi)^{n-2} d\phi.$$

Using the lower bound $\sin\phi \geq 2\phi/\pi$, for $0 \leq \phi \leq \pi/2$ and integrating, we get the Proposition.

∎

Proposition 6 Let KK be as in the proof of Lemma 1. Let T be a subset of ∂KK and suppose that $\mathrm{Vol}_{n-1}(T) \leq \mathrm{Vol}_{n-1}(\partial KK)/2$. Then,

$$\mathrm{Vol}_{n-2}(\partial T) \geq \frac{\mathrm{Vol}_{n-1}(T)}{6n^2}.$$

Proof: In the following m is a positive integer. Let $\omega_m = \int_0^\pi (\sin t)^{m-1} dt$. Then from the relation $\omega_m = \frac{m-2}{m-1}\omega_{m-2}, m \geq 3 \; and \; \omega_1 = \pi, \omega_2 = 2$, we deduce (inductively) that for $m \geq 2$, $\omega_m \geq \frac{1}{\sqrt{m-1}} \geq \frac{1}{\sqrt{m}}$ and $\omega_m \leq \frac{\pi}{\sqrt{m}}$. Let $A = (1 + m\omega_m)^{1/m} - 1$. It is easy to see that $A \geq \log m/2m$, from which it follows that $A \geq 1/m$ for all $m \geq 1$.

Let M be a Riemannian manifold without boundary of dimension m with everywhere non-negative (Ricci) curvature and diameter $d(M)$. Bérard, Besson and Gallot show that if $\Omega \subseteq M$ is such that

$$\frac{\mathrm{Vol}_m(\Omega)}{\mathrm{Vol}_m(M)} = \beta, \qquad \text{then}$$

$$\frac{\mathrm{Vol}_{m-1}(\partial\Omega)}{\mathrm{Vol}_m(M)} \geq \frac{\mathrm{Vol}_{m-1}(\partial B(\beta))}{\mathrm{Vol}_m(S^m)} \cdot \frac{A}{d(M)},$$

where S^m is the unit sphere and $B(\beta)$ is the spherical cap on S^m such that

$$\frac{\mathrm{Vol}_m(B(\beta))}{\mathrm{Vol}_m(S^m)} = \beta.$$

We can rewrite the above inequality as

$$\frac{\mathrm{Vol}_{m-1}(\partial\Omega)}{\mathrm{Vol}_m(\Omega)} \geq \frac{\mathrm{Vol}_{m-1}(\partial(B(\beta))}{\mathrm{Vol}_m(B(\beta))}\frac{A}{d(M)}.$$

Now we can show straightforwardly, that the ratio $\dfrac{\mathrm{Vol}_{m-1}(\partial B(\beta))}{\mathrm{Vol}_m(B(\beta))}$ decreases with β, so for $\beta \leq 1/2$, we get

$$\frac{\mathrm{Vol}_{m-1}(\partial B(\beta))}{\mathrm{Vol}_m(B(\beta))} \geq \left(\int_0^{\pi/2} (\sin t)^{m-1} dt\right)^{-1} = \frac{2}{\omega_m}.$$

$$\text{Thus, } \frac{\mathrm{Vol}_{m-1}(\partial\Omega)}{\mathrm{Vol}_m(\Omega)} \geq \frac{2}{\omega_m}\frac{A}{d(M)} \geq \frac{2\sqrt{m}}{\pi d(M)m}.$$

We use this with $M = \partial KK$, $m = n-1$, and $\Omega = T$. Observe that $d(\partial KK) \leq \pi(\sqrt{n}(n+1)+\alpha)$. A simple calculation now completes the proof of the Proposition.

∎

For the next Proposition we need to define a function $\phi : \mathbf{R}^n \to \mathbf{R}^n$ as follows: If $x \in \mathbf{R}^n$ let $J = \{j : |x_j| > \frac{1}{\sqrt{2n}}\}$ and $\xi = \xi(x) = \sum_{j\in J} x_j^2$. Then let $\phi_j(x) = x_j^2/\xi$ if $j \in J$, and $\phi_j(x) = 0$ otherwise.

Proposition 7

Let $u_1, u_2, \ldots u_n$ be vectors in $\mathbf{R}^n$ with $|u_i| = 1 (\forall i)$ and $|u_i - u_j| \leq \frac{2}{3\sqrt{2n}}$ for $1 \leq i, j \leq n$. Then $\sum_{i=1}^n \phi_i(u_i) \leq 18$.

Proof : Observe first that $\xi(u_i) \geq |u_i|^2 - n \cdot \frac{1}{2n} = \frac{1}{2}$, $i = 1, 2, \ldots, n$. Now for any i, j we have $|u_{i,i}| - |u_{j,i}| \leq \frac{2}{3\sqrt{2n}}$ and so if $|u_{i,i}| \geq \frac{1}{\sqrt{2n}}$ then

$|u_{i,i}| \leq 3|u_{j,i}|$ and hence $\phi_i(u_i) \leq 2u_{i,i}^2 \leq 18u_{j,i}^2$. But if $|u_{i,i}| < \frac{1}{\sqrt{2n}}$ then $\phi_i(u_i) = 0 \leq 18u_{j,i}^2$ trivially. So

$$\sum_{i=1}^{n} \phi_i(u_i) \leq 18 \sum_{i=1}^{n} u_{j,i}^2 = 18$$

∎

Proposition 8

Let C' be any cube such that there exists $x \in C' \cap \partial K(\alpha)$. Let q be the closest point in K to x and let $u = (x-q)/|x-q| = (x-q)/\alpha$. For any k such that $|u_k| > 1/\sqrt{2n}$ and any l satisfying $2n \leq l \leq 20n$, the cube $C = C' - l\delta \text{ sign}(u_k)e_k$ is wholly contained in $K(\alpha)$ (e_k is the k th unit vector.)

Proof For l, k as above, let $x' = x - l\delta \text{ sign}(u_k)e_k$. Then we have,

$$|x'-q|^2 = |x-q|^2 - \Big((x_k-q_k)^2 - (x_k - l\text{sign}(u_k)\delta - q_k)^2\Big)$$

$$= \alpha^2 - \Big(2(x_k-q_k)l\delta\text{sign}(u_k) - l^2\delta^2\Big) \leq \alpha^2 - \left(\frac{2\alpha l\delta}{\sqrt{2n}} - l^2\delta^2\right) \quad \leq (\alpha - \delta\sqrt{n})^2$$

where the last inequality uses the fact that $2n \leq l \leq 20n$. From the above, we see that a sphere of radius $\delta\sqrt{n}$ around x' is contained in the sphere of radius α around q which is contained in $K(\alpha)$. This implies that the whole cube containing x' is inside $K(\alpha)$ proving the Proposition.

∎

Proposition 9

Fix $\theta > 0$. Let $x_1, x_2 \in \partial K(\theta)$ and let q_1, q_2 be the points in K nearest to x_1, x_2 respectively. Let $u_i = (x_i - q_i)/|x_i - q_i|$ for $i = 1, 2$. Then $|u_1 - u_2| \leq 2|x_1 - x_2|/\theta$.

Proof : Without loss of generality, move the origin to q_1. So, now, $q_1 = 0$ belongs to K. We have $u_i \cdot (y - x_i) \leq 0$ for $i = 1, 2$ and $y \in K(\theta)$. (Otherwise, we would have $x_i \in \operatorname{int} K(\theta)$.) Putting $i = 1, y = x_2$ gives $u_1 \cdot x_2 \leq \theta$ and $i = 2, y = \theta u_2$ gives $\theta \leq u_2 \cdot x_2$. Thus, $u_1 \cdot x_2 \leq u_2 \cdot x_2$. Now,

$$|x_2 - \theta u_2|^2 = |x_2|^2 - 2\theta u_2 \cdot x_2 + \theta^2 \leq |x_2|^2 - 2\theta u_1 \cdot x_2 + \theta^2 = |x_2 - \theta u_1|^2.$$

$$\text{Hence} \qquad |x_2 - \theta u_2| \leq |x_2 - \theta u_1| = |x_2 - x_1|.$$

$$\text{Now} \qquad \theta|u_2 - u_1| = |(x_2 - \theta u_1) - (x_2 - \theta u_2)| \leq |x_2 - \theta u_1| + |x_2 - \theta u_2| \leq 2|x_2 - x_1|.$$

∎

Proposition 10 : If S is any set of cubes meeting $K(\alpha)$, with S^I the subset of cubes in S that are wholly contained in $K(\alpha)$ and $S^B = S \setminus S^I$, we have,

$$|S^B| \leq 2n|(S, \bar{S})| + 18|S^I|$$

Proof : Let C' be any border cube and let $x \in C' \cap \partial K(\alpha)$; let q be the nearest point of K to x. Let $u = (x - q)/|x - q|$. Now, let $J = \{j : |u_j| > 1/\sqrt{2n}\}$, let $e'_j = \operatorname{sign}(u_j) e_j$ for $j \in J$. Then, we know by propostion 8 that $C_j = C' - 2n\delta e'_j \subseteq K(\alpha)$. Suppose first that some C_j, $j \in J$ is not in S. By convexity, the whole "stack" of cubes between C_j and C' meets $K(\alpha)$, and thus there is an $(S, \bar{S})$ facet F somewhere between C_j and C'. In this case, we will associate all the volume of C' with one such facet F. Note that any one facet may only "receive" the volume of a stack of $2n$ cubes by this process. If C_j is in S for all $j \in J$, we do the following : for each $j \in J$, we associate $\phi_j(u) = u_j^2/(\sum_{i \in J} u_i^2)$ of the volume of C' with C_j.

Now any $(S, \bar{S})$ facet receives volume at most $2n\delta^n$. Thus the volume mapped onto all $(S, \bar{S})$ facets is at most $2n\delta^n|(S, \bar{S})|$.

Now consider an inside cube C. This is mapped onto by border cubes $C^{(k)}$,using a direction $\pm e_k$, for $k \in A \subseteq \{1, 2, ..., n\}$. We use superscript (k) to refer to quantities associated with $C^{(k)}$.

Now $|x^{(k)} - x^{(l)}| \leq \delta\sqrt{2(2n+1)^2 + n - 2} \leq 4n\delta$. Thus, by Proposition 9, we have

$$|u^{(k)} - u^{(l)}| \leq \frac{2}{3\sqrt{2n}}$$

But, the total volume mapped onto C is

$$\delta^n \sum_{k \in A} \phi_k(u^{(k)}) \leq 18\delta^n \qquad \text{by Proposition 7}$$

Thus the total volume mapped onto inside cubes is at most $18\delta^n|S^I|$.

∎

Proposition 11

Let K be a convex body containing the unit ball and let S be a set of cubes that weakly intersect $K(\alpha)$. Let $S' \subseteq S$ be those cubes which actually intersect $K(\alpha)$. Then

$$|S| \leq |(S, \bar{S})| + 18|S'|.$$

Proof: Let $C \in S - S'$. Then there exists $x \in C \cap \partial K(\alpha + \alpha')$. Let $y \in K$ be the nearest point to x in K and $u = \frac{x-y}{|x-y|}$. Then $\alpha < |x - y| \leq \alpha + \alpha'$. Now let $J = \{j : |u_j| \geq \frac{1}{\sqrt{2n}}\}$ and observe now that if $j \in J$ then the point $x - \text{sign}(u_j)\delta e_j$ is at distance at most α from y and so is in $K(\alpha)$. Hence for every $j \in J$ the neighbouring cube C'_j across the face F_j in the direction -sign$(u_j)e_j$ meets $K(\alpha)$. If there exists $j \in J$ such that $C'_j \notin S$ then we map all of the volume of C onto any such F_j. Otherwise we share out the volume of C by mapping $\phi_j(u)\delta^n$ of it to $C'_j \in S'$ for $j \in J$. The result follows (as

in Proposition 10) once we have shown that a cube in S' has at most $18\delta^n$ in volume mapped onto it in this way. So now let $C' \in S'$ be fixed. This is mapped onto by cubes $C^{(k)} \in S - S'$, using $x^{(k)}, u^{(k)}, k \in K \subseteq \{1, 2, ..., n\}$ (in the notation of Proposition 10). Now

$$|x^{(k)} - x^{(l)}| \leq 3\sqrt{n}\delta \qquad k, l \in K$$

which implies

$$|u^{(k)} - u^{(l)}| \leq \frac{2}{3\sqrt{2}n}$$

and hence (Proposition 7)

$$\sum_{k \in K} \phi_k(u^{(k)})\delta^n \leq 18\delta^n.$$

∎

Remark: The term $2n|(S, \bar{S})|$ in the inequality of Proposition 10 can be replaced by $8\sqrt{2n}|(S, \bar{S})|$. This is done by modifying the argument, and using a strengthening of Proposition 9 to show that an inside cube can be reached in distance $\delta\sqrt{2n}/u_k$. However it turns out that this is not the dominant term in the complexity analysis, so we have omitted this refinement.

5. Remarks

Remark 1 If the convex body K is a polytope given explicitly by its constraints, then we can just use the natural random walk – since it is now possible to test in polynomial time if the body intersects $C(\alpha)$ for any cube C. This is done by solving a quadratic programming problem using the ellipsoid algorithm.

Remark 2 We do not quite need the oracle we have described. We may instead use the so-called "weak membership oracle" (Grötschel, Lovász and Schrijver [1988]). A "weak membership oracle" for a convex body K does the following : given a point x and a rational λ, it tells us (in unit time) either (i) x belongs to $K(\lambda)$ or (ii) tells us that x does not belong to $K(-\lambda)$, the set of points in K which are at distance at least λ from the boundary of K. It is straightforward to see that such an oracle will do for our purposes.

Remark 3 Given a weak oracle for a convex body K containing the origin in its interior, it is easy to construct an oracle for the so-called "polar" or "dual" body $K^* = \{u : \max\{u \cdot x : x \in K\} - \min\{u \cdot x : x \in K\} \leq 1\}$. We briefly sketch the argument. Given any u, we can find the approximate maximum and minimum of $u \cdot x$ over K to a desired degree of approximation using the weak oracle for K (see Grötschel, Lovász and Schrijver [1988]). Then if the difference between these is suitably close to 1, we answer yes, otherwise answer no. Thus, it is possible to find the volume of the polar body given an oracle for the "primal" body.

Remark 4 We can integrate any bounded nonnegative concave function defined over a convex body K in $\mathbf{R}^n$. This is because we can express $\int_K f$ as $\mathrm{Vol}_{n+1}(K_1)$ where $K_1 = \{(x,t) : x \in K \text{ and } 0 \leq t \leq f(x)\}$. Some non-concave functions that do not vary very rapidly may also be integrated by sampling values at random points (using our random walk to choose the points).

Remark 5 It would be interesting to show that the random walk over cubes that intersect any well-rounded convex body K is rapidly mixing. This would simplify our algorithm by avoiding the use of $K(\alpha)$.

Remark 6 We suspect the following result is true. If so, it would give us the required isoperimetric inequality more readily without having to look

at the boundary of the set T_2.

Suppose K is any convex body in $\mathbf{R}^n$ and S is some measurable subset of it. (It may or may not be necessary to assume any other properties of S like smoothness or connectedness.) If the volume of S is at most half the volume of K, is it true that the "exposed surface area of S", i.e. the $(n-1)$ volume of $\partial S \setminus \partial K$ is at least the n volume of K divided by a fixed polynomial in $n, d(K)$? (Here $d(K)$ is the diameter of K.) It is also possible that such a result may hold for nonconvex K as well, where now the denominator is also a function of the least (Ricci) curvature of the surface of K.

Remark 7 The random walk enables us to generate a random point in a polytope with nearly uniform distribution. Of some interest, for example, is the following polytope P in $\mathbf{R}^{n^2}$ where the variables are $\{x_{ij}, 1 \leq i,j \leq n\}$ and $P = \{x : 0 \leq x_{ij} \leq 1 \ , \ x_{ij} + x_{jk} \leq x_{ik} \ \forall i,j\}$. The points of P for example give us "costs" on the edges of a graph on n vertices which satisfy the triangle inequality. We expect that the random generation aspect of our result will have other applications.

Remark 8 As we remarked immediately after the algorithm, we conjecture that the bound of $O(n^{19})$ can be improved. Here we discuss some limits on the improvements. The diameter of the Markov chain we have is $O(r/\delta)$ which is $O(n^4)$. By working carefully through the proof of Lemmas 1 and 2, and taking note of Theorem 2, we see that the dependence of our upper bounds on the number of steps for rapid mixing on the diameter of the Markov chain is the fourth power of the diameter. (The Φ^2 of Theorem 2 contributes a 2 and Lemmas 1 and 2 already have a 2 in them.) By well-known results, (see Aldous [1981-1982], example 5.7), the dependence cannot be improved below the square of the diameter, even in the simple case that the convex body is a cube. (In fact, for the 1-dimensional random walk with

2 reflecting boundaries, after t steps, we are expected to be only at distance $\sqrt{t}$ from the starting point.) Thus, with our random walk, the best bound on the number of steps needed for rapid mixing is $\Omega(n^8)$. Thus, we must reduce the diameter of the Markov chain for more improvements. If the result stated in Remark 5 is true, then there is no need for going to $K(\alpha)$. Then going through our arguments carefully, it can be seen that $\delta = 1/O(n^{3/2})$ will work, whence the diameter will be $O(n^3)$.

Acknowledgements We are especially grateful to Mark Jerrum for his critical reading of the paper. We also thank David Applegate, Dick Karp, Marek Karpinski, Dick Maccamy, Victor Mizel, Alistair Sinclair, Mete Soner and Rick Statman for many helpful discussions.

References

D.Aldous, *Random walks on finite groups and rapidly mixing Markov chains*, Séminaire de Probabiliteś XVII, 1981-1982, Springer-Verlag Lecture Notes in Mathematics 986, pp. 243-297.

I.Bárány and Z.Füredi, *Computing the volume is difficult*, Proceedings of the Eighteenth Annual ACM Symposium on Theory of Computing (1986) 442-447.

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.

A.Z. Broder, *How hard is it to marry at random? (On the approximation of the permanent)*, Proceedings of the Eighteenth Annual ACM Symposium on the Theory of Computing (1986)50-58.

M.E.Dyer and A.M.Frieze, *On the complexity of computing the volume of a polyhedron*, SIAM Journal on Computing, Volume 17, No. 5, October (1988) pp 967-975.

G.Elekes, *A geometric inequality and the complexity of computing volume*, Discrete and Computational Geometry, Vol. 1, (1986) 289-292.

W.E.Feller, *Introduction to probability theory and its applications*, 3rd edition, Wiley, 1968.

D.Gilbarg and N.S.Trudinger, *Elliptic partial differential equations of second order*, §7.2, Springer-Verlag, 1983.

M.Grötschel, L.Lovász and A.Schrijver, *Geometric algorithms and combinatorial optimization*, Springer-Verlag (1988)

W.Hoeffding, *Probability inequalities for sums of bounded random variables*, Journal of the American Statistical Association 58 (1963) 13-30.

M.R.Jerrum and A.J.Sinclair, *Conductance and the rapid mixing property for Markov chains: the approximation of the permanent resolved*, Proceedings of the Twentieth Annual ACM Symposium on the Theory of Computing (1988) 235-244.

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.

R.M.Karp and M.Luby, *Monte Carlo algorithms for enumeration and reliability problems*, Proceedings of the Twenty-Fourth IEEE Symposium on Foundations of Computer Science (1983) 56-64.

L.Lovász, *An algorithmic theory of numbers graphs and convexity*, CBMS-NSF Regional Conference Series on Applied Mathematics, Philadelphia, 1986.

V.D.Milman and G.Schectmann, *Asymptotic theory of finite dimensional normed spaces*, Springer-Verlag Lecture Notes in Mathematics 1200, 1980.

A.J.Sinclair and M.R.Jerrum, *Approximate counting, uniform generation and rapidly mixing Markov chains*, Information and Computation (to appear).