Note on Random Permutations

By Guy de Balbine

The purpose of this note is to present a fast and simple method to generate random permutations of N objects, say of the numbers 1, 2, $\cdots$, N. Despite its simplicity this method by pairwise exchanges seems to have been overlooked in the past because references to more complicated and less efficient algorithms are still being made. To illustrate this fact, we shall first quote a method described in Birger Jansson's *Random Number Generators* [1]:

For each permutation of 1, 2, $\cdots$, N, let a_k be the number of integers following k that are less than k, for $k = 1, 2, \cdots, N$. For instance, when $N = 5$, the permutation 1 4 2 5 3 gives

k	1	2	3	4	5
a_k	0	0	0	2	1

Any integer n such that $0 \leqq n \leqq N! - 1$ has a unique factorial representation

$$n = a_1 0! + a_2 1! + \cdots + a_N (N-1)!$$

if each a_i is an integer between 0 and $i - 1$. Clearly a_1 is always 0 so that equivalently

$$n = a_2 1! + \cdots + a_N (N-1)!$$

To each integer n there corresponds a unique permutation, thus n can be called its serial number. For the permutation 1 4 2 5 3

$$n = 2.3! + 1.4! = 36 .$$

Conversely, the permutation can be obtained from the serial number by successive division by $(N-1)!$, $(N-2)!$, $\cdots$, $1!$, the quotients being the a's and the remainder of each division becoming the next dividend

$$\begin{aligned} 36 &= 1.4! + 12 , & a_5 &= 1 , \\ 12 &= 2.3! + 0 , & a_4 &= 2 , \\ 0 &= 0.2! + 0 , & a_3 &= 0 , \\ 0 &= 0.1! + 0 , & a_2 &= 0 . \end{aligned}$$

The permutation is then synthesized as

$$1, 1\,2, 1\,2\,3, 1\,4\,2\,3, 1\,4\,2\,5\,3 .$$

The drawbacks inherent to this method are:

(i) The difficulty of generating a random integer in the range $[0, N! - 1]$. Even for moderate N, say $N = 20$, multiple-precision arithmetic is necessary.

(ii) The number of operations required to build the permutation from the a's is

Received November 20, 1966.

approximately $N^2/4$, as the decision to place the kth object is based upon $(k-1)/2$ comparisons on the average.

Pairwise exchange method. We shall now describe a method for which the number of operations is $O(N)$. A random permutation is obtained from any arbitrary one by exchanging the first object with itself or any other object on the right with equal probability, then by exchanging the second object with itself or any other one on the right with equal probability . . . until the $(N-1)$st object has been exchanged. The probability that a given object be in the kth position in the generated permutation is the probability that the $k-1$ first steps leave it free whereas the kth one brings it in the kth position, where it clearly remains afterwards. That probability is

$$p = \left(\frac{N-1}{N}\right) \times \left(\frac{N-2}{N-1}\right) \times \cdots \times \left(\frac{N-k+1}{N-k+2}\right) \times \left(\frac{1}{N-k+1}\right) = \frac{1}{N}.$$

The algorithm proceeds as follows: assume that we can draw $N-1$ numbers ξ_i from a random number generator such that $0 \leqq \xi < 1$.

They are scaled to yield $N-1$ integers η_i

$$\eta_i = [\xi_i(N+1-i)], \qquad i = 1, 2, \cdots, N-1,$$

where $[x]$ denotes the greatest integer in x. Clearly

$$0 \leqq \eta_i \leqq N-i, \qquad i = 1, 2, \cdots, N-1.$$

Then, at the kth step, the kth current object is exchanged with the $(k+\eta_k)$th one, for $k = 1, 2, \cdots, N-1$.

At most $N-1$ exchanges are necessary. Actually, the kth step requires no exchange at all if $\eta_k = 0$, which occurs with probability $1/(N+1-k)$.

The expected value of the number of exchanges is therefore

$$\rho = N - 1 - \sum_{i=1}^{N-1} \frac{1}{N+1-i}$$

which is approximately $N - \log N$ for large N.

The advantages of this method are

(i) It is fast; at worst $N-1$ exchanges are necessary.

(ii) It only deals with numbers in the range $[0, N]$ and is therefore applicable to the generation of large permutations.

(iii) Random integers in the range $[0, N-1]$ are easily produced and even a lack of randomness in the least significant digits of the ξ_i's would have no practical influence.

Example. To find a random permutation of 5 numbers starting from 1 2 3 4 5

i	ξ_i	η_i	*Permutation*
1	0.32305	1	2 1 3 4 5
2	0.80612	3	2 5 3 4 1
3	0.50989	1	2 5 4 3 1
4	0.18278	0	2 5 4 3 1
5	0.46436	0	2 5 4 3 1

One might try to simplify this method by avoiding the variable scaling but the

permutations obtained are no longer random. Consider the algorithm where at the kth step, the kth object is exchanged with any one of the N objects. This transformation when applied N times produces N^N equiprobable mappings of a particular permutation into the set of all permutations of N objects. But there are only $N!$ members in the set and N^N is not divisible by $N!$ if $N > 2$, so that each of the $N!$ permutations is not equiprobable.

The pairwise exchange method is equally well suited for the generation of permutations, combinations, or arrangements. A random combination or arrangement of p objects among N is obtained by performing only p exchanges, the result being the p first objects so generated.

Computing Center
California Institute of Technology
Pasadena, California 91109

1. B. JANSSON, *Random Number Generators*, V. Pettersons Bokindustri Aktiebolag, Stockholm, 1966, pp. 189–191.

2. D. H. LEHMER, "The machine tool of combinatorics," *Applied Combinatorial Mathematics*, edited by E. Beckenbach, Wiley, New York, 1964, pp. 19–23. MR **30** #4687.

On Finding the Disc of Minimum Radius Containing a Given Set of Points*

By L. J. Bass and S. R. Schubert

Recently many combinatorial problems have been found to be amenable to computer solution. This report presents a description of one such problem and its solution.

Let E be a given set of points of finite cardinality in the plane $\mathfrak{R}^2$. The problem is to determine the disc $D_{\min}$ of minimum radius such that $E \subset D_{\min}$.

This is a nontrivial problem. The centroid of E gives no information at all. A complete analytic solution appears extremely difficult, since probably new concepts are required. Moreover, any essentially exhaustive procedure formulated for machine solution is only feasible when E has very small cardinality. However, consideration of a few simple geometrical theorems quickly places the problem in a much more tractable setting.

Definition. Let $E \subset \mathfrak{R}^2$ be given as above. The convex hull of the extreme points of E is that convex polygon P such that $E \subset P$ and the vertices of P are points of E. These vertices are called the extreme points of E.

THEOREM 1. *The extreme points of E completely determine $D_{\min}$.*

Proof. This is clear since $E \subset P \subset D_{\min}$.

THEOREM 2. *There are at least two extreme points of E which are on the boundary of $D_{\min}$. Moreover, if there are exactly two points, then these are, in fact, the endpoints*

Received May 9, 1966. Revised April 24, 1967.
* Contract No. AFO4(695)-669.