Comp. & Maths. with Appls. Vol. 8, No. 1, pp. 1–13, 1982
Printed in Great Britain.

0097-4943/82/010001-13$03.00/0
Pergamon Press Ltd.

ON THE COMPUTER GENERATION OF RANDOM CONVEX HULLS

LUC DEVROYE
School of Computer Science, McGill University, 805 Sherbrooke Street West, Montreal, P.Q., Canada H3A 2K6

(*Received April* 1981)

Communicated by Ervin Y. Rodin

Abstract—The convex hull of $X_1, \ldots, X_n$, a sample of independent identically distributed R^d-valued random vectors with density f is called a random convex hull with parameters f and n. In this paper, we give an algorithm for the computer generation of random convex hulls when f is radial, i.e. when $f(x) = g(\|x\|)$ for some function g. Then we look at the average time $E(T)$ of the algorithm under a convenient computational model. We consider only $d = 2$.

We show that for any f, our algorithm takes average time $\Omega(\log n)$. This lower bound is achieved for all radial densities with a polynomially decreasing tail. For the radial densities with an exponentially decreasing tail, we show that $E(T) = 0(\log^{3/2} n)$. Finally, for the uniform density on the unit circle, we have $E(T) = 0(n^{1/3} \log^{2/3} n)$. This rate is also shown to be optimal for this density.

1. INTRODUCTION

In computer science, one needs random convex hulls to test and time various algorithms that perform certain operations on convex hulls. In statistics, random convex hulls are needed to obtain Monte Carlo estimates of various statistics derived from the random convex hull. In this paper, we look at some algorithms for the fast generation of random convex hulls and their complexities.

Definition. The *convex hull* of $\{x_1, \ldots, x_n\} \in R^d$ is the collection of all x_i, $1 \le i \le n$, with the property that there exists a closed linear halfspace H containing all x_j's while interior(H) does not contain x_i. When f is a density on R^d, and n is a positive integer, then we define a *random convex hull* with parameters (f, n) as the convex hull of a random sample $X_1, \ldots, X_n$ of independent identically distributed random vectors with common density f.

For an elegant analysis, we make the following convenient assumptions:

(1) Real numbers can be stored in our computer. All common operations (+, −, ., /, mod, truncate, compare, move) take time bounded between $a > 0$ and $b < \infty$, regardless of the size of the operands.

(2) We are given a perfect uniform random variate generator, capable of producing a sequence $U_1, U_2, \ldots$ of independent identically distributed random variables with a uniform density on (0, 1). The time taken per random variate is a positive constant.

(3) $\{Y_1, \ldots, Y_N\}$ (the random convex hull generated by our algorithm) and T (time taken by the algorithm before it halts) are Borel measurable functions of $U_1, U_2, \ldots$, and $T < \infty$ almost surely.

Assumption 3 essentially insures us that the cardinality N and the time T are random variables. Thus, we may speak of the average time $E(T)$ taken by the algorithm, etc. The Landau symbols 0, o and ~ will be used throughout the paper. The symbol Ω is defined as follows: if a_n and b_n are two positive number sequences, then $a_n = \Omega(b_n)$ when there exist n_0 and $k > 0$ such that $a_n \ge k b_n$ for all $n \ge n_0$.

Any algorithm for generating random convex hulls with parameters (f, n) must satisfy

$$E(T) = \Omega(E(N)). \tag{1}$$

We also have an upper bound for $E(T)$ when random convex hulls are generated by the naive algorithm given below:

(1) Generate $X_1, \ldots, X_n$, independent identically distributed random variates with common density f.

(2) Find the convex hull of $\{X_1, \dots, X_n\}$ and exit.

Step 1 takes average time $0(n)$ if X_1 can be generated in average time $0(1)$ (note: the latter part of this statement seems trivial, but it is necessary because some algorithms take average time $E(T) = \infty$ although $T < \infty$ almost surely, e.g. let $T = i$ with probability $1/((i+1)i)$, $i \geq 1$). In many instances, Step 2 takes average time $0(n)$ as well although the worst-case time of Step 2 may be much worse. Linear average time is usually achieved by means of an elimination algorithm [9, 11], a bucketing algorithm [10, 12]; or a divide-and-conquer algorithm [3, 13]. See Devroye [14] for a survey. In the plane, Step 2 can always be executed in time bounded by $0(n \log n)$ [15, 31]. Thus, for *all* densities f, the naive algorithm satisfies

$$E(T) = 0(n \log n). \tag{2}$$

For *some* densities f, the naive algorithm has $E(T) = 0(n)$, which is best possible since we must also have $E(T) = \Omega(n)$ in view of Step 1. In view of (1), the naive algorithm can only be expected to be a "good" algorithm for this problem when $E(N)$ is close to n. It is known however that $E(N) = o(n)$ for *all* densities f [11]. In most practical cases, $E(N)$ is much smaller than n, for example: $E(N) \sim (2k/3) \log n$ when f is uniform on a convex polygon of R^2 with k vertices [26, 27]; $E(N) \sim 2\sqrt{(2\pi \log n)}$ when f is normal in R^2 [26]; $E(N) \sim$ constant $n^{1/3}$ when f is uniform in the unit circle [6].

In view of this, even the best naive algorithm seems wasteful. We would like to give an algorithm in which the lower bound (1) is approached. Such an algorithm cannot possibly require the generation of $X_1, \dots, X_n$. For general densities f, this problem seems very complicated. We will restrict ourselves to *radial densities in the plane.*

Definition. A random variable X taking values in R^2 is said to be *radial* when it has a *radial density* f, i.e. when f can be written as

$$f(x) = g(\|x\|)$$

for some function g. Here $\|\cdot\|$ is the usual Euclidean norm.

For the distribution theory of radial random variables, see Kelker (1970). We would like to point out that $R = \|X\|$ has density

$$h(r) = 2\pi r g(r), \quad r > 0,$$

when $g(\|x\|)$ is the density of X in R^2. We will call the distribution function of R $H(r) = P(R \leq r) = 1 - G(r)$, $r \geq 0$.

The algorithm

Let $p_n \in (0, 1)$ be a given number depending upon f and n only. Determine a radius r_n such that $G(r_n) = p_n$. Let $f = f_1 + f_2 = f I_{[\|x\| \geq r_n]} + f I_{[\|x\| < r_n]}$ where I is the indicator function.

Step 1. Generate a binomial (n, p_n) random variable M. Given M, generate independent identically distributed random vectors $W_1, \dots, W_M$ with common density f_1/p_n.

Step 2. Find the convex hull of $\{W_1, \dots, W_M\}$, and find its radius R_n where

$$R_n = \begin{cases} 0, & \text{if } M = 0 \text{ or if the origin does not belong to the convex set defined by the convex hull;} \\ \min\limits_{\substack{\text{all edges } e \\ \text{determined by adjacent} \\ \text{vertices of the convex hull}}} & \text{distance } (e, \text{origin}), \text{ otherwise.} \end{cases}$$

Step 3. If $R_n \geq r_n$, exit with the given convex hull. Otherwise, generate $W_{M+1}, \dots, W_n$, independent random vectors with common density $f_2/(1-p)$, and conditionally independent of $W_1, \dots, W_M$ (the condition is on M). Find the convex hull of $W_{M+1}, \dots, W_n$, merge both convex hulls into a new convex hull, and exit.

Remarks

1. [*Validity*]. When $R_n \geq r_n$, no point inside the circle of radius r_n centered at the origin can possibly belong to the random convex hull. Thus, the algorithm given here is exact. Note here that to reduce $E(T)$, $P(R_n \geq r_n)$ should be close to 1.

2. [*Binomial random variate generation*]. A binomial (n, p) random variate can be obtained in average time bounded by a constant c not depending upon n or p [2, 8]. These algorithms are not crucial in the reduction of $E(T)$. We will not alter the asymptotic rate of $E(T)$ if binomial (n, p) random variates are generated in average time $0(1+np)$. This can be achieved by one of two simple "Exponential" algorithms:

(A) Generate independent exponential random variates $E_1, E_2, \ldots$ until for the first time the sum

$$\sum_{i=1}^{X+1} \left(1 + \operatorname{int}\left(\frac{E_i}{-\log(1-p)}\right)\right) > n.$$

Then X is binomial (n, p) [7].

(B) Generate independent exponential random variates $E_1, E_2, \ldots$ until for the first time the sum

$$\sum_{i=1}^{X+1} \frac{E_i}{n-i+1} > -\log(1-p).$$

Then X is binomial (n, p) [24].

3. [*Generating from* f_1/p_n]. Every radial random variable X is distributed as $(R\cos\theta, R\sin\theta)$ where R and θ are independent random variables: R has distribution function H, and θ is uniformly distributed on $(0, 2\pi)$. If H is invertible, then

$$H^{-1}(U), H^{-1}(p_nU + (1-p_n)) \text{ and } H^{-1}(U(1-p_n))$$

are random variables with densities f, f_1/p_n and $f_2/(1-p_n)$ respectively, when U is a uniform $(0, 1)$ random variable. Let T_n be the time needed to generate a random variate from each of these densities; then we will assume that

$$\sup_n E(T_n) < \infty. \tag{3}$$

In the case of the inversion method, this boils down to making an assumption about the average computation time of H^{-1}. It was reported in Devroye [7] that the inversion method is not very accurate when p_n is small for generating random variates with distribution function $(H(u) - H(r_n))/(1-H(r_n))$, $u > r_n$. Other methods, usually involving rejection at some point, seem to give more accurate results. If inversion cannot be used for generating a random variate R with distribution function $H(u)/H(r_n)$, $u \leq r_n$, then we can use the following trivial rejection method:

(1) Generate a random variate R with distribution function H.

(2) If $R > r_n$, go to 1. Otherwise, exit with R.

If generation from H takes average time c, then this algorithm takes average time proportional to $c/(1-p_n) = 0(1)$ when $p_n \to 0$ as $n \to \infty$, and condition (3) is satisfied.

4. [*Finding the convex hull*]. The convex hull of $\{W_1, \ldots, W_M\}$ with clockwise ordering of the vertices can be found as follows:

(A) Order $W_1, \ldots, W_M$ according to the polar angles $\theta_1, \ldots, \theta_M$ (each W_i is presumably generated as $(R_i\cos\theta_i, R_i\sin\theta_i)$ where R_i and θ_i are as explained in Remark 3). Find the maximal spacing $S = \max_{0\leq i\leq M} \theta_{(i+1)} - \theta_{(i)}$ where $0 = \theta_{(0)} < \theta_{(1)} < \cdots < \theta_{(M)} < \theta_{(M+1)} = 2\pi$ are the order statistics of $0, \theta_1, \theta_2, \ldots, \theta_M, 2\pi$. If the sorting is done by means of the bucket method, then all of this takes average time bounded by $cM + 1$ for some positive c not depending upon M [10].

(B) If $S \geq \pi$ (origin does not belong to convex set defined by convex hull), reorder $W_1, \ldots, W_M$ according to the angles of the lines joining these points with some interior point of the convex set. This can be done in time bounded by $cM + 1$ for some positive c because in Step (A) we already have done most of the work.

(C) Find the convex hull using Graham's algorithm[15]. Find R_n (note that $R_n = 0$ if and only if $M = 0$ or $S \geq \pi$). Both operations take time bounded by $cM + 1$ for some constant $c > 0$.

For given M, the average time of Step 2 in the algorithm is less than $cM + 1$. Thus, integrating over all values of M, we have an agerage time bounded by $0(E(M) + 1) = 0(np_n + 1)$.

5. [*Avoiding the sort*]. The order statistics of the polar angles $\theta_1, \ldots, \theta_M$ of the random vectors $W_1, \ldots, W_M$ can be generated directly in average time bounded by $cM + 1$ for some constant $c > 0$ when exponential random variates can be obtained in average time 0(1): let $E_1, \ldots, E_{M+1}$ be independent exponential random variables with sum V. Define

$$\theta_{(0)} = 0; \quad \theta_{(i+1)} = \theta_{(i)} + \frac{2\pi}{V} E_{i+1}, \quad 0 \leq i \leq M.$$

The random variables $(\theta_{(1)}, \ldots, \theta_{(M)})$ are distributed as the order statistics of M independent uniform $(0, 2\pi)$ random variables (see Pyke[25] for a survey of the properties of uniform spacings). For the first mention of the possibility of directly generating order statistics without sorting, see Lurie and Hartley[21], Schucany[30] or Lurie and Mason[22]. The remarks about the average time given in Remark 4 remain valid if the sorting step (A) is replaced by the direct generation step described here.

6. [*Merging convex hulls*]. Shamos[31] has indicated that two convex hulls with clockwise ordered vertices can be merged into a new convex hull with clockwise ordered vertices in time proportional to the total number of points in the convex hulls. Thus, with the assumption (3) (Remark 3), we see that Step 3 of the algorithm takes time bounded by c when $R_n \geq r_n$, and it takes average time bounded by cn otherwise where $c > 0$ is a constant.

7. [*Average time taken by the algorithm*]. If we take all the previous remarks into account, then the average time $E(T)$ of the entire algorithm satisfies

$$E(T) = 0(np_n + 1 + nP(R_n < r_n)) \tag{4}$$

and

$$E(T) = \Omega(np_n + 1 + nP(R_n < r_n)). \tag{5}$$

The problem we are now faced with is that of choosing p_n (and thus r_n) such that the r.h.s. of (4) is minimal. The choice of p_n will unfortunately enough depend upon f. In Sections 2 and 3, we take a closer look at (4) and (5) for large classes of radial densities.

8. [*Avoiding trigonometric functions*]. A radial random vector X was generated as RZ, where R is a random variable with distribution function H, and Z is a random vector independent of R, distributed as $(\cos\theta, \sin\theta)$ where θ is uniformly distributed on $(0, 2\pi)$. It is well-known that Z can also be generated as follows:

(1) Generate (U, V) uniformly in $[0, 1]^2$, and set $S \leftarrow U^2 + V^2$.

(2) If $S > 1$, go to 1.

(3) Exit with $Z \leftarrow (U/\sqrt{S}, V/\sqrt{S})$.

The square root can also be avoided by replacing 3 by 3′:

(3′) Exit with $Z \leftarrow [(U^2 - V^2)/S, (2UV/S)]$.

At one point we have to sort the polar angles of $W_1, \ldots, W_M$ where now each W_i is generated as $R_i Z_i$ and $Z_i = (U_i, V_i)$ is distributed as $(\cos\theta_i, \sin\theta_i)$. It is obvious that we should not have to compute θ_i as arc cos U_i or as arc sin V_i or as arc tan V_i/U_i. Rather, we propose to sort $W_1, \ldots, W_M$ in two steps:

(1) Sort all the W_i's with $U_i > 0$ according to increasing values of

$$\frac{V_i}{U_i}\left(1 + \left|\frac{V_i}{U_i}\right|\right)^{-1}.$$

(2) Sort all the W_i's with $U_i < 0$ according to decreasing values of the same function of U_i and V_i. Concatenate the sorted sets.

The density of V_1/U_1 is Cauchy. Now, if X is Cauchy distributed, then $X/(1+|X|)$ has density

$$f(x) = \frac{1}{\pi(1+2x^2-2|x|)}, \quad |x| \le 1.$$

Since this density is bounded and has compact support, we see that the sorting of the W_i's by the bucket method takes average time bounded by $cM+1$ for some constant $c>0$. The average time for the generation and the sorting of $W_1, \dots, W_M$ is bounded by $cM+1$ for fixed M, just as for the method explained in Remarks 3 and 4 with the trigonometric functions present. It is clear that we may expect a smaller constant "c" if these functions are avoided.

9. [*Modification of Step* 3]. The following time-saving step can be used instead of Step 3:

Step 3*. If $R_n \ge r_n$, exit with the given convex hull. Otherwise, compute $q \leftarrow (H(r_n) - H(R_n))/H(r_n)$, generate an independent binomial $(n-M, q)$ random variate M^*, and generate an independent sequence of random vectors $W_{M+1}, \dots, W_{M+M^*}$ with density $f(x)I_{[R_n \le \|x\| \le r_n]}/(q(1-p_n))$. Find the convex hull of this sequence, merge both convex hulls into a new convex hull, and exit.

The algorithm remains valid, and the upper bound for $E(T)$ (see (4)) is still applicable.

2. A LOWER BOUND FOR THE AVFRAGE COMPLEXITY

THEOREM 1

For every density f, the given algorithm must satisfy

$$E(T) = \Omega(\log n).$$

Proof. Consider the circle C centered at the origin with radius r_n. It is clear that

$$[R_n < r_n] \supseteq \bigcap_{i=1}^{n} [X_i \in C].$$

Thus, by (5),

$$E(T) = \Omega(np_n + 1 + n(1-p_n)^n). \tag{6}$$

The function $u + (1-u)^n$, $0 \le u \le 1$, is minimal when $1 - n(1-u)^{n-1} = 0$, i.e. for $u = 1 - n^{-1/(n-1)}$. Thus,

$$np_n + n(1-p_n)^n \ge n(1-n^{-1/(n-1)}) \ge n(1-n^{-1/n}) = n\left(1 - \exp\left(-\frac{\log n}{n}\right)\right)$$

$$\ge n\left(1 - \left(1 - \frac{\log n}{n} + \frac{1}{2}\left(\frac{\log n}{n}\right)^2\right)\right) = \log n - \frac{(\log n)^2}{2n}.$$

This concludes the proof of Theorem 1.

Remarks

(1) Theorem 1 remains valid for all the modified versions of the basic algorithm, including the version in which Step 3 is replaced by Step 3*.

(2) Theorem 1 is valid for all densities f, not just the radial densities. It is also obvious that the dimension is not used in the proof. Thus, the lower bound also applies to any algorithm that uses our strategy to generate a random convex hull in R^d. In R^1, the convex hull of $X_1, \dots, X_n$ consists of $\min_i X_i$ and $\max_i X_i$. Thus, the given algorithm allows us to generate the extreme order statistics of a random sample. However, as Theorem 1 shows, regardless of how p_n is chosen, the average time taken by the algorithm must be $\Omega(\log n)$. For a comparison of this algorithm with other algorithms for generating the extreme order statistics, see Devroye[7].

3. UPPER BOUNDS FOR THE AVERAGE COMPLEXITY

We will now show that $E(T) = 0(\log n)$ for the radial densities with a polynomial tail, and that $E(T) = 0(\log n)^{3/2})$ for radial densities with an exponential tail. We will not discuss other classes of radial densities because we could find no interesting class for which $E(N)/n$ converges quickly to 0. One should also keep in mind that for every monotonically increasing function w with $w(n)=o(n)$, there exists a radial density for which $E(N)=\Omega(w(n))$. For this density, we necessarily have $E(T)=\Omega(w(n))$ (1). In the last part of this section, we show that for the uniform density on the unit circle, $E(T)=0(n^{1/3}\log^{2/3}n)$, and we also prove that this is optimal. Unless explicitly indicated, all the results below remain valid for our algorithm with and without the modification of Remark 9.

3.1 *Two inequalities*

Consider the circle C centered at the origin with radius r_n, and let A be the collection of points (x, y) for which $x \ge r_n$. Thus, A is a halfspace determined by the tangent to C at $(r_n, 0)$. Let a_n be defined by

$$a_n=\int_A f(x)\,\mathrm{d}x.$$

Inequality 1

For all radial densities f,

$$P(R_n \le r_n) \le \mathrm{e}^{-np_n}+2enp_n\,\mathrm{e}^{-na_n}. \tag{7}$$

Proof. For each X_i outside C, consider the two tangents l_{i1} and l_{i2} to C. These lines define open outer halfspaces (halfspaces not containing the origin) A_{i1} and A_{i2}. Clearly,

$$[R_n \le r_n]=\bigcup_{i=1}^{n}[X_i \notin C; |A_{i1}| \text{ or } |A_{i2}|=0] \cup \bigcap_{i=1}^{n}[X_i \in C] \tag{8}$$

where $|\cdot|$ denotes the cardinality of a set (the number of X_j's, $1 \le j \le n$, contained in the set). Thus, by symmetry,

$$P(R_n \le r_n) \le 2nP(X_1 \in C; |A_{i1}|=0)+(1-p_n)^n \le 2np_n(1-a_n)^{n-1}+\mathrm{e}^{-np_n} \le 2enp_n\,\mathrm{e}^{-na_n}+\mathrm{e}^{-np_n}.$$

Inequality 2. [Lower bounds for a_n].

Let $\theta \in (0, \pi/2)$ be a given angle. Then, for *all* radial densities,

$$a_n \ge \frac{\theta}{\pi}G\left(\frac{r_n}{\cos\theta}\right). \tag{9}$$

When h is nonincreasing for $r \ge r^*$, then also

$$a_n \ge 2r_n(1-\cos\theta)^{3/2}h\left(\frac{r_n}{\cos\theta}\right), \quad r_n \ge r^*. \tag{10}$$

Proof. Consider the circle C' centered at the origin with radius $s=r_n/\cos\theta$, and let D be the cone $\{(x,y)|x>0, |\arctan(y/x)|<\theta\}$. It is obvious, from a simple geometrical argument, that A contains $D-C'$. But then

$$a_n=\int_A f(x)\,\mathrm{d}x \ge \int_{D-C'} f(x)\,\mathrm{d}x=\frac{\theta}{\pi}G(s).$$

This proves (9). To prove (10), we note that

$$\begin{aligned} a_n &= \int_A f(x)\,\mathrm{d}x \ge \int_{AC'} f(x)\,\mathrm{d}x = 2\int_{r_n}^{s} \arccos\frac{r_n}{r}\,h(r)\,\mathrm{d}r \\ &\ge 2\int_{r_n}^{s}\sqrt{[1-(r_n/r)^2]}h(r)\,\mathrm{d}r \ge \frac{2}{s}\int_{r_n}^{s}\sqrt{(r^2-r_n^2)}h(r)\,\mathrm{d}r \\ &\ge \frac{2\sqrt{2}}{\sqrt{r_n}}\cos\theta\int_{r_n}^{s}\sqrt{(r-r_n)}h(r)\,\mathrm{d}r \ge \frac{2\sqrt{2}}{\sqrt{r_n}}\cos\theta\left(\int_{r_n}^{s}h(r)\,\mathrm{d}r\right)\sqrt{\left[\left(\int_{r_n}^{s}rh(r)\,\mathrm{d}r\Big/\int_{r_n}^{s}h(r)\,\mathrm{d}r\right)-r_n\right]} \end{aligned} \tag{11}$$

where we used Jensen's inequality (last step: $\sqrt{(r-r_n)}$ is concave on $r \geq r_n$) and the fact that $\arccos u = \arcsin \sqrt{(1-u^2)} \geq \sqrt{(1-u^2)}$, $0 \leq u \leq 1$. But

$$\int_{r_n}^{s} (r-r_n)h(r)\,\mathrm{d}r \geq \frac{1}{2} r_n^2 \left(\frac{1}{\cos\theta}-1\right)^2 h(s), \quad r_n \geq r^*.$$

Combining these inequalities gives

$$\begin{aligned} a_n &\geq 2\cos\theta\left(\frac{1}{\cos\theta}-1\right)\sqrt{r_n}\sqrt{(h(s))}\sqrt{[H(s)-H(r_n)]} \\ &\geq 2(1-\cos\theta) r_n h(s) \sqrt{\left(\frac{1}{\cos\theta}-1\right)} \\ &\geq 2(1-\cos\theta)^{3/2} r_n h(s). \end{aligned}$$

Remark

From (11) we can easily obtain a slightly weaker inequality than (10) (one in which "2" is replaced by "$4\sqrt{(2)}/3$") as follows:

$$\begin{aligned} \frac{2}{s}\int_{r_n}^{s} \sqrt{(r^2-r_n^2)}h(r)\,\mathrm{d}r &\geq \frac{2h(s)}{s} 2r_n \int_0^{r_n(\cos^{-1}\theta-1)} \sqrt{r}\,\mathrm{d}r \\ &= \frac{4\sqrt{2}}{3} r_n h(s)(1-\cos\theta)^{3/2}/\sqrt{(\cos\theta)}, \quad r_n \geq r^*. \end{aligned}$$

3.2 *Densities with a polynomial tail*

Definition. $\mathscr{P}(\alpha)$ is the collection of radial densities such that G is regularly varying at infinity with parameter $-\alpha$, i.e. for all $c > 0$, we have

$$\lim_{r\to\infty} \frac{G(cr)}{G(r)} = \frac{1}{c^\alpha}.$$

THEOREM 2

When $f \in \mathscr{P}(\alpha)$ and $p_n = c(\alpha)(\log n/n)$, where $c(\alpha)$ is a constant greater than

$$\inf_{0<\theta<\pi/2} \frac{\pi}{\theta\,(\cos\theta)^\alpha},$$

then $E(T) = 0(\log n)$ for the algorithm described in Section 1.

Proof. The proof is based upon a combination of (4), (7) and (9): Note that for fixed angle $\theta \in (0, \pi/2)$, $a_n \geq (\theta/\pi)G(r_n/\cos\theta) \sim (\theta/\pi)G(r_n)(\cos\theta)^\alpha = (\theta/\pi)(\cos\theta)^\alpha p_n$. Thus,

$$\begin{aligned} E(T) &= 0(np_n + 1 + nP(R_n \geq r_n)) = 0(\log n) + 0(n\,\mathrm{e}^{-np_n}) + 0(n \log n\,\mathrm{e}^{-na_n}) \\ &= 0(\log n) + 0(n^{1-c(\alpha)}) + 0(\log n \cdot n^{1-c(\alpha)(\theta/\pi)(\cos\theta)^\alpha(1+o(1))}) \\ &= 0(\log n) \end{aligned}$$

in view of our choice of $c(\alpha)$: indeed, since $\alpha \geq 0$, we must have $c(\alpha) \geq 2$.

Remarks

1. [*Optimality of the result*]. In view of the lower bound of Theorem 1, we will not be able to improve upon Theorem 2.
2. [*The average value of N*]. Carnal (1970) has shown that for $f \in \mathscr{P}(\alpha)$,

$$\lim_{n\to\infty} E(N) = K(\alpha) = 4\pi\Gamma\left(\alpha+\frac{1}{2}\right)\Big/\Gamma^2\left(\frac{\alpha+1}{2}\right)$$

where

$$I(u) = 2\int_0^\infty \frac{1}{(1+z^2)^{u+1/2}}\,dz.$$

It is easy to check that $K(\alpha)$ is increasing in α, and that $K(0)=4$ and $K(1)=6$. Thus, the collections $\mathcal{P}(\alpha)$ have sparse convex hulls. It is interesting however that we can control to a certain extent the average size of our random convex hull by choosing α and applying our algorithm with a very large n.

3. [*Examples*]. The multivariate t-distribution with parameter $\nu > 0$ has density

$$f(x) = \frac{1}{2\pi\left(1+\frac{1}{\nu}\|x\|^2\right)^{1+\nu/2}}.$$

Thus, $h(r) = r/(1+r^2/\nu)^{1+\nu/2}$, $r>0$. When $\nu = 1$, we obtain the multivariate Cauchy distribution[17]. Random variables from this distribution can be obtained in many different manners: (1) as $\sqrt{(2\nu E/Y)}$ where E is an exponential random variate, and Y is a chi-square random variate with ν degrees of freedom; (2) by the rejection method. We also need to generate random variates from the tail of h in uniformly bounded average time: here the obvious method seems to be the rejection method with a dominating Pareto density $c/r^{1+\nu}$. The details are trivial to work out. For fast algorithms for the generation of chi-square random variates, we refer to a recent survey article by Tadikamalla and Johnson[32]. For ν greater than 2, competitive algorithms include G4PE[29], GRUB[20], and RGAMA[16, 23]. Best[4] has given a very short but marginally slower algorithm. For ν smaller than 2, see Ahrens and Dieter[1].

4. [*Choice of* $c(\alpha)$]. The function $\theta(\cos\theta)^\alpha$ is unimodal on $0 \le \theta \le \pi/2$, so its maximum can easily be obtained numerically for each $\alpha > 0$. For those who are not willing to go through this small effort and those who want an idea of how $c(\alpha)$ changes with α, we give a couple of tight sufficient lower bounds for $c(\alpha)$:

(1) $c(0) > 2$.

(2) For all $\alpha \ge 1$, $c(\alpha) > \pi/\cos 1$.

(3) For $\alpha > (4/\pi^2) - (1/2)$, it suffices to take $c(\alpha) > [\sqrt{(\alpha+1/2)}/\cos^\alpha(1/\sqrt{(\alpha+1/2)})]$.

To see this, note that $\theta(\cos\theta)^\alpha \ge \theta(1-\theta^2/2)^\alpha$, and that the latter expression is maximal when $\theta^2 = 1/(\alpha+1/2)$.

As $\alpha\to\infty$, the maximum of $\theta(\cos\theta)^\alpha$ is reached for $\theta(\alpha)\sim 1/\sqrt{\alpha}$, and the infimum of $\pi/(\theta(\cos\theta)^\alpha) \sim \pi\sqrt{(\alpha e)}$. It is easy to check that if the smallest possible value is taken for $c(\alpha)$, then our upper bound for $E(T)$ is $0(\log n)$ where the constant in "0" is proportional to $\sqrt{\alpha}$: thus, as α grows larger, our algorithm will require more time. This is not surprising since $E(N)$ is also an increasing function of α.

3.3 *Densities with an exponential tail*

Definition. $\mathscr{E}(\alpha)$ is the collection of radial densities such that H has a density h that is nonincreasing for all r large enough, and

$$\lim_{r\to\infty} \frac{rL'(r)}{L(r)} = \alpha > 0,$$

where $L(r) = -\log G(r)$.

THEOREM 3

When $f \in \mathscr{E}(\alpha)$ and $P_n = c(\alpha)[(\log n)^{3/2}/n]$, where $c(\alpha)$ is a constant greater than

$$\frac{e}{3}\left(\frac{2e\alpha}{3}\right)^{1/2},$$

then $E(T) = 0((\log n)^{3/2})$ for the algorithm described in Section 1.

Proof. The proof uses (4), (7) and (10). First we find $\epsilon \in (0,1)$ such that with $b = \alpha(1+\epsilon)$, $a = \alpha(1-\epsilon)$, we have

$$c(\alpha) > \left(\frac{2eb}{3}\right)^{3/2} \frac{1}{2a} = t. \tag{12}$$

Let r^* be so large that for all $r \geq r^*$, we have $(rL'(r)/L(r)) \in (a, b)$. Now, for $r \geq r^*$,

$$h(r) = L'(r)G(r) \geq \frac{a}{r} L(r)G(r) \tag{13}$$

and for $\delta > 0$,

$$\log L(r+\delta) = \log L(r) + \int_r^{r+\delta} \frac{L'(u)}{L(u)}\,\mathrm{d}u \leq \log L(r) + \int_r^{r+\delta} \frac{b}{u}\,\mathrm{d}u = \log L(r) + b \log\left(1+\frac{\delta}{r}\right).$$

Thus, $L(r+\delta) \leq L(r)(1+(\delta/r))^b$, and thus, for $\delta \geq 1$,

$$G(r\delta) = \mathrm{e}^{-L(r\delta)} \geq \mathrm{e}^{-L(r)\delta^b} = G(r)^{\delta^b}. \tag{14}$$

Assume that we can show that

$$a_n \geq (1+\mathrm{o}(1))p_n/t\sqrt{[\log(1/p_n)]}. \tag{15}$$

Then, by (4) and (7),

$$E(T) = 0(np_n + n\,\mathrm{e}^{-np_n} + 1 + n^2p_n\,\mathrm{e}^{-na_n}) = 0((\log n)^{3/2}(1+n\,\mathrm{e}^{-na_n})). \tag{16}$$

But $na_n \geq (1+\mathrm{o}(1))c(\log n)^{3/2}/t\sqrt{(\log n)} = (1+\mathrm{o}(1))(c/t)\log n$. Hence, $n\,\mathrm{e}^{-na_n} = 0(n^{1-(c/t)(1+\mathrm{o}(1))}) = 0(1)$ when $c = c(\alpha) > t$. Replacement in (16) gives the desired result. We are left now with the proof of (15). Combining (10), (13) and (14) gives for $r_n \geq r^*$, $0 < \theta < \pi/2$,

$$\begin{aligned} a_n &\geq 2r_n(1-\cos\theta)^{3/2}h(r_n/\cos\theta) \\ &\geq 2a\cos\theta L(r_n/\cos\theta)G(r_n/\cos\theta)(1-\cos\theta)^{3/2} \\ &\geq 2a\cos\theta L(r_n)G(r_n)^{\cos^{-b}\theta}(1-\cos\theta)^{3/2} \\ &= 2a\cos\theta\log\frac{1}{p_n}\,p_n^{\cos^{-b}\theta}(1-\cos\theta)^{3/2}. \end{aligned}$$

Let $\cos\theta = 1-u$ where $u = u(n) \to 0$ as $n \to \infty$. Then $(1-\cos\theta)^{3/2} = u^{3/2}$, $\cos\theta = 1+\mathrm{o}(1)$ and $\cos^{-b}\theta = (1-u)^{-b} = 1+bu+0(u^2)$. It is clear that we should choose u so as to maximize $u^{3/2}p_n^{bu}$: this gives the choice $u = 3/(2b\log(1/p_n))$, and we have $u^{3/2}p_n^{bu} = [3/(2be\log(1/p_n))]^{3/2}$. Also, $p_n^{u^2} \to 1$ as $n \to \infty$. Combining all these estimates gives

$$a_n \geq (1+\mathrm{o}(1))2a(3/(2be))^{3/2}p_n/\sqrt{\left(\log\frac{1}{p_n}\right)},$$

which is identical to (15).

Remarks

1. [*Examples*]. Assume that

$$G(r) = \exp(-r^\alpha Q(r)), \quad \alpha > 0,$$

where Q is such that $-G'(r)$ is eventually monotone and that $(rQ'(r)/Q(r)) \to 0$ as $r \to \infty$. Generally speaking, Q must be a function that does not increase or decrease too quickly as

$r \to \infty$. For example, with $Q(r) = 1$, we obtain an exponential family that includes the *normal density* for $\alpha = 2$, and generation of random variates with distribution function G is trivial by the inversion method. If Q satisfies the given conditions, then f is in $\mathscr{E}(\alpha)$. For more complicated functions Q, the inversion method will no longer be useful for the generation of random variates. Also, the solution of the equation $G(r_n) = p_n$ seems to be harder.

2. [*Average value of N*]. Carnal has shown in 1970 that for the class of radial densities with $G(r) = \exp(-r^\alpha)$, $\alpha > 0$, we have

$$E(N) \sim \surd(4\pi\alpha \log n).$$

As for the class $\mathscr{P}(\alpha)$, $E(T)$ is about $\log n$ times larger than $E(N)$.

3. [*Generalizations*]. It is easy to apply the principles developed in the present paper to other classes of distributions. In essence the class $\mathscr{P}(0)$ contains all very fat-tailed radial densities, and $\mathscr{U}_{\alpha>0} P(\alpha)$ contains all polynomial-tailed radial densities. As a prototype of small-tailed radial densities, we took $\mathscr{E}(\alpha)$, $\alpha > 0$. It is clear that there are many other classes with even smaller infinite tails.

3.4 *The uniform density on the circle*

Let f be the uniform density on the circle C with unit radius and center at the origin. Clearly, if $\theta \in (0, \pi/2)$ is the angle between the x-axis and the point where A cuts C, then θ depends upon n, and the following relations hold:

$$p_n = 1 - r_n^2, \quad r_n = \cos\theta, \quad a_n = \theta - \frac{1}{2}\sin 2\theta.$$

We have the following inequalities:

$$1 - \frac{\theta^2}{2} + \frac{\theta^4}{48} \ge r_n \ge 1 - \frac{\theta^2}{2};$$

$$\theta^2 \ge \theta^2 - \frac{\theta^4}{4} = 1 - \left(1 - \frac{\theta^2}{2}\right)^2 \ge p_n \ge 1 - \left(1 - \frac{\theta^2}{2} + \frac{\theta^4}{48}\right)^2 \ge \theta^2 - \frac{7\theta^4}{24} \ge \frac{\theta^2}{4};$$

$$\frac{2}{3}\theta^3 = \theta - \frac{1}{2}\left(2\theta - \frac{1}{6}(2\theta)^3\right) \ge a_n \ge \frac{2}{3}\theta^3 - \frac{2}{15}\theta^5;$$

$$\theta = \arccos \surd(1 - p_n) = \arcsin \surd p_n \ge \surd p_n.$$

As $\theta \to 0$, $p_n \to 0$, we have

$$r_n = 1 - \frac{\theta^2}{2} + 0(\theta^4); \quad p_n = \theta^2 + 0(\theta^4); \quad a_n = \frac{2\theta^3}{3} + 0(\theta^5); \quad \theta = \surd(p_n) + 0(p_n^{3/2}).$$

THEOREM 4

The original random convex hull algorithm without the modification of Remark 9 of Section 1 must always satisfy

$$E(T) = \Omega(n^{1/3} \log^{2/3} n)$$

when f is the uniform density on the circle C. Also, if we choose

$$p_n = \left(c \frac{\log n}{n}\right)^{2/3}$$

where $c \ge 3/2$ is a constant, then

$$E(T) = 0(n^{1/3} \log^{2/3} n).$$

Proof. Let

$$b_n = np_n + 1 + nP(R_n < r_n).$$

By (7) we have

$$P(R_n \le r_n) \le e^{-np_n} + 2enp_n\, e^{-na_n}.$$

To prove the second half of Theorem 4, we merely substitute the given value of p_n into the inequality for b_n. Since $n^{p_n} = \exp(p_n \log n) \to 1$ and $c \ge 3/2$, we have

$$b_n \le [c^2 n \log^2 n]^{1/3} + 1 + n \exp(-[c^2 n \log^2 n]^{1/3})$$
$$+ 2e[c^2 n \log^2 n]^{1/3} \exp\left(-\frac{2}{3} c \log n \cdot (1 - 0(p_n))\right) = 0(n^{1/3} \log^{2/3} n).$$

By (4), the second half of Theorem 4 follows.

To prove the first half of the Theorem, we fix $d = \overline{\pi/\theta}$ (≥ 2) disjoint open segments of the shape and size of A around the circle (all are outside the circle with radius r_n but touch it at some point). Call these segments $A_1, \ldots, A_d$. Then

$$P(R_n < r_n) \ge P\Big(\bigcup_{j=1}^{d} [|A_j| = 0]\Big) = 1 - \prod_{j=1}^{d} P\Big(|A_j| > 0 \Big| \bigcap_{i<j} [|A_i| > 0]\Big)$$
$$\ge 1 - \prod_{j=1}^{d} P(|A_j| > 0) = 1 - (1 - (1 - a_n)^n)^d$$
$$\ge 1 - \exp(-d(1 - a_n)^n) \ge \frac{1}{2} \min(1, d(1 - a_n)^n)$$

where we used the inequalities $1 - e^{-x} \ge x - x^2/2 \ge x/2$, $x \le 1$, and $1 - e^{-x} \ge 1 - 1/e \ge 1/2$, $x \le 1$. Thus,

$$b_n \ge np_n + \frac{n}{2} \min(1, d(1 - a_n)^n).$$

The theorem follows by (5) if we can show that $b_n = \Omega(n^{1/3} \log^{2/3} n)$ for any choice of p_n.

To see this, we consider three cases (with possible overlap):

(1) $d(1 - a_n)^n \ge 1$: $b_n \ge n/2$.

(2) $d(1 - a_n)^n < 1$, $\theta^3 \ge (\log n/n)(1 - (\log\log n/\log n))$: $b_n \ge n\theta^2/4 = (1 + 0(1)/4) n^{1/3} \log^{2/3} n$.

(3) $d(1 - a_n)^n < 1$, $\theta^3 < (\log n/n)(1 - (\log\log n/\log n))$: for n so large that $\theta^3 \le 3/2$, we have

$$b_n \ge n\left(1 - \frac{2\theta^3}{3}\right)^n \ge n \exp\left(-\frac{2\theta^3 n}{3(1 - 2\theta^3/3)}\right)$$

because $1 - x \ge \exp(-x/(1 - x))$, $x \in (0, 1)$.

Thus,

$$b_n \ge n \exp\left(\left(-\frac{2}{3}\log n + \frac{2}{3}\log\log n\right)\Big/\left(1 - \frac{2}{3}\frac{\log n}{n}\right)\right)$$
$$\ge n^{1/3} \log^{2/3} n \cdot \left(\frac{\log n}{n}\right)^{-(2/3)+(2/3-2\log n/n)} = n^{1/3} \log^{2/3} n \cdot (1 + o(1)).$$

Combining these cases shows that $b_n = \Omega(n^{1/3} \log^{2/3} n)$.

Remarks

1. [*Optimality*]. In Theorem 4, we established the optimal rate of convergence for our algorithm, and indicated how it can be achieved by a proper choice of p_n. Note that the optimal rate $n^{1/3} \log^{2/3} n$ for $E(T)$ is again slightly larger than the lower bound established in (1) for *all* algorithms: $E(T) = \Omega(E(N)) = \Omega(n^{1/3})$.

2. [*Generalizations*]. Carnal has shown that if $G(r) = 0$, $r > 1$, and $G(r) \sim c(1-r)^q$ for some $c, q > 0$ as $r \uparrow 1$, then $E(N) \sim c' n^{1/(2q+1)}$ for some $c' > 0$. This result takes care of a large group of radial densities with compact support. The uniform density on the unit circle is obtained for $G(r) = 1 - r^2 \sim 2(1-r)$, $r \uparrow 1$. With minor additional effort, Theorem 4 can be extended to include this class of radial densities as well.

4. ELLIPTICALLY SYMMETRIC DISTRIBUTIONS

Let A be a 2×2 positive definite matrix, and let L be the unique lower triangular matrix (2×2) such that $A = LL'$ (t denotes the transpose). Then, by elementary results on transformations of random vectors (see for example, Roussas ([28], p. 168)), we know that if X has the density

$$f(x) = g(x^t x) = g(\|x\|), \quad x \in R^2,$$

then $Y = LX$ has the density

$$|\det L|^{-1} g(x^t L^{-1t} L^{-1} x) = |\det A|^{-1/2} g(x^t A^{-1} x), \quad x \in R^2.$$

Any random variable that can be obtained by such a transformation from a radial random variable is said to be elliptically symmetric: its density has elliptical equal-probability contours. Since covex hulls are invariant under linear transformations, the problem of the generation of a random convex hull for an underlying density f of an elliptically symmetric random variable seems trivial: first generate the random convex hull for the corresponding radial density, and then apply the appropriate linear transformation to the components of the random convex hull.

5. REFERENCES

1. J. H. Ahrens and U. Dieter, Computer methods for sampling from gamma, beta, Poisson and binomial distributions. *Computing* **12**, 223–246 (1974).
2. J. H. Ahrens and U. Dieter, Sampling from binomial and Poisson distributions: a method with bounded computation times. *Computing* **25** (1980).
3. J. L. Bentley and M. I. Shamos, Divide and conquer for linear expected time. *Inform. Proc. Letters* **7**, 87–91 (1978).
4. D. J. Best, Letter to the editor. *Appl. Stat.* **27**, 181 (1978).
5. D. J. Best, A simple algorithm for the computer generation of random samples from a Student's t or symmetric beta distribution. *COMPSTAT* 1978, pp. 341–347. Physica-Verlag, Wien (1978).
6. H. Carnal, Die konvexe Hülle von n rotationssymmetrische verteilten Punkten. *Zeitschrift für Wahrscheinlichkeitstheorie und verwandte Gebiete* **15**, 168–176 (1970).
7. L. Devroye, Generating the maximum of independent identically distributed random variables. *Comput. Math. Applic.* **6**, 305–315 (1980).
8. L. Devroye and A. Naderisamani, *A binomial random variate generator.* School of Computer Science, McGill University, Montreal, 1980.
9. L. Devroye and G. T. Toussaint, A note on linear expected time algorithms for finding convex hulls. *Computing* **26**, 361–366 (1981).
10. L. Devroye and T. Klincsek, On the average time behavior of distributive sorting algorithms. *Computing* **26**, 1–7 (1981).
11. L. Devroye, How to reduce the average complexity of convex hull finding algorithms. *Comput Math. Applic.* **7**, 299–308 (1981a).
12. L. Devroye, On the average complexity of some bucketing algorithms. *Comput. Math. Applic.* **7**, 407–412 (1981b).
13. L. Devroye, Moment inequalities for random variables in computational geometry. School of Computer Science, McGill University, Montreal (1981c).
14. L. Devroye, Recent results on the average time behavior of some algorithms in computational geometry. *Proc. 13th Symp. Interface.* Computer Science and Statistics, Springer-Verlag, Berlin (1981d).
15. R. Graham, An efficient algorithm for determining the convex hull of a finite planar set. *Inform. Proc. Letters* **1**, 132–133 (1972).
16. A. J. Greenwood, A fast generator for gamma-distributed random variables. *COMPSTAT* 1974, pp. 19–27. Physica-Verlag, Wien (1974).
17. N. L. Johnson and S. Kotz, *Distributions in Statistics*: *Continuous Multivariate Distributions.* John Wiley, New York (1972).
18. D. Kelker, Distribution theory of spherical distributions and a location-scale parameter generalization. *Sankhya Series A* **32**, 419–430 (1970).
19. A. J. Kinderman, J. F. Monahan and J. G. Ramage, Computer methods for sampling from Student's t distribution. *Math. Comput.* **31**, 1009–1018 (1977).
20. A. J. Kinderman and J. F. Monahan, Recent developments in the computer generation of Student's t and gamma random variables. *Proc. ASA Statistical Computing Section*, pp. 90–94 (1978). Also: *Technical Report AMD-799*, BNL - 24679, Brookhaven National Laboratory (1978).
21. D. Lurie and H. O. Hartley, Machine generation of order statistics for Monte Carlo computation. *Am. Statistician* **26**, 26–27 (1972).

22. D. Lurie and R. L. Mason, Empirical investigation of several techniques for computer generation of order statistics. *Commun. Statistics* **2**, 363–371 (1973).
23. G. Marsaglia, The squeeze method for generating gamma variates. *Comput. Math. Applics* **3**, 321–325 (1977).
24. G. Marsaglia, Discrete random variate generation. *Proc. 13th Symp. Interface: Computer Science and Statistics.* Springer-Verlag, Berlin (1981).
25. R. Pyke, Spacings. *J. Roy. Statis. Soc. Ser. B* **27**, 395–449 (1965).
26. A. Renyi and R. Sulanke, Uber die konvexe Hülle von n zufällig gewählten Punkten. *Zeitschrift für Wahrscheinlichkeitstheorie und verwandte Gebiete* **2**, 75–84 (1963); **3**, 138–147 (1964).
27. A. Renyi and R. Sulanke, Zufällige konvexe Polygone in einem Ringgebeit. *Zeitschrift für Wahrscheinlichkeitstheorie und verwandte Gebiete* **9**, 146–157 (1968).
28. G. Roussas, *A First Course in Mathematical Statistics.* Addison-Wesley, Reading, Mass. (1973).
29. B. W. Schmeiser and R. Lal, Squeeze methods for generating gamma variates. *J. Am. Statist. Assoc.* **75**, 679–682 (1980).
30. W. R. Schucany, Order statistics in simulation. *J. Statist. Comput. Simulation* **1**, 281–286 (1972).
31. M. I. Shamos, Computational geometry. Ph.D. Dissertation, Yale University, New Haven, Connecticut (1978).
32. P. R. Tadikamalla and M. E. Johnson, A survey of gamma variate generators. *Tech. Rep.* LA-UR 80-3035. Los Alamos Scientific Laboratory, Los Alamos, New Mexico (1980).