
Chapter Fifteen

THE RANDOM BIT MODEL

1. THE RANDOM BIT MODEL.

1.1. Introduction.

Chapters I-XIV are based on the premises that a perfect uniform $[0,1]$ random variate generator is available and that real numbers can be manipulated and stored. Now we drop the first of these premises and instead assume a perfect bit generator (i.e., a source capable of generating iid $\{0,1\}$ random variates $B_1, B_2, \dots$), while still assuming that real numbers can be manipulated and stored, as before: this is for example necessary when someone gives us the probabilities p_n for discrete random variate generation. The cost of an algorithm can be measured in terms of the number of bits required to generate a random variate. This model is due to Knuth and Yao (1976) who introduced a complexity theory for nonuniform random variate generation. We will report the main ideas of Knuth and Yao in this chapter.

If random bits are used to construct random variates from scratch, then there is no hope of constructing random variates with a density in a finite amount of time. If on the other hand we are to generate a discrete random variate, then it is possible to find finite-time algorithms. Thus, we will mainly be concerned with discrete random variate generation. For continuous random variate generation, it is possible to study the relationship between the number of input bits needed per n bits of output, and to develop a complexity theory based upon this relationship. This will not be done here. See however Knuth and Yao (1976).

1.2. Some examples.

Assume first that we wish to generate a binomial random variate with parameters $n=1$ and $p \neq \frac{1}{2}$. This can be considered as the simulation of a biased coin flip, or the simulation of the occurrence of an event having probability p . If p were $\frac{1}{2}$, we could just exit with B_1 . When p has binary expansion

$$p = 0.p_1p_2p_3 \cdots$$

it suffices to generate random bits until for the first time $B_i \neq p_i$, and to return 1 if $B_i < p_i$ and 0 otherwise:

Binomial (1,p) generator

```

i ← 0
REPEAT
    i ← i + 1
    Generate a random bit B.
UNTIL B ≠ pi
RETURN X ← IB < pi

```

If we define the uniform [0,1] random variate

$$U = 0.B_1B_2B_3 \cdots,$$

then it is easy to see that this simple algorithm returns

$$I_{U \leq p}.$$

Interestingly, the probability of exiting after i bits is 2^{-i} , so that the expected number of bits needed is precisely 2, independent of p . We recognize in this example the inversion method.

The rejection method too has a nice analog. Suppose that we want to generate a random integer X where $P(X=i)=p_i$, $1 \leq i \leq n$, and that all probabilities p_i are multiples of $\frac{1}{M}$, where $2^{k-1} < M \leq 2^k$ for some integer k . Then we can consider consecutive k -tuples in the sequence $B_1, B_2, \dots$ and set up a table with 2^k entries: M entries are used for storing integers between 1 and M , and the remaining entries are 0. If $p_i = l_i/M$, then the integer i should appear l_i times in the table. An integer 0 indicates a rejection. Now use

Theorem 3.1.

Let $(p_1, p_2, \dots, p_n)$ be a discrete probability vector (where n may be infinite). Assume first that $\sum_{i=1}^n \nu(p_i) < \infty$. Then there exists a DDG-tree algorithm for which

$$E(N) = \sum_{i=1}^n \nu(p_i).$$

In fact, the following statements are equivalent for any DDG-tree algorithm:

- (I) $P(N > k)$ is minimized for all $k \geq 0$ over all DDG-tree algorithms for the given distribution.
- (II) For all $k \geq 0$ and all $1 \leq i \leq n$, there are exactly p_{ik} terminal nodes marked i on level k where p_{ik} denotes the coefficient of 2^{-k} in the binary expansion of p_i .
- (III) $E(N) = \sum_{i=1}^n \nu(p_i)$.

Assume next that $\sum_{i=1}^n \nu(p_i) = \infty$. Then, statements (I) and (II) are equivalent.

Proof of Theorem 3.1.

We inherit the notation of the proof of Theorem 2.1. By inspecting that proof, we note that a DDG-tree algorithm attains the lower bound (if it is finite) if and only if for all i and k , we have equality in

$$\sum_{j>k} \frac{t_i(j)}{2^j} = p_i - \sum_{0 \leq j \leq k} \frac{t_i(j)}{2^j} \geq \frac{\chi(2^j p_i)}{2^j}.$$

This means that

$$\sum_{j=0}^k t_i(j) 2^{k-j} = \lfloor 2^k p_i \rfloor.$$

But this says simply that $t_i(k)$ is p_{ik} for all k . The number of terminal nodes at level k for integer i is 0 or 1 depending upon the value of the k -th bit in the binary expansion of p_i . To prove that such DDG-trees actually exist, define $t_i(k)$ and $t(k)$ by

$$\begin{aligned} t_i(k) &= p_{ik} \\ t(k) &= p_1(k) + \dots + p_n(k). \end{aligned}$$

Thus, we certainly have

$$\begin{aligned} \sum_{k \geq 0} 2^{-k} t_i(k) &= p_i \\ \sum_{k \geq 0} 2^{-k} t(k) &= 1. \end{aligned}$$

A DDG-tree with these conditions exists if and only if the integers $b(k)$ defined by

$$\begin{aligned} b(0) + t(0) &= 1, \\ b(k) + t(k) &= 2b(k-1) \quad (k \geq 1) \end{aligned}$$

are nonnegative. But the $b(k)$'s thus defined have a solution

$$b(k) = \sum_{j > k} \frac{t(j)}{2^{j-k}}.$$

Hence $b(k) \geq 0$, and such trees exist. This proves all the statements involving (III). For the equivalence of (I) and (II) in all cases, we note that in Theorem 2.1, we have obtained a lower bound for $b(k)$ for all k , and that the construction of the present theorem gives us a tree for which the lower bound is attained for all k . But $P(N > k) = \frac{b(k)}{2^k}$, and we are done. ■

Let us give an example of the optimal construction.

Example 3.1. (Knuth and Yao, 1976)

Consider the transcendental probabilities

$p_1 = \frac{1}{\pi}$	$= 0.010100010111110...$
$p_2 = \frac{1}{e}$	$= 0.010111100010110...$
$p_3 = 1 - p_1 - p_2$	$= 0.010100000101010...$

The optimal tree is inherently infinite and cannot be obtained by a finite state machine (this is possible if and only if all probabilities are rational). The optimal tree has at each level between 0 and 3 terminal nodes, and can be constructed without too much trouble. Basically, all internal nodes have two children, and at each level, we put the terminal nodes to the right on that level. This usually gives an asymmetric left-heavy tree. Using the notation I for internal node, and 1,2,3 for terminal nodes for the integers 1,2,3 respectively, we can specify the optimal DDG-tree by specifying the nature of all the nodes on each level, from

left to right. In the present example, this gives

Level	Nodes			
0	I			
1	I	I		
2	I	1	2	3
3	I	I		
4	I	1	2	3
5	I	2		
6	I	2		
7	I	2		
8	I	1		
9	I	I		
10	I	I	1	3
11	I	I	1	2
12	I	I	1	3
13	I	I	1	2
14	I	1	2	3
15	I	I		

3.3. Distribution-free inequalities for the performance of optimal DDG-tree algorithms.

We have seen that an optimal DDG-tree algorithm requires on the average

$$E(N) = \sum_{i=1}^n \nu(p_i)$$

random bits. By an inequality shown in Theorem 2.1, $H(x) \leq \nu(x) < H(x) + 2x$, $x \in [0,1]$, we see that for optimal algorithms,

$$\begin{aligned} \sum_{i=1}^n H(p_i) &= H(p_1, \dots, p_n) \\ &\leq E(N) \leq H(p_1, \dots, p_n) + 2. \end{aligned}$$

Thus, the performance is roughly speaking proportional to the entropy of the distribution. In general, this quantity is not known beforehand. Often one wants a priori guarantees about the performance of the algorithm. Thus, distribution-free bounds on $E(N)$ for the optimal algorithm can be very useful. We offer:

Theorem 3.2. (Knuth and Yao, 1976)

Let $p_1, \dots, p_n$ be a finite probability vector. Then,

$$2^{-2^{2-n}} \leq \sum_{i=1}^n \nu(p_i) \leq \left\lceil \log_2(n) \right\rceil + (n-1)2^{1-\left\lceil \log_2(n) \right\rceil}.$$

Proof of Theorem 3.2.

By definition of χ and ν ,

$$\chi(2^k p_1) + \dots + \chi(2^k p_n) \leq \min(2^k, n-1)$$

for all $k \geq 0$. The $n-1$ upper bound follows by noting that the left hand side is less than n , and that it is integer valued because it can be written as

$$2^k - \left\lfloor 2^k p_1 \right\rfloor - \dots - \left\lfloor 2^k p_n \right\rfloor.$$

Thus,

$$\begin{aligned} \sum_{i=1}^n \nu(p_i) &= \sum_{k \geq 0} \sum_{i=1}^n 2^{-k} \chi(2^k p_i) \\ &\leq \sum_{k \geq 0} 2^{-k} \min(2^k, n-1) \\ &= \sum_{0 \leq k \leq \left\lfloor \log_2(n-1) \right\rfloor} 1 + \sum_{k > \left\lfloor \log_2(n-1) \right\rfloor} \frac{n-1}{2^k} \\ &= 1 + \left\lfloor \log_2(n-1) \right\rfloor + \frac{n-1}{2^{\left\lfloor \log_2(n-1) \right\rfloor + 1}}. \end{aligned}$$

The upper bound follows when we note that $\left\lfloor \log_2(n-1) \right\rfloor = \left\lceil \log_2(n) \right\rceil - 1$. Let us now turn to the lower bound. Using the notation of the proof of Theorem 2.1, an optimal DDG-tree always has

$$\begin{aligned} \sum_{i=1}^n \nu(p_i) &= \sum_{k \geq 1} \frac{kt(k)}{2^k} \\ &= \sum_{k \geq 1} \frac{k(2b(k-1) - b(k))}{2^k} \\ &= \sum_{k \geq 0} \frac{b(k)}{2^k}. \end{aligned}$$

Since $\sum_{k \geq 0} b(k) \geq n-1$ (there are $\geq n$ terminal nodes, and thus $\geq n-1$ internal nodes), and since conditional on the latter sum being equal to s , the minimum of $\sum_{k \geq 0} \frac{b(k)}{2^k}$ is reached for $b(0) = \dots = b(s-1) = 1$, we see that

$$\sum_{i=1}^n \nu(p_i) \geq 2^{-2^{1-s}} \geq 2^{-2^{2-n}}. \blacksquare$$

3.4. Exercises.

1. The bounds of Theorem 3.2 are best possible. By inspection of the proof, construct for each n a probability vector $p_1, \dots, p_n$ for which the lower bound is attained. (Conclude that for this family of distributions, the expected performance of optimal DDG-tree algorithms is uniformly bounded in n .) Show that the upper bound of the theorem is attained for

$$p_i = \begin{cases} 2^{-q} \left(\frac{2^n - 2^{i-1} - 1}{2^n - 1} \right) + 2^{-q} & , 1 \leq i \leq 2^q + 1 - n , \\ 2^{-q} \left(\frac{2^n - 2^{i-1} - 1}{2^n - 1} \right) & , 2^q + 1 - n < i \leq n , \end{cases}$$

where $q = \lceil \log_2(n) \rceil$ (Knuth and Yao, 1976).

2. Describe an optimal DDG-tree algorithm of the shape described in Example 3.1, which requires storage of the probability vector only. In other words, the tree is constructed dynamically. You can assume of course that the p_n 's can be manipulated in your computer.
3. **Finite state machines.** Show that there exists a finite state machine (edges correspond to random bits, nodes to internal nodes or terminal nodes) for generating a discrete random variate X taking values in $\{1, \dots, n\}$ if and only if all probabilities involved are rational. Give a general procedure for constructing such finite state machines from (not necessarily optimal) DDG-trees by introducing rejection nodes and feedbacks to internal nodes. For simulating one die, find a finite state machine requiring on the average $\frac{11}{3}$ random bits. Is this optimal? For simulating the sum of two dice, find a finite state machine which requires on the average $\frac{79}{18}$ random bits. For simulating two dice (NOT the sum), find a finite state machine which requires on the average $\frac{20}{3}$ random bits. Show that all of these numbers are optimal. Note that in the last case, we do better than just simulating one die twice with the first algorithm since this would have eaten up $\frac{22}{3}$ random bits on the average (Knuth and Yao, 1976).
4. Consider the following 5-state automaton: there is a START state, two terminal states, A and B, and two other states, S1 and S2. Transitions between states occur when bits are observed. In particular, we have:

START + 0 $\rightarrow$ S1
 START + 1 $\rightarrow$ S2
 S1 + 0 $\rightarrow$ A
 S1 + 1 $\rightarrow$ S2
 S2 + 0 $\rightarrow$ B
 S2 + 1 $\rightarrow$ START

If we start at START, and observe a perfect sequence of random bits, then what is $P(A)$, $P(B)$? Compute the expected number of bits before halting. Finally, construct the optimal DDG-tree algorithm for this problem and find a finite-state equivalent form requiring the same expected number of bits.

REFERENCES

- M. Abramowitz and I.A. Stegun, *Handbook of Mathematical Tables*, Dover Publications, New York, N.Y., 1970.
- A.G. Adams, "Algorithm 39. Areas under the normal curve," *Computer Journal*, vol. 12, pp. 197-198, 1969.
- A.V. Aho, J.E. Hopcroft, and J.D. Ullman, *Data Structures and Algorithms*, Addison-Wesley, Reading, Mass., 1983.
- J.H. Ahrens and U. Dieter, "Computer methods for sampling from the exponential and normal distributions," *Communications of the ACM*, vol. 15, pp. 873-882, 1972.
- J.H. Ahrens and U. Dieter, "Extensions of Forsythe's method for random sampling from the normal distribution," *Mathematics of Computation*, vol. 27, pp. 927-937, 1973.
- J.H. Ahrens and U. Dieter, "Computer methods for sampling from gamma, beta, Poisson and binomial distributions," *Computing*, vol. 12, pp. 223-246, 1974.
- J.H. Ahrens and U. Dieter, "Sampling from binomial and Poisson distributions: a method with bounded computation times," *Computing*, vol. 25, pp. 193-208, 1980.
- J.H. Ahrens and U. Dieter, "Generating gamma variates by comparison of probability densities," Institute of Statistics, Technical University Graz, Graz, Austria, 1981.
- J.H. Ahrens and K.D. Kohrt, "Computer methods for efficient sampling from largely arbitrary statistical distributions," *Computing*, vol. 26, pp. 19-31, 1981.
- J.H. Ahrens and U. Dieter, "Computer generation of Poisson deviates from modified normal distributions," *ACM Transactions on Mathematical Software*, vol. 8, pp. 163-179, 1982.
- J.H. Ahrens and U. Dieter, "Generating gamma variates by a modified rejection technique," *Communications of the ACM*, vol. 25, pp. 47-54, 1982.
- J.H. Ahrens, K.D. Kohrt, and U. Dieter, "Algorithm 599. Sampling from gamma and Poisson distributions," *ACM Transactions on Mathematical Software*, vol. 9, pp. 255-257, 1983.

- J.H. Ahrens and U. Dieter, "Sequential random sampling," *ACM Transactions on Mathematical Software*, vol. 11, pp. 157-169, 1985.
- J. Aitchison, "Inverse distributions and independent gamma-distributed products of random variables," *Biometrika*, vol. 50, pp. 505-508, 1963.
- H. Akima, "A new method of interpolation and smooth curve fitting based on local procedures," *Journal of the ACM*, vol. 17, pp. 589-602, 1970.
- B.J. Alder and T.E. Walnwright, "Phase transition in elastic disks," *Physical Review*, vol. 127, pp. 359-361, 1962.
- M.M. Ali, N.N. Mikhall, and M.S. Haq, "A class of bivariate distributions including the bivariate logistic," *Journal of Multivariate Analysis*, vol. 8, pp. 405-412, 1978.
- T.W. Anderson and D.A. Darling, "Asymptotic theory of certain goodness of fit criteria based on stochastic processes," *Annals of Mathematical Statistics*, vol. 23, pp. 193-213, 1952.
- D.F. Andrews and C.L. Mallows, "Scale mixtures of normal distributions," *Journal of the Royal Statistical Society Series B*, vol. 36, pp. 99-102, 1974.
- N.P. Archer, "The generation of piecewise linear approximations of probability distribution functions," *Journal of Statistical Computation and Simulation*, vol. 11, pp. 21-40, 1980.
- G. Arfwedson, "A probability distribution connected with Stirling's second class numbers," *Skandinavisk Aktuarietidskrift*, vol. 34, pp. 121-132, 1951.
- A.N. Arnason, "Simple exact, efficient methods for generating beta and Dirichlet variates," *Utilitas Mathematica*, vol. 1, pp. 249-290, 1972.
- B.C. Arnold, "A note on multivariate distributions with specified marginals," *Journal of the American Statistical Association*, vol. 62, pp. 1460-1461, 1967.
- B.C. Arnold and R.A. Groeneveld, "Some properties of the arcsine distribution," *Journal of the American Statistical Association*, vol. 75, pp. 173-175, 1980.
- D.B. Arnold and M.R. Sleep, "Uniform random number generation of n balanced parenthesis strings," *ACM Transactions on Programming Languages and Systems*, vol. 2, pp. 122-128, 1980.
- A.C. Atkinson and M.C. Pearce, "The computer generation of beta, gamma and normal random variables," *Journal of the Royal Statistical Society Series A*, vol. 139, pp. 431-461, 1976.
- A.C. Atkinson and J. Whittaker, "A switching algorithm for the generation of beta random variables with at least one parameter less than one," *Journal of the Royal Statistical Society Series A*, vol. 139, pp. 462-467, 1976.
- A.C. Atkinson, "An easily programmed algorithm for generating gamma random variables," *Applied Statistics*, vol. 140, pp. 232-234, 1977.
- A.C. Atkinson, "A family of switching algorithms for the computer generation of beta random variables," *Biometrika*, vol. 66, pp. 141-145, 1979.
- A.C. Atkinson and J. Whittaker, "The generation of beta random variables with one parameter greater than one and one parameter less than one," *Applied Statistics*, vol. 28, pp. 90-93, 1979.

- A.C. Atkinson, "The simulation of generalised inverse gaussian, generalised hyperbolic, gamma and related random variables," Research Report 52, Department of Theoretical Statistics, Aarhus University, Aarhus, Denmark, 1979.
- A.C. Atkinson, "Recent developments in the computer generation of Poisson random variables," *Applied Statistics*, vol. 28, pp. 260-263, 1979.
- A.C. Atkinson, "The computer generation of Poisson random variables," *Applied Statistics*, vol. 28, pp. 29-35, 1979.
- A.C. Atkinson, "The simulation of generalized inverse gaussian and hyperbolic random variables," *SIAM Journal on Statistical Computation*, vol. 3, pp. 502-515, 1982.
- S. Baase, *Computer Algorithms: Introduction to Design and Analysis*, Addison-Wesley, Reading, Mass., 1978.
- M. Badel, "Generation de nombres aleatoires correlates," *Mathematics and Computers in Simulation*, vol. 21, pp. 42-49, 1979.
- B.J.R. Bailey, "Alternatives to Hastings' approximation to the inverse of the normal cumulative distribution function," *Applied Statistics*, vol. 30, pp. 275-276, 1981.
- G. de Balbine, "Note on random permutations," *Mathematics of Computation*, vol. 21, pp. 710-712, 1967.
- J. Banks and J.S. Carson, *Discrete Event Simulation*, Prentice-Hall, Englewood Cliffs, N.J., 1984.
- G. Barbu, "On computer generation of a random variable by transformations of uniform variables," *Bull. Math. Soc. Sci. Math. Roumanie*, vol. 26, pp. 129-139, 1982.
- R.E. Barlow, A.W. Marshall, and F. Proschan, "Properties of probability distributions with monotone hazard rate," *Annals of Mathematical Statistics*, vol. 34, pp. 375-389, 1963.
- R.E. Barlow and F. Proschan, *Mathematical Theory of Reliability*, John Wiley, New York, N.Y., 1965.
- R.E. Barlow and F. Proschan, *Statistical Theory of Reliability and Life Testing*, Holt, Rinehart and Winston, New York, N.Y., 1975.
- D.R. Barnard and M.N. Cawdery, "A note on a new method of histogram sampling," *Operations Research Quarterly*, vol. 25, pp. 319-320, 1974.
- O. Barndorff-Nielsen, "Exponentially decreasing distributions for the logarithm of particle size," *Proceedings of the Royal Society of London Series A*, vol. 353, pp. 401-419, 1977.
- O. Barndorff-Nielsen and C. Halgreen, "Infinite divisibility of the hyperbolic and generalized inverse gaussian distributions," *Zeitschrift für Wahrscheinlichkeitstheorie und verwandte Gebiete*, vol. 38, pp. 309-311, 1977.
- O. Barndorff-Nielsen, "Hyperbolic distributions and distributions on hyperbolae," *Scandinavian Journal of Statistics*, vol. 5, pp. 151-157, 1978.

- O. Barndorff-Nielsen and P. Blaesild, "Hyperbolic Distributions," *Encyclopedia of Statistical Sciences*, John Wiley, New York, N.Y., 1980.
- O. Barndorff-Nielsen, J. Kent, and M. Sorensen, "Normal variance-mean mixtures and z distributions," *International Statistical Review*, vol. 50, pp. 145-159, 1982.
- V. Barnett, "Some bivariate uniform distributions," *Communications in Statistics*, vol. A9, pp. 453-461, 1980.
- D.R. Barr and N.L. Slezak, "A comparison of multivariate normal generators," *Communications of the ACM*, vol. 15, pp. 1048-1049, 1972.
- R. Bartels, "Generating non-normal stable variates using limit theorem properties," *Journal of Statistical Computation and Simulation*, vol. 7, pp. 199-212, 1978.
- R. Bartels, "Truncation bounds for infinite expansions for the stable distributions," *Journal of Statistical Computation and Simulation*, vol. 12, pp. 293-302, 1981.
- M.S. Bartlett, "Statistical estimation of density functions," *Sankhya Series A*, vol. 25, pp. 245-254, 1963.
- D.E. Barton, "The matching distributions: Poisson limiting forms and derived methods of approximation," *Journal of the Royal Statistical Society, Series B*, vol. 20, pp. 73-92, 1958.
- D.E. Barton and C.L. Mallows, "Some aspects of the random sequence," *Annals of Mathematical Statistics*, vol. 36, pp. 236-260, 1965.
- D. Basu and R.C. Tiwari, "A note on the Dirichlet process," In *Statistics and Probability: Essays in Honor of C.R. Rao*, ed. G. Kallianpur, P.R. Krishnaiah, J.K. Ghosh, pp. 89-103, North-Holland, 1982.
- J.D. Beasley and S.G. Springer, "The percentage points of the normal distribution," *Applied Statistics*, vol. 26, pp. 118-121, 1977.
- J.R. Bell, "Algorithm 334. Normal random deviates," *Communications of the ACM*, vol. 11, p. 498, 1968.
- R.B. Bendel and A.A. Afifi, "Comparison of stopping rules in forward stepwise regression," *Journal of the American Statistical Association*, vol. 72, pp. 46-53, 1977.
- R.B. Bendel and M.R. Mickey, "Population correlation matrices for sampling experiments," *Communications in Statistics, Section Simulation and Computation*, vol. 7, pp. 163-182, 1978.
- J.L. Bentley and J.B. Saxe, "Generating sorted lists of random numbers," *ACM Transactions of Mathematical Software*, vol. 6, pp. 359-364, 1980.
- H. Bergstrom, "On some expansions of stable distributions," *Arkiv fur Matematik, II*, vol. 18, pp. 375-378, 1952.
- M.B. Berman, "Generating gamma distributed variates for computer simulation models," Technical Report R-641-PR, Rand Corporation, 1971.
- D.J. Best, "Letter to the editor," *Applied Statistics*, vol. 27, p. 181, 1978.

Rejection algorithm

REPEAT

 Generate k random bits, forming the number $Z \in \{0, 1, \dots, 2^k - 1\}$.

UNTIL $Z < M$

RETURN $X \leftarrow A[Z]$ (where A is the table of M integers)

In this algorithm, the expected number of bits required is k divided by the probability of immediate acceptance, i.e.

$$\frac{k}{\frac{M}{2^k}} \leq 2k = 2 \lceil \log_2 M \rceil.$$

In both examples provided here, we can consider the complete unbounded binary tree in which we travel down by turning left when $B_i = 0$ and right when $B_i = 1$. In the rejection method, we have designated M nodes at the k -th level as terminal nodes. The remaining nodes at the k -th level are "rejection nodes", and are in turn roots of similar subtrees. Since these rejection nodes are identified with the overall root, we can superimpose them on the root, and form a pseudo-tree with some loopbacks from the k -th level to the root. But then, we have a finite directed graph, or a finite state machine.

In the inversion method, the expansion of p determines an unbounded path down the tree, and so does the expansion of U . Since we need only determine whether one path is to the left or the right of the other path, it suffices to travel down until the paths separate. With probability $\frac{1}{2}$, they separate right away.

Otherwise, they separate with probability $\frac{1}{2}$ at the next level, and so forth.

What we will do in the sections that follow is

- (i) Develop a lower bound for the expected number of bits in terms of $p_1, p_2, \dots$, the probability vector of the discrete random variate.
- (ii) Develop black box methods and study their expected complexity.

- D.J. Best, "A simple algorithm for the computer generation of random samples from a Student's t or symmetric beta distribution," in *COMPSTAT 1978: Proceedings in Computational Statistics*, ed. L.C.A. Corsten and J. Hermans, pp. 341-347, Physica Verlag, Wien, Austria, 1978.
- D.J. Best, "Some easily programmed pseudo-random normal generators," *Australian Computer Journal*, vol. 11, pp. 60-62, 1979.
- D.J. Best and N.I. Fisher, "Efficient simulation of the von Mises distribution," *Applied Statistics*, vol. 28, pp. 152-157, 1979.
- D.J. Best, "A note on gamma variate generators with shape parameter less than unity," *Computing*, vol. 30, pp. 185-188, 1983.
- W.H. Beyer, *Handbook of Tables for Probability and Statistics*, Cleveland: The Chemical Rubber Co., 1968.
- G.P. Bhattacharjee, "Algorithm AS32. The incomplete gamma integral," *Applied Statistics*, vol. 19, pp. 285-287, 1970.
- B.C. Bhattacharyya, "The use of McKay's Bessel function curves for graduating frequency distributions," *Sankhya Series A*, vol. 6, pp. 175-182, 1942.
- A. Bignami and A. de Mattels, "A note on sampling from combinations of distributions," *Journal of the Institute of Mathematics and its Applications*, vol. 8, pp. 80-81, 1971.
- P. Blaesild, "The shape of the generalized inverse gaussian and hyperbolic distributions," Research Report 37, Department of Theoretical Statistics, Aarhus University, Aarhus, Denmark, 1978.
- M. Blum, R.W. Floyd, V. Pratt, R.L. Rivest, and R.E. Tarjan, "Time bounds for selection," *Journal of Computers and System Sciences*, vol. 7, pp. 448-461, 1973.
- L.N. Bolshev, "On transformations of random variables," *Theory of Probability and its Applications*, vol. 4, pp. 136-149, 1959.
- L.N. Bolshev, "Asymptotic Pearson transformations," *Theory of Probability and its Applications*, vol. 8, pp. 129-155, 1963.
- L.N. Bolshev, "On a characterization of the Poisson distribution and its statistical applications," *Theory of Probability and its Applications*, vol. 10, pp. 446-456, 1965.
- L. Bondesson, "On simulation from infinitely divisible distributions," *Advances in Applied Probability*, vol. 14, pp. 855-869, 1982.
- G.E.P. Box and M.E. Muller, "A note on the generation of random normal deviates," *Annals of Mathematical Statistics*, vol. 29, pp. 610-611, 1958.
- J.M. Boyett, "Random $R \times C$ tables with given row and column totals," *Applied Statistics*, vol. 28, pp. 329-332, 1979.
- P. Bratley, B.L. Fox, and L.E. Schrage, *A Guide to Simulation*, Springer-Verlag, New York, N.Y., 1983.
- R.P. Brent, "A gaussian pseudo-random number generator," *Communications of the ACM*, vol. 17, pp. 704-706, 1974.

- G.W. Brown and J.W. Tukey, "Some distributions of sample means," *Annals of Mathematical Statistics*, vol. 17, pp. 1-12, 1946.
- M.C. Bryson and M.E. Johnson, "Constructing and simulating multivariate distributions using Khintchine's theorem," Technical Report LA-UR 81-442, Los Alamos Scientific Laboratory, Los Alamos, New Mexico, 1981.
- M.C. Bryson and M.E. Johnson, "Constructing and simulating multivariate distributions using Khintchine's theorem," *Journal of Statistical Computation and Simulation*, vol. 16, pp. 129-137, 1982.
- I.W. Burr, "Cumulative frequency functions," *Annals of Mathematical Statistics*, vol. 13, pp. 215-232, 1942.
- I.W. Burr and P.J. Cislak, "On a general system of distributions. I. The curve-shape characteristics. II. The sample median," *Journal of the American Statistical Association*, vol. 63, pp. 627-635, 1968.
- I.W. Burr, "Parameters for a general system of distributions to match a grid of a_3 and a_4 ," *Communications in Statistics*, vol. 2, pp. 1-21, 1973.
- J.C. Butcher, "Random sampling from the normal distribution," *Computer Journal*, vol. 3, pp. 251-253, 1961.
- E.L. Butler, "Algorithm 370. General random number generator," *Communications of the ACM*, vol. 13, pp. 49-52, 1970.
- T. Cacoullos, "A relation between t and F distributions," *Journal of the American Statistical Association*, vol. 60, pp. 528-531, p. 1249, 1965.
- A.G. Carlton, "Estimating the parameters of a rectangular distribution," *Annals of Mathematical Statistics*, vol. 17, pp. 355-358, 1946.
- C.P. Chalmers, "Generation of correlation matrices with given eigen-structure," *Journal of Statistical Computation and Simulation*, vol. 4, pp. 133-139, 1975.
- J.M. Chambers, C.L. Mallows, and B.W. Stuck, "A method for simulating stable random variables," *Journal of the American Statistical Association*, vol. 71, pp. 340-344, 1976.
- H.C. Chen and Y. Asau, "On generating random variates from an empirical distribution," *AIIE Transactions*, vol. 6, pp. 163-166, 1974.
- R.C.H. Cheng, "The generation of gamma variables with non-integral shape parameter," *Applied Statistics*, vol. 26, pp. 71-75, 1977.
- R.C.H. Cheng, "Generating beta variates with nonintegral shape parameters," *Communications of the ACM*, vol. 21, pp. 317-322, 1978.
- R.C.H. Cheng and G.M. Feast, "Some simple gamma variate generators," *Applied Statistics*, vol. 28, pp. 290-295, 1979.
- R.C.H. Cheng and G.M. Feast, "Gamma variate generators with increased shape parameter range," *Communications of the ACM*, vol. 23, pp. 389-393, 1980.
- K.C. Cherian, "A bivariate correlated gamma-type distribution function," *Journal of the Indian Mathematical Society*, vol. 5, pp. 133-144, 1941.
- M.A. Chmielewski, "Elliptically symmetric distributions: a review and bibliography," *International Statistical Review*, vol. 49, pp. 67-74, 1981.

- Y.S. Chow, "Some convergence theorems for independent random variables," *Annals of Mathematical Statistics*, vol. 37, pp. 1482-1493, 1966.
- Y.S. Chow and H. Telcher, *Probability Theory. Independence. Interchangeability. Martingales.*, Springer-Verlag, New York, N.Y., 1978.
- E. Cinlar, *Introduction to Stochastic Processes*, Prentice-Hall, Englewood Cliffs, N.J., 1975.
- J.M. Cook, "Rational formulae for the production of a spherically symmetric probability distribution," *Mathematics of Computation*, vol. 11, pp. 81-82, 1957.
- R.D. Cook and M.E. Johnson, "A family of distributions for modelling non-elliptically symmetric multivariate data," *Journal of the Royal Statistical Society, Series B*, vol. 43, pp. 210-218, 1981.
- B.E. Cooper, "Algorithm AS2. The normal integral," *Applied Statistics*, vol. 17, pp. 186-187, 1968.
- D.R. Cox and P.A.W. Lewis, *The Statistical Analysis of Series of Events*, Methuen, London, 1966.
- H. Cramer, *Mathematical Methods of Statistics*, Princeton University Press, Princeton, New Jersey, 1951.
- J.S. Dagpunar, "Sampling of variates from a truncated gamma distribution," *Journal of Statistical Computation and Simulation*, vol. 8, pp. 59-64, 1978.
- M. Darboux, "Sur les developpements en serie des fonctions d'une seule variable," *Journal de Mathematiques Series 3*, vol. 2, pp. 291-294, 1876.
- D.A. Darling, "The Kolmogorov-Smirnov, Cramer-von Mises tests," *Annals of Mathematical Statistics*, vol. 26, pp. 1-20, 1955.
- D. Davey and J.G. Vaucher, "Self-optimizing partition sequencing sets for discrete event simulation," *INFOR*, vol. 18, pp. 21-41, 1980.
- F.N. David and E. Flx, "Rank correlation and regression in a non-normal surface," *Proceedings of the Fourth Berkeley Symposium*, vol. 1, pp. 177-197, 1961.
- Ju.S. Davidovic, B.I. Korenbljum, and B.I. Hacet, "A property of logarithmically concave functions," *Dokl. Akad. Nauk SSR*, vol. 185, pp. 477-480, 1969.
- P.J. Davis and P. Rabinowitz, *Methods of Numerical Integration*, Academic Press, New York, 1975.
- I. Deak, "Comparison of methods for generating uniformly distributed random points in and on a hypersphere," *Problems of Control and Information Theory*, vol. 8, pp. 105-113, 1979.
- I. Deak and B. Bene, "Random number generation: a bibliography," Working paper, Computer and Automation Institute, Hungarian Academy of Sciences, 1979.
- I. Deak, "The ellipsoid method for generating normally distributed random vectors," *Zastosowania Matematyki*, vol. 17, pp. 95-107, 1979.
- I. Deak, "Fast procedures for generating stationary normal vectors," *Journal of Statistical Computation and Simulation*, vol. 16, pp. 225-242, 1980.

- I. Deak, "An economical method for random number generation and a normal generator," *Computing*, vol. 27, pp. 113-121, 1981.
- I. Deak, "General methods for generating non-uniform random numbers," Technical Report DALTR-84-20, Department of Mathematics, Statistics and Computing Science, Dalhousie University, Halifax, Nova Scotia, 1984.
- E.V. Denardo and B.L. Fox, "Shortest-route methods: 1. reaching, pruning, and buckets," *Operations Research*, vol. 27, pp. 161-186, 1979.
- L. Devroye and A. Naderisamanl, "A binomial random variate generator," Technical Report, School of Computer Science, McGill University, Montreal, 1980.
- L. Devroye, "Generating the maximum of independent identically distributed random variables," *Computers and Mathematics with Applications*, vol. 6, pp. 305-315, 1980.
- L. Devroye, "The computer generation of Poisson random variables," *Computing*, vol. 26, pp. 197-207, 1981.
- L. Devroye and C. Yuen, "Inversion-with-correction for the computer generation of discrete random variables," Technical Report, School of Computer Science, McGill University, Montreal, 1981.
- L. Devroye, "Programs for generating random variates with monotone densities," Technical report, School of Computer Science, McGill University, Montreal, Canada, 1981.
- L. Devroye, "Recent results in non-uniform random variate generation," *Proceedings of the 1981 Winter Simulation Conference*, Atlanta, GA., 1981.
- L. Devroye, "The computer generation of random variables with a given characteristic function," *Computers and Mathematics with Applications*, vol. 7, pp. 547-552, 1981.
- L. Devroye, "The series method in random variate generation and its application to the Kolmogorov-Smirnov distribution," *American Journal of Mathematical and Management Sciences*, vol. 1, pp. 359-379, 1981.
- L. Devroye and T. Klineck, "Average time behavior of distributive sorting algorithms," *Computing*, vol. 26, pp. 1-7, 1981.
- L. Devroye, "On the computer generation of random convex hulls," *Computers and Mathematics with Applications*, vol. 8, pp. 1-13, 1982.
- L. Devroye, "A note on approximations in random variate generation," *Journal of Statistical Computation and Simulation*, vol. 14, pp. 149-158, 1982.
- L. Devroye, "The equivalence of weak, strong and complete convergence in L_1 for kernel density estimates," *Annals of Statistics*, vol. 11, pp. 896-904, 1983.
- L. Devroye, "Random variate generation for unimodal and monotone densities," *Computing*, vol. 32, pp. 43-68, 1984.
- L. Devroye, "A simple algorithm for generating random variates with a log-concave density," *Computing*, vol. 33, pp. 247-257, 1984.

- L. Devroye, "On the use of probability inequalities in random variate generation," *Journal of Statistical Computation and Simulation*, vol. 20, pp. 91-100, 1984.
- L. Devroye, "Methods for generating random variates with Polya characteristic functions," *Statistics and Probability Letters*, vol. 2, pp. 257-261, 1984.
- L. Devroye, "The analysis of some algorithms for generating random variates with a given hazard rate," *Naval Research Logistics Quarterly*, vol. 0, pp. 0-0, 1985.
- L. Devroye and L. Györfi, *Nonparametric Density Estimation: The L_1 View*, John Wiley, New York, N.Y., 1985.
- L. Devroye, "An automatic method for generating random variables with a given characteristic function," *SIAM Journal of Applied Mathematics*, vol. 0, pp. 0-0, 1986.
- U. Dieter and J.H. Ahrens, "A combinatorial method for the generation of normally distributed random numbers," *Computing*, vol. 11, pp. 137-146, 1973.
- P.J. Diggle, J.E. Besag, and J.T. Gleaves, "Statistical analysis of spatial point patterns by means of distance methods," *Biometrics*, vol. 32, pp. 659-667, 1976.
- S.D. Dubey, "A compound Weibull distribution," *Naval Research Logistics Quarterly*, vol. 15, pp. 179-188, 1968.
- D. Dugue and M. Girault, "Fonctions convexes de Polya," *Publications de l'Institut de Statistique des Universités de Paris*, vol. 4, pp. 3-10, 1955.
- W.H. Dumouchel, "Stable distributions in statistical inference," Ph.D. Dissertation, Department of Statistics, Yale University, 1971.
- R. Durstenfeld, "Random permutation," *Communications of the ACM*, vol. 7, p. 420, 1964.
- A. Dvoretzky and H. Robbins, "On the parking problem," *Publications of the Mathematical Institute of the Hungarian Academy of Sciences*, vol. 9, pp. 209-225, 1964.
- R. Englebrecht-Wiggans and W.L. Maxwell, "Analysis of the time indexed list procedure for synchronization of discrete event procedures," *Management Science*, vol. 24, pp. 1417-1427, 1978.
- P. Erdos and M. Kac, "On certain limit theorems of the theory of probability," *Bulletin of the American Mathematical Society*, vol. 52, pp. 292-302, 1946.
- P. Erdos and A. Renyi, "On random graphs," *Publ. Math. Debrecen*, vol. 6, pp. 290-297, 1959.
- P. Erdos and A. Renyi, "On the evolution of random graphs," *Publications of the Mathematical Institute of the Hungarian Academy of Sciences*, vol. 5, pp. 17-61, 1960.
- J. Ernvall and O. Nevalainen, "An algorithm for unbiased random sampling," *Computer Journal*, vol. 25, pp. 45-47, 1982.
- V.N. Faddeeva, *Computational Methods of Linear Algebra*, Dover Publ., 1959.

- R. Fagin and T.G. Price, "Efficient calculation of expected miss ratios in the independent reference model," *SIAM Journal on Computing*, vol. 7, pp. 288-297, 1978.
- R. Fagin, J. Nievergelt, N. Pippenger, and H.R. Strong, "Extendible hashing - a fast access method for dynamic files," *ACM Transactions on Mathematical Software*, vol. 4, pp. 315-344, 1979.
- E. Fama and R. Roll, "Some properties of symmetric stable distributions," *Journal of the American Statistical Association*, vol. 63, pp. 817-836, 1968.
- C.T. Fan, M.E. Muller, and I. Rezucha, "Development of sampling plans by using sequential (item by item) selection techniques and digital computers," *Journal of the American Statistical Association*, vol. 57, pp. 387-402, 1962.
- D.J.G. Farlie, "The performance of some correlation coefficients for a general bivariate distribution," *Biometrika*, vol. 47, pp. 307-323, 1960.
- W. Feller, "On the Kolmogorov-Smirnov limit theorems for empirical distributions," *Annals of Mathematical Statistics*, vol. 19, pp. 177-189, 1948.
- W. Feller, *An Introduction to Probability Theory and its Applications*, Vol. 1, John Wiley, New York, N.Y., 1965.
- W. Feller, *An Introduction to Probability Theory and its Applications*, Vol. 2, John Wiley, New York, N.Y., 1971.
- C. Ferrerri, "A new frequency distribution for single variate analysis," *Statistica Bologna*, vol. 24, pp. 223-251, 1964.
- G.S. Fishman, "Sampling from the gamma distribution on a computer," *Communications of the ACM*, vol. 19, pp. 407-409, 1975.
- G.S. Fishman, "Sampling from the Poisson distribution on a computer," *Computing*, vol. 17, pp. 147-156, 1976.
- G.S. Fishman, *Principles of Discrete Event Simulation*, John Wiley, New York, N.Y., 1978.
- G.S. Fishman, "Sampling from the binomial distribution on a computer," *Journal of the American Statistical Association*, vol. 74, pp. 418-423, 1979.
- A.I. Fleishman, "A method for simulating non-normal distributions," *Psychometrika*, vol. 43, pp. 521-532, 1978.
- J.L. Folks and R.S. Chhikara, "The inverse gaussian distribution and its statistical application. A review," *Journal of the Royal Statistical Society, Series B*, vol. 40, pp. 263-289, 1978.
- G.E. Forsythe, "von Neumann's comparison method for random sampling from the normal and other distributions," *Mathematics of Computation*, vol. 26, pp. 817-826, 1972.
- B.L. Fox, "Generation of random samples from the beta and F distributions," *Technometrics*, vol. 5, pp. 269-270, 1963.
- B.L. Fox, "Monotonicity, extremal correlations, and synchronization: implications for nonuniform random numbers," Technical Report, Université de Montréal, 1980.

- J.R. Fraker and D.V. Rippey, "A composite approach to generating autocorrelated sequences," *Simulation*, vol. 23, pp. 171-175, 1974.
- J.N. Franklin, "Numerical simulation of stationary and nonstationary Gaussian random processes," *SIAM Review*, vol. 7, pp. 68-80, 1965.
- W.R. Franta and K. Maly, "An efficient data structure for the simulation event set," *Communications of the ACM*, vol. 20, pp. 596-602, 1977.
- W.R. Franta and K. Maly, "A comparison of heaps and TL structure for the simulation event set," *Communications of the ACM*, vol. 21, pp. 873-875, 1978.
- M. Frechet, "Sur les tableaux de correlation dont les marges sont donnees," *Annales de l'Universite de Lyon, Sec. A, Series 3*, vol. 14, pp. 53-57, 1951.
- M. Frechet, "Remarques au sujet de la note precedente," *Comptes Rendus de l'Academie des Sciences de Paris*, vol. 246, pp. 2719-2720, 1958.
- E. Fredkin, "Trie memory," *Communications of the ACM*, vol. 3, pp. 490-499, 1960.
- M.F. Freeman and J.W. Tukey, "Transformations related to the angular and square-root," *Annals of Mathematical Statistics*, vol. 21, pp. 607-611, 1950.
- D.P. Gaver, "Analytical hazard representations for use in reliability, mortality and simulation studies," *Communications in Statistics, Section Simulation and Computation*, vol. B8, pp. 91-111, 1979.
- H. Gebelein, "Das statistische Problem der Korrelation als Variations- und Eigenwertproblem und sein Zusammenhang mit der Ausgleichungsrechnung," *Zeitschrift fur Angewandte Mathematik und Mechanik*, vol. 21, pp. 364-379, 1941.
- H. Gehrke, "Einfache sequentielle Stichprobenentnahme," Diplomarbeit, University of Kiel, West Germany, 1984.
- E. Olusegun George and M.O. Ojo, "On a generalization of the logistic distribution," *Annals of the Institute of Statistical Mathematics*, vol. 32, pp. 161-169, 1980.
- E. Olusegun George and G.S. Mudholkar, "Some relationships between the logistic and the exponential distributions," in *Statistical Distributions in Scientific Work*, ed. C. Tallie, G.P. Patil, B.A. Baldessari, vol. 4, pp. 401-409, D. Reidel Publ. Co., Dordrecht, Holland, 1981.
- I. Gerontides and R.L. Smith, "Monte Carlo generation of order statistics from general distributions," *Applied Statistics*, vol. 31, pp. 238-243, 1982.
- J.D. Gibbons, *Nonparametric Statistical Inference*, McGraw-Hill, New York, 1971.
- M. Girault, "Les fonctions caracteristiques et leurs transformations," *Publications de l'Institut de Statistique des Universites de Paris*, vol. 4, pp. 223-299, 1954.
- N. Gluck, "Breaking records and breaking boards," *American Mathematical Monthly*, vol. 85, pp. 2-26, 1978.
- H.J. Godwin, *Inequalities on Distribution Functions*, Charles Griffin, London, 1964.

- G.H. Gonnet, "Heaps applied to event driven mechanisms," *Communications of the ACM*, vol. 19, pp. 417-418, 1976.
- R.D. Gordon, "Values of Mills' ratio of area to bounding ordinate and of the normal probability integral for large values of the argument," *Annals of Mathematical Statistics*, vol. 12, pp. 364-366, 1941.
- A. Grassia, "On a family of distributions with argument between 0 and 1 obtained by transformation of the gamma and derived compound distributions," *Australian Journal of Statistics*, vol. 19, pp. 108-114, 1977.
- F.A. Graybill, *Introduction to Matrices with Applications in Statistics*, Wadsworth, Belmont, CA., 1969.
- P.J. Green and R. Sibson, "Computing Dirichlet tessellations in the plane," *Computer Journal*, vol. 21, pp. 168-173, 1978.
- A.J. Greenwood, "A fast generator for gamma-distributed random variables," in *COMPSTAT 1974, Proceedings in Computational Statistics*, ed. G. Bruckmann, F. Ferschl, L. Schmetterer, pp. 19-27, Physica-Verlag, Vienna, Austria, 1974.
- A.J. Greenwood, "Moments of the time to generate random variables by rejection," *Annals of the Institute of Statistical Mathematics*, vol. 28, pp. 399-401, 1976.
- U. Grenander and M. Rosenblatt, "Statistical spectral analysis of time series arising from stationary stochastic processes," *Annals of Mathematical Statistics*, vol. 24, pp. 537-558, 1953.
- V.O. Guerra, R.A. Tapia, and J.R. Thompson, "A random number generator for continuous random variables based on an interpolation procedure of Akima," *Proceedings of the 1978 Winter Simulation Conference*, pp. 228-230, 1978.
- E.J. Gumbel, "Ranges and midranges," *Annals of Mathematical Statistics*, vol. 15, pp. 414-422, 1944.
- E.J. Gumbel, *Statistics of Extremes*, Columbia University Press, New York, N.Y., 1958.
- E.J. Gumbel, "Distributions a plusieurs variables dont les marges sont donnees (with remarks by M. Frechet)," *Comptes Rendus de l'Academie des Sciences de Paris*, vol. 246, pp. 2717-2720, 1958.
- E.J. Gumbel, "Distributions des valeurs extremes en plusieurs dimensions," *Publications de l'Institut de Statistique des Universites de Paris*, vol. 9, pp. 171-173, 1960.
- E.J. Gumbel, "Bivariate exponential distributions," *Journal of the American Statistical Association*, vol. 55, pp. 698-707, 1960.
- E.J. Gumbel, "Sommes et differences de valeurs extremes independantes," *Comptes Rendus de l'Academie des Sciences de Paris*, vol. 253, pp. 2838-2839, 1961.
- E.J. Gumbel, "Bivariate logistic distributions," *Journal of the American Statistical Association*, vol. 56, pp. 335-349, 1961.
- G. Guralnik, C. Zemach, and T. Warnock, "An algorithm for uniform random sampling of points in and on a hypersphere," *Information Processing Letters*, vol.

21, pp. 17-21, 1985.

P. Hall, "The distribution of means for samples of size N drawn from a population in which the variate takes values between 0 and 1, all such values being equally probable," *Biometrika*, vol. 19, pp. 240-244, 1927.

J.M. Hammersley and D.C. Handscomb, *Monte Carlo Methods*, Methuen, London, 1964.

G.H. Hardy, J.E. Littlewood, and G. Polya, *Inequalities*, Cambridge University Press, London, U.K., 1952.

C.M. Harris, "The Pareto distribution as a queue service discipline," *Operations Research*, vol. 16, pp. 307-313, 1968.

J.F. Hart, *Computer Approximations*, John Wiley, New York, N.Y., 1968.

C. Hastings, *Approximations for Digital Computers*, Princeton University Press, Princeton, New Jersey, 1955.

R.M. Helberger, "Generation of random orthogonal matrices," *Applied Statistics*, vol. 27, pp. 199-206, 1978.

J.O. Henriksen, "An improved events list algorithm," in *Proceedings of the 1977 Winter Simulation Conference*, pp. 554-557, 1977.

C. Heyde, "On a property of the lognormal distribution," *Journal of the Royal Statistical Society, Series B*, vol. 25, pp. 392-393, 1963.

D.P. Heyman and M.J. Sobel, *Stochastic Models in Operations Research, Vol. 1*, McGraw-Hill, New York, 1982.

T. Hickey and J. Cohen, "Uniform random generation of strings in a context-free language," *SIAM Journal on Computing*, vol. 12, pp. 645-655, 1983.

J.S. Hicks and R.F. Wheeling, "An efficient method for generating uniformly distributed points on the surface of an n -dimensional sphere," *Communications of the ACM*, vol. 2, pp. 17-19, 1959.

I.D. Hill, "Remark ASR2. A remark on algorithm AS2," *Applied Statistics*, vol. 18, pp. 299-300, 1969.

I.D. Hill, "Algorithm AS66. The normal integral," *Applied Statistics*, vol. 22, pp. 424-427, 1973.

T.W. Hill, "On determining a distribution function known only by its moments and/or moment generating function," Ph. D. Dissertation, Arizona State University, 1969.

D. Hitchin, "Remark ASR8. A remark on algorithms AS4 and AS5," *Applied Statistics*, vol. 22, p. 428, 1973.

W. Hoeffding, "Masstabinvariante Korrelationstheorie," *Schriften des Mathematischen Instituts und des Instituts für Angewandte Mathematik der Universität Berlin*, vol. 5, pp. 179-233, 1940.

R.G. Hoffman, "The simulation and analysis of correlated binary data," in *Proceedings of the Statistical Computing Section*, pp. 340-343, American Statistical Association, 1979.

- S.C. Hora, "Estimation of the inverse function for random variate generation," *Communications of the ACM*, vol. 26, pp. 590-594, 1983.
- F.C. Hsuan, "Generating uniform polygonal random pairs," *Applied Statistics*, vol. 28, pp. 170-172, 1979.
- T.C. Hu and A.C. Tucker, "Optimal computer search trees and variable-length alphabetic codes," *SIAM Journal of Applied Mathematics*, vol. 21, pp. 514-532, 1971.
- D. Huffman, "A method for the construction of minimum-redundancy codes," *Proceedings of the IRE*, vol. 40, pp. 1098-1101, 1952.
- T.P. Hutchinson, "Compound gamma bivariate distributions," *Metrika*, vol. 28, pp. 263-271, 1981.
- I.A. Ibragimov, "On the composition of unimodal distributions," *Theory of Probability and its Applications*, vol. 1, pp. 255-260, 1956.
- I.A. Ibragimov and K.E. Chernin, "On the unimodality of stable laws," *Theory of Probability and its Applications*, vol. 4, pp. 417-419, 1959.
- I.A. Ibragimov and Yu.V. Linnik, *Independent and Stationary Sequences of Random Variables*, Wolters-Noordhoff Publishing, Groningen, The Netherlands, 1971.
- P. Inzevitov, "An estimate of the remainder of the asymptotic expansion in the local limit theorem for densities," *Lithuanian Mathematical Journal*, vol. 17, pp. 111-120, 1977.
- P.A. Jacobs and P.A.W. Lewis, "A mixed autoregressive-moving average exponential sequence and point process, EARMA(1,1)," *Advances in Applied Probability*, vol. 9, pp. 87-104, 1977.
- B. Jansson, *Random Number Generators*, pp. 189-191, V. Pettersons Bokindustri Aktiebolag, Stockholm, 1966.
- M.D. Johnk, "Erzeugung von Betaverteilten und Gammaverteilten Zufallszahlen," *Metrika*, vol. 8, pp. 5-15, 1964.
- D.G. Johnson and W.J. Welch, "The generation of pseudo-random correlation matrices," *Journal of Statistical Computation and Simulation*, vol. 11, pp. 55-69, 1980.
- M.E. Johnson, "Models and Methods for Generating Dependent Random Vectors," Ph.D. Dissertation, University of Iowa, 1976.
- M.E. Johnson and J.S. Ramberg, "Elliptically symmetric distributions: characterizations and random variate generation," *Proceedings of the American Statistical Association, Statistical Computing Section*, pp. 262-265, 1977.
- M.E. Johnson and J.S. Ramberg, "A bivariate distribution system with specified marginals," Technical Report LA-6858-MS, Los Alamos Scientific Laboratory, Los Alamos, New Mexico, 1977.
- M.E. Johnson and P.R. Tadikamalla, "Computer methods for sampling from the gamma distribution," in *Proceedings of the Winter Simulation Conference, Miami Beach, Florida*, pp. 131-134, 1978.

2. THE KNUTH-YAO LOWER BOUND.

2.1. DDG trees.

Suppose that we wish to generate a discrete random variate X with probability vector $p_1, p_2, \dots$. The probability vector can be finite or infinite dimensional. Every algorithm based upon random bits can be represented as a binary tree (which is usually infinite), containing nodes of two types:

- (I) Branch nodes (or internal nodes), having two children. We can travel to the left child when a 0 bit is encountered, and to the right child otherwise.
- (II) Terminal nodes without children. These nodes are marked with an integer to be returned.

It is instructive to verify that this structure is present for the examples of the previous section. For example, for the binomial $(1, p)$ generator, consider the path for p , and assign terminal nodes marked 1 to all left children of nodes on the path that do not belong to the path themselves, and terminal nodes marked 0 to all right children of nodes on the path that do not belong to the path themselves.

Let us introduce the notation $t_i(k)$ for the number of terminal nodes on level k (the root is on level 0) which are marked i . Then we must have

$$\sum_{k \geq 0} \frac{t_i(k)}{2^k} = p_i \quad (\text{all } i).$$

When these conditions are satisfied, we say that we have a DDG-tree (discrete distribution generating tree, terminology introduced by Knuth and Yao, 1976). The corresponding algorithms are called DDG-tree algorithms. DDG-tree algorithms halt with probability one because the sum of the probabilities of reaching the terminal nodes is

$$\sum_i \sum_{k \geq 0} \frac{t_i(k)}{2^k} = \sum_i p_i = 1.$$

2.2. The lower bound.

Let us introduce the function $\chi(x) = x \bmod 1 = x - [x]$, the fractional part of x . Define furthermore

$$\nu(x) = \sum_{k \geq 0} \frac{\chi(2^k x)}{2^k} \quad (0 \leq x \leq 1),$$

and the entropy function

$$H(x) = x \log_2 \frac{1}{x} \quad (x > 0).$$

- M.E. Johnson and M.M. Johnson, "A new probability distribution with applications in Monte Carlo studies," Technical Report LA-7095-MS, Los Alamos Scientific Laboratory, Los Alamos, New Mexico, 1978.
- M.E. Johnson, "Computer generation of the exponential power distribution," *Journal of Statistical Computation and Simulation*, vol. 9, pp. 239-240, 1979.
- M.E. Johnson and A. Tenenbein, "Bivariate distributions with given marginals and fixed measures of dependence," Technical Report LA-7700-MS, Los Alamos Scientific Laboratory, Los Alamos, New Mexico, 1979.
- M.E. Johnson, G.L. Tietjen, and R.J. Beckman, "A new family of probability distributions with applications to Monte Carlo studies," *Journal of the American Statistical Association*, vol. 75, pp. 276-279, 1980.
- M.E. Johnson and A. Tenenbein, "A bivariate distribution family with specified marginals," *Journal of the American Statistical Association*, vol. 76, pp. 198-201, 1981.
- N.L. Johnson, "Systems of frequency curves generated by methods of translation," *Biometrika*, vol. 36, pp. 149-176, 1949.
- N.L. Johnson and C.A. Rogers, "The moment problem for unimodal distributions," *Annals of Mathematical Statistics*, vol. 22, pp. 433-439, 1951.
- N.L. Johnson, "Systems of frequency curves derived from the first law of Laplace," *Trabajos de Estadística*, vol. 5, pp. 283-291, 1954.
- N.L. Johnson and S. Kotz, *Distributions in Statistics: Discrete Distributions*, John Wiley, New York, N.Y., 1969.
- N.L. Johnson and S. Kotz, *Distributions in Statistics: Continuous Univariate Distributions - 1*, John Wiley, New York, N.Y., 1970.
- N.L. Johnson and S. Kotz, *Distributions in Statistics: Continuous Univariate Distributions - 2*, John Wiley, New York, N.Y., 1970.
- N.L. Johnson and S. Kotz, "Developments in discrete distributions," *International Statistical Review*, vol. 50, pp. 71-101, 1982.
- A. Jonassen and O.J. Dahl, "Analysis of an algorithm for priority queue administration," *BIT*, vol. 15, pp. 409-422, 1975.
- T.G. Jones, "A note on sampling from a tape-file," *Communications of the ACM*, vol. 5, p. 343, 1962.
- B. Jorgensen, *Statistical Properties of the Generalized Inverse Gaussian Distribution*, Lecture Notes in Statistics 9, Springer-Verlag, Berlin, 1982.
- V. Kachitvichyanukul, "Computer Generation of Poisson, Binomial, and Hypergeometric Random Variates," Ph.D. Dissertation, School of Industrial Engineering, Purdue University, 1982.
- V. Kachitvichyanukul and B.W. Schmeiser, "Computer generation of hypergeometric random variates," *Journal of Statistical Computation and Simulation*, vol. 22, pp. 127-145, 1985.
- F.C. Kaminsky and D.L. Rumpf, "Simulating nonstationary Poisson processes: a comparison of alternatives including the correct approach," *Simulation*, vol. 28, pp. 17-20, 1977.

- M. Kanter, "Stable densities under change of scale and total variation inequalities," *Annals of Probability*, vol. 3, pp. 697-707, 1975.
- J. Kawarasaki and M. Sibuya, "Random numbers for simple random sampling without replacement," *Keio Mathematical Seminar Reports*, vol. 7, pp. 1-9, 1982.
- T. Kawata, *Fourier Analysis in Probability Theory*, Academic Press, New York, N.Y., 1972.
- J. Kellson and F.W. Steutel, "Mixtures of distributions, moment inequalities and measures of exponentiality and normality," *Annals of Probability*, vol. 2, pp. 112-130, 1974.
- D. Kelker, "Distribution theory of spherical distributions and a location-scale parameter generalization," *Sankhya Series A*, vol. 32, pp. 419-430, 1970.
- D. Kelker, "Infinite divisibility and variance mixtures of the normal distribution," *Annals of Mathematical Statistics*, vol. 42, pp. 802-808, 1971.
- F.P. Kelly and B.D. Ripley, "A note on Strauss' model for clustering," *Biometrika*, vol. 63, pp. 357-360, 1976.
- A.W. Kemp and C.D. Kemp, "An alternative derivation of the Hermite distribution," *Biometrika*, vol. 53, pp. 627-628, 1966.
- A.W. Kemp and C.D. Kemp, "On a distribution associated with certain stochastic processes," *Journal of the Royal Statistical Society, Series B*, vol. 30, pp. 160-163, 1968.
- A.W. Kemp, "Efficient generation of logarithmically distributed pseudo-random variables," *Applied Statistics*, vol. 30, pp. 249-253, 1981.
- A.W. Kemp, "Frugal methods of generating bivariate discrete random variables," in *Statistical Distributions in Scientific Work*, ed. C. Tallis et al., vol. 4, pp. 321-329, D. Reidel Publ. Co., Dordrecht, Holland, 1981.
- A.W. Kemp, "Conditionality properties for the bivariate logarithmic distribution with an application to goodness of fit," in *Statistical Distributions in Scientific Work*, ed. C. Tallis et al., vol. 5, pp. 57-73, D. Reidel Publ. Co., Dordrecht, Holland, 1981.
- C.D. Kemp and A.W. Kemp, "Some properties of the Hermite distribution," *Biometrika*, vol. 52, pp. 381-394, 1965.
- C.D. Kemp and H. Papageorgiou, "Bivariate Hermite distributions," *Bulletin of the IMS*, vol. 5, p. 174, 1976.
- C.D. Kemp and S. Loukas, "The computer generation of bivariate discrete random variables," *Journal of the Royal Statistical Society, Series A*, vol. 141, pp. 513-519, 1978.
- C.D. Kemp and S. Loukas, "Fast methods for generating bivariate discrete random variables," in *Statistical Distributions in Scientific Work*, ed. C. Tallis et al., vol. 4, pp. 313-319, D. Reidel Publ. Co., Dordrecht, Holland, 1981.
- D.G. Kendall, "On some modes of population growth leading to R.A. Fisher's logarithmic series distribution," *Biometrika*, vol. 35, pp. 6-15, 1948.

- M. Kendall and A. Stuart, *The Advanced Theory of Statistics, Vol. 1*, Macmillan, New York, 1977.
- W.J. Kennedy, Jr. and J.E. Gentle, *Statistical Computing*, Marcel Dekker, New York, 1980.
- G. Klumeldorf and A. Sampson, "One-parameter families of bivariate distributions with fixed marginals," *Communications in Statistics*, vol. 4, pp. 293-301, 1975.
- G. Klumeldorf and A. Sampson, "Uniform representations of bivariate distributions," *Communications in Statistics*, vol. 4, pp. 617-627, 1975.
- G. Klumeldorf and A. Sampson, "Monotone dependence," *Annals of Statistics*, vol. 6, pp. 895-903, 1978.
- A.J. Klnderman, J.F. Monahan, and J.G. Ramage, "Computer generation of random variables with normal and student's t distribution," *Proceedings of the American Statistical Association, Statistical Computing Section*, pp. 128-131, Washington, D.C., 1975.
- A.J. Klnderman and J.G. Ramage, "The computer generation of normal random variables," *Journal of the American Statistical Association*, vol. 71, pp. 893-896, 1976.
- A.J. Klnderman, J.F. Monahan, and J.G. Ramage, "Computer methods for sampling from Student's t-distribution," *Mathematics of Computation*, vol. 31, pp. 1009-1018, 1977.
- A.J. Klnderman and J.F. Monahan, "Computer generation of random variables using the ratio of uniform deviates," *ACM Transactions on Mathematical Software*, vol. 3, pp. 257-260, 1977.
- A.J. Klnderman and J.G. Ramage, "FORTRAN programs for generating normal random variables," Technical Report 23, Department of Statistics, The Wharton School, University of Pennsylvania, Philadelphia, PA., 1977.
- A.J. Klnderman, J.F. Monahan, and J.G. Ramage, "FORTRAN programs for generating Student's t random variables," Technical Report No. 24, Department of Statistics, The Wharton School, University of Pennsylvania, 1977.
- A.J. Klnderman and J.F. Monahan, "Recent developments in the computer generation of Student's t and gamma random variables," *Proceedings of the ASA Statistical Computing Section*, pp. 90-94, 1978.
- A.J. Klnderman and J.F. Monahan, "New methods for generating student's t and gamma variables," Technical Report, Department of Management Science, California State University, Northridge, CA., 1979.
- J.H. Kingston, "Analysis of Henriksen's algorithm for the simulation event list," Technical Report 232, Basser Department of Computer Science, University of Sydney, Australia, 1984.
- J.H. Kingston, "Analysis of tree algorithms for the simulation event list," *Acta Informatica*, vol. 22, pp. 15-33, 1985.
- P. Klingsberg, Doctoral Dissertation, University of Washington, Seattle, Washington, 1977.

- K. Knopp, *Theorie und Anwendung der unendlichen Reihen*, Springer-Verlag, Berlin, 1964.
- G.D. Knott, "A numbering system for binary trees," *Communications of the ACM*, vol. 20, pp. 113-115, 1977.
- D.E. Knuth, *The Art of Computer Programming, Vol. 1. Fundamental Algorithms*, Addison-Wesley, Reading, Mass., 1968.
- D.E. Knuth, *The Art of Computer Programming, Vol. 2: Seminumerical Algorithms*, Addison-Wesley, Reading, Mass., 1969.
- D.E. Knuth, *The Art of Computer Programming, Vol. 3: Searching and Sorting*, Addison-Wesley, Reading, Mass., 1973.
- D.E. Knuth and A.C. Yao, "The complexity of nonuniform random number generation," in *Algorithms and Complexity*, ed. J.E. Traub, pp. 357-428, Academic Press, New York, N.Y., 1976.
- K.D. Kohrt, "Efficient sampling from non-uniform statistical distributions," Diploma Thesis, University Kiel, Kiel, West Germany, 1980.
- A.N. Kolmogorov, "Sulla determinazione empirica di una legge di distribuzione," *Giorn. Inst. Ital. Attuari*, vol. 4, pp. 83-91, 1933.
- S. Kotz and R. Srinivasan, "Distribution of product and quotient of Bessel function variates," *Annals of the Institute of Statistical Mathematics*, vol. 21, pp. 201-210, 1969.
- C.J. Kowalski, "Non-normal bivariate distributions with normal marginals," *The American Statistician*, vol. 27, pp. 103-106, 1973.
- R.A. Kronmal and A.V. Peterson, "On the alias method for generating random variables from a discrete distribution," *The American Statistician*, vol. 33, pp. 214-218, 1979.
- R.A. Kronmal and A.V. Peterson, "The alias and alias-rejection-mixture methods for generating random variables from probability distributions," in *Proceedings of the 1979 Winter Simulation Conference*, pp. 269-280, 1979.
- R.A. Kronmal and A.V. Peterson, "Programs for generating discrete random integers using Walker's alias method," Department of Biostatistics, University of Washington, 1979.
- R.A. Kronmal and A.V. Peterson, "Generating normal random variables using the alias-rejection-mixture method," *Proceedings of the 1979 ASA Annual Meeting, Computer Section*, Washington, D.C., 1980.
- R.A. Kronmal and A.V. Peterson, "A variant of the acceptance-rejection method for computer generation of random variables," *Journal of the American Statistical Association*, vol. 76, pp. 446-451, 1981.
- R.A. Kronmal and A.V. Peterson, "An acceptance-complement analogue of the mixture-plus-acceptance-rejection method for generating random variables," *ACM Transactions on Mathematical Software*, vol. 10, pp. 271-281, 1984.
- W.H. Kruskal, "Ordinal measures of association," *Journal of the American Statistical Association*, vol. 53, pp. 814-861, 1958.

- N.H. Kulper, "Tests concerning random points on a circle," *Koninklijke Nederlandse Akademie van Wetenschappen*, vol. A63, pp. 38-47, 1960.
- S. Kullback, "An application of characteristic functions to the distribution problem of statistics," *Annals of Mathematical Statistics*, vol. 5, pp. 264-305, 1934.
- R.G. Laha, "On some properties of Bessel function distributions," *Bulletin of the Calcutta Mathematical Society*, vol. 46, pp. 59-71, 1954.
- R.G. Laha, "An example of a non-normal distribution where the quotient follows the Cauchy law," *Proceedings of the National Academy of Sciences*, vol. 44, pp. 222-223, 1958.
- V.C. Lakhan, "Generating autocorrelated pseudo-random numbers with specific distributions," *Journal of Statistical Computation and Simulation*, vol. 12, pp. 303-309, 1981.
- H.O. Lancaster, "Correlation and complete dependence of random variables," *Annals of Mathematical Statistics*, vol. 34, pp. 1315-1321, 1963.
- A.M. Law and W.D. Kelton, *Simulation Modeling and Analysis*, McGraw-Hill, New York, 1982.
- A.J. Lawrance and P.A.W. Lewis, "A moving average exponential point process, EMA(1)," *Journal of Applied Probability*, vol. 14, pp. 98-113, 1977.
- A.J. Lawrance and P.A.W. Lewis, "The exponential autoregressive moving average EARMA(p, q) process," *Journal of the Royal Statistical Society Series B*, vol. 42, pp. 150-161, 1980.
- A.J. Lawrance and P.A.W. Lewis, "A new autoregressive time series model in exponential variables," *Advances in Applied Probability*, vol. 13, pp. 826-845, 1981.
- D.H. Lehmer, "The machine tool of combinatorics," in *Applied Combinatorial Mathematics*, ed. E. Beckenbach, pp. 19-23, John Wiley, New York, N.Y., 1964.
- R. Lelplnk, "The lognormal distribution and strong non-uniqueness of the moment problem," *Theory of Probability and its Applications*, vol. 26, pp. 850-852, 1981.
- C.G. Lekkerkerker, "A property of log-concave functions I, II," *Indagationes Mathematicae*, vol. 15, pp. 505-521, 1953.
- G. Letac, "On building random variables of a given distribution," *Annals of Probability*, vol. 3, pp. 298-306, 1975.
- P. Levy, "Sur certains processus stochastiques homogenes," *Compositio Mathematica*, vol. 7, pp. 283-339, 1940.
- P.A.W. Lewis and G.S. Shedler, "Simulation of nonhomogeneous Poisson point processes with log-linear rate function," *Biometrika*, vol. 63, pp. 501-505, 1976.
- P.A.W. Lewis and G.S. Shedler, "Simulation of nonhomogeneous Poisson point processes with degree-two exponential polynomial rate function," *Operations Research*, vol. 27, pp. 1026-1040, 1979.
- P.A.W. Lewis and G.S. Shedler, "Simulation of nonhomogeneous Poisson processes by thinning," *Naval Research Logistics Quarterly*, vol. 26, pp. 403-413, 1979.

- S.T. Li and J.L. Hammond, "Generation of pseudorandom numbers with specified univariate distributions and correlation coefficients," *IEEE Transactions on Systems, Man and Cybernetics*, vol. 5, pp. 557-561, 1975.
- J. Lieblein, "Properties of certain statistics involving the closest pair in a sample of three observations," *Journal of Research of the National Bureau of Standards*, vol. 48, pp. 255-268, 1952.
- Yu.V. Linnik, "Linear forms and statistical criteria: I, II," *Selected Translations in Mathematical Statistics and Probability*, vol. 3, pp. 1-40, 41-90, 1962.
- Yu.V. Linnik, "Linear forms and statistical criteria, I, II," *Selected Translations in Mathematical Statistics and Probability*, vol. 3, pp. 1-90, 1962.
- M. Loeve, *Probability Theory*, Van Nostrand, Princeton, New Jersey, 1963.
- H.W. Lotwick, "Simulation of some spatial hard core models and the complete packing problem," *Journal of Statistical Computation and Simulation*, vol. 15, pp. 295-314, 1982.
- E. Lukacs, "A characterization of the gamma distribution," *Annals of Mathematical Statistics*, vol. 26, pp. 319-324, 1955.
- E. Lukacs and R.G. Laha, *Applications of Characteristic Functions*, Griffin, London, 1964.
- E. Lukacs, *Characteristic Functions*, Griffin, London, 1970.
- D. Lurie and H.O. Hartley, "Machine-generation of order statistics for Monte Carlo computations," *The American Statistician*, vol. 26, pp. 26-27, 1972.
- D. Lurie and R.L. Mason, "Empirical investigation of several techniques for computer generation of order statistics," *Communications in Statistics*, vol. 2, pp. 363-371, 1973.
- E.J. Lusk and H. Wright, "Deriving the probability density for sums of uniform random variables," *The American Statistician*, vol. 36, pp. 128-130, 1982.
- I. Lux, "A special method to sample some probability density functions," *Computing*, vol. 20, pp. 183-188, 1978.
- I. Lux, "Another special method to sample probability density functions," *Computing*, vol. 21, pp. 359-364, 1979.
- M.D. MacLaren, G. Marsaglia, and T.A. Bray, "A fast procedure for generating exponential random variables," *Communications of the ACM*, vol. 7, pp. 298-300, 1964.
- M. Maejima, "The remainder term in the local limit theorem for independent random variables," *Tokyo Journal of Mathematics*, vol. 3, pp. 311-329, 1980.
- W. Magnus, F. Oberhettinger, and R.P. Soni, *Formulas and Theorems for the Special Functions of Mathematical Physics*, Springer-Verlag, Berlin-Heidelberg, 1966.
- S. Malmquist, "On a property of order statistics from a rectangular distribution," *Skandinavisk Aktuarietidskrift*, vol. 33, pp. 214-222, 1950.
- B. Mandelbrot, "The variation of certain speculative prices," *Journal of Business*, vol. 36, pp. 349-419, 1963.

- D. Mannion, "Random space-filling in one dimension," *Publications of the Mathematical Institute of the Hungarian Academy of Sciences*, vol. 9, pp. 143-153, 1964.
- N. Mantel, "A characteristic function exercise," *The American Statistician*, vol. 27, p. 31, 1973.
- K.V. Mardia, "Multivariate Pareto distributions," *Annals of Mathematical Statistics*, vol. 33, pp. 1008-1015, 1962.
- K.V. Mardia, *Families of Bivariate Distributions*, Griffin, London, 1970.
- K.V. Mardia, "A translation family of bivariate distributions and Frechet's bounds," *Sankhya Series A*, vol. 32, pp. 119-122, 1970.
- K.V. Mardia, "Statistics of directional data," *Journal of the Royal Statistical Society Series B*, vol. 37, pp. 349-393, 1975.
- G. Marsaglia, "Expressing a random variable in terms of uniform random variables," *Annals of Mathematical Statistics*, vol. 32, pp. 894-899, 1961.
- G. Marsaglia, "Generating exponential random variables," *Annals of Mathematical Statistics*, vol. 32, pp. 899-902, 1961.
- G. Marsaglia, "Generating discrete random variables in a computer," *Communications of the ACM*, vol. 6, pp. 37-38, 1963.
- G. Marsaglia, M.D. MacLaren, and T.A. Bray, "A fast procedure for generating normal random variables," *Communications of the ACM*, vol. 7, pp. 4-10, 1964.
- G. Marsaglia and T.A. Bray, "A convenient method for generating normal random variables," *SIAM Review*, vol. 6, pp. 260-264, 1964.
- G. Marsaglia, "Choosing a point from the surface of a sphere," *Annals of Mathematical Statistics*, vol. 43, pp. 645-646, 1972.
- G. Marsaglia, K. Ananthanarayanan, and N.J. Paul, "Improvements on fast methods for generating normal random variables," *Information Processing Letters*, vol. 5, pp. 27-30, 1976.
- G. Marsaglia, "Random number generation," in *Encyclopedia of Computer Science*, ed. A. Ralston and C.L. Meek, pp. 1192-1197, Petrocelli/Charter, New York, N.Y., 1976.
- G. Marsaglia, "The squeeze method for generating gamma variates," *Computers and Mathematics with Applications*, vol. 3, pp. 321-325, 1977.
- G. Marsaglia, "Generating random variables with a t-distribution," *Mathematics of Computation*, vol. 34, pp. 235-236, 1979.
- G. Marsaglia, "The exact-approximation method for generating random variables in a computer," *Journal of the American Statistical Association*, vol. 79, pp. 218-221, 1984.
- G. Marsaglia and W.W. Tsang, "A fast, easily implemented method for sampling from decreasing or symmetric unimodal density functions," *SIAM Journal on Scientific and Statistical Computing*, vol. 5, pp. 349-359, 1984.
- G. Marsaglia and I. Olkin, "Generating correlation matrices," *SIAM Journal on Scientific and Statistical Computations*, vol. 5, pp. 470-475, 1984.

- A.W. Marshall and I. Olkin, "A multivariate exponential distribution," *Journal of the American Statistical Association*, vol. 62, pp. 30-44, 1967.
- A.W. Marshall and I. Olkin, *Inequalities: Theory of Majorization and its Applications*, Academic Press, London, England, 1979.
- A.W. Marshall and I. Olkin, "Domains of attraction of multivariate extreme value distributions," *Annals of Probability*, vol. 11, pp. 168-177, 1983.
- J.H. May and R.L. Smith, "Random polytopes: their definition, generation and aggregate properties," *Mathematical Programming*, vol. 24, pp. 39-54, 1982.
- W.M. McCormack and R.G. Sargent, "Analysis of future event set algorithms for discrete event simulation," *Communications of the ACM*, vol. 24, pp. 801-812, 1981.
- E.J. McGrath and D.C. Irving, "Techniques for efficient Monte Carlo simulation: volume 2: random number generation for selected probability distributions," Technical Report SAI-72-590-LJ, Science Applications, Inc., La Jolla, CA., 1973.
- A.T. McKay, "A Bessel function distribution," *Biometrika*, vol. 24, pp. 39-44, 1932.
- J.K.S. McKay, "Algorithm 262. Number of restricted partitions of N ," *Communications of the ACM*, vol. 8, p. 493, 1965.
- J.K.S. McKay, "Algorithm 263. Partition generator," *Communications of the ACM*, vol. 8, p. 493, 1965.
- J.K.S. McKay, "Algorithm 264. Map of partitions into integers," *Communications of the ACM*, vol. 8, p. 493, 1965.
- P. McMullen, "The maximum number of faces of a convex polytope," *Mathematika*, vol. 17, pp. 179-184, 1970.
- J.R. Michael, W.R. Schucany, and R.W. Haas, "Generating random variates using transformations with multiple roots," *The American Statistician*, vol. 30, pp. 88-90, 1976.
- G.A. Mikhailov, "On modelling random variables for one class of distribution laws," *Theory of Probability and its Applications*, vol. 10, pp. 681-682, 1965.
- G.A. Mikhailov, "On the reproduction method for simulating random vectors and stochastic processes," *Theory of Probability and its Applications*, vol. 19, pp. 839-843, 1974.
- L. Mirsky, *Introduction to Linear Algebra*, Oxford University Press, 1955.
- R. von Mises, "On the asymptotic distribution of differentiable statistical functions," *Annals of Mathematical Statistics*, vol. 18, pp. 309-348, 1947.
- R. von Mises, *A Mathematical Theory of Probability and Statistics*, Academic Press, New York, N.Y., 1964.
- R.L. Mitchell, "Table lookup methods for generating arbitrary random numbers," *IEEE Transactions on Computers*, vol. C-26, pp. 1006-1008, 1977.
- S.S. Mitra, "Distribution of symmetric stable laws of index 2 to the power $-n$," *Annals of Probability*, vol. 9, pp. 710-711, 1981.

Theorem 2.1

Let N be the number of random bits taken by a DDG-tree algorithm. Then:

- A. $E(N) \geq \sum_i \nu(p_i)$.
- B. Let $H(p_1, p_2, \dots) = \sum_i H(p_i)$ be the entropy of the probability distribution $(p_1, p_2, \dots)$. Then
- $$H(p_1, p_2, \dots) \leq \sum_i \nu(p_i).$$
- C. $\sum_i \nu(p_i) \leq H(p_1, p_2, \dots) + 2$.

Proof of Theorem 2.1.

We begin with an expression for $E(N)$:

$$\begin{aligned} E(N) &= \sum_{k \geq 0} P(N > k) \\ &= \sum_{k \geq 0} \frac{b(k)}{2^k} \end{aligned}$$

where $b(k)$ is the number of internal (or: branch) nodes at level k . We obtain the lower bound by finding a lower bound for $b(k)$. Let us use the notation $t(k)$ for the number of terminal nodes at level k . Thus,

$$\begin{aligned} b(0) + t(0) &= 1, \\ b(k) + t(k) &= 2b(k-1) \quad (k \geq 1). \end{aligned}$$

Using these relations, we can show that

$$b(k) = \sum_{j > k} \frac{t(j)}{2^{j-k}}.$$

(Note that this is true for $k=0$, and use induction from there on.) But

$$\sum_{j > k} \frac{t_i(j)}{2^j} = p_i - \sum_{0 \leq j \leq k} \frac{t_i(j)}{2^j} \geq \frac{\chi(2^j p_i)}{2^j}.$$

This is true because the left-hand-sum is nonnegative, and the right-hand-sum is an integer multiple of 2^{-k} . Combining all of this yields

$$b(k) \geq \sum_i \chi(2^k p_i).$$

This proves part A. Part B follows if we can show the following:

$$H(x) \leq \nu(x) \leq H(x) + 2x \quad (\text{all } x).$$

Note that this is more than needed, but the second part of the inequality will be useful elsewhere. For a number $x \in [0,1)$, we will use the notation $x = 0.x_1x_2 \dots$ for the binary expansion. By definition of $\nu(x)$,

$$\begin{aligned}\nu(x) &= \sum_{k \geq 0} 2^{-k} \sum_{j > k} \frac{x_j}{2^{j-k}} \\ &= \sum_{j \geq 0} \sum_{0 \leq k \leq j} \frac{x_j}{2^j} \\ &= \sum_{j \geq 0} \frac{jx_j}{2^j}.\end{aligned}$$

Now, $\nu(0) = H(0) = 0$. Also, if $2^{-k} \leq x < 2^{1-k}$,

$$\begin{aligned}\nu(x) &= \sum_{j \geq k} \frac{jx_j}{2^j} \\ &\geq \sum_{j \geq k} \frac{\log_2(\frac{1}{x})x_j}{2^j} \\ &= H(x).\end{aligned}$$

Also, because $x_k = 1$,

$$\begin{aligned}H(x) + 2x - \nu(x) &= \sum_{j \geq k} \frac{(\log_2(\frac{1}{x}) + 2 - j)x_j}{2^j} \\ &> \sum_{j \geq k} \frac{(k+1-j)x_j}{2^j} \\ &= 2^{-k} - \sum_{j \geq k+2} \frac{(j-k-1)x_j}{2^j} \\ &> 2^{-k} - \sum_{j \geq 1} \frac{j}{2^{j+k+1}} \\ &= 0. \blacksquare\end{aligned}$$

The lower bound of Theorem 2.1 is related to the entropy of the probability vector. Let us briefly look at the entropy of some probability vectors: if $p_i = \frac{1}{n}$, $1 \leq i \leq n$, then

$$H(p_1, \dots, p_n) = \log_2 n.$$

In fact, because H is invariant under permutations of its arguments, and is a concave function, it is true that for probability vectors

$$(p_1, \dots, p_n), (q_1, \dots, q_n),$$

$$H(p_1, \dots, p_n) \leq H(q_1, \dots, q_n),$$

when the p_n vector is stochastically smaller than the q_n vector, i.e. if the p_i 's and q_i 's are in increasing order, then

$$p_1 \leq q_1;$$

$$p_1 + p_2 \leq q_1 + q_2;$$

$$\dots$$

$$p_1 + p_2 + \dots + p_n \leq q_1 + q_2 + \dots + q_n.$$

This follows from the theory of Schur-convexity (Marshall and Olkin, 1979). In particular, for all probability vectors $(p_1, \dots, p_n)$, we conclude that

$$0 \leq H(p_1, \dots, p_n) \leq \log_2 n.$$

Both bounds are attainable. In a sense, entropy increases when the probability vector becomes smoother, more uniform. It is smallest when there is no randomness, i.e. all the probability mass is concentrated in one point. According to Theorem 2.1, we are tempted to conclude that uniform random variates are the costliest to produce. This is indeed the case if we compare optimal algorithms for distributions, and if the lower bounds can be attained for all distributions (this will be dealt with in the next sub-section). If we consider discrete distributions with n infinite, then it is possible to have $H(p_1, p_2, \dots) = \infty$. To construct counterexamples very easily, we note that if the p_n 's are $\downarrow$, then

$$H(p_1, \dots) \geq E(\log(X))$$

where X is a random variate with the given probability vector. To see this, note that $p_n \leq \frac{1}{n}$, and thus that $-p_n \log(p_n) \geq p_n \log(n)$. Thus, whenever

$$p_n \sim \frac{c}{n \log^{1+\epsilon}(n)},$$

as $n \rightarrow \infty$, for some $\epsilon \in (0, 1]$, we have infinite entropy. The constant c may be difficult to calculate except in special cases. The following example is due to Knuth and Yao (1976):

$$p_1 = 0; p_n = 2^{-\lfloor \log_2(n) \rfloor - 2 \lfloor \log_2(\log_2(n)) \rfloor - 1} \quad (n \geq 2).$$

Note that this corresponds to the case $\epsilon = 1$. Thus, we note that for any DDG-tree algorithm, $E(\log(X)) = \infty$ implies $E(N) = \infty$, regardless of whether the probability vector is monotone or not. The explanation is very simple: $E(\log_2(X))$ is the expected number of bits needed to store, or describe, X . If this is ∞ , there is little hope of generating X requiring only $E(N) < \infty$ provided that the distribution of X is sufficiently spread out so that no bits are "redundant" (see exercises).

2.3. Exercises.

1. **The entropy.** This is about the entropy H of a probability vector $(p_1, p_2, \dots)$. Show the following:
 - A. There exists a probability vector such that $E(\log_2(X)) = \infty$, yet $E(N) < \infty$. Here X is a discrete random variate with the given probability vector. Hint: clearly, the counterexample is not monotone.
 - B. Is it true that when the probability vector is monotone, then $E(\log_2(X)) < \infty$ implies $H(p_1, \dots) < \infty$?
 - C. Show that the p_n 's defined by

$$p_1 = 0; p_n = 2^{-\lfloor \log_2(n) \rfloor - 2 \lfloor \log_2(\log_2(n)) \rfloor - 1} \quad (n \geq 2)$$

form a probability vector, and that its entropy is ∞ .

- D. Show that if one finite probability vector is stochastically larger than another probability vector, then its entropy is at most equal to the entropy of the second probability vector.
- E. Prove that when $x \in [0, 1]$ is a power of 2, we have $\nu(x) = H(x)$, and that for any $x \in [0, 1]$, $\nu(x) = 2^n \nu(\frac{x}{2^n}) - nx$.

3. OPTIMAL AND SUBOPTIMAL DDG-TREE ALGORITHMS.

3.1. Suboptimal DDG-tree algorithms.

We know now what we can expect at best from any DDG-tree algorithm in terms of the expected number of random bits. It is another matter altogether to construct feasible DDG-tree algorithms. Some algorithms require unwieldy set-up times and/or calculations which would overshadow the contribution to the total complexity from the random bit generator. In fact, most practical DDG-tree algorithms correspond to algorithms described in chapter III. Let us quickly check what kind of DDG-tree algorithms are hidden in that chapter.

In section III.2, we introduced inversion of a uniform $[0, 1]$ random variate U . In sequential inversion, we compared U with successive partial sums of p_n 's. This corresponds to the following infinite DDG-tree: consider all the paths for the partial sums, i.e. the path for p_1 , for $p_1 + p_2$, etcetera. In case of a finite vector, we define the last cumulative sum by the binary expansion $0.11111111\dots$. Then generate random bits until the path traveled by the random bits deviates for the first time from any of the p_n paths. If that path in question is for p_n , then return n if the last random bit was 0 (the corresponding bit on the path is 1), and return $n + 1$ otherwise. This method has two problems: first, the set-up is impossible except in the following special case: all p_n 's have a finite binary expansion, and the probability vector is finite. In all other cases, the DDG-tree must be constructed as we go along.

The analysis for this DDG-tree algorithm is not very difficult. Construct (just for the analysis) the trie in which terminal nodes are put at the points where the paths for the p_n 's diverge for the first time. For example, for the probability vector

$p_1 = 0.00101$
$p_2 = 0.001001$
$p_3 = 0.101101$

we have the cumulative probabilities 0.00101, 0.010011, 0.11111111.... Thus, we can put terminal nodes at the positions 00, 01, and 1. It is easy to see that once the terminal nodes are reached, then on the average 2 more random bits are needed. Thus, $E(N) = 2 +$ expected depth of the terminal nodes in the trie defined above. In our example, this would yield $E(N) = 2 + \frac{1}{2}1 + \frac{1}{2}2 = \frac{7}{2}$. In another example, if all the p_n 's are equal to 2^{-k} , $1 \leq n \leq 2^k$, for some integer k , then $E(N) = 2 + k$, which grows as $\log_2 n$. In general, we have

$$E(N) \leq 2 + \sum_{i=1}^n p_i \left\lceil \log_2 \left(\frac{1}{p_i} \right) \right\rceil \leq 3 + H(p_1, \dots, p_n).$$

This follows from a simple argument. Consider the uniform $[0,1]$ random variate U formed by the random bits of the random bit generator. Also mark the partial sums of p_i 's on $[0,1]$, so that $[0,1]$ is partitioned into n intervals. The expected depth of a terminal node in the trie is

$$\int_0^1 D(x) dx$$

where $D(x)$ is the smallest nonnegative integer k such that the 2^k dyadic partition of $[0,1]$ is such that only one of the partial sums (0 is also considered as a partial sum) falls in the same interval. The i -th partial sum "controls" an interval in which $D(x) \leq \left\lceil \log_2 \left(\frac{1}{p_i} \right) \right\rceil$, and the size of the interval itself is a power of 2. Thus,

$$\int_0^1 D(x) dx \leq \sum_{i=1}^n p_i \left\lceil \log_2 \left(\frac{1}{p_i} \right) \right\rceil,$$

from which we derive the result shown above. We conclude that sequential search type DDG-tree algorithms are nearly optimal for all probability vectors (compare with Theorem 2.1).

The method of guide tables, and the Huffman-tree based methods are similar, with the sole exception that the probability vector is permuted in the Huffman tree case. All these methods can be translated into a DDG-tree algorithm of the type described for the sequential search method, and the performance bounds given above remain valid. In view of the lower bound of Knuth and Yao, we don't gain by using special truncation-based tricks, because truncation corresponds to search into a trie formed with equally-spaced points, and

takes time proportional to $\log_2$ of the number of intervals.

Thus, it comes as no surprise that the alias method (section III.4) has an unimpressive DDG-tree analog. We can consider the following DDG-tree algorithm: first, generate a uniform $\{1, \dots, n\}$ -valued random integer (this requires on the average $\geq \log_2 n$ and $\leq 1 + \log_2 n$ random bits, as we remarked above). Then, having picked a slab, we need to make one more comparison between a uniform random variate and a threshold, which takes on the average 2 comparisons by the binomial $(1, p)$ algorithm described in section XV.1. Thus,

$$2 + \log_2 n \leq E(N) \leq 3 + \log_2 n.$$

This performance grows with n , while for the optimal DDG-tree algorithms we will see that there are sequences of probability vectors for which $E(N)$ remain bounded as $n \rightarrow \infty$. In many cases, the alias algorithm does not even come close to the lower bound of Theorem 2.1.

The rejection method corresponds to the following DDG-tree: construct a DDG-tree in the obvious fashion with two types of terminal nodes, terminal nodes corresponding to a successful return (acceptance), and rejection nodes. Make the rejection nodes roots of isomorphic trees again, and continue at infinitum.

3.2. Optimal DDG-tree algorithms.

The notation of section XV.2 is inherited. We start with the following Theorem, due to Knuth and Yao (1976). It states that optimal algorithms achieving the lower bound do indeed exist.