

## A RETROSPECTIVE AND PROSPECTIVE SURVEY OF THE MONTE CARLO METHOD\*

JOHN H. HALTON†

### CONTENTS

1. Introduction	2
Elementary definition of the Monte Carlo method; primary and secondary estimators; evaluation of sums, infinite series, and integrals; random generators; breadth of application of the method (sampling in Fréchet spaces; sequential Monte Carlo; biased estimators; random search techniques); random variables in Fréchet spaces; Monte Carlo processes; random generators (general and canonical); Monte Carlo procedures; pseudorandom and quasi random generators; practical and logical difficulties of pseudo-Monte-Carlo calculation.	
2. Retrospect	6
2.1. Early work and general descriptions	6
2.2. Variance-reducing techniques for evaluating sums and integrals	7
Easy functions; correlated (or control-variate) sampling; importance-sampling; relative merits of correlated and importance-sampling; stratified (or systematic) sampling; the problem of signed probabilities; weighted uniform sampling; antithetic variates; implicit multicorrelated sampling (or the E-Z-H method); conditional expectations; conditional Monte Carlo; the rejection technique; sampling in infinite-dimensional spaces.	
2.3. Techniques for solving linear equations	13
Algebraic systems, infinite systems, integral and differential equations; iterative schemes; inconsistent and overdetermined systems; the sum of squares; least-squares solutions; eigenvalue problems; computations involving large matrix products; zeroth-, first-, second-, and third-level methods; random walks; the estimators of von Neumann and Ulam, and of Wasow and Curtiss; dual (or adjoint) sampling; the Monte Carlo Gram-Schmidt process of weak orthogonalization; the sequential grid-refinement technique; three methods for (third-level) sequential Monte Carlo; Monte Carlo for eigenvalue problems; the power method; Rayleigh quotients and other estimators compared.	
2.4. Applications of the Monte Carlo techniques	28
Applications to the absorption of high energy radiation; intranuclear cascade reactions; atomic wave functions and energy levels; thermodynamic properties of gas models, quantum mechanical systems, ferromagnets, long chain polymers; reaction kinetics; Wiener integrals; radiation shielding; criticality studies of nuclear fission weapons and reactors; development of statistical tests; cell population studies; combinatorial problems; search and optimization procedures; operations research, systems analysis, war games and other simulations; signal detection.	
2.5. Random, pseudorandom, and quasirandom sequences	28
General, canonical, and discrete canonical random generators; pseudorandom and quasirandom generators; the generation of an arbitrarily distributed sequence of random variables from a canonical sequence; the direct method; the rejection technique; the composition technique; true random generators; pseudorandom sequences (middle-square; multiplicative-congruential (or power-residue, or Multiply); mixed-congruential; additive-congruential (or sum-residue); Fibonacci sequence); dependence of period on parameters; statistical tests (frequency test; serial test; poker test; gap test; serial correlation; proportion of m-tuples; runs; coupon collector's test; $d^2$ -test) and their theoretical limitations; the asymptotic frequency approach; asymptotic serial correlation; uniform distribution modulo one; k-equidistributed and completely (or totally) equidistributed sequences; the local, minimum, maximum, extreme (or $L^\infty$ ), and (root) mean square (or $L^2$ ) discrepancy; quasirandom sequences;	

\* Received by the editors March 4, 1968, and in revised form April 29, 1969.

† Computer Sciences Department, University of Wisconsin, Madison, Wisconsin 53706. This research was sponsored in part by the Mathematics Research Center, United States Army, Madison, Wisconsin, under Contract DA-31-124-ARO-D-462, and was revised with partial support from the National Science Foundation under Grant GJ-171 and from the University of Wisconsin Computing Center. This paper is a revision of the report [248].

the Fourier analysis approach; the relation of discrepancy to absolute bounds on quasi-Monte-Carlo integration errors; the Roth–Halton–Zaremba theory of various radical inverse sequences; drawbacks of quasi-Monte-Carlo integration.

3. Prospect	47
3.1. General discussion	47
3.2. Monte Carlo processes as stochastic processes	48
3.3. Analysis of the quasi-Monte-Carlo method	48
3.4. Monte Carlo techniques	49
3.5. Random generators	50
3.6. Summary	50
A list of 24 research problems.	
References	51
Author index	60
List of notations	63

**1. Introduction.** The Monte Carlo method is generally defined as *representing the solution of a problem as a parameter of a hypothetical population, and using a random sequence of numbers to construct a sample of the population, from which statistical estimates of the parameter can be obtained.*

Very often, the solution consists of a real number, which can be expressed as the expected value of a random variable  $\tau$  with finite variance, on a probability space  $(M, \mathbf{M}, \mu)$ :

$$(1) \quad \begin{aligned} \mathbf{E}[\tau] &= \int_M \tau(\zeta) d\mu(\zeta) = \theta, \\ \text{var } [\tau] &= \mathbf{m}_2[\tau] = \int_M |\tau(\zeta) - \theta|^2 d\mu(\zeta) < \infty; \end{aligned}$$

and  $\tau$  is then called a *primary estimator* for  $\theta$ . If points  $\zeta_1, \zeta_2, \zeta_3, \dots$  are sampled independently from  $(M, \mathbf{M}, \mu)$ , the *secondary estimator*  $\phi_k$ , defined by the arithmetic mean

$$(2) \quad \phi_k(\zeta_1, \zeta_2, \dots, \zeta_k) = k^{-1} \sum_{i=1}^k \tau(\zeta_i),$$

has

$$(3) \quad \mathbf{E}[\phi_k] = \theta, \quad \text{var } [\phi_k] = k^{-1} \text{var } [\tau],$$

and converges in quadratic mean, in probability, and with probability one, to  $\theta$ , as  $k \rightarrow \infty$  (by the weak and strong laws of large numbers: see, e.g., [1, pp. 230 and 245]).

For example, if the problem consists of evaluating a real sum

$$(4) \quad \theta = \sum_{s=1}^N f(s),$$

where  $N$  is enormously large, so that the direct calculation of  $\theta$  by successive additions is prohibitively laborious, and if no analytic means of reducing the problem to manageable proportions are available, we may resort to the Monte

Carlo method. The simplest technique depends on choosing a real-valued function  $p(s)$ , defined on the summation-set  $S = \{1, 2, \dots, N\}$ , whose partial sums

$$(5) \quad q(n) = \sum_{s=1}^n p(s)$$

are known or calculable, and such that

$$(6) \quad 0 \leq p(s) \leq 1, \quad s \in S,$$

$$(7) \quad \sum_s p(s) = 1,$$

and  $p(s) > 0$  for any  $s$  in  $S$  at which  $f(s) \neq 0$ . (The last condition is rather important, but it is not usually mentioned.) If we define the subsets of  $S$ ,

$$(8) \quad F = \{s : f(s) = 0\}, \quad G = \{s : p(s) = 0\}, \quad R = SG^c,$$

where  $c$  denotes the complement; then the last condition is

$$(9) \quad F \subseteq G.$$

We now define the probability space  $(M, \mathbf{M}, \mu)$  by taking  $M$  to be  $S$ ,  $\mathbf{M}$  to be the class of all subsets of  $S$ , and  $\mu$  to be given by

$$(10) \quad \mu(A) = \sum_{s \in A} p(s), \quad A \in \mathbf{M};$$

that is, each point  $s$  of  $S$  is assigned the probability  $p(s)$ ; and the estimator  $g$  is defined as

$$(11) \quad g(s) = \begin{cases} f(s)/p(s) & \text{when } s \in R, \\ 1 & \text{when } s \in G. \end{cases}$$

This satisfies the conditions (1). (The simplest choice of  $p$  is the *uniform distribution*, with  $p(s) = 1/N$  for all  $s \in S$ ; and then  $g(s) = Nf(s)$ ; but this may not be the most efficient choice.) To obtain the sample points  $\zeta_i$ , we may proceed in various ways. Sometimes a direct source of such points with the chosen probabilities is available (this may be the reason for our choice of  $p$ ). More often, we make use of a *random generator of canonical type*: this is a device which is purported to generate a sequence of independent samples of a random variable  $\xi$  distributed uniformly over the real unit interval  $[0, 1]$ . We then define the corresponding  $\zeta$  by

$$(12) \quad \zeta(\xi) = n \quad \text{if } q(n-1) \leq \xi < q(n), \quad \zeta(0) = \zeta(1) = 1,$$

where we take  $q(0) = 0$ . (In the case of uniform  $p$ , this reduces to

$$(13) \quad \zeta(\xi) = [N\xi] + 1, \quad 0 \leq \xi < 1, \quad \zeta(1) = 1,$$

where  $[x]$  denotes the largest integer not greater than  $x$ .)

By going to the limit, as  $N \rightarrow \infty$ , we may extend the above technique to the evaluation of *infinite series* and *Riemann integrals*, provided that appropriate convergence conditions are satisfied. In fact, it is fair to say that virtually all applications of the Monte Carlo method, with the exception of certain random search procedures, reduce basically to this technique, combined with various numerical and analytic transformations and refinements.

However, in its most general form, the method has a much broader range of application than might be inferred from this:

(i) The solution  $\theta$  may be a vector, a function [2], or a point in a Fréchet space [3], [4]; and the estimators will then take their values from a suitable solution space  $H$ , containing  $\theta$ .

(ii) The choice of even a simple primary estimator is very wide and can profoundly influence the efficiency of the method. This question has been given a great deal of consideration, and many ways of increasing the efficiency of the estimators have been devised.

(iii) The primary estimators used in the course of a computation need not all be the same; and a correlation may be introduced between them, to make advantageous use of the information being acquired during the sampling. (This is *sequential Monte Carlo* [5], [6].) Nor need the secondary estimators be simple arithmetic means of the primary estimators.

(iv) In these circumstances, it is no longer necessary that the primary or secondary estimators be *unbiased* (i.e., that they have expected value  $\theta$ ), so long as the latter converge to  $\theta$  in some acceptable sense, as the size of the sample tends to infinity.

(v) The population  $M$ , with its probability structure  $(M, \mathbf{M}, \mu)$ , can be very complicated; and the sampling of each point  $\zeta$  from  $M$  will frequently involve a lengthy computation, such as the tracing of a random walk in an intricate and highly inhomogeneous space.

(vi) As was mentioned above, there are situations in which we cannot think of the computation as any reasonable kind of averaging, but must rather see it as a *random search*, which can always be viewed either as a minimization or as zero-seeking, on a suitable function, subject to imposed conditions. In this case, there are no primary estimators; but there are still secondary estimators, converging (one hopes) to the required solution  $\theta$ .

Taking these generalizations into account, we may give a more explicit probabilistic definition of the Monte Carlo method as follows [3], [4]. We define a suitable Fréchet space  $H$  as our solution space, in which points can be represented by sequences of real numbers

$$(14) \quad \mathbf{a} = [a_n]_n = [a_n]_{n=1}^{\infty} = [a_1, a_2, a_3, \dots],$$

with the linear structure defined by

$$(15) \quad \mathbf{x} + \mathbf{y} = [x_n + y_n]_n, \quad p\mathbf{x} = [px_n]_n, \quad \mathbf{0} = [0, 0, 0, \dots],$$

for all  $\mathbf{x}$  and  $\mathbf{y}$  in  $H$  and all real  $p$ , where  $\mathbf{0}$  is the null vector; and with the topology induced by the metric

$$(16) \quad d(\mathbf{x}, \mathbf{y}) = Q(\mathbf{x} - \mathbf{y}),$$

where

$$(17) \quad Q(\mathbf{x}) = \sum_{n=1}^{\infty} c_n |x_n| / (1 + |x_n|),$$

with the  $c_n$  all strictly positive and  $\sum_n c_n$  convergent (see [7, pp. 112–114], [8, pp. 133–142]). We can now define a *random variable* of  $M$  in  $H$  as a function  $\phi$

mapping  $M$  into  $H$ , such that the set

$$(18) \quad \phi^{-1}(V) = \{\zeta \in M : \phi(\zeta) \in V\}$$

is in  $\mathbf{M}$  whenever  $V$  is a spherical neighborhood in  $H$ . (This definition can usefully be extended to even more general spaces; but the essential ideas are already exhibited in the space described above.) It follows that  $\phi$  is a random variable if and only if every component  $f_n$  of its sequence representation is a real-valued random variable of  $M$ . (The representation is that of each  $\phi(\zeta)$  as  $\mathbf{f}(\zeta) = [f_n(\zeta)]_n$  for all  $\zeta$  in  $M$ .) The induced probability space  $(H, \mathbf{H}, p_\mu)$ , where  $\mathbf{H}$  is the class of all Borel subsets of  $H$  and  $p_\mu = \mu\phi^{-1}$ , is called the *distribution* of  $\phi$  in  $H$ .

Let  $\mathbf{V}$  be the set of all random variables of  $M$  in  $H$ , and give  $\mathbf{V}$  a topology by defining the convergence of a sequence  $\Phi = [\phi_m]_m$  in  $\mathbf{V}$  (for example, uniform convergence, pointwise convergence, convergence with probability one, or convergence in probability). If a sequence  $\Phi$  converges to  $\theta$ , under the adopted definition, we call it a *Monte Carlo process* for  $\theta$ .

If  $\Omega$  is a practical device (such as a roulette wheel, or a circuit triggered by thermal or radioactive impulses) which constructs or selects points of  $M$  in accordance with the probability structure denoted by  $(M, \mathbf{M}, \mu)$ , we call it a *random generator* for  $(M, \mathbf{M}, \mu)$ . The *Monte Carlo procedure*  $(\Omega, \Phi)$  for  $\theta$  then consists of generating a point  $\zeta$  of  $M$  by means of the random generator  $\Omega$ , and computing a corresponding value  $\phi_t(\zeta)$  in the process  $\Phi$ , far enough along the sequence to give the accuracy required. (The processes which are used invariably require an amount of computation which increases rapidly as the index  $t$  increases.)

It is clear that, for our purpose of estimating  $\theta$ , we are only interested in the distribution of the sequence  $[\phi_m(\zeta)]_m$  in  $H$ , and not in the particular probability space  $(M, \mathbf{M}, \mu)$  and random sequence  $[\phi_m]_m$  from which it is derived. It has been shown [9] that, given a sequence  $\Xi = [\xi_n]_n$  of independent random variables, each uniformly distributed in  $U = [0, 1]$  (so that  $\Xi$  is in the *canonical probability space*  $(L, \mathbf{L}, \lambda)$ : the corresponding *canonical random generator* is denoted by  $\Lambda$ ), and an arbitrary sequence  $\Phi = [\phi_m]_m$  of random variables in  $H$ ; we can construct a sequence  $\Psi$  of random variables of the form  $\psi_m(\xi_1, \xi_2, \dots, \xi_m)$ , taking  $L$  into  $H$ , which have the same joint probability distribution in  $H$  as the  $\phi_m$ . Thus we may put any Monte Carlo procedure into the canonical form  $(\Lambda, \Psi)$ .

These definitions make the study of Monte Carlo processes a part of the theory of probability, as it applies to stochastic processes. They treat the Monte Carlo method as a class of techniques of statistical estimation, as it has traditionally been approached, and its error analysis is couched in statistical terms. Typically, an answer  $\Theta = \Theta(\zeta)$  is given with a statement such as “the probability that the error exceeds  $\epsilon$  is  $\rho(\epsilon)$ ,” the answer being considered accurate if  $\epsilon$  and  $\rho(\epsilon)$  can be made simultaneously small. This view of the method is predicated on the existence and availability of random generators which produce random sequences of the required kind; for the above statement means that the set  $A(\epsilon)$  of points  $\zeta$  in  $M$ , yielding answers  $\Theta(\zeta)$  farther than  $\epsilon$  from the correct solution  $\theta$ , has the probability  $\mu[A(\epsilon)] = \rho(\epsilon)$ .

Currently, however, it is the almost universal practice to use, as “random generators,” devices (such as lists, decks of punched cards, or programs executing numerical algorithms) which do not even pretend to have more than a trace of true

randomness (this randomness lies mainly in the choice of a few parameters, usually only an initial value). The sequences they yield are of two types. Those which have, for a considerable length at least, all the more usually considered properties of randomly generated sequences, as tested by standard statistical tests, are called *pseudorandom*, and are used in general purpose “random generators,” such as those usually provided in the library of frequently used subroutines which is part of the “software” of any modern digital computer. The remaining sequences lay no general claim even to “random behavior,” but are, in certain specific and useful aspects (most often, their density in the unit interval  $U$ ), effectively “random,” or even “superrandom” (e.g., their uniformity is better than would be expected of a randomly generated sequence). They are termed *quasirandom*. These latter sequences, appropriately used, can increase the efficiency of a Monte Carlo procedure very appreciably.

It should be realized that it is irrelevant, and largely meaningless, to ask whether a given finite sequence of numbers is “truly random.” At best, it can be subjected to a battery of statistical tests, each of whom only yields the probability that a randomly generated sequence would deviate from expectation by at least as much as does the given sequence, in the particular respect being tested. Since we can neither prove that any particular process or device is *a priori* random, nor test its output exhaustively, the search for randomness is evidently futile. This would be very discouraging, were it not for the fact that, when “random numbers” are used in practice, we generally require only a few of the properties of randomness, and all others are immaterial.

Nevertheless, it is clearly *not* valid (without ad hoc justification) to use error estimates based on the probability that a given sequence  $\xi_1, \xi_2, \xi_3, \dots$  lies in a certain set, if it is sampled from a probability space  $(L, \mathcal{L}, \lambda)$ , when we know very well that the sequence is, in fact, taken from an extremely small subset (often a single point) of  $L$ , with a probability structure which is often largely conjectural. Yet this is what is customarily done, and with remarkable success! While a few results have been obtained, in the direction of regularizing this situation [10]–[15] by giving absolute, rigorous bounds for the error of Monte Carlo integration in certain cases, the question remains open, and evidently much further work is needed. A critical discussion of this peculiar state of affairs is given by Zaremba [53].

## 2. Retrospect.

**2.1. Early work and general descriptions.** The Monte Carlo method has been traced as far back as Babylonian and Old Testament times [16]–[18]; and mention should be made of the early ideas due to Lord Rayleigh [19] in 1899, “Student” [20] in 1908, Courant, Friedrichs, and Lewy [21] in 1928, Kolmogorov [22] in 1931, and Pólya [23] in 1938. However, the systematic use of the method, and its name, date back only about 20–25 years, to the “Los Alamos School” of mathematicians and physicists, and more especially to the work of von Neumann, Ulam, Metropolis, Kahn, Fermi, and their collaborators [24], [25].

The only books on the subject are [4], [17], [31]–[33], [51], [241], [247]; and [4] and [241] are not yet published, while [31] is not commercially available. (Of [33] and [51], both translations of the same Russian text, the latter is preferable,

as it has been revised and augmented by the original authors.) Other general descriptions of the method may be found in [3], [16], [24]–[30], and an extensive bibliography up to 1961 may be found in [34]. The most complete bibliography available to date is in [4].

**2.2. Variance-reducing techniques for evaluating sums and integrals.** The basic technique for evaluating large or infinite sums, and integrals, by the Monte Carlo method is described at the beginning of this survey. An unbiased primary estimator  $\tau$  of the answer  $\theta$  is defined (see (1) and (11)), and it is sampled repeatedly and independently to yield a convergent secondary estimator  $\phi_k$ , taking the form of a simple arithmetic mean (see (2) and (3)). In view of the relations (3), it is clearly important to choose  $\tau$  so as to make  $\text{var}[\tau]$  as small as possible, so long as this does not involve too much extra computation in the evaluation of each sample value of  $\tau$ . Thus the main effort, in this branch of the subject, has been directed to the invention of techniques for constructing estimators  $\tau$  with small variances. These techniques are essentially the same for sums, infinite series, and integrals, so that one may avoid the consideration of convergence conditions, while demonstrating the ideas behind the techniques, by describing them in the case of a finite sum (4).

Sometimes we can find a function  $\varphi(s)$  which approximates the summand function  $f(s)$  in  $S = \{1, 2, \dots, N\}$ , and for which the sum over  $S$  is relatively easily obtained. We shall call such a  $\varphi$  an *easy function*. Then, since

$$(19) \quad \theta = \sum_s [f(s) - \varphi(s)] + \sum_s \varphi(s),$$

where

$$(20) \quad \Phi = \sum_s \varphi(s)$$

is known, we may sample the estimator

$$(21) \quad u(s) = \begin{cases} \frac{f(s) - \varphi(s)}{p(s)} + \Phi & \text{when } s \in R, \\ 1 & \text{when } s \in G, \end{cases}$$

just as we did  $g(s)$  in the basic method, under the condition

$$(22) \quad F_\varphi = \{s : f(s) = \varphi(s)\} \supseteq G,$$

instead of (9); and then, clearly,

$$(23) \quad \mathbf{E}[u] = \theta, \quad \text{var}[u] = \sum_R \frac{[f(s) - \varphi(s)]^2}{p(s)} - \left\{ \sum_R [f(s) - \varphi(s)] \right\}^2;$$

so that, if we can make  $|f(s) - \varphi(s)|$  much smaller than  $|f(s)|$ , the variance of  $u$  will be much smaller than that of  $g$ . This technique is called *correlated sampling* or “control-variate sampling.”

Alternatively, if we can put

$$(24) \quad p(s) = \varphi(s)/\Phi,$$

which is allowable if  $\varphi(s)$  is of the same sign everywhere in  $S$  and satisfies (22), then the estimator  $g$  becomes

$$(25) \quad v(s) = \begin{cases} \Phi f(s)/\varphi(s) & \text{when } s \in R, \\ 1 & \text{when } s \in G, \end{cases}$$

and again

$$(26) \quad \mathbf{E}[v] = \theta, \quad \text{var}[v] = \Phi \sum_R \frac{[f(s)]^2}{\varphi(s)} - \theta^2,$$

and the variance of  $v$  can be made much smaller than that of  $g$  by approximating  $f$  with  $\varphi$  closely enough. This technique is called *importance sampling*.

The technique of *stratified sampling* (or “systematic sampling”) is a method of sampling in which the set  $S$  is partitioned into disjoint subsets  $S_h$ ,  $h = 1, 2, \dots, k$ , so that

$$(27) \quad \theta = \sum_{h=1}^k \theta_h,$$

where

$$(28) \quad \theta_h = \sum_{S_h} f(s);$$

and then each  $\theta_h$  is estimated separately by the Monte Carlo method (or, sometimes, certain of the  $\theta_h$  can be evaluated by other means, such as asymptotic approximation or direct computation). If the “stratification” is properly carried out, so as to reduce the variation of  $f$  within each set  $S_h$ , and the sampling is appropriately chosen, a considerable reduction of variance will result.

These three techniques have long been known, and references to them are scattered throughout the literature, including the general references given above. Given an easy function  $\varphi$  approximating  $f$ , it may be asked, which of the estimators,  $u$  in (21), with uniform  $p(s) = 1/N$ , or  $v$  in (25), should be used. It has been shown (see [35]) that

$$(29) \quad \begin{aligned} \text{var}[u] - \text{var}[v] &= N \sum_R [f(s) - \varphi(s)]^2 - \sum_R \frac{[f(s) - \varphi(s)]^2}{\varphi(s)} \sum_R \varphi(s) \\ &= N^2 \text{cov} \left[ \frac{\{f(s) - \varphi(s)\}^2}{\varphi(s)}, \varphi(s) \right], \end{aligned}$$

where the covariance is calculated for uniform  $s$  in  $S$ . Therefore, if, in particular, the approximation of  $f(s)$  by  $\varphi(s)$  is “absolutely uniform” in  $S$  (i.e.,  $|f(s) - \varphi(s)|$  is approximately constant over  $S$  and for all values of  $|\varphi(s)|$  in  $S$ ), then correlated sampling is more efficient; while if the approximation is “relatively uniform” (i.e.,  $|f(s) - \varphi(s)|$  is approximately proportional to  $|\varphi(s)|$  in  $S$ ), then importance sampling is preferable.

If  $f(s)$  changes sign in  $S$ , then so will any reasonably good approximation  $\varphi(s)$  to it, so that we cannot simply take (24) for our probability distribution.

If  $\varphi(s) > -B$ , a known lower bound, then we can sample

$$(30) \quad w(s) = \begin{cases} \frac{(\Phi + NB)[f(s) + B]}{\varphi(s) + B} - NB & \text{when } s \in R, \\ 1 & \text{when } s \in G, \end{cases}$$

with the probability

$$(31) \quad p(s) = [\varphi(s) + B]/(\Phi + NB),$$

in a form of modified importance sampling. However, this is not a very efficient method if  $B$  is large. (An analogous trick can be applied if we have an upper bound for  $\varphi(s)$ , instead of a lower bound.) If  $\varphi(s)$  has no known bounds in  $S$ , we must abandon the use of importance sampling, unless we can give a practical interpretation of *signed probabilities*. Such an interpretation has been given in [36], in terms of sampling two independent random variables, whose expected values are the sums of  $f(s)$  over the subsets of  $S$  in which  $f(s)$  is respectively positive and negative. (Note that this interpretation differs from the purely formal one proposed by Bartlett [37], which would not seem to be useful in the present context.)

An interesting variation on importance sampling has recently been suggested by Powell and Swan [52], following an idea of Handscomb [46, and below]; they call it *weighted uniform sampling*. The estimator used is (in slightly more general form than they write)

$$(32) \quad W_n(s_1, s_2, \dots, s_n) = \sum_{i=1}^n g(s_i) / \sum_{i=1}^n \gamma(s_i),$$

where  $g(s)$  is defined as in (11),  $\gamma(s)$  is defined similarly in terms of  $\varphi$  instead of  $f$ , and the  $s_i$  are sampled independently from  $S$  with probability  $p(s)$ . Since the numerator and denominator of (32) are unbiased estimators of  $n\theta$  and  $n\Phi$ , respectively, it follows that  $W_n$  is a biased estimator of  $\theta/\Phi$ , converging to  $\theta/\Phi$  in quadratic mean, in probability, and with probability one. This technique replaces sampling from what may be a complicated distribution defined by  $\varphi(s)$  (see (24)), by sampling from an arbitrarily chosen simple distribution  $p(s)$  (Powell and Swann simply take  $p(s)$  to be uniform on  $S$ ). This technique provides another answer to the question of what to do if  $f$ , and so any good  $\varphi$ , changes sign in  $S$ .

The technique of *antithetic variates* [38]–[44] is related to that of correlated sampling; but, instead of subtracting an easy approximation  $\varphi$  from  $f$ , to yield a relatively little-varying estimator, we use  $f$  itself, by averaging different segments of  $f(s)$ , by means of a linear transformation. This concept is due to Hammersley and Morton [38]. The method depends on the smoothness of the function  $f$  and is usually discussed in the case of the integration of a multiply-differentiable function. For instance, if  $f(s)$  is monotone, it is evident that the transformation

$$(33) \quad f^*(s) = \mathcal{F}_1 f(s) = [f(s) + f(N - s)]/2$$

(the simplest of the family of transformations considered) will yield an estimator  $\tau^*(s)$  with a much smaller variance than the original  $\text{var}[\tau]$ . The method can be very powerful; but it is weakest when the function  $f$  is very irregular (e.g., when one

is evaluating a multidimensional integral in which  $f$  varies rapidly in every direction).

Correlated and importance sampling depend on knowing an easy function  $\phi(s)$  which approximates the *difficult functions*  $f(s)$  in  $S$ . Suppose, instead, that, having selected a probability function  $p(s)$  and defined the function  $g(s)$  as in (11), we can find a linearly independent set of easy functions  $v_i(s)$ ,  $i = 1, 2, \dots, n$ , such that

$$(34) \quad \mathbf{E}[v_i] = \sum_S v_i(s)p(s) = 0,$$

and such that there is an unknown set of coefficients  $x_i$ , for which

$$(35) \quad h(s) = g(s) - \sum_{i=1}^n x_i v_i(s)$$

is approximately constant in  $S$ . Then  $\mathbf{E}[h] = \theta$  and (see [4])  $\text{var}[h]$  is minimized when the  $x_i$  satisfy

$$(36) \quad \sum_{i=1}^n x_i \mathbf{E}[v_i v_j] = \mathbf{E}[g v_j], \quad j = 1, 2, \dots, n;$$

and then  $h(s)$  is orthogonal to every  $v_i(s)$  and  $\sqrt{\text{var}[h]}$  is the distance  $d(g, L)$  from the function  $g(s)$  to the linear space spanned by the  $v_i$  and a constant function, say  $v_0(s) = 1$ , relative to the scalar product

$$(37) \quad (g_1, g_2) = \sum_S g_1(s)g_2(s)p(s).$$

Since the computation of  $\mathbf{E}[g v_j]$  is of the same order of difficulty as that of  $\mathbf{E}[g] = \theta$ , the exact optimum (36) must be replaced by an approximation. It is natural to consider Monte Carlo approximations. We combine (36) with  $x_0 = \mathbf{E}[g]$ , using (34), to yield

$$(38) \quad \sum_{i=0}^n x_i \mathbf{E}[v_i v_j] = \mathbf{E}[g v_j], \quad j = 0, 1, 2, \dots, n.$$

The simplest Monte Carlo estimate of (38) is

$$(39) \quad \sum_{i=0}^n z_i v_i(s_j) = g(s_j), \quad j = 0, 1, 2, \dots, n,$$

where the  $s_j$  are random points of  $S$  (and we have eliminated the common factor  $v_j(s_j)$  from the  $j$ th equation). Since it is our assumption that the two sides of each equation (39) vary similarly, it is reasonable, by the principle of correlated sampling, to use the same  $s_j$  in estimating every term of each equation.

The estimator of  $x_0 = \theta$  is clearly  $z_0$ , and, by Cramer's rule,

$$(40) \quad z_0 = z_0(s_0, s_1, s_2, \dots, s_n) = \Delta_g / \Delta_1,$$

where

$$(41) \quad \Delta_g = \Delta(g, v_1, v_2, \dots, v_n) = \begin{vmatrix} g(s_0) & v_1(s_0) & \cdots & v_n(s_0) \\ \vdots & \vdots & & \vdots \\ g(s_n) & v_1(s_n) & \cdots & v_n(s_n) \end{vmatrix}.$$

At first sight, we would sample the  $s_j$  independently with probability  $p$ ; but then the nonlinear estimator  $z_0$  would have an unknown constant bias. It has been shown [4], [17], [45], [46] that this difficulty can be circumvented in two ways. First, one may sample the  $s_j$  with joint probability  $Dp(s_0)p(s_1) \cdots p(s_n)$ , where

$$(42) \quad D = D(s_0, \dots, s_n) = \Delta_1^2 / \mathbf{E}[\Delta_1^2];$$

when it turns out that, if we write  $\mathbf{E}_D[y] = \mathbf{E}[Dy]$  for the expectation with the relative joint probability  $D$ , and  $\text{var}_D[y]$  for the corresponding variance,

$$(43) \quad \mathbf{E}_D[z_0] = \theta \quad \text{and} \quad \text{var}_D[z_0] = [d(g, L)]^2,$$

so that the exact minimum value of  $\text{var}[h]$  can be attained (at the expense of using a more complicated sampling scheme than the sampling of  $h$ ).

Secondly, one may sample a rather large number  $m$  of independent values  $s_k$  from  $S$  with probability  $p$  and use them to form the more accurate approximation

$$(44) \quad \sum_{i=0}^n w_i \left\{ \sum_{k=1}^m v_i(s_k) v_j(s_k) \right\} = \sum_{k=1}^m g(s_k) v_j(s_k), \quad j = 0, \dots, n,$$

to (36), yielding an estimator  $w_0$  of  $\theta$  which, though still biased, converges to  $\theta$  with probability one, as  $m \rightarrow \infty$ .

These two techniques may be given the name of *implicit multicorrelated sampling* (or the *E-Z-H method*, after Ermakov, Zolotukhin and Handscomb, who devised them). They have not yet seen much practical application; but they appear to be well worth trying, when the complexity of the problem warrants the considerable extra labor required to generate each estimate.

We now turn to a type of problem closely related to the straight summations (4) hitherto envisaged. Suppose that a probability  $p(s)$  and a real-valued function  $g(s)$  are defined on the set  $S = \{1, 2, \dots, N\}$ . We seek the *conditional expectation* of  $g(s)$ , given that a certain condition  $C$  is satisfied by  $s$ , when  $s$  has the unconditional probability  $p(s)$ . We suppose that the probability of  $C$  (that is,  $\sum_{s:C \text{ holds}} p(s)$ ) is nonzero. (Analogous problems for  $S$  an infinite set can be defined, and it is these which are generally considered in the literature; but the introduction of Jacobians, Haar measure, and other analytic considerations can be avoided by examining the finite form of the problem.)

The condition  $C$  is defined as follows. We define a function  $\mathbf{C}(s)$  on  $R$  (see (8)), whose values are one-to-one transformations  $\mathbf{t}$  of  $R$  onto itself, and we denote by  $\mathbf{T}$  the group of such transformations generated from the set of all values of  $\mathbf{C}(s)$  by finite sequences of multiplications and inversions, in the usual way. We suppose that  $\mathbf{C}$  is homogeneous: if  $\mathbf{t} \in \mathbf{T}$ ,

$$(45) \quad \mathbf{C}(\mathbf{t}s) = \mathbf{t}\mathbf{C}(s).$$

Then every  $\mathbf{t} \in \mathbf{T}$  is the value of  $\mathbf{C}(s)$  for some  $s \in R$  (for if some  $\mathbf{C}(s') = \mathbf{t}'$ , then  $\mathbf{t} = \mathbf{C}(\mathbf{t}'^{-1}s')$ ). Thus the set  $\mathbf{T}$  is finite, since  $R$  is finite, and, if  $\mathbf{1}$  denotes the identity transformation of  $\mathbf{T}$  and

$$(46) \quad V = \{s \in R : \mathbf{C}(s) = \mathbf{1}\},$$

then, for all  $\mathbf{t} \in \mathbf{T}$ ,

$$(47) \quad S(\mathbf{t}) = \{s \in R : \mathbf{C}(s) = \mathbf{t}\} = \{\mathbf{tv} : v \in V\};$$

and we have a one-to-one correspondence between the  $s \in R$  and the ordered pairs  $[\mathbf{t}, v]$  with  $\mathbf{t} \in \mathbf{T}$  and  $v \in V$ , given by

$$(48) \quad s = \mathbf{tv}, \quad \mathbf{t} = \mathbf{C}(s), \quad v = \mathbf{C}(s)^{-1}s.$$

Given all this structure, we assume that the condition  $C$  takes the form

$$(49) \quad \mathbf{C}(s) = \mathbf{t}_0.$$

It follows from our assumption that the probability of  $C$  is

$$(50) \quad P(\mathbf{t}_0) = \sum_{S(\mathbf{t}_0)} p(s) = \sum_V p(\mathbf{t}_0 v) > 0,$$

and that the required conditional expectation is

$$(51) \quad \theta = \mathbf{E}_p[g(s)|\mathbf{C}(s) = \mathbf{t}_0] = \sum_{S(\mathbf{t}_0)} \frac{g(s)p(s)}{P(\mathbf{t}_0)}.$$

It can be seen from this that, if we select arbitrary probabilities  $q(s) > 0$  on  $R$  and, for each  $v \in V$ ,  $Q(\mathbf{t}, v)$  on  $\mathbf{T}$ ; then, if  $s$  is sampled from  $R$  with probability  $q(s)$ , and we adopt the estimator

$$(52) \quad g^*(s) = g(s^*)w^*(s),$$

where

$$(53) \quad s^* = \mathbf{t}_0 \mathbf{C}(s)^{-1} s, \quad w^*(s) = \frac{p(s^*)}{q(s)} \frac{Q[\mathbf{C}(s), \mathbf{C}(s)^{-1}s]}{P(\mathbf{t}_0)},$$

then

$$(54) \quad \mathbf{E}[g^*] = \theta.$$

The kind of situation in which this technique is applicable is when, for instance,  $S$  is a multidimensional Euclidean space (this is the integral form of the problem, of course) and the condition  $C$  fixes either the distance of  $s$  from the origin, or the values of a subset of the coordinates of  $s$ . In the first example, we would take  $\mathbf{T}$  to be the multiplicative group of positive real numbers; and in the second example,  $\mathbf{T}$  would be the additive group of displacements in the subspace related to the mentioned subset of coordinate directions.

This technique was named *conditional Monte Carlo* by Trotter and Tukey [47], [48], who invented it. See also [4], [17], [49], [50]. Its advantage is that it provides a direct method of sampling for the solution  $\theta$ , using every sample value obtained, instead of the more obvious *rejection technique*, in which the estimator takes the value  $g(s)/P(\mathbf{t}_0)$  if  $s$ , sampled from  $S$  with probability  $p(s)$ , satisfies the condition  $C$ , and the value zero (rejection) otherwise. If  $P(\mathbf{t}_0)$  is small (and especially in the integral case, when  $P(\mathbf{t}_0) = 0$ ), this method can be extremely inefficient, while conditional Monte Carlo works well. The arbitrary probability functions  $q(s)$  and  $Q(t, v)$  supplement  $p(s)$  in providing the solver with flexibility in devising a sampling scheme tailored to the particular properties of his problem.

We consider, finally, the problems which arise if  $\theta$  and the functions  $f(s)$  take their values in a multidimensional space or a function space,  $H$ . If  $H$  is a field, all the foregoing methods carry over to this case without difficulty, except for importance sampling (unless the ideas of [36] or [52] will produce workable sampling schemes). Otherwise, one has to apply the real-function techniques to each component of the solution, or at least to a “representative and adequate” sample of these components. This sample itself could be a random one, leading to a new kind of Monte Carlo sampling problem, not hitherto considered. Little has been done on these questions (but see [2], [4]).

**2.3. Techniques for solving linear equations.** One of the most fruitful fields for the application of the Monte Carlo method is in the solution of *linear equations*. As in § 2.2, we find essentially the same techniques being applied to solve large *systems*, and *integral* and *differential equations*; and again, to simplify the presentation, we limit ourselves mainly to *finite* (though large) systems of equations. Just as we limited our integrals in § 1 to be Riemann integrals, so that they could be expressed as the limits of discrete sums; so we now consider only those infinite and continuous sets of equations which are expressible as the limits of discrete approximations (see [55], [59], [60]).

We begin by considering a nonsingular system of equations

$$(55) \quad \sum_{s=1}^N A_{rs}x_s = b_r, \quad r \in S = \{1, 2, \dots, N\},$$

where the  $A_{rs}$  and  $b_r$  are given real numbers, and the  $x_s$  are the unknowns to be estimated, forming the solution vector  $\mathbf{x}$ . The nonsingularity implies that the  $A_{rs}$  form a matrix  $\mathbf{A}$  whose columns are linearly independent, so that (55), which may be written  $\mathbf{Ax} = \mathbf{b}$ , will have the unique solution

$$(56) \quad \mathbf{x} = \mathbf{A}^{-1}\mathbf{b}.$$

If (55) is put into the form (see (75)–(77) below)

$$(57) \quad \mathbf{x} = \mathbf{a} + \mathbf{Hx},$$

where the spectral radius (see (66) below) of  $\mathbf{H}$  is less than one, we have

$$(58) \quad \mathbf{x} = (\mathbf{I} - \mathbf{H})^{-1}\mathbf{a} = \mathbf{a} + \mathbf{Ha} + \mathbf{H}^2\mathbf{a} + \dots + \mathbf{H}^m\mathbf{a} + \dots = \sum_{m=0}^{\infty} \mathbf{H}^m\mathbf{a},$$

and the Neumann series is absolutely convergent. If we write

$$(59) \quad \mathbf{X}_m = \sum_{h=0}^m \mathbf{H}^h\mathbf{a},$$

we have  $\mathbf{X}_m \rightarrow \mathbf{x}$  (componentwise) as  $m \rightarrow \infty$ , and we can set up *iterative schemes* such as

$$(60) \quad \mathbf{X}_0 = \mathbf{a}, \quad \mathbf{X}_m = \mathbf{a} + \mathbf{H}\mathbf{X}_{m-1}, \quad m > 0.$$

In many practical instances, the “known” quantities  $A_{rs}$  and  $b_r$ , or  $H_{rs}$  and  $a_r$ , are themselves the result of lengthy calculations. An important case is when we have more equations than unknowns, with experimental or other errors making

the system *inconsistent*, as well as *overdetermined*. We then have a system of approximate equations

$$(61) \quad \sum_{s=1}^N L_{us}x_s \approx f_u, \quad u \in T = \{1, 2, \dots, Q\},$$

with

$$(62) \quad Q > N,$$

and we still assume that the columns of the matrix  $\mathbf{L}$  are linearly independent. If we decide to minimize the “sum of squares”

$$(63) \quad S(\mathbf{x}) = \sum_{u=1}^Q \omega_u \left\{ f_u - \sum_{s=1}^N L_{us}x_s \right\}^2 = (\mathbf{f} - \mathbf{L}\mathbf{x})^\top \boldsymbol{\Omega} (\mathbf{f} - \mathbf{L}\mathbf{x}),$$

where the  $\omega_u > 0$  are diagonal elements of the diagonal matrix  $\boldsymbol{\Omega}$ , as our criterion of closeness of approximation in (61); it is easily verified that a minimum is uniquely attained when  $\mathbf{x}$  is the (unique) solution of (55), with

$$(64) \quad \begin{aligned} A_{rs} &= \sum_{u=1}^Q \omega_u L_{ur} L_{us}, \quad \text{or} \quad \mathbf{A} = \mathbf{L}^\top \boldsymbol{\Omega} \mathbf{L}, \\ b_r &= \sum_{u=1}^Q \omega_u L_{ur} f_u, \quad \text{or} \quad \mathbf{b} = \mathbf{L}^\top \boldsymbol{\Omega} \mathbf{f}. \end{aligned}$$

The resulting vector  $\mathbf{x}$  is often called the *least-squares solution* of (61).

Related with problems of the form  $\mathbf{Ax} = \mathbf{b}$ , we find the *eigenvalue problems*: to find the values of  $\lambda$  for which there exist nonnull solutions  $\mathbf{x}$  to the system of equations

$$(65) \quad \sum_{s=1}^N A_{rs}x_s = \lambda x_r, \quad r \in S, \quad \text{or} \quad \mathbf{Ax} = \lambda \mathbf{x}.$$

The *spectral radius* of  $\mathbf{A}$  is defined as

$$(66) \quad \rho(\mathbf{A}) = \sup \{ |\lambda| : (\exists \mathbf{x} \neq \mathbf{0}) \mathbf{Ax} = \lambda \mathbf{x} \}$$

and it is known (see [54]–[56]) that

$$(67) \quad \rho(\mathbf{A}) = \lim_{m \rightarrow \infty} \|\mathbf{A}^m\|^{1/m},$$

where the *matrix norm* may be defined by

$$(68) \quad \|\mathbf{A}\| = \sup \{ \|\mathbf{Ax}\| : \|\mathbf{x}\| = 1 \},$$

where  $\|\mathbf{x}\|$  is the vector norm. In fact, for a matrix  $\mathbf{A}$  there is at least one eigenvalue  $\mu$  such that  $|\mu| = \rho(\mathbf{A})$ ; and it can be shown that, if  $\mu$  is unique (i.e., for every eigenvalue  $\lambda \neq \mu$ ,  $|\lambda| < |\mu|$ ) and if  $\mathbf{y}$  is an arbitrary vector whose projection on the *Jordan subspace* of  $\mathbf{A}$  belonging to the eigenvalue  $\mu$  (this is the subspace of *Jordan vectors* of  $\mathbf{A}$  belonging to  $\mu$ , i.e., vectors annihilated by some power of  $\mathbf{A} - \mu \mathbf{I}$ ) is

not null; then there is an eigenvector  $\mathbf{z}$  belonging to  $\mu$  and an integer  $r \geq 0$ , such that

$$(69) \quad \mathbf{A}^m \mathbf{y} \sim m^r \mu^m \mathbf{z},$$

in the sense that

$$(70) \quad \frac{\|\mathbf{A}^m \mathbf{y} - m^r \mu^m \mathbf{z}\|}{m^r |\mu|^m \|\mathbf{z}\|} \rightarrow 0 \quad \text{as } m \rightarrow \infty.$$

We note also that, as a result of Gershgorin's theorem (see e.g., [57], [58], [63], [64]),

$$(71) \quad \rho(\mathbf{A}) \leq \max_{r \in S} \sum_{s \in S} |A_{rs}| = G(\mathbf{A});$$

and, further, that, if

$$(72) \quad \mathbf{A}\mathbf{x} = \lambda\mathbf{x}, \quad \text{then } f(\mathbf{A})\mathbf{x} = f(\lambda)\mathbf{x},$$

whenever the function  $f(\mathbf{A})$  either is rational (i.e., can be written as  $P_1^{-1}(\mathbf{A})P_2(\mathbf{A})$ , where  $P_1$  and  $P_2$  are polynomials and  $P_1(\mathbf{A})$  is invertible), or is definable as a convergent Neumann series in  $\mathbf{A}$ . This shows how we can obtain other than the greatest eigenvalue of  $\mathbf{A}$  by a process of iteration such as (69): for instance, if  $\mathbf{A}$  has real eigenvalues bounded away from a real  $\alpha$ , then  $(\mathbf{A} - \alpha\mathbf{I})^2$  has positive eigenvalues and the largest eigenvalue of  $\{[G(\mathbf{A}) + |\alpha|]^2\mathbf{I} - (\mathbf{A} - \alpha\mathbf{I})^2\}$  is  $(G^2 + 2G|\alpha| + 2\alpha\lambda_\alpha - \lambda_\alpha^2)$ , where  $\lambda_\alpha$  is the eigenvalue of  $\mathbf{A}$  closest to  $\alpha$  (the case  $\alpha = 0$  is particularly simple); and again, if we seek that eigenvalue  $\omega$  of  $\mathbf{A}$ , whose real part is algebraically greatest, we find that we must iterate  $\exp \mathbf{A} = \sum_{m=0}^{\infty} (1/m!) \mathbf{A}^m$ , whose greatest eigenvalue has the magnitude  $\exp(\operatorname{Re} \omega)$ .

All the problems described above have solutions depending on the evaluation of *large matrix products*, each of whose elements consists of large sums (or, more generally, infinite sums or integrals), of just the type that can be estimated by the Monte Carlo method. According to the magnitude of the problem, Monte Carlo processes may be introduced in several ways, leading to a classification by "levels" of complexity (see [4], [61]).

First, we consider situations in which the final equation to be solved takes the form (55) or (65), with a moderate-sized  $N$ ; but in which the matrix  $\mathbf{A}$  (and often also the vector  $\mathbf{b}$ ) is the result of a number of arithmetic operations excessively large for direct calculation. The example of the least-squares solution of (61), where  $Q$  is very large, by (64) and (55), is typical. The procedure is then to compute a single Monte Carlo estimate of each component of  $\mathbf{A}$  (and  $\mathbf{b}$ , if necessary), and then to apply classical numerical techniques of direct elimination or iteration to the resulting approximate equation, to obtain an estimate of the solution. We shall refer to this as a *zeroth-level method*. Note that the resulting estimates of the solution will generally be *biased*; but they will converge in probability (and usually with probability one), as the estimates of the  $A_{rs}$  and  $b_r$  converge.

The basic estimators involved are rather simple. For example, (64) leads to estimators of the form

$$(73) \quad g_{rsu} = \begin{cases} \omega_u L_{ur} L_{us} / p_{rsu} & \text{if } p_{rsu} \neq 0, \\ 1 & \text{if } p_{rsu} = 0 \text{ (and then } L_{ur} L_{us} = 0\text{);} \end{cases}$$

$$g_{ru} = \begin{cases} \omega_u L_{ur} f_u / p_{ru} & \text{if } p_{ru} \neq 0, \\ 1 & \text{if } p_{ru} = 0 \text{ (and then } L_{ur} f_u = 0\text{).} \end{cases}$$

If  $u$  is sampled from  $T$  with probability  $p_{rsu}$  (or  $p_{ru}$ ), then  $g_{rsu}$  (or  $g_{ru}$ ) is an unbiased estimator of  $A_{rs}$  (or  $b_r$ , respectively). In practice, good primary estimators  $p_{rs}$  and  $p_r$  would be derived from these basic  $g_{rsu}$  and  $g_{ru}$ , with due regard to the variance-reducing techniques discussed in § 2.2, and more accurate secondary estimators  $\phi_{rs}(u_1, u_2, \dots, u_{k_{rs}})$  and  $\phi_r(u_1, u_2, \dots, u_{k_r})$  would be obtained, usually (hitherto always) by forming the arithmetic means of repeated independent samples of the corresponding primary estimators.

If we plan to solve the final equation, say (55), (57) or (65), by an iterative scheme, it can be more convenient to use *independent* estimates of the elements of the equation each time that they are needed. This leads to *unbiased* estimates of the solution (which are generally easier to handle) and eliminates storage difficulties. The estimators are similar to those in the zeroth-level method; but they are applied repeatedly. We shall classify this type of procedure as a *first-level method*. (In [61], where these ideas were introduced, both zeroth and first-level schemes were termed ‘‘first-level.’’)

Given a problem of the form (57), whose solution can be written as the Neumann series (58); when the order  $N$  is large, the components of the series are large sums, and, following a suggestion of J. von Neumann and S. M. Ulam, one can construct a Monte Carlo method for estimating these sums, in terms of *random walks* on the index set  $S$  (see below). It is clear that, if the matrix elements occurring in the Neumann series are themselves large sums of given numbers, one should be able to estimate them by zeroth or first-level methods, within the von Neumann–Ulam scheme. This can indeed be done [61], and such a scheme will be termed a *second-level method*.

Finally, certain procedures have been devised (see [61], [78]) for sequentially improving the von Neumann–Ulam scheme, and these also involve the computation of large sums, arising from additional matrix products. Here again, it is clear that a new level of Monte Carlo computation can be invoked to yield efficient schemes, which will be referred to as *third-level methods*.

For information on the classical direct and iterative methods, which inspire and are combined with the Monte Carlo schemes described here, the reader is referred, for example, to [62]–[66].

The fundamental method of von Neumann and Ulam was first published by Forsythe and Leibler [67]. They consider the problem of *inverting a matrix*: thus a matrix Neumann series of the form

$$(74) \quad (\mathbf{I} - \mathbf{H})^{-1} = \sum_{m=0}^{\infty} \mathbf{H}^m$$

is to be evaluated, rather than the vector Neumann series (58) above. The treatments of the series (58) and (74) are completely analogous, however.

(We observe, incidentally, that, given (55), it can always be put into the form (57); most simply by

$$(75) \quad \mathbf{H} = \mathbf{I} - \mathbf{A}, \quad \mathbf{a} = \mathbf{b},$$

and more generally by

$$(76) \quad \mathbf{H} = \mathbf{I} - \mathbf{M}\mathbf{A}, \quad \mathbf{a} = \mathbf{M}\mathbf{b},$$

where  $\mathbf{M}$  is an arbitrary matrix. In particular, we may assume  $\mathbf{A}$  to be symmetric and positive definite (as in the case of (64); in general, if not, we can always pre-multiply (55) by  $\mathbf{A}^T$ ). With this assumption, all the eigenvalues of  $\mathbf{A}$  will be real and positive, and we may take, for instance,

$$(77) \quad \mathbf{M} = c\mathbf{I},$$

with any  $0 < c < 2/G(\mathbf{A})$ , to ensure that  $\rho(\mathbf{H}) < 1$ , since, by (71),  $c < 2/\rho(\mathbf{A})$ .)

A random walk is defined on the “augmented index set”  $\bar{S} = \{0, 1, 2, \dots, N\}$  (see [78]), the extra index value 0 corresponding to a “stop.” Here  $p_{rs}$  denotes the probability of transition from index  $r$  to index  $s$  ( $p_{r0}$  being denoted by  $p_r = 1 - \sum_{s=1}^N p_{rs} > 0$ , with  $p_{0s} = \delta_{0s}$ ), with  $p_{rs} \neq 0$  unless  $H_{rs} = 0$ , and each walk  $\Gamma = [r, s_1, s_2, \dots, s_m, 0]$  with  $r, s_1, \dots, s_m \neq 0$  corresponds to precisely one term in the series (74). Exactly as in (11), one uses the estimator

$$(78) \quad Z_{rs}(\Gamma) = \frac{H_{rs} H_{s_1 s_2} \cdots H_{s_{m-1} s_m} \delta_{s_m 0}}{p_{rs} p_{s_1 s_2} \cdots p_{s_{m-1} s_m} p_{s_m}}$$

(where the denominator is seen to be the probability of occurrence  $p(\Gamma)$  of the given  $m$ -step random walk  $\Gamma$  beginning at index  $r$ ) for the component  $[(\mathbf{I} - \mathbf{H})^{-1}]_{rs}$ . This estimator can be shown to be *unbiased* if  $\rho(\mathbf{H}^+) < 1$ , where

$$(79) \quad (\mathbf{H}^+)_rs = H_{rs}^+ = |H_{rs}|.$$

In the analogous method for solving (57) by (58), the estimator for  $x_r$  would be of the form (again unbiased if  $\rho(\mathbf{H}^+) < 1$ )

$$(80) \quad X_r(\Gamma) = \frac{H_{rs} H_{s_1 s_2} \cdots H_{s_{m-1} s_m} a_{s_m}}{p_{rs} p_{s_1 s_2} \cdots p_{s_{m-1} s_m} p_{s_m}},$$

and if (57) arises from prior formulas, such as (61), (64) and (75)–(77), then the  $H_{rs}$  and  $a_s$  in (80) should be replaced by estimators  $\phi_{rs}$  and  $\phi_s$  sampled in the zeroth or (more usually) first-level manners described above. In order that the variances of the estimators (78) and (80) be finite it is necessary that  $\rho(\mathbf{K}) < 1$ , where

$$(81) \quad (\mathbf{K})_{rs} = K_{rs} = H_{rs}^2/p_{rs}$$

(this is discussed in [61]).

Some alternatives arise here. First, one may dispense with the “stop index” 0, and work in  $S$ , by fixing an arbitrary stopping rule, depending on estimates of the rapidity of convergence of the Neumann series. (This leads to a bias, but it need never be a large one.) Secondly, instead of treating each element of the Neumann series as an infinite sum, one may treat each element as an infinite series of large sums; that is, one may evaluate each term by a Monte Carlo method, and then

sum them. A convenient version of this approach was devised by Wasow [68], on the basis of ideas first discussed by Courant, Friedrichs and Lewy [21], for the solution of elliptic differential and difference equations; and similar ideas were studied independently by Curtiss [18]. In [69], Wasow describes the form of his method applicable to matrix inversion and compares its efficiency to the method of Forsythe and Leibler.

In Wasow's method, one begins with an *infinite* random walk  $\Gamma = [r, s_1, s_2, s_3, \dots]$  beginning at index  $r$  and generated just as in the Forsythe–Leibler method. (As far as the scoring procedure is concerned, the walk is effectively made to terminate, either by fiat or by first passage through the index 0, by taking all  $H_{0s} = 0$ : with all  $H_{r0} = a_r = x_r = 0$ , (57) remains true over the augmented set.) The “score” after  $t$  steps, which corresponds to the partial sum

$$(82) \quad Z_t = \sum_{m=0}^t \mathbf{H}^m \quad \text{of } X_t = \sum_{m=0}^t \mathbf{H}^m \mathbf{a} = Z_t \mathbf{a},$$

is taken to be

$$(83) \quad Z_{rst}(\Gamma) = \sum_{m=0}^t \frac{H_{rs_1} H_{s_1 s_2} \cdots H_{s_{m-1} s_m}}{p_{rs_1} p_{s_1 s_2} \cdots p_{s_{m-1} s_m}} \delta_{s_m s},$$

or

$$(84) \quad X_{rt}(\Gamma) = \sum_{m=0}^t \frac{H_{rs_1} H_{s_1 s_2} \cdots H_{s_{m-1} s_m}}{p_{rs_1} p_{s_1 s_2} \cdots p_{s_{m-1} s_m}} a_{s_m},$$

respectively; and satisfies simple recurrence relations, which greatly facilitate the computation.

Note that the same random walk, but now started at a random index  $s_0$ , sampled with probability  $q_{s_0}$ , say, can be viewed in the reverse direction, to yield scores such as

$$(85) \quad Z_{sr}(\Gamma) = \frac{\delta_{ss_m} H_{s_m s_{m-1}} \cdots H_{s_2 s_1} H_{s_1 s_0} \delta_{s_0 r}}{p_{s_m} p_{s_{m-1} s_m} \cdots p_{s_1 s_2} p_{s_0 s_1} q_{s_0}},$$

$$(86) \quad X_s(\Gamma) = \frac{\delta_{ss_m} H_{s_m s_{m-1}} \cdots H_{s_2 s_1} H_{s_1 s_0} a_{s_0}}{p_{s_m} p_{s_{m-1} s_m} \cdots p_{s_1 s_2} p_{s_0 s_1} q_{s_0}},$$

$$(87) \quad Z_{srt}(\Gamma) = \sum_{m=0}^t \frac{\delta_{ss_m} H_{s_m s_{m-1}} \cdots H_{s_2 s_1} H_{s_1 s_0} \delta_{s_0 r}}{p_{s_{m-1} s_m} \cdots p_{s_1 s_2} p_{s_0 s_1} q_{s_0}},$$

$$(88) \quad X_{st}(\Gamma) = \sum_{m=0}^t \frac{\delta_{ss_m} H_{s_m s_{m-1}} \cdots H_{s_2 s_1} H_{s_1 s_0} a_{s_0}}{p_{s_{m-1} s_m} \cdots p_{s_1 s_2} p_{s_0 s_1} q_{s_0}},$$

corresponding to the earlier scores for the *transposed* matrix equation: this approach is the *dual* or *adjoint sampling* of nuclear engineers.

Further treatments of these methods for various problems can be found in references [70]–[74], [81]–[85]. More general classes of estimators are also defined by these authors, especially by Page [73] and Muller [84], [85].

While the full question, of necessary and sufficient conditions for  $\rho(\mathbf{H}) < 1$  to imply the existence of probabilities  $p_{rs}$  for which  $\rho(\mathbf{K}) < 1$ , is still unsolved;

I am indebted to a conversation with B. N. Parlett, M. J. D. Powell and P. Rabinowitz for the following partial results. First, suppose that

$$\mathbf{H} = \begin{pmatrix} \sigma & -\sigma & 0 & \cdots & 0 \\ \sigma & -\sigma & 0 & \cdots & 0 \\ 0 & 0 & \lambda_3 & \cdots & 0 \\ \vdots & & & \ddots & \\ 0 & 0 & 0 & \cdots & \lambda_N \end{pmatrix},$$

with  $|\sigma| > 1$ ,  $|\lambda_3| < 1, \dots, |\lambda_N| < 1$ ; so that

$$\mathbf{K} = \begin{pmatrix} \sigma^2/p_{11} & \sigma^2/p_{12} & 0 & \cdots & 0 \\ \sigma^2/p_{21} & \sigma^2/p_{22} & 0 & \cdots & 0 \\ 0 & 0 & \lambda_3^2/p_{33} & \cdots & 0 \\ \vdots & & & \ddots & \\ 0 & 0 & 0 & \cdots & \lambda_N^2/p_{NN} \end{pmatrix}.$$

Then it is readily verified that  $\det(\mathbf{H} - \lambda\mathbf{I}) = \lambda^2(\lambda_3 - \lambda) \cdots (\lambda_N - \lambda)$ ; so that  $\rho(\mathbf{H}) < 1$ ; while  $\det(\mathbf{K} - \lambda\mathbf{I}) = [(p_{11}^{-1}p_{22}^{-1} - p_{12}^{-1}p_{21}^{-1})\sigma^4 - (p_{11}^{-1} + p_{22}^{-1})\sigma^2\lambda + \lambda^2] \cdot (p_{33}^{-1}\lambda_3^2 - \lambda) \cdots (p_{NN}^{-1}\lambda_N^2 - \lambda)$ ; so that  $\mathbf{K}$  has at least one eigenvalue which is greater than  $\sigma^2$  in magnitude; whence  $\rho(\mathbf{K}) > 1$  for all choices of the  $p_{rs}$ . Thus it is not true that, for all  $\mathbf{H}$  such that  $\rho(\mathbf{H}) < 1$ , we can find  $p_{rs}$  such that  $\rho(\mathbf{K}) < 1$ . Secondly, suppose that  $\mathbf{H}$  is an upper (or, alternatively, lower) triangular matrix, whose diagonal elements  $\lambda_1, \lambda_2, \dots, \lambda_N$  (which are its eigenvalues also) are all less than 1 in magnitude. Then  $\mathbf{K}$  will also be upper (or, respectively, lower) triangular, and its diagonal elements (and eigenvalues) will be  $\lambda_1^2/p_{11}, \lambda_2^2/p_{22}, \dots, \lambda_N^2/p_{NN}$ . Clearly,  $\rho(\mathbf{H}) < 1$ ; and if we choose (as we can, since  $|\lambda_r| < 1$ )  $p_{rr} = |\lambda_r|$ , then  $|\lambda_r^2/p_{rr}| = |\lambda_r| < 1$ ; so that  $\rho(\mathbf{K}) < 1$ . Thus it is true that, for some classes of matrices  $\mathbf{H}$  with  $\rho(\mathbf{H}) < 1$  (including the triangular matrices described above), we can always find  $p_{rs}$  (with all  $p_{rs} > 0$  and all  $\sum_{s=1}^N p_{rs} = 1$ ) such that  $\rho(\mathbf{K}) < 1$ .

Taking another point of view, based on the observation that  $\rho(\mathbf{A}) \leq G(\mathbf{A})$  (see (71)), we note that the conditions

$$(89) \quad \rho(\mathbf{H}) < 1, \quad \rho(\mathbf{H}^+) < 1, \quad \rho(\mathbf{K}) < 1$$

will all be satisfied if  $G(\mathbf{H}) < 1$  and  $G(\mathbf{K}) < 1$  (see (79) and (81)). Further, we note that the choice of probabilities

$$(90) \quad p_{rs} = |H_{rs}| / \sum_{t \in S} |H_{rt}|$$

(which is always permissible and practically possible) yields

$$(91) \quad G(\mathbf{K}) = [G(\mathbf{H})]^2;$$

whence, whenever  $G(\mathbf{H}) < \alpha \leq 1$ , then  $G(\mathbf{K}) < \alpha^2 \leq \alpha \leq 1$ . Therefore the conditions (89) can all be satisfied by choosing the  $p_{rs}$  as in (90), provided that  $G(\mathbf{H}) < 1$ . (This matter was first taken up in [61], and was discussed in the report [248],

of which the present paper is a revised version. The treatment given below is an improvement on that of [248], thanks to criticisms made by J. D. Pincus, to whom I am grateful for a lengthy discussion of the matter.)

As before, we take  $\mathbf{H} = \mathbf{I} - c\mathbf{A}$ , where  $c > 0$  and  $\mathbf{A}$  is symmetric and positive-definite (so that all the diagonal elements  $A_{rr} > 0$ ). Thus  $H_{rs} = -cA_{rs}$  when  $r \neq s$ , and  $H_{rr} = 1 - cA_{rr}$ . Let us adopt the notations

$$(92) \quad \begin{aligned} T_r &= \sum_{s \neq r} |A_{rs}|, \\ S_r &= T_r + A_{rr} = \sum_{s \in S} |A_{rs}|, \\ G &= G(\mathbf{A}) = \max_{r \in S} S_r, \\ J &= G(\mathbf{H}) = \max_{r \in S} (cT_r + |1 - cA_{rr}|); \end{aligned}$$

and define the assertions

$$(93) \quad \begin{aligned} \mathfrak{A}_r(\theta, c) &: cT_r + |1 - cA_{rr}| < \theta, \\ \mathfrak{B}_r(\theta) &: T_r < \theta A_{rr}, \\ \mathfrak{C}_r(\theta, c) &: c < (1 + \theta)/S_r, \\ \mathfrak{D}(\theta) &: \max_{r \in S} A_{rr}^{-1} < (1 + \theta)/G, \\ \mathfrak{E}(\theta, c) &: \max_{r \in S} A_{rr}^{-1} \leq c < (1 + \theta)/G, \end{aligned}$$

for  $c > 0$  and  $0 < \theta \leq 1$ .

LEMMA 1. If  $0 < \alpha \leq 1$  and  $\mathfrak{D}(\alpha)$  holds; then, by choosing any  $c$  satisfying  $\mathfrak{E}(\alpha, c)$ , we ensure that  $J < \alpha$ .

*Proof.* We note that

$$(94) \quad J < \alpha \text{ if and only if } \forall r \in S, \quad \mathfrak{A}_r(\alpha, c).$$

Also,  $\mathfrak{D}(\alpha)$  is a necessary and sufficient condition for it to be possible to choose a  $c > 0$  such that  $\mathfrak{E}(\alpha, c)$  holds. Now,  $\mathfrak{E}(\alpha, c)$  implies both that  $\forall r \in S, cA_{rr} \geq 1$  and that  $\forall r \in S, \mathfrak{C}_r(\alpha, c)$ . The former assertion implies the equivalence of the latter and  $\forall r \in S, \mathfrak{A}_r(\alpha, c)$ . Thus, by (94), if  $\mathfrak{E}(\alpha, c)$  then  $J < \alpha$ .

LEMMA 2. Let  $0 < \alpha \leq 1$  and suppose that  $\mathfrak{D}(\alpha)$  does not hold. Let

$$(95a) \quad D_\alpha = \{r \in S : A_{rr}^{-1} < (1 + \alpha)/G\}$$

and let  $E_\alpha$  be the (nonempty) complement of  $D_\alpha$  in  $S$ . Suppose that

$$(95b) \quad \max_{r \in S} A_{rr}^{-1} < \left( \frac{1 + \alpha}{1 - \alpha} \right) / G,$$

and that there is a  $\beta$  such that  $\mathfrak{B}_r(\beta)$  holds for all  $r \in E_\alpha$  and

$$(95c) \quad 0 < \beta < 1 - \left( \frac{1 - \alpha}{1 + \alpha} \right) G \max_{r \in S} A_{rr}^{-1}.$$

Then, by choosing any  $c$  satisfying

$$(95d) \quad \left\{ \begin{array}{l} \left( \frac{1-\alpha}{1-\beta} \right) \max_{r \in S} A_{rr}^{-1} \\ \max_{r \in D_\alpha} A_{rr}^{-1} \end{array} \right\} < c < \frac{1+\alpha}{G},$$

we ensure that  $J < \alpha$ .

*Proof.* If  $D_\alpha = S$ ,  $\mathfrak{D}(\alpha)$  holds, by (93) and (95a); thus, since  $\mathfrak{D}(\alpha)$  does not hold,  $E_\alpha$  is indeed nonempty. Also, by (95b),

$$\left( \frac{1-\alpha}{1+\alpha} \right) G \max_{r \in S} A_{rr}^{-1} < 1,$$

so that a  $\beta$  satisfying (95c) can exist; and it follows from (95c) that, since  $0 < \alpha \leq 1$ ,  $G > 0$ , and all  $A_{rr} > 0$ , we must have  $0 < \beta < 1$ ; and further, that

$$0 \leq \left( \frac{1-\alpha}{1-\beta} \right) \max_{r \in S} A_{rr}^{-1} < \frac{1+\alpha}{G};$$

so that, by (95a), a choice of  $c$  satisfying (95d) can be made. Again, since  $0 < c < (1+\alpha)/G$ , by (95d), it follows from (95a) that  $0 < cA_{rr} < 1$  for all  $r \in E_\alpha$ .

Now, for all  $r \in E_\alpha$ , since  $cA_{rr} < 1$ ,

$$cT_r + |1 - cA_{rr}| = 1 - c(A_{rr} - T_r),$$

and since we suppose that  $\mathfrak{B}_r(\beta)$  holds for all  $r \in E_\alpha$  and  $c > 0$ ,

$$1 - c(A_{rr} - T_r) < 1 - (1 - \beta)cA_{rr},$$

and since  $\beta < 1$ , (95d) yields that

$$1 - (1 - \beta)cA_{rr} < 1 - (1 - \alpha)A_{rr} \max_{r \in S} A_{rr}^{-1},$$

and since  $\max_{r \in S} A_{rr}^{-1} \geq A_{rr}^{-1}$  and  $\alpha \leq 1$ ,

$$1 - (1 - \alpha)A_{rr} \max_{r \in S} A_{rr}^{-1} \leq 1 - (1 - \alpha) = \alpha.$$

Combining all these inequalities, we obtain  $\mathfrak{A}_r(\alpha, c)$  for all  $r \in E_\alpha$ .

Finally, for all  $r \in D_\alpha$ , by (95a) and (95d),  $cA_{rr} \geq 1$  and  $\mathfrak{C}_r(\alpha, c)$  holds; so that, as in the proof of Lemma 1,  $\mathfrak{A}_r(\alpha, c)$  also holds. Thus we have proved  $\mathfrak{A}_r(\alpha, c)$  for all  $r \in E_\alpha$  and for all  $r \in D_\alpha$ ; whence, by (94),  $J < \alpha$ .

**COROLLARY.** Let  $\alpha = 1$ . If  $\mathfrak{B}_r(1)$  holds for all  $r \in E_1$ ; then, by choosing any  $c$  satisfying

$$(95e) \quad \max_{r \in D_1} A_{rr}^{-1} < c < 2/G,$$

we ensure that  $J < 1$ .

*Proof.* We first note that, since  $\mathfrak{B}_r(\theta)$  is an open (strict) inequality, we can always find  $0 < \theta' < \theta$  such that  $\mathfrak{B}_r(\theta')$  holds also. Let  $\alpha = 1$ . We observe that (95b) always holds, since the right-hand (upper) side of the inequality becomes infinite; and (95c) reduces to  $0 < \beta < 1$ . If  $\mathfrak{B}_r(1)$  holds, we can find  $\beta \in (0, 1)$  such that  $\mathfrak{B}_r(\beta)$  holds also. Finally, we see that (95d) reduces simply to (95e). Thus the

conditions of this corollary imply those of Lemma 2 when  $\alpha = 1$ , and these imply  $J < 1$ .

*Remark.* When  $r \in D_\alpha$ ,  $A_{rr}^{-1} < (1 + \alpha)/S_r$ , whence  $\mathfrak{B}_r(\alpha)$  holds. Note, too, that since  $E_\alpha$  is nonempty,

$$(95f) \quad \max_{r \in S} A_{rr}^{-1} \geq (1 + \alpha)/G.$$

Thus (95c) yields  $0 < \beta < 1 - (1 - \alpha) = \alpha$ ; whence, *under the conditions of Lemma 2*,  $\mathfrak{B}_r(\alpha)$  holds, not only in  $E_\alpha$  but also in  $D_\alpha$ ; that is, throughout  $S$ .

The next lemma uses the fact, easily deduced from the well-known theorems about positive-definite quadratic forms and their reduction by Jacobi's method to diagonal form (see, e.g., [250], [251]), that there exists a lower-triangular matrix  $\mathbf{T}$ , with positive diagonal elements, such that

$$(96a) \quad \mathbf{T}^\top \mathbf{A} \mathbf{T} = \mathbf{I}.$$

Clearly,  $\mathbf{T}$  is nonsingular; and if  $\mathbf{Ax} = \mathbf{b}$ , then  $\mathbf{T}^{-1}\mathbf{x} = \mathbf{T}^\top \mathbf{b}$ ; so that

$$(96b) \quad \mathbf{x} = \mathbf{A}^{-1}\mathbf{b} = \mathbf{T}\mathbf{T}^\top \mathbf{b}.$$

(In particular, if

$$(96c) \quad \mathbf{A} = \mathbf{F}^\top \mathbf{F},$$

as in the least-squares problem (64) treated in [61] [in (64),  $\mathbf{A} = \mathbf{L}^\top \mathbf{\Omega} \mathbf{L}$ , where  $(\mathbf{\Omega})_{uv} = \omega_u \delta_{uv}$  and  $\omega_u > 0$ : so let  $(\mathbf{V})_{uv} = \omega_u^{1/2} \delta_{uv}$ ; then  $\mathbf{\Omega} = \mathbf{V}^\top \mathbf{V}$ , and if  $\mathbf{F} = \mathbf{VL}$ , we get (96c)], then (96a) means that  $\mathbf{T}$  is a transformation which orthonormalizes the columns of the matrix  $\mathbf{F}$ : for instance,  $\mathbf{T}$  can be the matrix of the Gram-Schmidt process.)

LEMMA 3. *If  $0 < \alpha \leq 1$  and if  $\mathbf{T}$  is the nonsingular matrix of a congruence-transformation reducing the symmetric positive-definite matrix  $\mathbf{A}$  to the unit matrix, and if, for any  $\varepsilon > 0$ , we can find a nonsingular matrix  $\mathbf{S}$  approximating  $\mathbf{T}$ , in the sense that every  $|S_{rs} - T_{rs}| < \varepsilon$ ; then we can always choose  $\varepsilon > 0$  and then  $c > 0$ , in such a way that, if*

$$(96d) \quad \mathbf{A}^0 = \mathbf{S}^\top \mathbf{A} \mathbf{S}, \quad \mathbf{H}^0 = \mathbf{I} - c\mathbf{A}^0, \quad G^0 = G(\mathbf{A}^0), \quad J^0 = G(\mathbf{H}^0),$$

*we ensure that  $J^0 < \alpha$ .*

*Proof.* By (96d),

$$\begin{aligned} A_{rs}^0 &= (\mathbf{A}^0)_{rs} = \sum_{i=1}^N \sum_{j=1}^N A_{ij} S_{ir} S_{js} \\ &= \sum_{i,j} A_{ij} T_{ir} T_{js} + \sum_{i,j} A_{ij} T_{ir} (S_{js} - T_{js}) + \sum_{i,j} A_{ij} (S_{ir} - T_{ir}) S_{js}; \end{aligned}$$

whence, by (96a), if all  $|A_{rs}| < C_1$ , all  $|T_{rs}| < C_2$ , all  $|S_{rs}| < C_3$ , and all  $|S_{rs} - T_{rs}| < \varepsilon$ , then

$$(96e) \quad |A_{rs}^0 - \delta_{rs}| < N^2 C_1 (C_2 + C_3) \varepsilon;$$

that is, if  $r \neq s$ ,

$$|A_{rs}^0| < N^2 C_1 (C_2 + C_3) \varepsilon$$

and

$$1 - N^2 C_1(C_2 + C_3)\varepsilon < A_{rr}^0 < 1 + N^2 C_1(C_2 + C_3)\varepsilon.$$

In particular, if we choose any

$$(96f) \quad \varepsilon < \alpha/N^2 C_1(C_2 + C_3)(N + \alpha + 1),$$

then (96e) yields, after some simple algebra, that

$$(96g) \quad \max_{r \in S} (A_{rr}^0)^{-1} < \frac{N + \alpha + 1}{N + 1} < \frac{1 + \alpha}{G^0}.$$

Clearly, (96g) implies the assertion  $\mathfrak{D}^0(\alpha)$  (that is,  $\mathfrak{D}(\alpha)$  with  $\mathbf{A}$  replaced by  $\mathbf{A}^0$ ), which, by Lemma 1, implies that we can choose a  $c > 0$  such that  $J^0 < \alpha$ .

**COROLLARY.** *A slightly weaker condition than (96f), namely*

$$(96h) \quad \varepsilon < \alpha/N^3 C_1(C_2 + C_3),$$

suffices to ensure that, for a suitable choice of  $c > 0$ , we have  $J^0 < \alpha$ .

*Proof.* In proving Lemma 3, we showed that the conditions of Lemma 1 were satisfied if the accuracy of the approximation  $\mathbf{S}$  to  $\mathbf{T}$  was given by (96f). We now weaken the bound on  $\varepsilon$  to the form in (96h) and appeal to Lemma 2 instead. If (96h) holds, and if we define

$$(96i) \quad \beta_0 = 1 - \left( \frac{1 - \alpha}{1 + \alpha} \right) G^0 \max_{r \in S} (A_{rr}^0)^{-1},$$

then (96e) yields that

$$(96j) \quad \beta_0 > 1 - \left( \frac{1 - \alpha}{1 + \alpha} \right) (1 + \alpha) \left( \frac{N}{N - \alpha} \right) = \frac{\alpha(N - 1)}{N - \alpha},$$

whence

$$(96k) \quad T_r^0 = \sum_{s \neq r} |A_{rs}^0| < \frac{\alpha(N - 1)}{N} < \beta_0 A_{rr}^0.$$

This last inequality shows that  $\mathfrak{B}_r^0(\beta_0)$  (that is,  $\mathfrak{B}_r(\beta_0)$  with  $\mathbf{A}$  replaced by  $\mathbf{A}^0$ ) holds for all  $r \in S$ . Also, (96j) shows that  $\beta_0 > 0$ . It follows that we can find a  $\beta \in (0, \beta_0)$  such that  $\mathfrak{B}_r^0(\beta)$  is true (and, of course,  $\beta$  satisfies the equivalent of (95c)). Therefore, by Lemma 2, we can find a  $c > 0$  such that  $J^0 < \alpha$ .

These three lemmas give us different ways in which we can be sure that  $J < \alpha$ , and so ensure that the inequalities (89), which allow us to use the Monte Carlo techniques described earlier, are true. While Lemmas 1 and 2 are “passive”, Lemma 3 gives us an “active” result: given any linear problem (55), it indicates how we can transform the problem into another,

$$(97a) \quad \mathbf{A}^0 \mathbf{x}^0 = \mathbf{b}^0 = \mathbf{S}^T \mathbf{b},$$

by the transformation (96d), so that the solution of the original problem is

$$(97b) \quad \mathbf{x} = \mathbf{S} \mathbf{x}^0,$$

and  $J^0 < \alpha$ ; so that we can apply the Monte Carlo techniques.

The calculation of the “exact” transformation  $\mathbf{T}$  is equivalent to a laborious computation of the inverse of  $\mathbf{A}$ , and is therefore not usually practicable. However, it may be possible to estimate the elements of  $\mathbf{T}$  by a relatively quick computation, with sufficient accuracy to yield a transformation  $\mathbf{S}$ , satisfying (96f) or (96h), and so ensuring that  $J^0 < \alpha$ . In particular, as was first suggested in [61], one may be able to perform an approximate orthonormalization of the columns of the matrix  $\mathbf{F}$  (or  $\mathbf{L}$ ), by the so-called *Monte Carlo Gram-Schmidt process*, in which the numerous scalar products are replaced by corresponding Monte Carlo estimates in the usual way, as described in (4)–(11) above. In this connection, it is interesting to note that the relation  $\mathfrak{B}_r(\beta)$ , which is the basic condition of Lemma 2, may be written (by (96c))

$$(97c) \quad \sum_{s \neq r} |(\mathbf{F}_r, \mathbf{F}_s)| < \beta(\mathbf{F}_r, \mathbf{F}_r),$$

where  $\mathbf{F}_r$  denotes the  $r$ th column of the matrix  $\mathbf{F}$  and  $(\mathbf{X}, \mathbf{Y})$  denotes the scalar product  $\sum_{u=1}^Q X_u Y_u$ ; so that (97c) may be looked upon as a *weak orthogonality* relation.

The final, third-level Monte Carlo method involves the concept of *sequential Monte Carlo*, briefly mentioned in § 1. This is defined in general terms in [5], [6], [78] ([78] is the final revised form of the paper, which will appear in [4]). Three workable sequential schemes are defined there, for the solution of linear problems (55). The concept of “sequential analysis,” introduced by Wald [76] and his co-workers, is mainly concerned with decision procedures for terminating sampling, rather than with modification of the estimator and sampling scheme. A two-stage scheme was briefly discussed by Marshall [75]. But the full development of the method is found only in papers by Halton [3], [5], [6], [61], [77], [78].

The “first sequential method” [78] makes use of the fact that, if one chooses the transition probabilities

$$(98) \quad p_{rs} = H_{rs}x_s / \sum_t H_{rt}x_t$$

(when this is allowable, e.g., when all  $H_{rs}$ ,  $a_r$  and  $x_r$  are of the same sign), then the estimators of the form (84) have zero variance; that is, one obtains the exact solution with probability one. This may be looked upon as a situation similar to that in which *importance sampling* was applied. What is done is to conduct the computation in stages: at each stage, the  $x_r$  in (98) are replaced by the best available estimates resulting from previous stages of the work. (All the  $p_{rs}$  are also multiplied by  $1 - \varpi^{(s)}$  where  $\varpi^{(s)}$  is the stopping probability adopted for stage  $s$ .) This yields a convergence in which the variance of the current best estimate at stage  $s$  is bounded asymptotically by a multiple of  $s^{-2(p+1)}$ , where  $p$  is a nonnegative parameter of the sampling scheme, so long as one uses stopping probabilities  $\varpi^{(s)}$  of the order of  $s^{-2(p+1)}$  or less. The “second sequential method” [78] uses the same approach; but now the  $p_{rs}$  in (98) (with the  $x_r$  replaced by their best estimates—without the factor  $1 - \varpi^{(s)}$ ) are used in the scoring procedure (84), while another, arbitrary probability distribution determines the random walk  $\Gamma$ . This introduces a *bias*; but it can be shown that the bias at stage  $s$  is bounded asymptotically by a multiple of  $s^{-D(p+1)}$  and the corresponding variance is bounded asymptotically by a multiple

of  $s^{-2(p+1)}$  or  $s^{-2D(p+1)-1}$  (whichever is the larger); where  $p$  is the same parameter as before, and  $D$  is another parameter:

$$(99) \quad D = 1 - \frac{\max_{i \in S} \left\{ \sum_{j=1}^N |x_i^{-1} H_{ij} x_j - (1 - a_i/x_i) \bar{p}_{ij}| \right\}}{1 - \max_{i \in S} |1 - a_i/x_i|},$$

with  $\bar{p}_{ij}$  denoting the actual transition probability in the random walks  $\Gamma$ . There is thus convergence if

$$(100) \quad |1 - a_i/x_i| < 1 \quad \text{and} \quad D > 0.$$

The second method thus extends the idea of the first method to cases when expression (98) has variable sign.

The “third sequential method” [78] takes a different, rather simpler line, reminiscent of *correlated sampling*. It uses the fact that, if  $\mathbf{X}^{(s)}$  denotes the approximation to  $\mathbf{x}$  obtained at stage  $s$ , so that  $\mathbf{y}^{(s)} = \mathbf{x} - \mathbf{X}^{(s)}$  is the correction required; then (57) yields

$$(101) \quad \mathbf{y}^{(s)} = \mathbf{d}^{(s)} + \mathbf{H}\mathbf{y}^{(s)},$$

where  $\mathbf{d}^{(s)} = \mathbf{a} + \mathbf{H}\mathbf{X}^{(s)} - \mathbf{X}^{(s)}$ . The basic random-walk techniques applied to (101) now yield estimates  $\mathbf{Y}^{(s)}$  of  $\mathbf{y}^{(s)}$ , and we take  $\mathbf{X}^{(s+1)} = \mathbf{X}^{(s)} + \mathbf{Y}^{(s)}$ . It can be shown that this method yields unbiased estimates of  $\mathbf{x}$ , whose variances are bounded asymptotically by a multiple of  $G^{s-1}$ , where (see (71) and (81))

$$(102) \quad G = G(\mathbf{K})/[1 - G(\mathbf{K})].$$

There is thus a rapid (geometric) convergence whenever

$$(103) \quad G(\mathbf{K}) < \frac{1}{2}.$$

We note that, if we choose the probabilities (90), then (103) will hold if

$$(104) \quad G(\mathbf{H}) < 1/\sqrt{2} \approx 0.707,$$

and this will be achieved if, by Lemma 1 and (93) with  $\alpha = 1/\sqrt{2}$ ,

$$(105) \quad \max_{r \in S} A_{rr}^{-1} \leq c < 1.7/G(\mathbf{A});$$

and this condition can be satisfied (if necessary by appeal to weak orthogonalization). Alternatively, following Lemma 2, we may require that

$$(106a) \quad \max_{r \in S} A_{rr}^{-1} < 5.8/G(\mathbf{A})$$

and for every  $r \in S$

$$(106b) \quad (1 - 0.185G(\mathbf{A}) \max_{r \in S} A_{rr}^{-1}) A_{rr} > \sum_{s \neq r} |A_{rs}|,$$

with a choice of  $c$  dictated by (95d).

The ideas of sequential Monte Carlo developed in [5], [6], [78] have led to further work in three different directions: first, to a development of practical means of applying the method to linear problems [61], including the application of the “Monte Carlo Gram–Schmidt” technique to ensure the condition (103), and the use of coarse-grid approximations to speed up the process; secondly,

to a study of the stochastic convergence of general linear averages of sequences [3], [77]; and finally to a development of a general formulation of Monte Carlo procedures [3], [4].

We turn finally to eigenvalue problems. Here, the most natural method is to sample a random vector  $\mathbf{y}$ , in the hope that it will have a nonnull projection in the Jordan subspace belonging to the largest eigenvalue  $\mu$  of  $\mathbf{A}$  (see (65)–(72)) (as indeed will be the case with probability one, for almost all distributions of the vectors  $\mathbf{y}$ ). At the “first level,” we now operate on  $\mathbf{y}$  repeatedly with  $\mathbf{A}$  (or a Monte Carlo estimate of  $\mathbf{A}$ ) and appeal to (69) in the obvious way to find  $\mu$  and the eigenvector  $\mathbf{z}$ . At the “second level,” we replace the evaluation of the product  $\mathbf{A}^m \mathbf{y}$  by a Monte Carlo estimate, such as

$$(107) \quad Q_{rm}(\Gamma) = \frac{A_{rs_1} A_{s_1 s_2} \cdots A_{s_{m-1} s_m} y_{s_m}}{p_{rs_1} p_{s_1 s_2} \cdots p_{s_{m-1} s_m}}$$

(compare (80)), where  $\Gamma$  is a walk on the original index set  $S$  and  $m$  is preassigned. (See also the discussion in [17].)

We saw that, to obtain the asymptotic behavior (69), we required, first, that  $\mathbf{A}$  have a unique eigenvalue of largest magnitude; that is, if the distinct eigenvalues of  $\mathbf{A}$  are  $\lambda_1 = \mu, \lambda_2, \lambda_3, \dots, \lambda_k$  (possibly complex), then  $|\lambda_i| < |\mu|$  if  $i \neq 1$  (since  $\mathbf{A}$  is real, this means that  $\mu$  must be real); and second, that  $\mathbf{y}$  be a vector whose projection on the Jordan subspace of  $\mathbf{A}$  belonging to  $\mu$  is nonnull. Let  $\mathbf{x}$  be an arbitrary vector such that  $\mathbf{x}^\top \mathbf{z} \neq 0$ , where  $\mathbf{z}$  is the eigenvector of  $\mathbf{A}$  belonging to  $\mu$  which appears in (69). Consider the three expressions

$$(108) \quad \begin{aligned} R_m &= (\mathbf{A}^m \mathbf{y})^\top (\mathbf{A}^{m+1} \mathbf{y}) / (\mathbf{A}^m \mathbf{y})^\top (\mathbf{A}^m \mathbf{y}), \\ S_m^2 &= (\mathbf{A}^{m+1} \mathbf{y})^\top (\mathbf{A}^{m+1} \mathbf{y}) / (\mathbf{A}^m \mathbf{y})^\top (\mathbf{A}^m \mathbf{y}), \\ T_m &= \mathbf{x}^\top (\mathbf{A}^{m+1} \mathbf{y}) / \mathbf{x}^\top (\mathbf{A}^m \mathbf{y}). \end{aligned}$$

The first of these,  $R_m$ , is called the *Rayleigh quotient*; the second,  $|S_m| = \|\mathbf{A}^{m+1} \mathbf{y}\| / \|\mathbf{A}^m \mathbf{y}\|$  gives an estimate of magnitude only (but since  $\mu$  must be real, under our assumptions, it is no great problem to discover its sign; for instance, by observing a few values of  $T_m$ ); and, in practice, the third expression,  $T_m$ , represents the ratio of successive values of some component of the iterated vector. By (70), it is clear that

$$(109) \quad R_m \sim \mu, \quad |S_m| \sim |\mu|, \quad T_m \sim \mu \quad \text{as } m \rightarrow \infty.$$

Note that, if we look at  $T_m(\mathbf{x})$  for  $\mathbf{x} = \mathbf{e}_1, \mathbf{e}_2, \dots, \mathbf{e}_N$  (where  $(\mathbf{e}_r)_s = \delta_{rs}$ ), at least one  $\mathbf{e}_r^\top \mathbf{z} \neq 0$ ; so that the greatest of these ratios  $T_m(\mathbf{e}_r)$  will certainly be asymptotic to  $\mu$ . Note, too, that all three expressions can be approximated (with a bias which can be made arbitrarily small) by the ratios of Monte Carlo estimators of the type (107): for example,  $R_m$  can be estimated by the ratio

$$(110) \quad \begin{aligned} &\frac{1}{k} \sum_{i=1}^k \left[ \frac{y_{s_0} \left( \prod_{\alpha=1}^m \frac{A_{s_\alpha s_{\alpha-1}}}{p_{s_\alpha - 1 s_\alpha}} \right) \left( \prod_{\beta=0}^{m-1} \frac{A_{s_{m+\beta} s_{m+\beta+1}}}{p_{s_{m+\beta} s_{m+\beta+1}}} \right) y_{s_{2m+1}}}{q_{s_0}} \right]_{\Gamma=\Gamma_i}, \\ &\frac{1}{k'} \sum_{j=1}^{k'} \left[ \frac{y_{s_0} \left( \prod_{\alpha=1}^m \frac{A_{s_\alpha s_{\alpha-1}}}{p_{s_\alpha - 1 s_\alpha}} \right) \left( \prod_{\beta=0}^{m-1} \frac{A_{s_{m+\beta} s_{m+\beta+1}}}{p_{s_{m+\beta} s_{m+\beta+1}}} \right) y_{s_{2m}}}{q_{s_0}} \right]_{\Gamma=\Gamma'_j}, \end{aligned}$$

where the  $\Gamma_i$  and  $\Gamma'_i$  all represent independent random walks on  $S$ , started at a random index  $s_0$  with probability  $q_{s_0}$ . (It is alternatively possible to introduce a useful correlation (in the spirit of importance sampling) by making  $k = k'$  and  $\Gamma_i = \Gamma'_i$  for  $i = 1, 2, \dots, k$ .) An essentially similar estimator to (110) is given by

$$(111) \quad \frac{\frac{1}{k} \sum_{i=1}^k Q_{s_0 m}(\Gamma_i^{(1)}) Q_{s_0(m+1)}(\Gamma_i^{(2)}) / q_{s_0}}{\frac{1}{k'} \sum_{j=1}^{k'} Q_{s'_0 m}(\Gamma_j^{(1)'}) Q_{s'_0 m}(\Gamma_j^{(2)'}) / q_{s'_0}},$$

where the walks  $\Gamma_i^{(1)}$  and  $\Gamma_i^{(2)}$  begin at a random index  $s_0 = s_0(i)$  and the walks  $\Gamma_j^{(1)'}$  and  $\Gamma_j^{(2)'}$  begin at a random index  $s'_0 = s'_0(j)$ , all walks being independent (with the alternative  $k = k'$ ,  $\Gamma_i^{(1)} = \Gamma_i^{(1)'}$ ,  $\Gamma_i^{(2)} = \Gamma_i^{(2)'}$ ,  $s_0(i) = s'_0(i)$ , as before).

We observe that, by the Cauchy-Schwarz inequality,

$$(112) \quad |R_m| \leq |S_m|.$$

If we further assume that  $\mathbf{A}$  is *normal* (defined by  $\mathbf{A}^\mathsf{H}\mathbf{A} = \mathbf{A}\mathbf{A}^\mathsf{H}$ ; or, since our  $\mathbf{A}$  is real,  $\mathbf{A}^\mathsf{T}\mathbf{A} = \mathbf{A}\mathbf{A}^\mathsf{T}$ ), this is equivalent (see, e.g., [57], [58], [63]) to requiring that  $\mathbf{A}$  be unitarily equivalent to a diagonal matrix, and this, in turn, is easily seen to be a necessary and sufficient condition for the existence of a complete orthogonal set of eigenvectors of  $\mathbf{A}$  (if  $\mathbf{U}$  is unitary and  $\mathbf{U}^\mathsf{H}\mathbf{A}\mathbf{U}$  is diagonal, then the columns of  $\mathbf{U}$  form such a set). This implies that we may uniquely express any  $\mathbf{y}$  as a sum  $\sum_{i=1}^k \mathbf{z}_i$ , where  $\mathbf{A}\mathbf{z}_i = \lambda_i \mathbf{z}_i$  (but  $\mathbf{z}_i$  may be null for some  $i \neq 1$ ; though  $\mathbf{z}_1 \neq \mathbf{0}$ ) and  $\mathbf{z}_i^\mathsf{H} \mathbf{z}_j = \delta_{ij} \|\mathbf{z}_i\|^2$  (note that some of the  $\mathbf{z}_i$  and  $\lambda_i$  may be complex; though  $\mathbf{A}, \mathbf{y}, \mu = \lambda_1$  are real). Therefore,

$$(113) \quad \mathbf{A}^m \mathbf{y} = \sum_{i=1}^k \lambda_i^m \mathbf{z}_i, \quad \|\mathbf{A}^m \mathbf{y}\|^2 = \sum_{i=1}^k |\lambda_i|^{2m} \|\mathbf{z}_i\|^2,$$

and so

$$(114) \quad |S_m| \leq |\mu|.$$

With (112), this means that  $|S_m|$  is a better approximation to  $|\mu|$  than is  $|R_m|$ . On the other hand, if  $\mathbf{x}^\mathsf{H} \mathbf{z}_i = \xi_i$  and  $\xi_1 \neq 0$ ,

$$(115) \quad \mu - T_m = \frac{\sum_{i=1}^k \lambda_i^m (\mu - \lambda_i) \xi_i}{\sum_{i=1}^k \lambda_i^m \xi_i}, \quad \mu - R_m = \frac{\sum_{i=1}^k |\lambda_i|^{2m} (\mu - \lambda_i) \|\mathbf{z}_i\|^2}{\sum_{i=1}^k |\lambda_i|^{2m} \|\mathbf{z}_i\|^2};$$

so that, because  $|\lambda_i/\mu| < 1$  for  $i \neq 1$ , as  $m \rightarrow \infty$ , we have the asymptotic behavior described by

$$(116) \quad |\mu - T_m| \lesssim \sum_{i=2}^k \left| \frac{\lambda_i}{\mu} \right|^m \left| \frac{\xi_i}{\xi_1} \right| |\mu - \lambda_i|, \quad |\mu - R_m| \lesssim \sum_{i=2}^k \left| \frac{\lambda_i}{\mu} \right|^{2m} \frac{\|\mathbf{z}_i\|^2}{\|\mathbf{z}_1\|^2} |\mu - \lambda_i|,$$

indicating that  $R_m$  converges towards  $\mu$  twice as fast as does  $T_m$ . Thus, finally,  $|S_m|$  appears to be the best estimator of  $|\mu|$ , of the three expressions in (108), if  $\mathbf{A}$  is normal.  $R_m$  and  $S_m$  take just about the same amount of work to compute (or

estimate stochastically). The Monte Carlo estimate of  $T_m$  takes half the time to give (roughly) half as many digits of accuracy as that of  $R_m$ . This again indicates the advantage of  $S_m$ .

**2.4. Applications of the Monte Carlo techniques.** We have now reviewed most of the principal techniques used in implementing the Monte Carlo method. The vast majority of the literature referring to the Monte Carlo method deals with the results of calculations which use the method to solve practical problems; but most of these calculations are either rather straightforward simulations, or direct applications of the techniques already described. Many of them are rather primitive and artless.

It is not proposed, in the present survey, to do more than give passing mention to these applications, referring the reader to the literature for all the details. Only a small selection of representative papers will be mentioned individually. (For a large number of references, see [4].)

Applications in physics are numerous. To a high energy particle, a nucleus appears rather as a large spherical region containing a randomly located set of smaller hard (nonintersecting) spherical particles. This model has been applied to studies of the absorption of high energy radiation [87] and of intranuclear cascade reactions [88], [113].

As has already been mentioned in connection with the discussion of eigenvalue problems, the computation of atomic wave functions and eigenvalues of energy by Monte Carlo methods has received considerable attention [68], [79], [80], [86], [89]–[91].

Statistical mechanics is a subject to which Monte Carlo methods apply naturally, since it involves the averaging of global properties over very large sets of configurations or states of given systems. This approach has been applied to the computation of the thermodynamic properties (partition function, equation of state) of various systems; such as classical gas models [93], [114]–[122], quantum-mechanical systems [95], [98], materials exhibiting long range order (cooperative) phenomena [94], [96], [97], [123]–[126], and long chain coiling polymer molecules (the problem of the “self-avoiding random walk”) [27], [28], [92], [106], [127]–[130]. Mention should also be made of calculations of reaction kinetics [131], and the development of techniques for evaluating Wiener integrals [132]–[135].

The largest number of calculations has undoubtedly been performed in connection with the design of nuclear weapons and reactors. This subject has many tricks and devices of its own, and much of the work has never been published, because of security regulations. Problems are mainly of two kinds: “shielding calculations”, of the attenuation of radiation by its passage through matter, and “criticality studies” which are of the eigenvalue type. (See [27], [99]–[105], [136].)

Monte Carlo simulation of a rather direct sort has been used in many fields, such as the development of statistical tests [20], cell population studies [107], [108], combinatorial problems [109], search and optimization procedures [109], [137]–[140], operations research [26], [110], [111], and studies of signal detection in the presence of random noise [112].

**2.5. Random, pseudorandom and quasirandom sequences.** In § 1, we defined a *random generator*  $\Omega$  for a probability space  $(M, \mathcal{M}, \mu)$  as a device which

constructs or selects points of  $M$  in accordance with the probability structure indicated by  $\mathbf{M}$  and  $\mu$ . It was pointed out that, as is proved in [9], an arbitrary random sequence  $\Phi = [\phi_m]_m$  in the space  $H$  can always be represented as a sequence of functions  $\psi_m(\xi_1, \xi_2, \dots, \xi_m)$ ,  $m = 1, 2, 3, \dots$ , on  $(L, \mathbf{L}, \lambda)$  to  $H$ , where  $L = U^\infty$  is the infinite-dimensional unit hypercube whose points are sequences  $\Xi = [\xi_1, \xi_2, \xi_3, \dots]$  of numbers in the unit interval  $U = [0, 1]$ , and where  $\mathbf{L}$  and  $\lambda$  refer to the infinite product of Lebesgue measures, which makes the  $\xi_m$  independent and uniformly distributed in  $U$ . Thus any Monte Carlo procedure may be put into the canonical form  $(\Lambda, \Psi)$ , requiring only *canonical random generators*  $\Lambda$  associated with  $(L, \mathbf{L}, \lambda)$ .

Since actual computations are carried out in finite terms, what is really sought is a *discrete random generator*  $\Lambda_D$ , which generates discrete random variables (e.g., finite sequences of digital "words" interpreted as fixed-point or floating-point numbers) with a probability  $(L_D, \mathbf{L}_D, \lambda_D)$  approximating  $(L, \mathbf{L}, \lambda)$ . For example, we may specify that we wish to be able to generate up to  $10^{12}$  independent "random numbers," each in the form of a 64-bit "word," interpreted as a normalized floating-point number with binary mantissa  $+0.1b_3b_4 \dots b_{52} = \alpha$  and binary exponent  $-b_{54}b_{55} \dots b_{64} = -\beta$  (the digits  $b_1, b_2$  and  $b_{53}$  being respectively the sign (0, corresponding to +) and first bit (1) of the mantissa and the sign (1, corresponding to -) of the exponent). To any given sequence of  $64 \times 10^{12}$  binary digits (of which  $3 \times 10^{12}$  are predetermined by the specified form above) we must assign a probability equal to the product of the  $10^{12}$  factors  $2^{-\beta-51}$  for the numbers  $\alpha \times 2^\beta$ . Not much attention has been paid to the (usually rather small) effect of the use of discrete generators  $\Lambda_D$  instead of canonical generators  $\Lambda$ : it is assumed that this may be treated as an aspect of the general problem of roundoff and truncation errors. However, since  $\lambda(L_D) = 0$  while  $\lambda_D(L_D) = 1$ , it is clear that considerable bias could be introduced at times, and should be guarded against.

We have alluded in § 1 to the adoption of deterministic *pseudorandom* and *quasirandom* generators, and have indicated some of the theoretical and practical difficulties involved. On the one hand, it is impossible to prove the "true randomness" of a device; and it is not even desirable to require it, since all that is really needed is to get satisfactory answers to a class of problems. On the other hand, one cannot apply statistical tests to deterministic sequences and expect the resulting probabilistic "levels of significance" to have more than a qualitative meaning. At best these tests give us crude empirical guides as to the general suitability of the tested sequences for Monte Carlo computations. Apparently nothing has been done to find a validation for such tests, when they are applied to pseudorandom and quasirandom sequences. Nevertheless, the literature continues to produce numerous tables of statistical test results for a variety of such sequences. A number of alternative approaches have also been tried, for the evaluation of the usefulness of these sequences, and we shall return to this question later.

First we should examine how one may generate an arbitrary sequence of random variables, given a canonical random generator  $\Lambda$ . In its broadest sense, this is the question of implementing any Monte Carlo method; but generally part of the question is answered by the definition of the particular method. For example, we may wish to estimate the integral  $\int_a^b f(x) dx$  by sampling the estimator

$v(\eta) = \Phi f(\eta)/\phi(\eta)$ , where  $\Phi = \int_a^b \phi(x) dx$ ,  $\phi(x) > 0$  for all  $a \leq x \leq b$ , and  $\eta$  is sampled from  $[a, b]$  with probability density  $\phi(x)/\Phi$ . This is done repeatedly with independent sample values  $\eta_1, \eta_2, \dots, \eta_k, \dots$ , and yields a sequence of secondary estimates  $\phi_k(\eta_1, \eta_2, \dots, \eta_k) = k^{-1} \sum_{i=1}^k v(\eta_i)$  converging to the required answer. Thus the implementation problem reduces to that of generating a sequence of independent random variables  $\eta_i$  distributed with density  $\phi(x)/\Phi$ . Since the random variables  $g(\xi_i)$  are independent whenever the  $\xi_i$  are independent, the question reduces further to that of generating a single  $\eta$ . On the other hand, in the *E-Z-H* method, one samples several random variables with a fairly complicated joint distribution (see (42)). There is not much in the literature on the latter, more complicated and less common, problem. There is some discussion in [4] and in [51], mainly of the basic, rather laborious method of forming successive conditional probability distributions of  $\eta_k$  given  $\eta_1, \eta_2, \dots, \eta_{k-1}$  and sampling from these univariate distributions as they become known. The case of an arbitrarily autocorrelated sequence has also been studied [51], [143]. However, the bulk of published work in this area deals with methods of generating a single random variable with a given distribution, and here some general principles and special techniques have been developed. General discussions will be found in [4], [17], [28], [31], [33], [51], [141], [142], [144]–[147]; particular mention should be made of the pioneering paper of von Neumann [145], of the extensive coverage by Jansson [141] and Kahn [31], and of the comprehensive bibliographies of Hull and Dobell [142] and Halton [4].

Of the general procedures, the first is the *direct method*, exemplified in §1 by the relations (12) with (5). In general, if the required random variable has the cumulative distribution function  $q(x) = \mu(\{\zeta \in M : \eta(\zeta) < x\})$ , we can, in principle, invert the function  $q$  and define our random variables as  $g(\xi)$ , where  $\xi$  is canonical (uniformly distributed in  $U$ ) and

$$(117) \quad g(\xi) = \inf \{x : \xi \leq q(x)\}.$$

Clearly,

$$\begin{aligned} \omega(\{\xi \in U : g(\xi) < x\}) &= \omega(\{\xi \in U : \inf\{y : \xi \leq q(y)\} < x\}) \\ &= \omega(\{\xi \in U : \xi \leq q(x)\}) = q(x), \end{aligned}$$

where  $\omega$  is the Lebesgue measure (defining uniform distribution in  $U$  by

$$(118) \quad \omega(\{\xi \in U : \xi \leq c\}) = c,$$

as required for  $\xi$ ); the second step being obtained from the fact that  $q$  is a monotone nondecreasing left-continuous function. (If we write  $X = \{\xi \in U : \inf\{y : \xi \leq q(y)\} < x\}$  and  $Y = \{\xi \in U : \xi \leq q(x)\}$ ; we have that, for any  $\xi \in X$ , there is a  $y_0$ , such that  $\xi \leq q(y_0)$  and  $y_0 < x$ , whence  $\xi \in Y$ , i.e.,  $X \subseteq Y$ . If  $\xi \in X^c Y$ , then we see that  $\inf\{y : \xi \leq q(y)\} = x$ ; i.e.,  $\xi > q(y)$  for all  $y < x$  and  $\xi \leq q(y)$  for all  $y \geq x$ . Since  $q(x)$  is left-continuous, this implies that  $\xi = q(x)$ . Thus  $\omega(X) = \omega(Y) - \omega(X^c Y) = \omega(Y) - \omega(\{\xi = q(x)\}) = \omega(Y)$ , since a single value of  $\xi$  has zero Lebesgue measure.) This shows that  $g(\xi)$  has the same distribution as is required of  $\eta$ . Except in specially simple cases, this method can be very tedious;

but it is convenient in sampling from small discrete distributions and can be the only feasible technique for sampling from empirical distributions. Time can be saved by using the “binary-chopping” technique in searching through a table of values of  $q(n)$  for the proper  $n(\xi)$  (see (12)): this consists of comparing  $\xi$  first with  $q(n_1)$ , where  $n_1$  is close to  $N/2$ ; then with  $q(n_2)$ , where  $n_2$  is close to  $N/4$  if  $\xi < q(n_1)$  and close to  $3N/4$  if  $\xi > q(n_1)$ ; and so on, at each stage picking an index  $n_r$  near the middle of the interval of index values to which  $n(\xi)$  has been restricted.

The second general procedure is the *rejection technique* invented by von Neumann [145]: if  $\eta$  has probability density  $p(x) \leq c$  in  $[a, b]$ ; first set  $m = 1$ , sample independent canonical random values  $\xi_1$  and  $\xi_2$ , and put  $\eta = a + (b - a)\xi_1$  if

$$(119) \quad c\xi_{2m} \leq p(a + (b - a)\xi_{2m-1});$$

while if (119) is not satisfied, reject the pair  $\xi_1, \xi_2$ , add 1 to  $m$ , pick a new independent pair  $\xi_3, \xi_4$ , and test it by (119). The process continues until the inequality (119) is satisfied for some value of  $m$ , and the corresponding value  $\eta = a + (b - a)\xi_{2m-1}$  is accepted. The expected value of  $m$  will be  $c(b - a)$ , and the method will be efficient so long as this is not too much larger than 1. Butler [146] generalizes the method to multivariate distributions. The following special scheme can be viewed as a kind of rejection technique: if the required cumulative distribution function is  $q(x) = q_1(x)q_2(x) \cdots q_m(x)$  and if each factor  $q_i(x)$  has an inverse  $g_i(\xi)$  as in (117), then take  $\eta = \max\{g_1(\xi_1), g_2(\xi_2), \dots, g_m(\xi_m)\}$ . In the simplest case, every  $q_i(x) = x$ ,  $g_i(\xi) = \xi$ , and the distribution function of  $\max\{\xi_1, \xi_2, \dots, \xi_m\}$  is  $x^m$ .

The third general procedure is the *composition technique*, first described by Butler [146] and developed for discrete compositions by Butcher [148] and by Marsaglia and his collaborators [149], [150]. If  $\eta$  has a probability density

$$(120) \quad p(x) = \int_{-\infty}^{+\infty} p_y(x) dF(y),$$

we sample a value  $y$  of  $y$  from the distribution  $F(y)$  by one of the available techniques, and then sample  $\eta$  with density  $p_y(x)$ , again by some suitable scheme. The method leads to great efficiency if (see [17]) one arranges for the cost function  $\int_{-\infty}^{+\infty} T_y dF(y)$  to be small, where  $T_y$  is the cost function (e.g., the computational time for sampling a single number with density  $p_y(x)$ ) for the parameter value  $y$ . For example, Marsaglia, MacLaren and Bray [150] put, for the normal distribution (with positive  $x$ ),

$$(121) \quad p(x) = (\pi/2)^{-1/2} e^{-x^2/2} = a_1 p_1(x) + a_2 p_2(x) + a_3 p_3(x)$$

where  $a_1 \approx 0.96$ ,  $a_2 \approx 0.04$ ,  $a_3 \approx 0.003$ ,  $p_1(x)$  is a step function approximation to  $p(x)$  in  $[0, 3]$  with steps of 0.1,  $p_2(x)$  is the saw-tooth-shaped correction to  $p_1$  in  $[0, 3]$ , and  $p_3(x)$  (invoked only about 1/400 of the time) is the tail of  $p(x)$ , with  $x > 3$ . Generation of random variables with density  $p_1$  is very fast,  $p_2$  somewhat slower, and  $p_3$  very slow.

Besides these general procedures, there are various special techniques; these have been developed most extensively for the normal distribution, especially by Box and Muller [151], [152], Butcher [148], and Marsaglia [149], [150]. For other special techniques, see [31], [141], [153]–[157].

Because of the technical difficulties of constructing and testing efficient *true random generators*, and the general adoption of pseudorandom generators instead, not too much effort has gone into the design of the former. However, the more exact theoretical discussions tending to cast doubt on pseudorandom generators may well revive this line of endeavor. Discussions may be found in [33], [51], [141].

The earliest generators were typically based on gambling devices: they were mechanical devices in which randomness was introduced by a human operator. Among these, we may include ordinary cubic dice, decagonal prisms and eicosahedral dice (see [141]), and coins or counters (all of which are shaken or spun randomly, and tossed onto a flat horizontal surface to see which of the faces, marked with digits, comes uppermost); and the many pivoted devices which are spun and allowed to come to rest in a position indicating a digit on a circular scale, from spin-the-bottle to the classic roulette wheel and ball after whose traditional home the Monte Carlo method was named; and the various chance-selection processes, such as lotteries, card games, lucky dips, and picking straws; and games in which objects are tossed onto a surface marked so as to yield a digit where the object falls (notably the famous needle of Buffon: see [158]–[161] and for extensions [38], [158], [162], [163]). All of these devices are far too slow and unreliable for use in connection with modern electronic computers.

More useful are various electrical and electronic devices, from the automated roulettes of Kendall and Babington Smith [164], [165], and the RAND Corporation [166], [167], to various electronic circuits [33], [51], [168], [169] using thermal, shot-effect, and radioactive “noise.” The three biggest problems encountered in using these generators appear to be stability (and the need for frequent testing), the nonrepeatability of computations (unless all the numbers used are stored), and speed.

By far the most commonly used source of “random numbers” has been the computer algorithm generating a *pseudorandom sequence*. Originally, with tongue in cheek or not, these were subjected to, and expected to pass, precisely the same statistical tests as true random sequences; more recently (see below), somewhat different criteria have been applied; but these generators have always been thought of as general purpose devices, whose output “looks random.” We refer once again to the general texts [4], [17], [32], [33], [51], more especially to Jansson [141], and to review papers [28], [29], [142], [144], [170]–[172], in particular, to Hull and Dobell [142].

It appears that the first pseudorandom sequence was suggested by von Neumann, Metropolis and Ulam (to whom so much of the Monte Carlo method is attributable): it is the *middle-square* method, given by the recurrence relation

$$(122) \quad x_{n+1} = \{[x_n^2 M^{3/2}] / M\}$$

(where  $[\alpha]$  and  $\{\alpha\}$  respectively denote the integer part and fractional part of the number  $\alpha$ ; so that  $\alpha = [\alpha] + \{\alpha\}$  and  $0 \leq \{\alpha\} < 1$ , with  $[\alpha]$  an integer). Thus, if

$M = R^{2t}$  and  $x_n$  is expressed as a  $2t$ -digit fraction to base  $R$ , then  $x_{n+1}$  is obtained by squaring  $x_n$  and forming a new  $2t$ -digit fraction by discarding the top and bottom  $t$  digits of the  $4t$ -digit square (see [173], [174]). Though some success was achieved with this method, it appears that degeneracy to zero can occur in ways that are difficult to predict and the consensus seems to be unfavorable. It was suggested that (122) be replaced by

$$(123) \quad x_{n+2} = \{[x_n x_{n+1} M^{3/2}] / M\},$$

but no great improvement was found [170].

The next, and by far the most successful and popular method is due to Lehmer [175], and is variously called the *multiplicative-congruential, power-residue, and Multiply* ([176]: the imperative of the verb) method. It is defined by

$$(124) \quad x_{n+1} = \{\lambda x_n\}, \quad x_n = \{\lambda^n x_0\},$$

where  $\lambda$  is a (large) integer. The greater part of the literature is related to the study of this method.

We note that if  $x_n$  is an  $s$ -digit fraction to base  $R$ , then  $X_n = R^s x_n$  is an integer, and (122)–(124) may be written as

$$(125) \quad \begin{aligned} X_{n+1} &\equiv [X_n^2 / R^t] \pmod{M}, \\ X_{n+2} &\equiv [X_n X_{n+1} / R^t] \pmod{M}, \quad \text{with } M = R^{2t}, \\ X_{n+1} &\equiv \lambda X_n, \quad X_n \equiv \lambda^n X_0 \pmod{M}, \quad \text{with } M = R^s; \end{aligned}$$

whence one may apply number theory to the analysis of these sequences.

An easy generalization of (124) leads to the *mixed-congruential* method, first mentioned in passing by Lehmer [175] and rediscovered by Franklin [176], Coveyou [177] and Rotenberg [178], and defined by

$$(126) \quad x_{n+1} = \{\lambda x_n + \theta\}, \quad \text{or} \quad X_{n+1} \equiv \lambda X_n + \mu \pmod{M},$$

where  $\theta = \mu/M$  and  $\mu$  is an integer. These sequences have also received much theoretical and experimental discussion. We see that (126) yields

$$(127) \quad x_n = \left\{ \lambda^n x_0 + \frac{\lambda^n - 1}{\lambda - 1} \theta \right\} \quad \text{or} \quad X_{n+1} \equiv \lambda^n X_0 + \frac{\lambda^n - 1}{\lambda - 1} \mu \pmod{M}.$$

More general homogeneous or mixed linear congruences can clearly be used, with a general form

$$(128) \quad x_{n+k} = \{\lambda_0 x_n + \lambda_1 x_{n+1} + \cdots + \lambda_{k-1} x_{n+k-1} + \theta\}$$

or

$$(128') \quad X_{n+k} \equiv \lambda_0 X_n + \lambda_1 X_{n+1} + \cdots + \lambda_{k-1} X_{n+k-1} + \mu \pmod{M},$$

and such methods (some also involving circular shifting of digits) have been investigated, but have not been widely adopted, because they do not seem to yield improvements proportional to their greater complexity (see [179]–[182]). The same may be true of a method for combining a number of relatively short periodic sequences to yield a longer one (see [172], [183]). However, it may be that they should be reconsidered more thoroughly.

If the  $\lambda_i$  and  $\theta$  in (128) and (128') are taken to be 0 or 1, we obtain an *additive-congruential* or *sum-residue* method. The simplest of these is the *Fibonacci sequence*

$$(129) \quad x_n = \{F_n/M\} \quad \text{with } F_{n+2} = F_n + F_{n+1}.$$

Since the solutions of recurrences of the type (128), (128') will generally produce linear combinations of powers of constants, we see that such a method is asymptotic to a multiplicative-congruential method. For instance,

$$(130) \quad F_n = A \left( \frac{1 + \sqrt{5}}{2} \right)^n + B \left( \frac{1 - \sqrt{5}}{2} \right)^n \sim A \left( \frac{1 + \sqrt{5}}{2} \right)^n.$$

The literature on Fibonacci sequences and other integer sequences generated by linear recurrences is vast, and a considerable new interest has arisen in these sequences and their properties, because of the search for pseudorandom sequences (see, for example, [15], [184]–[194]). The intention of the additive-congruential method was to substitute addition for (relatively slow) multiplication, and still yield a sequence of multiplicative-congruential type. This was also a motive in using mixed formulas (126) rather than (124), because the factors  $\lambda$  could be made very simple in the former, but not in the latter (see below).

The question of the best choices for  $\lambda$  and  $\mu$  in (124) and (126) is crucial and has been answered by a mixture of empiricism and number theory. We refer the reader to previously mentioned books (especially Jansson [141]) and review papers, particularly those of Juncosa [171] and Hull and Dobell [142]; and also to papers [177], [178], [195]–[198], [207]–[209], [211], [212]. The first criterion used was that the recurrence relation should generate a sequence (necessarily periodic with period  $\leq M$ ) with *as large a period as possible*. This is discussed in [141], [142], [171], [172], [178], [195], [196]. Hull and Dobell [142] summarize the results obtained, as follows:

(i) If  $\mu \neq 0$ , then the sequence has period  $M$  if: (a)  $\mu$  is relatively prime to  $M$ , (b) for every prime factor  $p$  of  $M$ ,  $\mu \equiv 1 \pmod{p}$ , and (c) if  $M$  is divisible by 4,  $\mu \equiv 1 \pmod{4}$ .

(ii) If  $\mu = 0$  and  $M = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$ , then the maximum period of the sequence (as  $\lambda$  varies) is the least common multiple of the maximum periods for  $M = p_r^{\alpha_r}$ ,  $r = 1, 2, \dots, s$ ; and there exist values of  $\lambda$  for which all these  $s + 1$  maximum periods are simultaneously attained.

(iii) If  $\mu = 0$  and  $M = p^\alpha$ ,  $p \neq 2$ , then the maximum period is  $(p - 1)p^{\alpha - 1}$ , and it is attained for some  $\lambda$  (such a  $\lambda$  is a “primitive root” for  $p^\alpha$ ); the same is true if  $M = 2$  and 4 (with maximum periods 1 and 2, attained when  $\lambda = 1$  and 3, respectively: hardly useful for pseudorandom sequences!); while if  $M = 2^\alpha$ ,  $\alpha \geq 3$ , the maximum period is  $2^{\alpha - 2}$ . In every case,  $X_0$  must be relatively prime to  $M$ .

(iv) In practice, only  $p = 2, 3, 5$  are of importance. (a) For  $M = 2^\alpha$ ,  $\alpha \geq 3$ ,  $\lambda$  yields the maximum period of  $2^{\alpha - 2}$  if and only if  $\lambda \equiv \pm 3 \pmod{8}$ . (b) For  $p = 3$ , the maximum period  $2 \times 3^\alpha$  is attained if  $\lambda \equiv 2$  or  $5 \pmod{9}$ . (c) For  $p = 5$ , the maximum period  $4 \times 5^\alpha$  is attained if  $\lambda \equiv \pm 2, \pm 3, \pm 8$ , or  $\pm 12 \pmod{25}$ . (d) Finally, (by (a), (c), (ii), (iii)) for  $M = 10, 100, 1000$ , and  $10^\alpha$ ,  $\alpha \geq 4$ , the maximum

periods 4, 20, 100 and  $5 \times 10^{\alpha-2}$ , respectively, are attained if  $\lambda = 3$  or 7 ( $\alpha = 1$ ),  $\lambda = 3, 23, 27, 47, 63, 67, 83$  or 87 ( $\alpha = 2$ ), and  $\lambda \equiv \pm 3, \pm 13, \pm 27, \pm 37, \pm 53, \pm 67, \pm 77$  or  $\pm 83 \pmod{200}$  ( $\alpha \geq 3$ ).

(v) Conditions (b), (c) and (d) of (iv) are sufficient, but not necessary. For example, if  $M = 10^\alpha$  ( $\alpha \geq 3$ ), we obtain maximum periods with  $\lambda \equiv \pm 11, \pm 19, \pm 21, \pm 29, \pm 59, \pm 61, \pm 69, \pm 91 \pmod{200}$ .

The earliest approach to testing the usefulness of pseudorandom sequences was by way of *statistical tests*. We find these taking a prominent part in [141], [142], [164]–[172], [179]–[183], [197], [198], and the same point of view is adopted in testing the distribution of digits in transcendental numbers [199]–[203] and of coefficients in continued fraction expansions of algebraic numbers [204]. As has been argued before, the results of these tests should not be interpreted literally, in the terms in which they are expressed in truly stochastic situations; but these results are clearly of considerable relevance in judging the usefulness of pseudorandom sequences. It would be most advantageous if their precise significance in a deterministic situation could be clarified.

Among statistical tests which have been applied to pseudorandom sequences, we may mention Kendall and Babington Smith's [165] "frequency test" (proportion of occurrence of digit values), "serial test" (proportion of occurrence of pairs of digits), "poker test" (in blocks of four digits, occurrence of four of one kind, three of one kind, two pairs, one pair, and all different digits), and "gap test" (lengths of gaps between successive zeros), used in conjunction with the known statistical expectations for a canonical random sequence, and with the  $\chi^2$ -test. These tests, or slight variations on them, have remained standard in the literature. Other parameters tested have been serial correlation, proportion of occurrence of  $m$ -tuples with  $m > 2$ , notably by MacLaren and Marsaglia [181], and lengths of runs of the same digit; Greenwood's "coupon collector's test" (length of run to obtain a given number of occurrences of one digit value) [227], and Gruenberger's " $d^2$ -test" (distribution of distances between points  $(\xi_n, \xi_{n+1})$  and  $(\xi_{n+2}, \xi_{n+3})$  in the unit square) [228] have also been applied.

Two theoretical points may be made here. First, the acceptance of a finite sequence of points from a random generator as a sample suitable for a Monte Carlo calculation subsumes the concept of *repeated independent trials* (it is on this basis that all Monte Carlo theory rests); so however impeccably generated and well-behaved a sample may be, it can only be used *once*, if its qualifications are not to be nullified. Thus, in principle, a list such as [165], [167] should be used only once, and similarly a pseudorandom algorithm should be taken only once through its full period (only nonoverlapping sections being used). It may be argued that the same list might safely be employed in *entirely unrelated* calculations; but this begs the crucial question of what calculations are truly unrelated in every way. Secondly, as is pointed out by Kendall [165], every finite sequence, even if it is quite acceptable as a sample, will contain subsequences which are clearly unrepresentative (i.e., in important respects correspond to regions of the sample space having very low probabilities) and computationally undesirable. Thus, again, a sample will never be passed unconditionally by any battery of statistical tests, even on their own criteria. In addition, of course, every sequence, however well tested, will prove to be unsuitable on some grounds or other; for example, in its

less significant digits [181] or in a complicated sequential relationship [205], [206]. In some cases, such failures can be theoretically explained, but generally only with hindsight [197], [206].

A number of more rigorous approaches to the judgment of pseudorandom sequences have been tried, with varying degrees of success. The earliest of these was the *asymptotic frequency* approach. This will be found in [176], [177], [207]–[210]. Essentially, it appeals to the empirical concept of probability and defines the probability of an event  $E$  with respect to a sequence  $\Xi = [\xi_1, \xi_2, \xi_3, \dots]$  as

$$(131) \quad p(E) = \lim_{N \rightarrow \infty} (v_N(E)/N),$$

where  $v_N(E)$  is the number of points among  $\xi_1, \xi_2, \dots, \xi_N$  which fall in the region corresponding to  $E$ . Thus  $p(E)$  is the asymptotic (or limiting) frequency of the event  $E$  in the sequence  $\Xi$ . This point of view is ancient in probability theory, but appears to have been first applied to pseudorandom sequences by Coveyou [177]. His work, followed by further studies by Greenberger [207], [208] and Jansson [142], [209], was initially applied to the explicit computation of asymptotic *serial correlations* in mixed congruential generators, in order to determine optimum constants  $\lambda$  and  $\mu$ .

Following the work of Bohl, Sierpiński, Weyl, van der Corput, Koksma, and others on *uniform distribution modulo one* (see [213]–[226]), Franklin [176] adopted the following criterion. For a canonical random sequence  $\Xi = [\xi_i], i = 1, 2, \dots$ , any subsequence of  $k$  numbers  $[\xi_{n+1}, \xi_{n+2}, \dots, \xi_{n+k}]$  has probability  $\alpha_1\alpha_2 \cdots \alpha_k$  of lying in the “hyperbrick” defined by

$$(132) \quad 0 \leq \xi_{n+i} < \alpha_i \leq 1, \quad i = 1, 2, \dots, k.$$

We say that an arbitrary sequence  $\Xi$  of points in  $U = [0, 1]$  is  $k$ -equidistributed if

$$(133) \quad p(E(\alpha_1, \alpha_2, \dots, \alpha_k)) = \alpha_1\alpha_2 \cdots \alpha_k$$

for every choice of  $\alpha_1, \alpha_2, \dots, \alpha_k$  in  $[0, 1]$ ; where  $p$  is defined by (131) and  $E(\alpha_1, \alpha_2, \dots, \alpha_k)$  is the event (132); and that  $\Xi$  is *completely equidistributed* if it is  $k$ -equidistributed for every integer  $k > 0$ . The analogous definition for discrete variables (in  $L_D$ : see above) is easily made. Franklin obtained a considerable number of results on the equidistribution properties (and related “equipartition” and serial-correlation properties) of various pseudorandom sequences, including the Multiply sequences (124) and (126) with  $\theta$  possibly irrational, and the related “polynomial sequences,”

$$(134) \quad x_n = \{n^p\alpha + c_1 n^{p-1} + c_2 n^{p-2} + \cdots + c_p\}$$

with  $\alpha$  irrational, and

$$(135) \quad x_n = \{\theta^n\},$$

and the Weyl sequence

$$(136) \quad x_n = \{n\alpha\}.$$

For example, we may mention that:

- (i) a Multiply sequence may fail to be (1-) equidistributed even if  $x_0$  is transcendental;
- (ii) no Multiply sequence is  $k$ -equidistributed for any  $k > 1$ ;
- (iii) for any sequence (124) (with  $\lambda$  an integer),  $p(x_n > x_{n+1} > x_{n+2}) = \frac{1}{6}(1 + \lambda^{-1})$  (the theoretical probability for a canonical random sequence is  $\frac{1}{6}$ );
- (iv) fixing  $x_0$  and  $\theta$  in (126), write  $x_n = x_n(\lambda)$ ; then, for all  $k$  and  $\alpha_1, \alpha_2, \dots, \alpha_k$ ,

$$(137) \quad \lim_{\lambda \rightarrow \infty} p(E_\lambda(\alpha_1, \alpha_2, \dots, \alpha_k)) = \alpha_1 \alpha_2 \cdots \alpha_k$$

holds for almost all  $x_0$ , where  $E_\lambda(\alpha_1, \alpha_2, \dots, \alpha_k)$  denotes the event (132) with  $x_{n+i}(\lambda)$  replacing  $\xi_{n+i}$ ;

- (v) if  $f(z_1, z_2, \dots, z_k)$  is Riemann integrable in the  $k$ -dimensional unit cube (and Riemann integrable along all line segments in the cube), then, for all  $k$ , for almost all  $x_0$ ,

$$(138) \quad \begin{aligned} & \lim_{\lambda \rightarrow \infty} \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{n=0}^{N-1} f(x_{n+1}(\lambda), x_{n+2}(\lambda), \dots, x_{n+k}(\lambda)) \\ &= \int_0^1 dz_1 \int_0^1 dz_2 \cdots \int_0^1 dz_k f(z_1, z_2, \dots, z_k); \end{aligned}$$

- (vi) the sequence (135) is completely equidistributed for almost all  $\theta > 1$ ; and if it is  $k$ -equidistributed, then  $\theta$  cannot be an algebraic number of degree less than  $k$ ; thus if it is completely equidistributed,  $\theta$  must be transcendental. This last result was taken up by Knuth [210], who pointed out that there was no explicit  $\theta$  for which  $\{\theta^n\}$  was known to be completely equidistributed, nor was any other sequence known so to be: he constructed such a sequence explicitly.

Let us put  $\alpha = [\alpha_i]_{i=1}^k$  and  $V(\alpha) = \prod_{i=1}^k \alpha_i$  for the volume of the region (132) defined by the  $k$ -dimensional point  $\alpha$ . Let us renumber the  $\xi_i$  in the sequence  $\Xi$  and group them into  $k$ -tuples  $\xi_n = [\xi_{n,i}]_{i=1}^k$ , with the double index  $(n, i)$  replacing the single index  $(n-1)k + i$ , so that  $\Xi$  becomes a sequence  $[\xi_n]_{n=1}^\infty$  of points in  $U^k$ . Then we see that (131) and (133) are equivalent to

$$(139) \quad \lim_{N \rightarrow \infty} \Delta_N(\alpha) = 0,$$

where

$$(140) \quad \Delta_N(\alpha) = N^{-1} v_N(\alpha) - V(\alpha)$$

is the *local discrepancy* of the sequence  $[\xi_n]_{n=1}^N$  at the point  $\alpha$ , with  $v_N(\alpha)$  denoting  $v_N(E(\alpha_1, \alpha_2, \dots, \alpha_k))$  for brevity. From this we may derive various measures of the imperfection of equidistribution of the sequence in  $U^k$ :

$$(141) \quad \mathcal{M}_N = - \inf_{\alpha \in U^k} \Delta_N(\alpha),$$

$$(142) \quad \mathcal{N}_N = \sup_{\alpha \in U^k} \Delta_N(\alpha),$$

$$(143) \quad \mathcal{D}_N = \sup_{\alpha \in U^k} |\Delta_N(\alpha)| = \max(\mathcal{M}_N, \mathcal{N}_N)$$

and

$$(144) \quad \mathcal{T}_N = \left[ \int_0^1 d\alpha_1 \int_0^1 d\alpha_2 \cdots \int_0^1 d\alpha_k |\Delta_N(\alpha)|^2 \right]^{1/2}$$

are respectively termed the *minimum*, *maximum*, *extreme* (or  $L^\infty$ -), and *mean-square* (or  $L^2$ -) *discrepancy* ( $\mathcal{D}_N$  was formerly called just the “discrepancy,” before the  $L^2$ -discrepancy (also termed the *turpitude*, whence the notation) was introduced).

The sequence  $\Xi$  is equidistributed in the  $k$ -dimensional unit hypercube  $U^k$  if (139) holds for every  $\alpha$  in  $U^k$ ; and this entails that  $\mathcal{M}_N$ ,  $\mathcal{N}_N$ ,  $\mathcal{D}_N$  and  $\mathcal{T}_N$  all tend to zero as  $N \rightarrow \infty$ . However, the inadequacy of the asymptotic frequency approach lies in the fact that no account is taken of *how fast* these quantities tend to zero. Now, for a true canonical random sequence,  $v_N(\alpha)$  counts the number of successes in a series of  $N$  Bernoulli trials with probability of success  $V(\alpha)$ ; so that the

probability that  $v_N(\alpha) = r$  is  $\binom{N}{r} [V(\alpha)]^r [1 - V(\alpha)]^{N-r}$ , and the mean values of  $\Delta_N(\alpha)$  and  $|\Delta_N(\alpha)|^2$  are 0 and  $V(\alpha)[1 - V(\alpha)]/N$ , respectively. It follows that

$$(145) \quad \begin{aligned} \mathbf{E}[\mathcal{T}_N^2] &= \int_0^1 d\alpha_1 \int_0^1 d\alpha_2 \cdots \int_0^1 d\alpha_k \mathbf{E}[|\Delta_N(\alpha)|^2] \\ &= \int_0^1 d\alpha_1 \int_0^1 d\alpha_2 \cdots \int_0^1 d\alpha_k \left( \frac{\alpha_1 \alpha_2 \cdots \alpha_k - \alpha_1^2 \alpha_2^2 \cdots \alpha_k^2}{N} \right) \\ &= [(\frac{1}{2})^k - (\frac{1}{3})^k] N^{-1}. \end{aligned}$$

Thus we would hope that  $\mathcal{T}_N$  for a pseudorandom sequence would diminish at least as fast as a constant multiple of  $N^{-1/2}$ . The study of the behavior of the discrepancies of sequences as functions of  $N$  has had relatively little attention (but see [5], [15], [17], [30], [53], [215], [220], [221], [229]–[233], and also the computational results in [234]). We shall return to it below.

An approach which has proved to be of considerable value in determining the usefulness of pseudorandom sequences, and which has led to the very important concept of *quasirandom sequences* (sequences which are good for certain classes of Monte Carlo calculations, but which lay no claim to the appearance of randomness), is simply to examine the behavior of the error

$$(146) \quad \delta_N(f) = \left| \frac{1}{N} \sum_{n=1}^N f(\xi_{n1}, \xi_{n2}, \dots, \xi_{nk}) - \int_0^1 dz_1 \int_0^1 dz_2 \cdots \int_0^1 dz_k f(z_1, z_2, \dots, z_k) \right|$$

in integrating certain classes of functions by applying the basic Monte Carlo technique, using the given sequence  $\Xi$  of points in  $U^k$ . The simplest case is when  $f(\mathbf{z})$  is the characteristic function of the set  $E(\alpha)$ , and then  $\delta_N(f) = |\Delta_N(\alpha)|$ . It is clear that the class of functions may be extended to the finite linear combinations of such characteristic functions without difficulty. Further, quite a lot of work has been done on the behavior of  $\delta_N(f)$  when  $f$  is restricted by conditions on the coefficients of its Fourier series. We refer to the work of Richtmyer [204], [235],

[237], Peck [236], Hlawka [13], [14], [215], Jagerman [211], Zaremba [15], [53], and Coveyou and Macpherson [212]. Examples of the results obtained are:

(i) Peck [236] showed that, if  $\xi_{ni} = \{n\alpha_i\}$ ,  $i = 1, 2, \dots, k$ ,  $n = 1, 2, 3, \dots$ , where the  $\alpha_i$  are in a real algebraic field of degree  $k+1$ , and if they are linearly independent (over the rationals), while the Fourier coefficients of  $f$ , defined by

$$(147) \quad f(\mathbf{z}) = \sum_{q_1=-\infty}^{+\infty} \sum_{q_2=-\infty}^{+\infty} \cdots \sum_{q_k=-\infty}^{+\infty} a(q_1, q_2, \dots, q_k) \cdot \exp(2\pi i(q_1x_1 + q_2x_2 + \cdots + q_kx_k)),$$

satisfy the inequality

$$(148) \quad |a(q_1, q_2, \dots, q_k)| < C/\max_j |q_j|^{k+\varepsilon},$$

for some finite  $C > 0$  and  $\varepsilon > 0$ ; then  $\delta_N(f) = O(N^{-1})$ .

(ii) Coveyou and Macpherson [212] have developed a novel line of attack, which may be summarized as follows. Suppose that the  $\xi_{ni}$  can only take the  $P$  values which are integer multiples of  $1/P$ , with  $P$  an integer and  $0 \leq \xi_{ni} < 1$ . Then we do not really hope to obtain an estimate of the integral of  $f(\mathbf{z})$  in  $U^k$ , but only of its Riemann approximation (for large  $P$ )

$$(149) \quad c = c(0, 0, \dots, 0) = P^{-k} \sum_{q_1=0}^{P-1} \sum_{q_2=0}^{P-1} \cdots \sum_{q_k=0}^{P-1} f\left(\frac{q_1}{P}, \frac{q_2}{P}, \dots, \frac{q_k}{P}\right).$$

Write  $\mathbf{p} = [p_i]_{i=1}^k$ ,  $\mathbf{q} = [q_i]_{i=1}^k$ , and denote by  $J$  the set  $\{0, 1, 2, \dots, P-1\}$ . Then define

$$(150) \quad c(\mathbf{p}) = P^{-k} \sum_{\mathbf{q} \in J^k} f(P^{-1}\mathbf{q}) e^{-2\pi i(\mathbf{p} \cdot \mathbf{q})/P},$$

where  $\mathbf{p} \cdot \mathbf{q} = \sum_{i=1}^k p_i q_i$  as usual; so that (149) is a particular case, and

$$(151) \quad f(P^{-1}\mathbf{q}) = \sum_{\mathbf{p} \in J^k} c(\mathbf{p}) e^{2\pi i(\mathbf{p} \cdot \mathbf{q})/P}.$$

(The proof of (151) is straightforward, by direct elimination of the  $c(\mathbf{p})$  between (150) and (151), and summation.) It now follows that, if the “asymptotic frequency”  $p(E)$  defined in (131) is denoted by  $d(\mathbf{q})$  when  $E$  is the event that  $\xi = P^{-1}\mathbf{q}$ , and if

$$(152) \quad b(\mathbf{p}) = \sum_{\mathbf{q} \in J^k} d(\mathbf{q}) e^{2\pi i(\mathbf{p} \cdot \mathbf{q})/P},$$

whence

$$(153) \quad d(\mathbf{q}) = P^{-k} \sum_{\mathbf{p} \in J^k} b(\mathbf{p}) e^{-2\pi i(\mathbf{p} \cdot \mathbf{q})/P};$$

then the “asymptotic expectation” of the Monte Carlo sum  $N^{-1} \sum_{n=1}^N f(\xi_n)$  is given by

$$(154) \quad \begin{aligned} \mathbf{E}[f] &= \sum_{\mathbf{q} \in J^k} f(P^{-1}\mathbf{q}) d(\mathbf{q}) \\ &= P^{-k} \sum_{\mathbf{q} \in J^k} \sum_{\mathbf{p}' \in J^k} \sum_{\mathbf{p}'' \in J^k} c(\mathbf{p}') b(\mathbf{p}'') e^{2\pi i(\mathbf{p}' - \mathbf{p}'') \cdot \mathbf{q}/P} \\ &= \sum_{\mathbf{p}' \in J^k} \sum_{\mathbf{p}'' \in J^k} c(\mathbf{p}') b(\mathbf{p}'') \delta_{\mathbf{p}' \mathbf{p}''} = \sum_{\mathbf{p} \in J^k} c(\mathbf{p}) b(\mathbf{p}). \end{aligned}$$

From this it would appear that, if we assume that the Fourier coefficients (in this finite sense) of  $f$ ,  $c(\mathbf{p})$ , diminish as  $|\mathbf{p}|$  increases, it will suffice that the  $b(\mathbf{p})$  should be small only for small  $|\mathbf{p}| \neq 0$ , with  $b(\mathbf{0}) = \sum_{\mathbf{q} \in J^k} d(\mathbf{q}) = 1$  (which is necessarily true in every case), in order that the error  $\delta_N(f)$  (in the above discretized sense) be asymptotically small.

While this approach is basically sound, and leads to sensible criteria for rejecting many sequences as obviously unsuitable, it suffers from two defects. It gives an inadequately worked-out, qualitative criterion for the class of functions for which a given sequence is suitable (the criterion will have to be that  $\sum_{\mathbf{p} \in J^k - \{\mathbf{0}\}} c(\mathbf{p})b(\mathbf{p})$  be small enough to be negligible : this can be very stringent); and, like the other asymptotic arguments, it does not discuss how fast the error converges to an acceptably small value. However, further work along these lines may well be valuable; and these authors have already imposed necessary sanctions on some classes of generators.

(iii) Zaremba [15], [53], improving on some results of Hlawka [14], looks at the functions (in our notation)

$$(155) \quad R(\mathbf{q}) = \prod_{i=1}^k \max(1, |q_i|)$$

and

$$(156) \quad \rho(\mathbf{g}) = \min \{R(\mathbf{q}) : \mathbf{q} \neq \mathbf{0}, \mathbf{g} \cdot \mathbf{q} \equiv 0 \pmod{P}\},$$

where  $P$  is a given integer, and  $\mathbf{g} = [g_i]_{i=1}^k$  is a vector with integer components. He is concerned with approximating the integral

$$(157) \quad a(\mathbf{0}) = \int_0^1 dz_1 \int_0^1 dz_2 \cdots \int_0^1 dz_k f(z_1, z_2, \dots, z_k)$$

by means of the sum (see (147))

$$(158) \quad P^{-1} \sum_{r=0}^{P-1} f\left(\frac{rg_1}{P}, \frac{rg_2}{P}, \dots, \frac{rg_k}{P}\right) = \sum_{\mathbf{q}} \{a(\mathbf{q}) : \mathbf{g} \cdot \mathbf{q} \equiv 0 \pmod{P}\}.$$

He mainly considers the case of integration in the unit square ( $k = 2$ ) and explains that the only case of practical significance had  $g_1 = 1$  and  $0 < g_2 = g < P$  with  $g$  relatively prime to  $P$ . For this case, he shows that if the Fourier coefficients of  $f$  satisfy the inequality

$$(159) \quad |a(q_1, q_2)| \leq K[R(q_1, q_2)]^{-m}$$

for some constants  $K > 0$  and  $m \geq 2$ , and  $P \geq 5$ , then

$$\begin{aligned} (160) \quad \delta(f) &= \left| \sum_{\mathbf{q}} \{a(\mathbf{q}) : \mathbf{q} \neq \mathbf{0}, \mathbf{g} \cdot \mathbf{q} \equiv 0 \pmod{P}\} \right| \\ &= \left| \sum_{q_1, q_2} \{a(q_1, q_2) : |q_1| + |q_2| > 0, q_1 + gq_2 \equiv 0 \pmod{P}\} \right| \\ &\leq K \left| \sum_{q_1, q_2} \{[R(q_1, q_2)]^{-m} : |q_1| + |q_2| > 0, q_1 + gq_2 \equiv 0 \pmod{P}\} \right| \\ &< K[36 \log P/\rho^2 + 60/P^2]\rho^{2-m} \\ &< K[36(A+2)^2 \log P + 60](A+2)^{m-2}/P^m, \end{aligned}$$

where  $\rho = \rho(1, g)$  and  $A$  is the maximum coefficient in the (finite) continued fraction expansion of  $g/P$  (it having been shown that  $\rho \geq P/(A + 2)$ ). If  $g = F_{n-1}$  or  $F_{n-2}$  while  $P = F_n$  (where the  $F_n$  are the Fibonacci numbers:  $F_0 = 0$ ,  $F_1 = 1$ ,  $F_{n+2} = F_n + F_{n+1}$ ; here again emerging as a useful subject for investigation), then  $\rho(1, g) = F_{n-2}$ , while otherwise  $\rho(1, g) \leq (10/29)P$ . In the former, preferable, special case, since  $F_n \sim \tau^n/\sqrt{5}$ , where  $\tau = (1 + \sqrt{5})/2$ ,

$$(161) \quad \delta(f) < K[36 \log F_n/F_{n-2}^2 + 60/F_n^2]/F_{n-2}^{m-2} = O(n\tau^{-mn})$$

as  $n \rightarrow \infty$ . This is equivalent to the asymptotic inequality

$$(162) \quad \delta(f) \lesssim O(P^{-m} \log P).$$

Zaremba points out that the condition (159) holds if  $f(\mathbf{z})$  is periodic in each  $z_i$ , with period 1, and has every partial derivative, of order less than  $m$  in each  $z_i$ , continuous and of bounded variation in the sense of Hardy and Krause ([53], [243]: see below). This condition is rather severe but can yield very accurate integration formulas. If  $f$  has continuous partial derivatives of the required order in  $U^2$ , but they are not periodic, then the sum of a polynomial in  $z_1$ , with coefficients depending on  $z_2$ , and a polynomial in  $z_2$ , with coefficients depending on  $z_1$ , can be found, whose integral in  $U^2$  is zero and such that all the relevant partial derivatives of its sum with  $f$  are equal on opposite sides of the square  $U^2$ , thus allowing extension to a periodic function. Zaremba has shown that this yields a new kind of integration formula, of great efficiency. The ideas can clearly be extended to  $k > 2$  dimensions; though the result on Fibonacci numbers does not generalize.

Turning from restrictions on Fourier coefficients, we consider what may be the most important approach of all, due to the work of Koksma [10], [215], Bertrandias [11], Haselgrove [12], Hlawka [13], [14], [215] and Zaremba [15], [53], [238], [239]. Consider the sequence  $\Xi = [\xi_n]_{n=1}^\infty$  in  $U$ . Then, by (140), (143) and (146), with an integration by parts, we proceed formally (and justifiably) to obtain that

$$(163) \quad \begin{aligned} \delta_N(f) &= \left| N^{-1} \sum_{n=1}^N f(\xi_n) - \int_0^1 dz f(z) \right| = \left| \int_0^1 d[N^{-1}v_N(z) - z]f(z) \right| \\ &= \left| \int_0^1 d\Delta_N(z) \cdot f(z) \right| = \left| \int_0^1 \Delta_N(z) \cdot df(z) \right| \\ &\leq \sup_{z \in U} |\Delta_N(z)| \int_0^1 |df(z)| = \mathcal{D}_N V(f), \end{aligned}$$

where  $V(f)$  is the *total variation* of  $f$  in  $U$ . This result is due to Koksma [10]. Hlawka [13] extended the result to any number of dimensions, and Zaremba [53], [239] has produced a simplified proof of this general result and has presented a new result in general form, which, for  $k = 1$ , is obtained by an application of the Cauchy-Schwarz inequality to (163); namely, by (144), if  $f(z)$  has a first order

derivative bounded in quadratic mean,

$$(164) \quad \begin{aligned} \delta_N(f) &= \left| \int_0^1 \Delta_N(z) f'(z) dz \right| \\ &\leq \left( \int_0^1 |\Delta_N(z)|^2 dz \right)^{1/2} \left( \int_0^1 |f'(z)|^2 dz \right)^{1/2} = \mathcal{T}_N W(f), \end{aligned}$$

where

$$(165) \quad W(f) = \left( \int_0^1 |f'(z)|^2 dz \right)^{1/2} \leq \sup_{z \in U} |f'(z)|.$$

The general results are as follows. We consider  $f(\mathbf{z})$  on  $U^k$  and  $\Xi = [\xi_n]_{n=1}^\infty$ . The  $k$ -dimensional total variation of  $f$  in  $U^k$  in the sense of Vitali can formally be written as

$$(166) \quad V^k(f) = \int_{U^k} |d_{z_1 z_2 \cdots z_k}^k f(z)|;$$

and this is rigorously defined by considering  $k$  partitions  $\pi_i$  of  $U$  at points  $0 = x_{i0} < x_{i1} < \cdots < x_{in_i} = 1$ ,  $i = 1, 2, \dots, k$ , defining

$$(167) \quad \begin{aligned} \delta_{z_i} \phi(\mathbf{z}) &= \phi(z_1, z_2, \dots, x_{ij_i}, \dots, z_k) - \phi(z_1, z_2, \dots, x_{i(j_i-1)}, \dots, z_k), \\ \delta_{z_1 z_2 \cdots z_k}^k \phi(\mathbf{z}) &= \delta_{z_1} \delta_{z_2} \cdots \delta_{z_k} \phi(\mathbf{z}), \end{aligned}$$

where the  $x_{ij}$  occur in place of  $z_i$ , and the indices  $j_i$  are omitted for brevity, and then

$$(168) \quad V^k(f) = \sup_{\pi_1, \pi_2, \dots, \pi_k} \sum_{j_1=1}^{n_1} \sum_{j_2=1}^{n_2} \sum_{j_k=1}^{n_k} |\delta_{z_1 z_2 \cdots z_k}^k f(\mathbf{z})|.$$

The function  $f$  is of bounded variation in the sense of Vitali if  $V^k(f)$  is finite. It is said to be of bounded variation in the sense of Hardy and Krause, if  $V^k(f)$  is finite and also  $V^h(\phi)$  is finite whenever  $h < k$  and  $\phi$  is a function of  $h$  variables obtained by fixing any  $k - h$  of the  $z_i$  to be 1. Let us now write  $f_{\sigma_h}$  for such a  $\phi$ , where  $\sigma_h$  is any choice of  $h$  of the  $z_i$  (there are  $\binom{k}{h}$  such choices), and similarly let  $\mathcal{D}_{N, \sigma_h}$  and  $\mathcal{T}_{N, \sigma_h}$  denote the

$L^\infty$ - and  $L^2$ -discrepancies of the sequence  $\Xi_{\sigma_h} = [\xi_{n, \sigma_h}]_{n=1}^\infty$ , where  $\xi_{n, \sigma_h}$  is the  $h$ -dimensional vector consisting of the  $h$  components of  $\xi_n$  selected by  $\sigma_h$ . Then we have

$$(169) \quad \delta_N(f) \leq \sum_{h=1}^k \sum_{\sigma_h} \mathcal{D}_{N, \sigma_h} V^h(f_{\sigma_h}),$$

for functions  $f$  of bounded variation in the sense of Hardy and Krause, and

$$(170) \quad \delta_N(f) \leq \sum_{h=1}^k \sum_{\sigma_h} \mathcal{T}_{N, \sigma_h} W^h(f_{\sigma_h}),$$

where

$$(171) \quad W^h(f_{\sigma_h}) = \left( \int_{U^h} |D_{\sigma_h}^h f_{\sigma_h}|^2 d_{\sigma_h}^h \mathbf{z} \right)^{1/2},$$

with  $d_{\sigma_h}^h \mathbf{z}$  denoting the product of the  $dz_i$  selected by  $\sigma_h$  and  $D_{\sigma_h}^h$  denoting partial differentiation, once each, with respect to each of these same  $z_i$ . Thus (170) holds

for functions with all  $D_{\sigma_h}^k f_{\sigma_h}$  bounded in quadratic mean (it suffices that  $D_{z_1 z_2 \dots z_k}^k f$  be bounded in  $U^k$ ).

The aforementioned investigations of the discrepancies of sequences are clearly very important to these criteria of the accuracy of *quasi-Monte-Carlo* estimates, and it is interesting to seek sequences with the *smallest possible discrepancies*. A theorem of Roth [220] improving on investigations of van der Corput [244] and Mrs. van Aardenne-Ehrenfest states, in our notation, that, for any  $k \geq 2$ , there is a constant  $c_k$  such that, for any sequence  $\Xi$  in  $U^k$  and any integer  $N > 1$ ,

$$(172) \quad \mathcal{T}_N > c_k N^{-1} (\log N)^{(k-1)/2}.$$

Davenport [221] proved, for  $k = 2$  only, that (172) was optimal, in the sense that it is false if  $c_k$  is made too large, even for arbitrarily large  $N$ . (The same question for  $k > 2$  is unsolved.) Using an idea of van der Corput [244], Roth showed how a two-dimensional sequence could be constructed, for which  $\mathcal{D}_N < CN^{-1} \log N$ , for a suitable constant  $C$ , and since  $\mathcal{T}_N \leq \mathcal{D}_N$ , this yields an upper bound for  $\mathcal{T}_N$  (for this particular sequence), corresponding to the lower bound  $c_2 N^{-1} (\log N)^{1/2}$  from (172). On the basis of a suggestion of Hammersley [30], Halton [230] generalized Roth's sequence to  $k$  dimensions and obtained analogous upper bounds. These sequences are all based on the *radical-inverse* function: any nonnegative integer  $n$  is uniquely expressible to base (or *radix*)  $R$  (an arbitrary integer) as

$$(173) \quad n \equiv (n_M n_{M-1} \dots n_2 n_1 n_0)_R = n_0 + n_1 R + n_2 R^2 + \dots + n_M R^M,$$

where each *digit*  $n_i = 0, 1, 2, \dots$  or  $R - 1$ ,  $n_M \neq 0$ ,  $M = [\log_R n]$ . By reflecting the digits in the *radical point* we obtain a unique fraction

$$(174) \quad \phi_R(n) \equiv (0 \cdot n_0 n_1 n_2 \dots n_M)_R = n_0 R^{-1} + n_1 R^{-2} + n_2 R^{-3} + \dots + n_M R^{-M-1},$$

the *R-inverse* of  $n$ , and clearly

$$(175) \quad 0 \leq \phi_R(n) < 1.$$

*Van der Corput's sequence* is now expressible as

$$(176) \quad \Xi_{\text{van der Corput}} = [\phi_2(n)]_{n=0}^{2^M-1}$$

and *Roth's sequence* is

$$(177) \quad \Xi_{\text{Roth}} = [(n/2^M, \phi_2(n))]_{n=0}^{2^M-1},$$

so that it consists of the set of points

$$(178) \quad \left\{ \left( \frac{t_1}{2} + \frac{t_2}{2^2} + \dots + \frac{t_M}{2^M}, \frac{t_M}{2} + \frac{t_{M-1}}{2^2} + \dots + \frac{t_1}{2^M} \right) : \text{for all } i, t_i = 0 \text{ or } 1 \right\}.$$

*Hammersley's sequence* is

$$(179) \quad \Xi_{\text{Hammersley}} = [(n/N, \phi_{R_2}(n), \phi_{R_3}(n), \dots, \phi_{R_k}(n))]_{n=0}^{N-1},$$

with  $R_2 = 2, R_3 = 3, R_4 = 5, \dots$ , successive primes. Halton [230] generalized this to having the  $R_i$  all pairwise relatively prime, but not necessarily prime numbers, and proposed the similar sequence

$$(180) \quad \Xi_{\text{Halton}} = [(\phi_{R_1}(n), \phi_{R_2}(n), \phi_{R_3}(n), \dots, \phi_{R_k}(n))]_{n=0}^{\infty},$$

for which  $N$  need not be preassigned. He proved that constants  $B_k$  and  $C_k$  exist, such that

$$(181) \quad \begin{aligned} \mathcal{D}_N(\Xi_{\text{Hammersley}}) &< C_{k-1}N^{-1}(\log N)^{k-1}, & \mathcal{D}_N(\Xi_{\text{Halton}}) &< C_kN^{-1}(\log N)^k, \\ \mathcal{T}_N(\Xi_{\text{Hammersley}}) &< B_{k-1}N^{-1}(\log N)^{k-1}, & \mathcal{T}_N(\Xi_{\text{Halton}}) &< B_kN^{-1}(\log N)^k. \end{aligned}$$

The gap between the upper bounds (181) and Roth's lower bound (172) has been the subject of conjectures, and partial answers were provided by Gabai [231] and Haber [232] for the cases  $k = 1, 2$  (van der Corput and Roth sequences). Halton and Zaremba [233] have obtained the most complete answers to date, for the Roth sequence and a modification of it due to Zaremba. *Zaremba's sequence* consists of the set of points (compare (178))

$$(182) \quad \left\{ \left( \frac{t'_1}{2} + \frac{t'_2}{2^2} + \cdots + \frac{t'_M}{2^M}, \frac{t_M}{2} + \frac{t_{M-1}}{2^2} + \cdots + \frac{t_1}{2^M} \right) : \right. \\ \left. \text{for all } i, t_i = 0 \text{ or } 1, t'_i = \frac{1}{2} + (-1)^i \left( t_i - \frac{1}{2} \right) \right\}$$

(i.e.,  $t'_i = t_i$  if  $i$  is even,  $t'_i = 1 - t_i$  if  $i$  is odd). For Roth's sequence, they have proved that, when  $N = 2^M$ ,

$$(183) \quad \mathcal{M}_N = 0, \quad \mathcal{N}_N = \frac{1}{3}MN^{-1} + \frac{13}{9}N^{-1} - \frac{4}{9}s_M N^{-2},$$

the maximum being attained at the two points

$$(184) \quad \left( \frac{3}{4} + \frac{1}{12}s_M s_0 + \frac{2}{3}s_0 N^{-1}, \frac{3}{4} + \frac{1}{12}s_0 + \frac{2}{3}s_M s_0 N^{-1} \right),$$

where

$$(185) \quad s_M = (-1)^M, \quad s_0 = \pm 1.$$

(The only exceptions are: (i)  $\mathcal{N}_2 = \frac{1}{2}$  at  $(\frac{1}{2}, \frac{1}{2})$ ; (ii)  $\mathcal{N}_4$  occurs at  $(\frac{1}{2}, \frac{1}{2})$  only; (iii)  $\mathcal{N}_8$  occurs at  $(\frac{3}{4}, \frac{3}{4})$  only.) Thus, for  $N = 2^M$  and  $M \geq 2$ ,

$$(186) \quad \mathcal{D}_N(\Xi_{\text{Roth}}) = \frac{1}{3}MN^{-1} + \frac{13}{9}N^{-1} - \frac{4}{9}s_M N^{-2}.$$

Also, they have shown that

$$(187) \quad \mathcal{T}_N(\Xi_{\text{Roth}}) = \left( \frac{1}{64}M^2 + \frac{29}{192}M + \frac{3}{8} - \frac{1}{16}MN^{-1} + \frac{1}{4}N^{-1} - \frac{1}{72}N^{-2} \right)^{1/2} N^{-1}.$$

The exact results give

$$(188) \quad \mathcal{D}_N \sim \frac{1}{3}N^{-1} \log_2 N, \quad \mathcal{T}_N \sim \frac{1}{8}N^{-1} \log_2 N,$$

which agrees with the upper bound given by Roth [220] and Halton [230], rather than with Roth's absolute lower bound (172). For Zaremba's sequence, however, the situation is a little different. The exact results obtained by Halton and Zaremba

for  $N = 2^M$  are:

$$(189) \quad \mathcal{M}_N = \frac{1}{5}MN^{-1} + \left( \frac{9}{50} - \frac{1}{10}s_M \right)N^{-1} + \frac{1}{25}(-1)^{(2M-3-s_M)/4} \left( \frac{3}{2} + \frac{1}{2}s_M \right)N^{-2},$$

attained at two points,

$$\left( \frac{2}{5} + \frac{1}{5}N^{-1}, \frac{2}{5} + \frac{1}{5}N^{-1} \right) \text{ and } \left( \frac{3}{5} - \frac{1}{5}N^{-1}, \frac{3}{5} - \frac{1}{5}N^{-1} \right) \text{ if } M = 4m + 1,$$

(190a)

$$\left( \frac{2}{5} - \frac{1}{5}N^{-1}, \frac{3}{5} + \frac{1}{5}N^{-1} \right) \text{ and } \left( \frac{3}{5} + \frac{1}{5}N^{-1}, \frac{2}{5} - \frac{1}{5}N^{-1} \right) \text{ if } M = 4m + 3,$$

and at four points,

$$\left( \frac{9}{20} + \frac{1}{4}s_0 + \frac{1}{5}N^{-1}, \frac{2}{5} + \frac{2}{5}N^{-1} \right) \text{ and } \left( \frac{11}{20} + \frac{1}{4}s_0 - \frac{1}{5}N^{-1}, \frac{3}{5} - \frac{2}{5}N^{-1} \right)$$

(190b) if  $M = 4m + 2$ ,

$$\left( \frac{9}{20} + \frac{1}{4}s_0 - \frac{1}{5}N^{-1}, \frac{3}{5} + \frac{2}{5}N^{-1} \right) \text{ and } \left( \frac{11}{20} + \frac{1}{4}s_0 + \frac{1}{5}N^{-1}, \frac{2}{5} - \frac{2}{5}N^{-1} \right)$$

if  $M = 4m + 4$ .

(The only exceptions are: (i)  $\mathcal{M}_2$  occurs at  $(\frac{1}{2}, \frac{1}{2})$  only; (ii)  $\mathcal{M}_4$  occurs at  $(\frac{1}{4}, \frac{1}{2})$  and  $(\frac{3}{4}, \frac{1}{2})$  only.) Also, they proved that, when  $M = 2m$ ,

$$(191) \quad \mathcal{N}_N = \frac{1}{5}MN^{-1} + \frac{37}{25}N^{-1} - \frac{12}{25}s_mN^{-2},$$

attained at two points

$$(192) \quad \left( \frac{3}{4} + \frac{1}{8}s_0 - \frac{1}{40}s_m - \frac{3}{5}N^{-1}, \frac{4}{5} - \frac{4}{5}s_mN^{-1} \right);$$

while, when  $M = 2m + 1$ ,

$$(193) \quad \mathcal{N}_N = \frac{1}{5}MN^{-1} + \left( \frac{587}{400} + \frac{1}{80}s_m \right)N^{-1} + \left( \frac{3}{5} - \frac{24}{25}s_m \right)N^{-2},$$

attained at every point whose coordinates are (in either order)

$$(194) \quad \frac{13}{16} - \frac{1}{80}s_m - \frac{3}{5}N^{-1} \text{ and } \frac{4}{5} + \left( 1 - \frac{8}{5}s_m \right)N^{-1}.$$

These coordinates are equal if  $m$  is even ( $s_m = 1$ ) or if  $m = 3$ ,  $M = 7$ ,  $N = 128$ , giving a single maximum; otherwise there are two maxima. (The only exception to (191) and (192) is:  $\mathcal{N}_4 = 7/16$  at  $(\frac{3}{4}, \frac{3}{4})$ . The only exceptions to (193) and (194) for  $M \leq 17$  are: (i)  $\mathcal{N}_2 = \frac{3}{4}$  at  $(\frac{1}{2}, \frac{1}{2})$ ; (ii)  $\mathcal{N}_8 = 15/64$  at  $(\frac{5}{8}, \frac{5}{8})$  and  $(\frac{7}{8}, \frac{7}{8})$ .) Thus, for  $N = 2^M$  and  $M \geq 4$ ,

$$(195) \quad \mathcal{D}_N(\Xi_{Zaremba}) = \frac{1}{5}MN^{-1} + \left( \frac{37}{25} - \frac{1}{40}v_M \right)N^{-1} + \frac{3}{25}w_MN^{-2},$$

where

$$(196) \quad v_M = \begin{cases} 1 & \text{if } M \equiv 3 \pmod{4}, \\ 0 & \text{otherwise;} \end{cases}$$

while

$$(197a) \quad w_M = -4, -3, +4, +13,$$

according as

$$(197b) \quad M \equiv 0, 1, 2, 3 \pmod{4},$$

respectively. Finally Halton and Zaremba have proved that

$$(198) \quad \mathcal{T}_N(\Xi_{\text{Zaremba}}) = \left[ \frac{5}{192}M + \left( \frac{41}{128} + \frac{7}{128}s_M \right) \right. \\ \left. + \left( \frac{9}{32} - \frac{1}{32}s_M \right) N^{-1} - \frac{1}{72}N^{-2} \right]^{1/2} N^{-1}.$$

These exact results give

$$(199) \quad \mathcal{D}_N \sim \frac{1}{5}N^{-1} \log_2 N, \quad \mathcal{T}_N \sim \frac{1}{8}\left(\frac{5}{3}\right)^{1/2} N^{-1}(\log_2 N)^{1/2},$$

and though  $\mathcal{D}_N$  still adheres to the upper bound of both Roth and Halton, we see that  $\mathcal{T}_N$  has the behavior of Roth's lower bound (172).

In [15], Zaremba obtained some bounds for the extreme discrepancy  $\mathcal{D}_P$  of the sequence  $[(\{r/P\}, \{rg/P\})]_{r=0}^{P-1}$  (see (158)): he shows that

$$(200) \quad \mathcal{D}_P < 4A \left( \frac{\log(A+1)P}{P \log(A+1)} \right) + \frac{1}{P},$$

where  $A$  is defined as before; and when  $g = F_{n-1}$  or  $F_{n-2}$  and  $P = F_n$ ,

$$(201) \quad \mathcal{D}_P < \left[ \frac{7}{6} \log(6F_n) + 1 \right] / F_n \sim \frac{7}{6} \log P / P.$$

He also proved the following useful general result: if  $\Xi = [\zeta_n]_{n=0}^{\infty}$  is any sequence in  $U$  and  $D_{v,N}$  denotes the extreme discrepancy of the subsequence  $[\zeta_n]_{n=v}^{v+N-1}$  and if a constant  $d$  exists, such that for every  $v$  and every  $N \leq P$ , we have

$$(202) \quad D_{v,N} \leq d/N;$$

then, for the sequence  $[(n/P, \zeta_n)]_{n=0}^{P-1}$  in  $U^2$ ,

$$(203) \quad \mathcal{D}_P \leq (d+1)/P.$$

It is clear, from the foregoing results, that sequences with satisfactorily low discrepancies can be found, and that such sequences will be useful as quasirandom sequences for integrating functions which are, at least, of bounded variation in the sense of Hardy and Krause in the unit hypercube  $U^k$ . Of course, this can be extended to integrals in regions which are easily transformed into  $U^k$ ; but the condition of bounded variation is not trivial. For example, one might be tempted to apply the error bound (169) or (170) to an integral of a well-behaved function in an

oval-shaped region  $R$ , by enclosing  $R$  in a unit cube  $U^k$  (with a trivial rescaling, if necessary) and defining a new integrand equal to the old one in  $R$ , and to zero outside  $R$ . However, this function will generally have its  $k$ -dimensional total variation infinite. Indeed, Hlawka [13] was only able to obtain an error bound for  $\delta_N(f)$  of the order of  $\mathcal{D}_N^{1/k}$ , and Zaremba [53], [238] was able to show a simple case, of a function equal to 1 on one side of an oblique hyperplane crossing  $U^k$ , and 0 on the other side, for which the sequence of points  $\{\{ng_i/P\}\}_{i=1}^k$ ,  $n = 0, 1, 2, \dots, P - 1$ , gave an error of at least  $1/(2(4k)^{k-1}P^{1/k})$ , which is worse than the expected random error,  $O(P^{-1/2})$ . Thus problems of great significance still remain.

### 3. Prospect.

**3.1. General discussion.** Like numerical analysis in general, the study of the Monte Carlo method has produced a bewildering hodge-podge of specialized techniques; and it is only recently that certain underlying structures and regularities have begun to emerge. Although any proposal for future work necessarily suffers from our ignorance of results yet to be obtained, certain general guidelines have become apparent.

First, it is clear that the subject is splitting into two distinct fields of study. On the one hand, there is the study of the *Monte Carlo method proper* as a branch of *probability theory*, with Monte Carlo processes forming a class of *convergent stochastic processes* [3], [77], [240], [242]. On the other hand, recent investigations of the behavior of pseudorandom and quasirandom sequences have opened up the study of the *quasi-Monte-Carlo method* as a branch of *numerical analysis*, concerned principally with certain *multidimensional quadrature formulas* [10], [13], [15], [53], [176], [212], [220], [230], [232], [233], [235]–[239]. Because of difficulties inherent in both of these approaches, it would seem that both will continue to be studied, at least as heuristic guides, and neither should be neglected in the pursuit of the other.

A second natural dichotomy of the subject is that into the studies of *Monte Carlo processes* and of *random generators*. As was explained in § 1, a *Monte Carlo procedure* may be thought of as the combination of a process  $\Phi$  with a generator  $\Omega$ ; and there is ample room for new developments in both areas, as much in ad hoc techniques as in general principles.

The Monte Carlo method was developed for use on large electronic digital computers, and although it can be applied to pencil and paper calculations [27], [111], its exponents have always worked close to computers, both in judging the usefulness of their techniques and in developing the theory of their subject. The study of the Monte Carlo method is one of the best examples of the *creative use of computers as a research tool*, and it is to be hoped and expected that future work will be in the same spirit. Incidentally, the study of the Monte Carlo method draws on an extremely broad range of mathematical disciplines, from probability theory to number theory, and from mathematical analysis to numerical analysis; so that it constitutes an excellent training ground for researchers in computer science and applied mathematics.

Trotter and Tukey said in 1954 [47] that “the only good Monte Carlos are dead Monte Carlos;” and indeed it seems that whenever randomness can be

avoided, a better answer is obtained. This is the basis of the quasi-Monte-Carlo method, and of all the methods of systematic sampling (stratified sampling, antithetic variates [38]–[44]) and sequential sampling [5], [6], [78]. It appears therefore, that classical, deterministic numerical methods will ever be stepping on the heels of Monte Carlo techniques; but there will always be problems too large for the systematic treatments, and it is for these that we should try to develop the Monte Carlo method. It may be that, one day, deterministic numerical techniques will become so powerful that they will be able to handle any problem to which the Monte Carlo method is suited; but that day is not yet in sight; and meanwhile, the Monte Carlo method will continue to be used and developed, and we shall learn a great deal in the process.

**3.2. Monte Carlo processes as stochastic processes.** The Monte Carlo method was originally invented as a statistical method [4], [17], [19]–[26], [29], [32], [33], [51]; and the recent work of Halton [3]–[6], [9], [77] has defined Monte Carlo processes as a class of stochastic processes  $\Phi = [\phi_m]_m$  converging to the constant  $\theta$  in a suitable manner. The definition allows  $\theta$  and the  $\phi_m$  to range in the Fréchet space defined in (14)–(17) of § 1; and more recent work has extended the solution space  $H$  to be any *separable Fréchet space* [240]. The points of such a space can be shown to be represented by sequences

$$(204) \quad \mathbf{x} = [x_n]_n = [x_1, x_2, x_3, \dots],$$

where, for each  $n$ ,  $x_n$  is an element of a *separable Banach space*  $X_n$ . The topology of  $H$  is then that induced by the metric (16), where

$$(205) \quad Q(\mathbf{x}) = \sum_{n=1}^{\infty} c_n \|x_n\|_n / (1 + \|x_n\|_n),$$

with all  $c_n > 0$ ,  $\sum_n c_n < \infty$ , and  $\|\cdots\|_n$  denoting the norm of the space  $X_n$ . Convergence in  $H$  is then equivalent to convergence in each component space  $X_n$ , and  $\phi$  is a random variable in  $H$  if and only if each corresponding component function  $f_n$  is a random variable in  $X_n$ . Since the theory of random variables in separable Banach spaces is relatively well understood, the theory can readily be extended to general separable Fréchet spaces, and most of the important convergence theorems will go through. Such a theory should be developed, in order to obtain a global treatment of the Monte Carlo solution of problems in which the solution takes the form of a function, with an inhomogeneous cost function for errors. Some work on the convergence of linear averages has already been done [242].

The theory is likely to have an application in the field of *pattern recognition*, where each sample pattern may be thought of as a Monte Carlo estimate of an idealized pattern.

The theory will also relate to that of *random equations*, and this relationship should be investigated.

**3.3. Analysis of the quasi-Monte-Carlo method.** The theory of the quasi-Monte-Carlo method, as it applies to integration in  $k$ -dimensional unit hypercubes  $U^k$ , has been studied a little, notably by Koksmo [10], Hlawka [13], [14],

and Zaremba [15], [53], [238], [239]. The theory of other quasi-Monte-Carlo techniques is nonexistent, and it is clearly desirable that it should be developed.

Concomitant with this is the theory of *quasirandom sequences*. This, too, is in its infancy [15], [53], [176], [212], [220], [230], [232], [233], and it is important that a big effort be made to obtain values, or at least bounds, for the *discrepancies* ( $L^\infty$  and  $L^2$ ) of known pseudorandom and quasirandom sequences. Such studies should lead into a search for better quasirandom sequences.

Eventually, it should be possible to construct optimal quasirandom sequences, given a definition of the class of problems to be solved with their aid.

Connected with this question is that of interpreting the meaning of statistical test parameters, when they are computed for deterministic, quasirandom sequences of points.

Again, it is of interest to inquire whether a statistical theory of quasi-Monte-Carlo calculations might not be possible, in which one *averaged*, not over random sequences, but over *classes of problems*.

**3.4. Monte Carlo techniques.** Although much has already been achieved in developing special Monte Carlo techniques for solving particular problems, a great deal remains to be done. Existing techniques should be reexamined for possible improvements or new applications.

The development of techniques for the generalized Monte Carlo processes has hardly begun (see Frolov and Chentsov [2]), and the same is true of combinatorial problems (see Page [109]). Little has been done in *random search* and optimization techniques [109], [111], [137]–[140], and there is clearly much to be discovered here. Nothing of note has been done to apply the Monte Carlo ideas to *nonlinear problems*, except in cases of direct simulation of stochastic situations: this seems to be a very hard problem.

The general question of designing *optimum estimators* is an open one. Little analysis has been done of nonlinear secondary estimators, even. This question leads into that of developing *sequential Monte Carlo methods* for problems other than linear algebraic equations (see § 2.3). One aspect which is now being examined is the *sequential stratification* of integrals [246].

Importance sampling with *signed probabilities* should be further studied and compared with biased methods such as *weighted uniform sampling* [52]. The *E-Z-H method* [45], [46] also deserves more study. Monte Carlo techniques for multivariable *interpolation and reduction* [30] are yet to be fully developed.

Turning to *linear algebraic equations*, we find a wealth of existing techniques. However, much of the detail remains to be worked out. Among questions to be examined are the best allocation of effort to computing zeroth- and first-level estimators, the adaptation of various types of iterative schemes to second-level Monte Carlo computation, the elaboration of schemes of grid-refinement in continuous problems, together with third-level sequential schemes and the Monte Carlo Gram-Schmidt orthogonalization process. This last process should be further explored for use as a conditioning method for classical computations.

In the study of *eigenvalue problems*, attention should be turned to the use of various accelerated techniques, such as are given by Wilkinson [66], in conjunction with the Monte Carlo method. Further study should also be made of the more subtle methods for Kac, Donsker, Fortet and Wasow [68], [79], [80], [86].

**3.5. Random generators.** Here again, we find a wealth of open questions. First, if we are to perform true Monte Carlo calculations, at least for problems for which no quasi-Monte-Carlo theory is available, we must have *true random generators*; and much improvement of existing designs is required. Together with this engineering problem, there is the statistical one of how best to *test* the output of such generators for randomness.

The problem of generating *arbitrary random sequences* from canonical ones still needs much attention. New techniques, both general and particular should be sought, and especially for generating sequences with complicated joint distributions.

Turning to pseudorandom and quasirandom generators, we must first ask whether it is possible or desirable to have built-in *general purpose* pseudorandom generators at all. If so, surely they should be tested in a much more rational manner than hitherto; and maybe new, improved generators can be found.

Certain auxiliary questions arise. The effect of replacing continuous random generators  $\Lambda$  by *discrete* generators  $\Lambda_D$  should be more closely examined. Also [245], it has been pointed out that *sample variances* are not of much use as estimators of the error in a pseudo-or quasi-Monte-Carlo scheme. Better estimators must be found.

Finally, we return to the problems connected with *quasirandom generators*, which have already been described in § 3.3.

**3.6. Summary.** In §§ 3.2–3.5 above, we have briefly discussed the most likely developments in Monte Carlo research in the future. This discussion is best summarized by posing a number of questions, which we hope that future work will answer.

- (i) Can we obtain a theory of convergence, with weak and strong laws of large numbers, for random variables taking their values in separable Fréchet spaces?
- (ii) Can the study of Monte Carlo estimates in separable Fréchet spaces give a theory of global approximation for problems whose solutions are functions in such spaces, and are there useful applications of such a theory?
- (iii) When sampling functions, what constitutes a representative sample of function values? If the points at which the function is evaluated are themselves random, how does this affect the behavior of the estimates obtained?
- (iv) Can one apply the generalized Monte Carlo theory to pattern recognition problems?
- (v) Relate the generalized Monte Carlo theory to the theory of random equations.
- (vi) What can be said about quasi-Monte-Carlo estimates for finite-dimensional integrals in general classes of domains, and for countable or uncountable infinite-dimensional problems, such as random-walk averages and Wiener integrals?
- (vii) Obtain expressions, asymptotic forms, or at least upper bounds for the  $L^2$ - and  $L^\infty$ -discrepancies of quasirandom sequences in general use. Failing this, give computational results on these discrepancies, and develop programs to determine them for arbitrary sequences.

- (viii) How should one set about constructing or improving quasirandom sequences? Are there best possible quasirandom sequences, in any sense?
- (ix) How are we to interpret the results of the standard statistical tests, when they are applied to pseudorandom or quasirandom sequences? What is their relevance?
- (x) Can we develop a meaningful statistical theory of quasi-Monte-Carlo estimates, based on sampling from populations of problems?
- (xi) Can existing Monte Carlo techniques be improved, extended, or elaborated? Can we find better variance reducing techniques? Can we apply the Monte Carlo method to new classes of problems; such as nonlinear problems, combinatorial problems, random search, optimization?
- (xii) Can the design of Monte Carlo estimators be made more systematic and aimed at an optimization procedure?
- (xiii) How can the idea of sequential Monte Carlo be extended, for example, to stratified sampling and to the computation of eigenvalues?
- (xiv) Can sampling with signed probabilities be made practical?
- (xv) What is the best allocation of effort in obtaining zeroth- and first-level estimators in linear algebraic problems?
- (xvi) Examine the Monte Carlo analogues of the various matrix iterative schemes.
- (xvii) Develop the schemes of grid refinement in continuous problems and Monte Carlo Gram-Schmidt orthogonalization, both in Monte Carlo computations and in general matrix-calculations. Can the latter be made the basis of a technique for improving ill-conditioned systems?
- (xviii) Develop new Monte Carlo eigenvalue and eigenvector techniques.
- (xix) Develop fast, reliable true canonical random generators.
- (xx) How is the output of a true random generator to be tested?
- (xxi) Develop fast, efficient methods for generating arbitrary random variables and random sequences.
- (xxii) Can we have really useful general purpose pseudorandom sequences? If so, find some new, better ones.
- (xxiii) What is the effect of the discreteness of digital computers on the results of Monte Carlo calculations? What is the effect of using discrete random generators  $\Lambda_D$  instead of continuous generators  $\Lambda$ ?
- (xxiv) Since sample variances give us little information, is there a way of estimating the accuracy of quasi-Monte-Carlo estimates?

#### REFERENCES

- [1] B. V. GNEDENKO, *The Theory of Probability*, Chelsea, New York, 1962.
- [2] A. S. FROLOV AND N. N. CHENTSOV, *Use of dependent tests in the Monte Carlo method for obtaining smooth curves*, Proc. Sixth All-Union Conf. Theor. Prob. Math. Stat., Vilna, Lithuania, 1960, pp. 425–437.
- [3] J. H. HALTON, *A general formulation of the Monte Carlo method and “strong laws” for certain sequential schemes*, MRC Tech. Summary Rep. 690, Mathematics Research Center, University of Wisconsin, Madison, 1966.
- [4] ———, *The Monte Carlo Method*, Pruet Press, Boulder, Colorado, to appear.
- [5] ———, *Studies in the theory of the Monte Carlo method*, Doctoral thesis, Oxford University, 1960.
- [6] ———, *Sequential Monte Carlo*, Proc. Cambridge Philos. Soc., 58 (1962), pp. 57–78; revised in [78].

- [7] W. J. PERVIN, *Foundations of General Topology*, Academic Press, New York, 1964.
- [8] W. SIERPIŃSKI, *General Topology*, University of Toronto Press, Toronto, Ontario, 1956.
- [9] J. H. HALTON, *On the generation of random sequences in Fréchet spaces*, Rep. AMD 374/BNL 8996, Brookhaven National Laboratory, Upton, N.Y., 1965; reprinted in [4].
- [10] J. F. KOKSMA, *A general theorem from the theory of uniform distribution modulo 1*, Mathematika Zutphen, B11 (1942), pp. 7–11. (In Dutch.)
- [11] J. P. BERTRANDIAS, *Calculation of an integral by means of the sequence  $X_n = An$ . Evaluation of the error*, Publ. Inst. Statist. Univ. Paris, 9 (1960), pp. 335–357.
- [12] C. B. HASELGROVE, *A method for numerical integration*, Math. Comp., 15 (1961), pp. 323–337.
- [13] E. HLAWKA, *Functions of bounded variation in the theory of uniform distribution*, Ann. Mat. Pura Appl., IV:54 (1961), pp. 325–334. (In German.)
- [14] ———, *On the approximate computation of multiple integrals*, Monatsh. Math., 66 (1962), pp. 140–151.
- [15] S. K. ZAREMBA, *Good lattice points, discrepancy, and numerical integration*, Ann. Mat. Pura Appl., IV:73 (1966), pp. 293–317.
- [16] J. M. HAMMERSLEY AND K. W. MORTON, *Discussion, R. S. S. symposium on Monte Carlo methods*, J. Roy. Statist. Soc. Ser. B, 16 (1954), pp. 61–75; reprinted in [4].
- [17] J. M. HAMMERSLEY AND D. C. HANDSCOMB, *Monte Carlo Methods*, Methuen, London, 1964.
- [18] J. H. CURTISS, *Sampling methods applied to differential and difference equations*, Seminar on Scientific Computation, I.B.M. Corp., New York, 1949, pp. 87–109; reprinted in [4].
- [19] LORD RAYLEIGH, *On James Bernoulli's theorem in probabilities*, Philos. Mag., 47 (1899), pp. 246–251.
- [20] “STUDENT”, *Probable error of a correlation coefficient*, Biometrika, 6 (1908), pp. 302–310.
- [21] R. COURANT, K. O. FRIEDRICHHS AND H. LEWY, *On the partial difference equations of mathematical physics*, Math. Ann., 100 (1928), pp. 32–74; English transl., Courant Institute of Mathematical Sciences, New York University, 1956.
- [22] A. N. KOLMOGOROV, *On the analytic method in probability theory*, Math. Ann., 104 (1931), pp. 415–458.
- [23] G. PÓLYA, *On a random walk in a network of streets*, Colloque consacré à la théorie des probabilités. I: Conférences d'introduction, Actualités scientifiques et industrielles, no. 734, Hermann, Paris, 1938, pp. 25–44.
- [24] N. METROPOLIS AND S. M. ULAM, *The Monte Carlo method*, J. Amer. Statist. Assoc., 44 (1949), pp. 335–341; reprinted in [4].
- [25] S. M. ULAM, *On the Monte Carlo method*, Proc. Second Symposium on Large-Scale Digital Calculating Machinery, Harvard University Press, Cambridge, Massachusetts, 1951, pp. 207–212; reprinted in [4].
- [26] G. W. KING, *The Monte Carlo method as a natural mode of expression in operations research*, J. Operations Res. Soc. Amer., 1 (1953), pp. 46–51; reprinted in [4].
- [27] J. M. HAMMERSLEY AND K. W. MORTON, *Poor man's Monte Carlo*, J. Roy. Statist. Soc. Ser. B, 16 (1954), pp. 23–38; reprinted in [4].
- [28] K. D. TOCHER, *The application of automatic computers to sampling experiments*, Ibid., 16 (1954), pp. 39–61; reprinted in [4].
- [29] W. F. BAUER, *The Monte Carlo method*, J. Soc. Indust. Appl. Math., 6 (1958), pp. 438–451; reprinted in [4].
- [30] J. M. HAMMERSLEY, *Monte Carlo methods for solving multivariable problems*, Ann. New York Acad. Sci., 86 (1960), pp. 844–874; reprinted in [4].
- [31] H. KAHN, *Applications of Monte Carlo*, Rep. RM 1237-AEC, RAND Corp., Santa Monica, California, 1956.
- [32] H. A. MEYER, ed., *Symposium on Monte Carlo Methods*, John Wiley, New York, 1956.
- [33] YU. A. SHREIDER, ed., *Method of Statistical Testing (Monte Carlo Method)*, Elsevier, Amsterdam, 1964.
- [34] R. KRAFT AND C. J. WENSRICH, *Monte Carlo methods—A bibliography covering the period 1947 to June 1961*, Rep. UCRL 6581, Lawrence Radiation Laboratory, University of California, Berkeley, 1961.
- [35] J. H. HALTON, *On the relative merits of correlated and importance sampling for Monte Carlo integration*, Proc. Cambridge Philos. Soc., 61 (1965), pp. 497–498; reprinted in [4].
- [36] ———, *An interpretation of negative probabilities*, Ibid., 62 (1966), pp. 83–86; reprinted in [4].
- [37] M. S. BARTLETT, *Negative probability*, Ibid., 41 (1945), pp. 71–73.

- [38] J. M. HAMMERSLEY AND K. W. MORTON, *A new Monte Carlo technique: antithetic variates*, *Ibid.*, 52 (1956), pp. 449–475; reprinted in [4].
- [39] J. M. HAMMERSLEY AND J. G. MAULDON, *General principles of antithetic variates*, *Ibid.*, 52 (1956), pp. 476–481; reprinted in [4].
- [40] D. C. HANDSCOMB, *Proof of the antithetic variate theorem for  $n > 2$* , *Ibid.*, 54 (1958), pp. 300–301; reprinted in [4].
- [41] K. W. MORTON, *A generalization of the antithetic variate technique for evaluating integrals*, *J. Math. Phys.*, 36 (1957), pp. 289–293; reprinted in [4].
- [42] J. H. HALTON AND D. C. HANDSCOMB, *A method for increasing the efficiency of Monte Carlo integration*, *J. Assoc. Comput. Mach.*, 4 (1957), pp. 329–340; reprinted in [4].
- [43] D. C. HANDSCOMB, *A rigorous lower bound for the efficiency of Monte Carlo integration*, *Proc. Cambridge Philos. Soc.*, 60 (1964), pp. 357–358; reprinted in [4].
- [44] P. J. LAURENT, *Remark on the evaluation of integrals by the Monte Carlo method*, *C.R. Acad. Sci. Paris*, 253 (1961), pp. 610–612.
- [45] S. M. ERMakov AND V. G. ZOLOTUKHIN, *Polynomial approximations and the Monte Carlo method*, *Teor. Veroyatnost. i Primenen.*, 5 (1960), pp. 473–476. (English summary.)
- [46] D. C. HANDSCOMB, *Remarks on a Monte Carlo integration method*, *Numer. Math.*, 6 (1964), pp. 261–268; reprinted in [4].
- [47] H. F. TROTTER AND J. W. TUKEY, *Conditional Monte Carlo for normal samples*, *Symposium on Monte Carlo Methods* (University of Florida, 1954), H. A. Meyer, ed., John Wiley, New York, 1956, pp. 64–79.
- [48] H. J. ARNOLD, B. D. BUCHER, H. F. TROTTER AND J. W. TUKEY, *Monte Carlo techniques in a complex problem about normal samples*, *Symposium on Monte Carlo Methods* (University of Florida, 1954), H. A. Meyer, ed., John Wiley, New York, 1956, pp. 80–88.
- [49] J. M. HAMMERSLEY, *Conditional Monte Carlo*, *J. Assoc. Comput. Mach.*, 3 (1956), pp. 73–76; reprinted in [4].
- [50] J. G. WENDEL, *Groups and conditional Monte Carlo*, *Ann. Math. Statist.*, 28 (1957), pp. 1048–1052; reprinted in [4].
- [51] YU. A. SHREIDER, ed., *The Monte Carlo Method (The Method of Statistical Trials)*, Pergamon Press, Oxford, 1966.
- [52] M. J. D. POWELL AND J. SWANN, *Weighted uniform sampling—a Monte Carlo technique for reducing variance*, *J. Inst. Math. Appl.*, 2 (1966), pp. 228–236.
- [53] S. K. ZAREMBA, *The mathematical basis of Monte Carlo and quasi-Monte Carlo methods*, this Review, 10 (1968), pp. 303–314; reprinted in [4].
- [54] R. E. EDWARDS, *Functional Analysis: Theory and Applications*, Holt, Rinehart & Winston, New York, 1965.
- [55] L. V. KANTOROVICH AND G. P. AKILOV, *Functional Analysis in Normed Spaces*, Pergamon Press, New York, 1964.
- [56] K. YOSIDA, *Functional Analysis*, Springer-Verlag, Heidelberg, 1965.
- [57] M. MARCUS AND H. MINC, *A Survey of Matrix Theory and Matrix Inequalities*, Allyn & Bacon, Boston, 1964.
- [58] L. MIRSKY, *An Introduction to Linear Algebra*, Clarendon Press, Oxford, 1955.
- [59] P. M. ANSELONE, *Convergence and error bounds for approximate solutions of integral and operator equations*, *Error in Digital Computation*, vol. 2, L. B. Rall, ed., John Wiley, New York, 1965.
- [60] K. E. ATKINSON, *Extensions of the Nyström method for the numerical solution of linear integral equations of the second kind*, MRC Tech. Summary Rep. 686, Mathematics Research Center, University of Wisconsin, Madison, 1966.
- [61] J. H. HALTON, *Least-squares Monte Carlo methods for solving linear systems of equations*, Rep. AMD 388/BNL 9678, Brookhaven National Laboratory, Upton, New York, 1965.
- [62] G. E. FORSYTHE AND C. B. MOLER, *Computer Solution of Linear Algebraic Systems*, Prentice-Hall, Englewood Cliffs, New Jersey, 1967.
- [63] A. S. HOUSEHOLDER, *The Theory of Matrices in Numerical Analysis*, Blaisdell, New York, 1964.
- [64] R. S. VARGA, *Matrix Iterative Analysis*, Prentice-Hall, Englewood Cliffs, New Jersey, 1962.
- [65] J. H. WILKINSON, *Rounding Errors in Algebraic Processes*, Prentice-Hall, Englewood Cliffs, New Jersey, and H.M. Stationery Office, London, 1963.
- [66] ———, *The Algebraic Eigenvalue Problem*, Clarendon Press, Oxford, 1965.

- [67] G. E. FORSYTHE AND R. A. LEIBLER, *Matrix inversion by a Monte Carlo method*, Math. Tables Aids Comput., 4 (1950), pp. 127–129; 5 (1951), p. 55; reprinted in [4].
- [68] W. R. WASOW, *Random walks and the eigenvalues of elliptic difference-equations*, J. Res. Nat. Bur. Standards, 46 (1951), pp. 65–73; reprinted in [4].
- [69] ———, *A note on the inversion of matrices by random walks*, Math. Tables Aids Comput., 6 (1952), pp. 78–81; reprinted in [4].
- [70] H. P. EDMUNDSON, *Monte Carlo matrix inversion and recurrent events*, Ibid., 7 (1953), pp. 18–21; reprinted in [4].
- [71] J. H. CURTISS, *Monte Carlo methods for the iteration of linear operators*, J. Math. Phys., 32 (1954), pp. 209–232; reprinted in [4].
- [72] R. E. CUTKOSKY, *A Monte Carlo method for solving a class of integral equations*, J. Res. Nat. Bur. Standards, 47 (1951), pp. 113–115; reprinted in [4].
- [73] E. S. PAGE, *The Monte Carlo solution of some integral equations*, Proc. Cambridge Philos. Soc., 50 (1954), pp. 414–425; reprinted in [4].
- [74] A. OPLER, *Monte Carlo matrix calculations with punched card machines*, Math Tables Aids. Comput., 5 (1951), pp. 115–120.
- [75] A. W. MARSHALL, *The use of multi-stage sampling schemes in Monte Carlo computation*, Symposium on Monte Carlo Methods (University of Florida, 1954), H. A. Meyer, ed., John Wiley, New York, 1956, pp. 123–140.
- [76] A. WALD, *Sequential Analysis*, John Wiley, New York, 1950.
- [77] J. H. HALTON, *On the strong convergence of linear averages*, MRC Tech. Summary Rep. 719, Mathematics Research Center, University of Wisconsin, Madison, 1966.
- [78] ———, *Sequential Monte Carlo (revised)*, MRC Tech. Summary Rep. 816, Mathematics Research Center, University of Wisconsin, Madison, 1967; reprinted in [4].
- [79] M. D. DONSKER AND M. KAC, *A sampling method for determining the lowest eigenvalue and the principal eigenfunction of Schrödinger's equation*, J. Res. Nat. Bur. Standards, 44 (1950), pp. 551–557; reprinted in [4].
- [80] M. KAC AND M. COHEN, *A statistical method for determining the lowest eigenvalue of Schrödinger's equation*, Rep. 1553, National Bureau of Standards, Washington, D.C., 1952.
- [81] W. R. WASOW, *On the mean duration of random walks*, J. Res. Nat. Bur. Standards, 46 (1951), pp. 462–471.
- [82] ———, *On the duration of random walks*, Ann. Math. Statist., 22 (1951), pp. 199–216.
- [83] ———, *Probabilistic methods for the numerical solution of some problems in analysis and algebra*, Univ. Roma Ist. Naz. Alta Mat. Rend. Mat. e Appl., 11 (1953), pp. 336–346.
- [84] M. E. MULLER, *Some continuous Monte Carlo methods for the Dirichlet problem*, Ann. Math. Statist., 27 (1956), pp. 569–589.
- [85] ———, *On discrete operators connected with the Dirichlet problem*, J. Math. Phys., 35 (1956), pp. 89–113.
- [86] R. FORTET, *On the estimation of an eigenvalue by an additive functional of a stochastic process, with special reference to the Kac-Donsker method*, J. Res. Nat. Bur. Standards, 48 (1952), pp. 68–75; reprinted in [4].
- [87] N. R. STEENBERG ET AL., *The absorption of high energy radiation, a Monte Carlo study. I: Rectangular geometry. II: Spherical geometry. III: Density and transparency distributions*, Canad. J. Phys., 41 (1963), pp. 632–650, 651–663, 2206–2240; reprinted in [4].
- [88] N. METROPOLIS ET AL., *Monte Carlo calculations on intranuclear cascades. I: Low-energy studies. II: High-energy studies and pion processes*, Phys. Rev., 110 (1958), pp. 185–203, 204–219; reprinted in [4].
- [89] G. W. KING, *Stochastic methods in quantum mechanics*, Proc. Seminar on Scientific Computation, IBM Corp., New York, 1949, pp. 42–48; *Further remarks*, pp. 92–94; reprinted in [4].
- [90] M. H. KALOS, *Monte Carlo calculations of the ground state of three- and four-body nuclei*, Phys. Rev., 128 (1962), pp. 1791–1795; reprinted in [4].
- [91] ———, *Stochastic wave-function for atomic helium*, J. Comp. Phys., 1 (1966), pp. 257–275; reprinted in [4].
- [92] G. W. KING, *Stochastic methods in statistical mechanics*, Monte Carlo Methods, National Bureau of Standards Applied Mathematics Series, No. 12, U.S. Government Printing Office, Washington, D.C., 1951, pp. 12–18; reprinted in [4].

- [93] N. METROPOLIS ET AL., *Equation of state calculations by fast computing machines*, J. Chem. Phys., 21 (1953), pp. 1087–1092; reprinted in [4].
- [94] J. B. EHRMAN, L. D. FOSDICK AND D. C. HANDSCOMB, *Computation of order parameters in an Ising lattice by the Monte Carlo method*, J. Mathematical Phys., 1 (1960), pp. 547–558; reprinted in [4].
- [95] D. C. HANDSCOMB, *The Monte Carlo method in quantum statistical mechanics*, Proc. Cambridge Philos. Soc., 58 (1962), pp. 594–598; reprinted in [4].
- [96] ———, *A Monte Carlo method applied to the Heisenberg ferromagnet*, Ibid., 60 (1964), pp. 115–122; reprinted in [4].
- [97] J. R. BEELER, JR. AND J. A. DELANEY, *Order-disorder events produced by single vacancy migration*, Phys. Rev., 130 (1963), pp. 962–971; reprinted in [4].
- [98] L. D. FOSDICK, *Numerical estimation of the partition function in quantum statistics*, J. Mathematical Phys., 3 (1962), pp. 1251–1264; reprinted in [4].
- [99] M. J. BERGER AND J. DOGGETT, *Reflection and transmission of gamma radiation by barriers. I: Monte Carlo calculation by a collision-density method. III: Semianalytic Monte Carlo calculation*, J. Res. Nat. Bur. Standards, 55 (1955), pp. 343–350, 56 (1956), pp. 89–98; reprinted in [4].
- [100] H. KAHN, *Random sampling (Monte Carlo) techniques in neutron attenuation problems*, Nucleonics, 6 (1950), no. 5, pp. 27–33; no. 6, pp. 60–65; reprinted in [4].
- [101] A. S. HOUSEHOLDER, *Neutron age calculations in water, graphite, and tissue*, Monte Carlo Methods, National Bureau of Standards Applied Mathematics Series, No. 12, U. S. Government Printing Office, Washington, D.C., 1951, pp. 6–8; reprinted in [4].
- [102] W. C. DE MARCUS AND L. NELSON, *Methods of probabilities in chains applied to particle transmission through matter*, Monte Carlo Methods, National Bureau of Standards Applied Mathematics Series, No. 12, U.S. Government Printing Office, Washington, D.C., 1951, pp. 9–11; reprinted in [4].
- [103] K. W. MORTON, *Scaling neutron tracks in Monte Carlo shielding calculations*, J. Nuclear Energy, 5 (1957), pp. 320–324; reprinted in [4].
- [104] M. H. KALOS, *Importance sampling in Monte Carlo shielding calculations. I: Neutron penetration through thick hydrogen slabs*, Nuclear Sci. Engrg., 16 (1963), pp. 227–234; reprinted in [4].
- [105] J. SPANIER, *A unified approach to Monte Carlo methods and an application to a multigroup calculation of absorption rates*, this Review, 4 (1962), pp. 115–134; reprinted in [4].
- [106] F. T. WALL ET AL., *Self-avoiding walks as a model of coiling polymer molecules*, J. Chem Phys., *Statistical computation of mean dimensions of macromolecules*, 22 (1954), pp. 1036–1041, 23 (1955), pp. 913–921, 2314–2321, 26 (1957), pp. 1742–1749; *Improved statistical method for computing mean dimensions of polymer molecules*, 27 (1957), pp. 186–188; *New method for the statistical computation of polymer dimensions*, 30 (1959), pp. 634–637; *Statistical computation of radii of gyration and mean internal dimensions of polymer molecules*, 30 (1959), pp. 637–640; *Monte Carlo procedures for generation of non-intersecting chains*, 37 (1962), pp. 1461–1465; *Monte Carlo study of coiling-type molecules. I: Macromolecular configurations. II: Statistical thermodynamics*, 38 (1963), pp. 2220–2227, 2228–2232, 39 (1963), pp. 1900; reprinted in [4].
- [107] J. G. HOFFMAN, N. METROPOLIS AND V. GARDINER, *Study of tumor cell populations by Monte Carlo methods*, Science, 122 (1955), pp. 465–466; *Digital computer studies of cell multiplication by Monte Carlo methods*, J. Nat. Cancer Inst., 17 (1956), pp. 175–188; reprinted in [4].
- [108] P. H. LESLIE AND J. C. GOWER, *The properties of a stochastic model for two competing species*, Biometrika, 45 (1958), pp. 316–330, 46 (1959), p. 279; reprinted in [4].
- [109] E. S. PAGE, *On Monte Carlo methods in congestion problems. I: Searching for an optimum in discrete situations*, Operations Res., 13 (1965), pp. 291–299; reprinted in [4].
- [110] A. BLUMSTEIN, *A Monte Carlo analysis of the Ground Controlled Approach system*, Ibid., 5 (1957), pp. 397–408; reprinted in [4].
- [111] J. E. BEARDWOOD, J. H. HALTON AND J. M. HAMMERSLEY, *The shortest path through many points*, Proc. Cambridge Philos. Soc., 55 (1959), pp. 299–327; reprinted in [4].
- [112] J. H. HALTON AND A. D. SPAULDING, *Error rates in differentially coherent phase systems in non-Gaussian noise*, IEEE Trans. Comm. Tech., COM-14 (1966), pp. 594–601; reprinted in [4].
- [113] H. W. BERTINI, *Monte Carlo calculations on intranuclear cascades*, Reps. ORNL 3360, 3383, 3433, Oak Ridge National Laboratories, Oak Ridge, Tennessee, 1963.

- [114] M. N. ROSENBLUTH AND A. W. ROSENBLUTH, *Further results on Monte Carlo equations of state*, J. Chem. Phys., 22 (1954), pp. 881–884.
- [115] W. W. WOOD ET AL., *Monte Carlo equation of state of molecules interacting with the Lennard-Jones and hard sphere potentials*, J. Chem. Phys., 27 (1957), pp. 720–733, 1207–1208, Nuovo Cimento Suppl. Ser. 10, 9 (1958), pp. 133–143.
- [116] W. W. WOOD AND J. D. JACOBSON, *Monte Carlo calculations in statistical mechanics*, Proc. Western Joint Computer Conference, 1959, pp. 261–269.
- [117] Z. W. SALSBURG, J. D. JACOBSON, W. FICKETT AND W. W. WOOD, *Application of the Monte Carlo method to the lattice gas model. I: Two-dimensional triangular lattice*, J. Chem. Phys., 30 (1959), pp. 65–72.
- [118] B. J. ALDER AND T. E. WAINWRIGHT, *Studies in molecular dynamics*, Ibid., 31 (1959), pp. 459–466, 33 (1960), pp. 1439–1451, 40 (1964), pp. 2724–2730.
- [119] Z. W. SALSBURG AND W. W. WOOD, *Equation of state of classical hard spheres at high density*, Ibid., 37 (1962), pp. 798–804.
- [120] D. A. CHESNUT AND Z. W. SALSBURG, *Monte Carlo procedure for statistical mechanical calculations in a grand canonical ensemble of lattice systems*, Ibid., 38 (1963), pp. 2861–2875.
- [121] ———, *Monte Carlo calculations for the two-dimensional triangular lattice gas: supercritical region*, Ibid., 39 (1963), pp. 2081–2084.
- [122] E. B. SMITH AND K. R. LEA, *Thermodynamic properties of mixtures of hard sphere molecules by Monte Carlo methods*, Trans. Faraday Soc., 59 (1963), pp. 1535–1543.
- [123] L. D. FOSDICK, *Calculation of order parameters in a binary alloy by the Monte Carlo method*, Phys. Rev., 116 (1959), pp. 565–573.
- [124] P. A. FLINN AND G. M. McMANUS, *Monte Carlo calculation of the order-disorder transformation in the body-centered cubic lattice*, Ibid., 124 (1961), pp. 54–59.
- [125] J. R. BEELER, JR., *High speed computer experiment techniques: Many particle systems*, Rep. GEMP-252, General Electric Co., Schenectady, New York, 1963.
- [126] L. D. FOSDICK, *Monte Carlo computations on the Ising lattice*, Methods in Computational Physics, vol. I, Academic Press, New York, 1963, pp. 245–280.
- [127] M. N. ROSENBLUTH AND A. W. ROSENBLUTH, *Monte Carlo calculation of the average extension of molecular chains*, J. Chem. Phys., 23 (1955), pp. 356–359.
- [128] P. J. MARCER, *Further investigations of the mean dimensions of non-intersecting chains on simple lattices*, Doctoral thesis, Oxford University, Oxford, 1960.
- [129] M. A. D. FLUENDY AND E. B. SMITH, *The application of Monte Carlo methods to physicochemical problems*, Quart. Rev. Chem. Soc., London, 16 (1962), pp. 241–266.
- [130] M. A. D. FLUENDY, *Calculation of cyclization probabilities and other configuration properties of alkane-type chains by a Monte Carlo method*, Trans. Faraday Soc., 59 (1963), pp. 1681–1694.
- [131] N. C. BLAIS AND D. L. BUNKER, *Monte Carlo calculations (Reaction kinetics)*, J. Chem. Phys., 37 (1962), pp. 2713–2720, 39 (1963), pp. 315–322.
- [132] I. M. GELFAND AND A. M. YAGLOM, *Integration in functional spaces and its application in quantum physics*, Upsekhi Mat. Nauk, 11 (1956), pp. 77–114.
- [133] I. M. GELFAND AND N. N. CHENTSOV, *The evaluation of Wiener integrals*, Zh. Eksper. Teoret. Fiz., 31 (1956), pp. 1106–1107.
- [134] I. M. GELFAND, A. S. FROLOV AND N. N. CHENTSOV, *The evaluation of Wiener integrals by the Monte Carlo method*, Izv. Vyssh. Uchebn. Zaved. Matematika, 5 (1958), pp. 32–45.
- [135] L. D. FOSDICK, *The Monte Carlo method in quantum statistics*, this Review, 10 (1968), pp. 315–328.
- [136] E. M. GERLBARD AND J. SPANIER, *Use of superposition principle in Monte Carlo resonance escape calculations*, Trans. Amer. Nuclear Soc., 7 (1964), pp. 259–260.
- [137] I. B. MOTSKUS, *On a method of distributing random trials for solving multi-extremal problems*, Zh. Vychisl. Mat. i Mat. Fiz., 4 (1964), pp. 380–385.
- [138] J. MATYAS, *Random optimization*, Avtomat i Telemekh., 26 (1965), pp. 246–253.
- [139] R. ZIELIŃSKI, *On the Monte Carlo evaluation of the extremal value of a function*, Algorytmy, 2 (1965), pp. 7–13.
- [140] A. RÉNYI, *On the theory of random search*, Bull. Amer. Math. Soc., 71 (1965), pp. 809–828.
- [141] B. JANSSON, *Random number generators*, Doctoral thesis, Faculty of Mathematics and Natural Sciences, University of Stockholm, 1966.

- [142] T. E. HULL AND A. R. DOBELL, *Random number generators*, this Review, 4 (1962), pp. 230–254; reprinted in [4].
- [143] J. H. HALTON, *On the generation of arbitrarily autocorrelated sequences of random variables from a sequence of independent random numbers*, Rep. AMD-322, Brookhaven National Laboratory, Upton, N.Y., 1963.
- [144] E. S. PAGE, *Pseudo-random elements for computers*, Appl. Statist., 8 (1959), pp. 124–131; reprinted in [4].
- [145] J. VON NEUMANN, *Various techniques used in connection with random digits*, Monte Carlo Methods, National Bureau of Standards Applied Mathematics Series No. 12, U.S. Government Printing Office, Washington, D.C., 1951, pp. 36–38; reprinted in [4].
- [146] J. W. BUTLER, *Machine sampling from given probability distributions*, Symposium on Monte Carlo Methods, H. A. Meyer, ed., John Wiley, New York, 1956, pp. 249–264.
- [147] D. F. VOTAW, JR. AND J. A. RAFFERTY, *High-speed sampling*, Math. Tables Aids Comput., 5 (1951), pp. 1–8.
- [148] J. C. BUTCHER, *Random sampling from the normal distribution*, Comput. J., 3 (1961), pp. 251–253.
- [149] G. MARSAGLIA, *Expressing a random variable in terms of uniform random variables*, Ann. Math. Statist., 32 (1961), pp. 894–898.
- [150] G. MARSAGLIA, M. D. MACLAREN AND T. A. BRAY, *A fast procedure for generating normal random variables*, Comm. ACM, 7 (1964), pp. 4–10; reprinted in [4].
- [151] G. E. P. BOX AND M. E. MULLER, *A note on the generation of random normal deviates*, Ann. Math. Statist., 29 (1958), pp. 610–611.
- [152] M. E. MULLER, *A comparison of methods for generating normal deviates on digital computers*, J. Assoc. Comput. Mach., 6 (1959), pp. 376–383; reprinted in [4].
- [153] G. BÁNKÖVI, *A note on the generation of beta-distributed and gamma-distributed random variables*, Magyar Tud. Akad. Mat. Kutató Int. Közl., 9 (1964), pp. 555–563.
- [154] A. BÉKÉSSY, *Remarks on beta-distributed random numbers*, Ibid., 9 (1964), pp. 565–571.
- [155] G. MARSAGLIA, *Generating exponential random variables*, Ann. Math. Statist., 32 (1961), pp. 899–900.
- [156] ———, *Generating discrete random variables in a computer*, Comm. ACM, 6 (1963), pp. 37–38.
- [157] M. SIBUYA, *On exponential and other random variable generators*, Ann. Inst. Statist. Math. Tokyo, 13 (1962), pp. 231–237.
- [158] J. V. USPENSKY, *Introduction to Mathematical Probability*, McGraw-Hill, New York, 1937.
- [159] BUFFON, *Essai d'arithmétique morale*, 1777.
- [160] A. HALL, *On an experimental determination of  $\pi$* , Messeng. Math., 2 (1873), pp. 113–114.
- [161] J. W. L. GLAISHER, *Remarks on the calculation of  $\pi$* , Ibid., 2 (1873), pp. 119–128.
- [162] N. MANTEL, *An extension of the Buffon needle problem*, Ann. Math. Statist., 24 (1953), pp. 674–677.
- [163] B. C. KAHAN, *A practical demonstration of a needle experiment designed to give a number of concurrent estimates of  $\pi$* , J. Roy. Statist. Soc., A 124 (1961), pp. 227–239.
- [164] M. G. KENDALL AND B. BABINGTON SMITH, *Randomness and random sampling numbers*, Ibid., 101 (1938), pp. 147–166; *Second paper on random sampling numbers*, J. Roy. Statist. Soc. Suppl., 6 (1939), pp. 51–61.
- [165] ———, *Tables of Random Sampling Numbers*, Tracts for Computers, No. 24, Department of Statistics, University College, London; Cambridge University Press, Cambridge, 1954.
- [166] G. W. BROWN, *History of RAND's random digits*, Monte Carlo Methods, National Bureau of Standards Applied Mathematics Series, No. 12, U.S. Government Printing Office, Washington, D.C., 1951, pp. 31–32.
- [167] RAND CORPORATION, *A Million Random Digits With 100,000 Normal Deviates*, Free Press, Glencoe, Illinois, 1955.
- [168] W. E. THOMSON, *ERNIE—a mathematical and statistical analysis*, J. Roy. Statist. Soc., A 122 (1959), pp. 301–324; discussion, pp. 324–333.
- [169] M. ISIDA AND H. IKEDA, *Random number generator*, Ann. Inst. Statist. Math. Tokyo, 8 (1956), pp. 119–126.
- [170] G. E. FORSYTHE, *Generation and testing of random digits at the National Bureau of Standards, Los Angeles*, Monte Carlo Methods, National Bureau of Standards Applied Mathematics Series, No. 12, U.S. Government Printing Office, Washington, D.C., 1951, pp. 34–35.

- [171] M. L. JUNCOSA, *Random number generation on the B.R.L. high speed computing machines*, Rep. 855, Ballistics Research Laboratory, 1953.
- [172] O. TAUSSKY and J. TODD, *Generation of pseudo-random numbers*, Symposium on Monte Carlo Methods (University of Florida, 1954), H. A. Meyer, ed., John Wiley, New York, 1956, pp. 15–28.
- [173] N. METROPOLIS, *Phase shifts—middle squares—wave equation*, Symposium on Monte Carlo Methods (University of Florida, 1954), H. A. Meyer, ed., John Wiley, New York, 1956, pp. 29–36.
- [174] N. METROPOLIS AND S. M. ULAM, *A property of randomness of an arithmetical function*, Amer. Math. Monthly, 60 (1953), pp. 252–253; reprinted in [4].
- [175] D. H. LEHMER, *Mathematical methods in large-scale computing units*, Proc. Second Symposium on Large-Scale Digital Calculating Machinery (1949), Harvard University Press, Cambridge, Massachusetts, 1951, pp. 141–146;
- [176] J. N. FRANKLIN, *Deterministic simulation of random processes*, Math. Comp., 17 (1963), pp. 28–59; reprinted in [4].
- [177] R. R. COVEYOU, *Serial correlation in the generation of pseudo-random numbers*, J. Assoc. Comput. Mach., 7 (1960), pp. 72–74; reprinted in [4].
- [178] A. ROTENBERG, *A new pseudo-random generator*, Ibid., 7 (1960), pp. 75–77; reprinted in [4].
- [179] A. VAN WIJNGARDEN, *Mathematics and computing*, Automatic Digital Computation, Proc. Symposium of the National Physics Laboratory, H.M. Stationery Office, London, 1954, pp. 125–129.
- [180] G. NEOVIUS, *Artificial traffic trials using digital computers*, Ericsson Technics, 11 (1955), pp. 279–291.
- [181] M. D. MACLAREN AND G. MARSAGLIA, *Uniform random number generators*, J. Assoc. Comput. Mach., 12 (1965), pp. 83–89.
- [182] W. J. WESTLAKE, *A uniform random number generator based on the combination of two congruential generators*, Ibid., 14 (1967), pp. 337–340.
- [183] G. E. FORSYTHE, *Generation and testing of 1,217,370 “random” binary digits on the SWAC*, Abstract, Bull Amer. Math. Soc., 57 (1951), p. 304.
- [184] E. LUCAS, *Theory of simply periodic numerical functions*, Amer. J. Math., 1 (1878), pp. 184–240, 289–321. (In French.)
- [185] R. D. CARMICHAEL, *On the numerical factors of the arithmetic form  $\alpha^n \pm \beta^n$* , Ann. Math., 15 (1913–14), pp. 30–70.
- [186] ———, *A simple principle of unification in the elementary theory of numbers*, Amer. Math. Monthly, 36 (1929), pp. 132–143.
- [187] D. D. WALL, *Fibonacci series modulo m*, Ibid., 67 (1960), pp. 525–532.
- [188] D. W. ROBINSON, *The Fibonacci matrix modulo m*, Fibonacci Quart., 1 (1963), no. 2, pp. 29–36.
- [189] J. VINSON, *The relation of the period modulo m to the rank of apparition of m in the Fibonacci sequence*, Ibid., 1 (1963), no. 2, pp. 37–45.
- [190] J. H. HALTON, *On Fibonacci residues*, Ibid., 2 (1964), pp. 217–218.
- [191] ———, *On a general Fibonacci identity*, Ibid., 3 (1965), pp. 31–43.
- [192] ———, *A note on Fibonacci subsequences*, Ibid., 3 (1965), pp. 321–322.
- [193] ———, *On the divisibility properties of Fibonacci numbers*, Ibid., 4 (1966), pp. 217–240.
- [194] ———, *Some properties associated with square Fibonacci numbers*, Ibid., 5 (1967), pp. 347–355.
- [195] J. CERTAINE, *On sequences of pseudo-random numbers of maximal length*, J. Assoc. Comput. Mach., 5 (1958), pp. 353–356; reprinted in [4].
- [196] V. D. BARNETT, *The behavior of pseudo-random sequences generated on computers by the multiplicative congruential method*, Math. Comp., 16 (1962), pp. 63–69; reprinted in [4].
- [197] T. E. HULL, J. L. ALLARD AND A. R. DOBELL, *Mixed congruential random number generators*, J. Assoc. Comput. Mach., *For decimal machines*, 10 (1963), pp. 131–141; *For binary machines*, 11 (1964), pp. 31–40; reprinted in [4].
- [198] A. VAN GELDER, *Some new results in pseudo-random number generation*, Ibid., 14 (1967), pp. 785–792.
- [199] N. METROPOLIS, G. REITWIESNER AND J. VON NEUMANN, *Statistical treatment of values of first 2,000 decimal places of e and  $\pi$  calculated on the ENIAC*, Math. Tables Aids Comput., 4 (1950), pp. 109–111.
- [200] F. GRUENBERGER, *Further statistics on the digits of e*, Ibid., 6 (1952), pp. 123–124.

- [201] R. K. PATHRIA, *A statistical analysis of the first 2,500 decimal places of  $e$  and  $1/e$* , Proc. Nat. Inst. Sci. India Part A, 27 (1961), pp. 270–282.
- [202] ———, *A statistical study of randomness among the first 10,000 digits of  $\pi$* , Math. Comp., 16 (1962), pp. 188–197.
- [203] ———, *A statistical study of randomness among the first 60,000 digits of  $e$* , Proc. Nat. Inst. Sci. India Part A, 30 (1964), pp. 663–674.
- [204] R. D. RICHMYER, M. DEVANEY AND N. METROPOLIS, *Continued fraction expansions of algebraic numbers*, Numer. Math., 4 (1962), pp. 68–84; reprinted in [4].
- [205] J. LACH, *Random number generators*, Memo. 27, Yale University Computer Center, New Haven, Connecticut, 1963.
- [206] M. GREENBERGER, *Method in randomness*, Comm. ACM, 8 (1965), pp. 177–179.
- [207] ———, *An a priori determination of serial correlation in computer generated random numbers*, Math. Comp., 15 (1961), pp. 383–389; reprinted in [4].
- [208] ———, *Notes on a new pseudo-random generator*, J. Assoc. Comput. Mach., 8 (1961), pp. 163–167; reprinted in [4].
- [209] B. JANSSON, *Autocorrelations between pseudo-random numbers*, Nordisk Tidskr. Informations-Behandling, (BIT) 4 (1963), pp. 6–27.
- [210] D. E. KNUTH, *Construction of a random sequence*, Ibid., 5 (1965), pp. 246–250.
- [211] D. L. JAGERMAN, *Some theorems concerning pseudo-random numbers*, Math. Comp., 19 (1965), pp. 418–426.
- [212] R. R. COVEYOU AND R. D. MACPHERSON, *Fourier analysis of uniform random number generators*, J. Assoc. Comput. Mach., 14 (1967), pp. 100–119.
- [213] G. H. HARDY AND E. M. WRIGHT, *An Introduction to the Theory of Numbers*, Clarendon Press, Oxford, 1960.
- [214] J. F. KOKSMA, *Diophantische Approximationen*, Springer, Berlin, 1957; Chelsea, New York, 1936.
- [215] J. F. KOKSMA AND L. KUIPERS, eds., *Asymptotic Distribution Modulo 1*, Noordhoff, Groningen, 1964, also Compositio Math., 16 (1964), pp. 1–203.
- [216] H. WEYL, *On uniform distribution of numbers modulo one*, Math. Ann., 77 (1916), pp. 313–352.
- [217] J. G. VAN DER CORPUT, *Diophantine inequalities. I: On uniform distribution modulo one*, Acta Math., 56 (1931), pp. 373–456. [In German.]
- [218] J. F. KOKSMA, *A set-theoretical theorem on uniform distribution modulo one*, Compositio Math., 2 (1935), pp. 250–258.
- [219] N. G. DEBRUIJN AND P. ERDÖS, *Sequences of points on a circle*, Nederl. Akad. Wetensch. Proc. Ser. A, 52 (1949), pp. 46–49; reprinted in [4].
- [220] K. F. ROTH, *On irregularities of distribution*, Mathematika, 1 (1954), pp. 73–79; reprinted in [4].
- [221] H. DAVENPORT, *Note on irregularities of distribution*, Ibid., 3 (1956), pp. 131–135; reprinted in [4].
- [222] V. T. SÓS, *On the theory of Diophantine approximations. I*, Acta Math. Acad. Sci. Hungar., 8 (1957), pp. 461–472.
- [223] ———, *On the distribution mod 1 of the sequence  $n\alpha$* , Ann. Univ. Sci. Budapest Eötvös Sect. Math., 1 (1958), pp. 127–134.
- [224] J. SURÁNYI, *On the ordering of the multiples of a real number mod 1*, Ibid., 1 (1958), pp. 107–111. (In German.)
- [225] S. ŚWIERCZKOWSKI, *On successive settings of an arc on the circumference of a circle*, Fund. Math., 46 (1958), pp. 187–189.
- [226] J. H. HALTON, *The distribution of the sequence  $\{n\xi\}$  ( $n = 0, 1, 2, \dots$ )*, Proc. Cambridge Philos. Soc., 61 (1965), pp. 665–670; reprinted in [4].
- [227] R. E. GREENWOOD, *Coupon collector's test for random digits*, Math. Tables Aids Comput. 9 (1955), pp. 1–5.
- [228] F. GRUENBERGER AND A. M. MARK, *Tests of random digits*, Ibid., 4 (1950), pp. 244–245; *The  $d^2$ -test*, 5 (1951), pp. 109–110.
- [229] A. OSTROWSKI, *Remarks on the theory of Diophantine approximation*, Abh. Math. Sem. Univ. Hamburg, 1 (1922), pp. 77–98.
- [230] J. H. HALTON, *On the efficiency of certain quasi-random sequences of points in evaluating multi-dimensional integrals*, Numer. Math., 2 (1960), pp. 84–90; 196; reprinted in [4]; *Algorithm 247: radical-inverse quasi-random point sequence* [G5], Comm. ACM, 7 (1964), pp. 701–702 (with G. B. SMITH).

- [231] H. GABAI, *On the discrepancy of certain sequences mod 1*, Nederl. Akad. Wetensch. Proc. Ser. A, 66 (1963), pp. 603–605.
- [232] S. HABER, *On a sequence of points of interest for numerical quadrature*, J. Res. Nat. Bur. Standards Ser. B, 70 (1966), pp. 127–136.
- [233] J. H. HALTON AND S. K. ZAREMBA, *The extreme and  $L^2$  discrepancies of some plane sets*, Monatsh. Math., to appear.
- [234] P. ROOS AND L. ARNOLD, *Numerical experiments in multidimensional quadrature*, Sitz. Österreich. Akad. Wiss. (Math. Natur. Kl.), 172:II (1963), pp. 271–286.
- [235] R. D. RICHTMYER, *The evaluation of definite integrals, and a quasi-Monte-Carlo method based on the properties of algebraic numbers*, Rep. LA-1342, Los Alamos Scientific Laboratory, Los Alamos, New Mexico, 1951.
- [236] L. G. PECK, *On uniform distribution of algebraic numbers*, Proc. Amer. Math. Soc., 4 (1953), pp. 440–443.
- [237] R. D. RICHTMYER, *A non-random sampling method, based on congruences, for “Monte Carlo” problems*, Atomic Energy Commission Computer and Applied Mathematics Center, New York University, NYO 8674, 1958.
- [238] S. K. ZAREMBA, *Good lattice-points in the sense of Hlawka and Monte-Carlo integration*, Monatsh. Math., to appear.
- [239] ———, *Some applications of multidimensional integration by parts*, Ann. Polon. Math., 21 (1968), pp. 85–96.
- [240] J. H. HALTON, *On sequences of random variables in separable Fréchet spaces*, in preparation.
- [241] ———, *An Introduction to the Monte Carlo Method*, Prentice-Hall, Englewood Cliffs, New Jersey, to be published.
- [242] ———, *On the strong convergence of linear averages of generalized random variables*, in preparation.
- [243] S. FAEDO, *Order of magnitude of Euler-Fourier coefficients of functions of two variables*, Ann. Scuola Norm. Sup. Pisa, (II) 6 (1937), pp. 225–246.
- [244] J. G. VAN DER CORPUT, *Distribution functions*, Nederl. Akad. Wetensch. Proc. Ser. A, 38 (1938), pp. 813–821, 1058–1066; 39 (1939), pp. 10–19, 19–26, 149–153, 339–344, 489–494, 579–590. (See especially 38 (1938), pp. 1058–1066.) [In German.]
- [245] J. H. HALTON, *On the inadequacy of the sample-variance as an error-estimate in quasi-Monte-Carlo calculations*, in preparation.
- [246] J. H. HALTON AND E. A. ZEIDMAN, *Monte Carlo integration with sequential stratification*, Comp. Sci. Tech. Rep. 61, University of Wisconsin, Madison, 1969.
- [247] J. SPANIER AND E. M. GELBARD, *Monte Carlo Principles and Neutron Transport Problems*, Addison-Wesley, Reading, Massachusetts, 1969.
- [248] J. H. HALTON, *A retrospective and prospective survey of the Monte Carlo method*, Comp. Sci. Tech. Rep. 13, University of Wisconsin, Madison, 1968.
- [249] E. A. ZEIDMAN, *The evaluation of multidimensional integrals by sequential stratification*, in preparation.
- [250] I. M. GELFAND, *Lectures on Linear Algebra*, Interscience, New York, 1961.
- [251] G. E. SHILOV, *An Introduction to the Theory of Linear Spaces*, Prentice-Hall, Englewood Cliffs, New Jersey, 1961.

#### AUTHOR INDEX

In the following lexicographically ordered list of authors, the numbers refer to the preceding list of references. All authors are listed (including those described for brevity, as “et al.”, among the references, and including authors of all articles in collections listed under their editors’ names).

- |                      |                              |
|----------------------|------------------------------|
| Akilov, G. P. 55     | Atkinson, K. E. 60           |
| Albert, G. E. 32     | Babington Smith, B. 164, 165 |
| Alder, B. J. 118     | Bánkövi, G. 153              |
| Allard, J. L. 197    | Barnett, V. D. 196           |
| Anselone, P. M. 59   | Bartlett, M. S. 37           |
| Arnold, H. J. 32, 48 | Bauer, W. F. 29              |
| Arnold, L. 234       | Beach, L. A. 32              |
| Atchison, W. F. 106  | Beardwood, J. E. 111         |

- Beeler, J. R., Jr. 97, 125  
 Békésy, A. 154  
 Berger, M. J. 32, 99  
 Bertini, H. W. 113  
 Bertrandias, J. P. 11, 215  
 Bivins, R. 88  
 Blais, N. C. 131  
 Blumstein, A. 110  
 Box, G. E. P. 151  
 Bray, T. A. 150  
 Brown, G. W. 166  
 Bucher, B. D. 32, 48  
 Buffon 159  
 Bunker, D. L. 131  
 Buslenko, N. P. 33, 51  
 Butcher, J. C. 148  
 Butler, J. W. 32, 146  
 Carmichael, R. D. 185, 186  
 Certaine, J. 195  
 Chentsov, N. N. 2, 133, 134  
 Chesnut, D. A. 120, 121  
 Cigler, J. 215  
 Cohen, M. 80  
 Courant, R. 21  
 Coveyou, R. R. 177, 212  
 Crofts, W. P. 87  
 Curtiss, J. H. 18, 32, 71  
 Cutkosky, R. E. 72  
 Davenport, H. 221  
 De Bruijn, N. G. 219  
 Delaney, J. A. 97  
 De Marcus, W. C. 102  
 Devaney, M. 204  
 DeVroedt 215  
 Dismuke, N. M. 32  
 Dobell, A. R. 142, 197  
 Doggett, J. 99  
 Donsker, M. D. 79  
 Edmundson, H. P. 70  
 Edwards, R. E. 54  
 Ehrman, J. R. 94  
 Erdős, P. 215, 219  
 Ermakov, S. M. 45  
 Erpenbeck, J. J. 106  
 Faedo, S. 243  
 Fickett, W. 117  
 Flinn, P. A. 124  
 Fluendy, M. A. D. 129, 130  
 Forsythe, G. E. 62, 67, 170, 183  
 Fortet, R. 86  
 Fosdick, L. D. 94, 98, 123, 126, 135  
 Franklin, J. N. 176  
 Friedlander, G. 88  
 Friedrichs, K. O. 21  
 Frolov, A. S. 2, 134  
 Gabai, H. 231  
 Gans, P. J. 106  
 Gardiner, V. 107  
 Gelbard, E. M. 136, 247  
 Gelfand, I. M. 132, 133, 134, 250  
 Glaisher, J. W. L. 161  
 Gnedenko, B. V. 1  
 Golenko, D. I. 33, 51  
 Gosset, W. S. 20  
 Gower, J. C. 108  
 Greenberger, M. 206, 207, 208  
 Greenwood, R. E. 227  
 Gruenberger, F. 200, 228  
 Haber, S. 232  
 Hall, A. 160  
 Halton, J. H. 3, 4, 5, 6, 9, 35, 36, 42, 61, 77, 78,  
     111, 112, 143, 190, 191, 192, 193, 194, 226, 230,  
     233, 240, 241, 242, 245, 246, 248  
 Hammersley, J. M. 16, 17, 27, 30, 38, 39, 49, 111  
 Handscomb, D. C. 17, 40, 42, 43, 46, 94, 95, 96  
 Hardy, G. H. 213  
 Hartman, S. 215  
 Haselgrove, C. B. 12  
 Helmberg, G. 215  
 Hiller, L. A., Jr. 106  
 Hlawka, E. 13, 14, 215  
 Hoffman, J. G. 107  
 Householder, A. S. 63, 101  
 Hull, T. E. 142, 197  
 Ikeda, H. 169  
 Isaacson, L. M. 106  
 Isida, M. 169  
 Jacobson, J. D. 115, 116, 117  
 Jagerman, D. L. 211  
 Jansson, B. 141, 209  
 Juncosa, M. L. 171  
 Kac, M. 79, 80  
 Kahan, B. C. 163  
 Kahn, H. 31, 32, 100  
 Kalos, M. H. 90, 91, 104  
 Kantorovich, L. V. 55  
 Kemperman, J. H. B. 215  
 Kendall, M. G. 164, 165  
 King, G. W. 26, 89, 92  
 Knuth, D. E. 210  
 Koksma, J. F. 10, 214, 215, 218  
 Kolmogorov, A. N. 22  
 Kraft, R. 34  
 Kuipers, L. 215  
 Lach, J. 205  
 Laurent, P. J. 44  
 Lea, K. R. 122  
 Lehmer, D. H. 175  
 Leibler, R. A. 67  
 Leslie, P. H. 108  
 Lewy, H. 21  
 Lucas, E. 184

- Lytle, E. J., Jr. 32  
 MacLaren, M. D. 150, 181  
 Macpherson, R. D. 212  
 Mantel, N. 162  
 Marcer, P. J. 128  
 Marcus, M. 57  
 Mark, A. M. 228  
 Marsaglia, G. 149, 150, 155, 156, 181  
 Marshall, A. W. 32, 75  
 Matyaš, J. 138  
 Mauldon, J. G. 39  
 McManus, G. M. 124  
 Metropolis, N. 24, 32, 88, 93, 107, 173, 174, 199,  
   204  
 Meyer, H. A. 32  
 Miller, J. M. 88  
 Mine, H. 57  
 Mirsky, L. 58  
 Moler, C. B. 62  
 Morton, K. W. 16, 27, 38, 41, 103  
 Motzkin, T. S. 32  
 Motskus, I. B. 137  
 Muller, M. E. 84, 85, 151, 152  
 Nelson, L. 102  
 Neovius, G. 180  
 Niven, I. 215  
 Opler, A. 74  
 Ostrowski, A. 229  
 Parker, F. R. 115  
 Pathria, R. K. 201, 202, 203  
 Page, E. S. 73, 109, 144  
 Peck, L. G. 236  
 Pervin, W. J. 7  
 Philipp, W. 215  
 Pisot, C. 215  
 Pólya, G. 23  
 Powell, M. J. D. 52  
 Rafferty, J. A. 147  
 RAND Corporation 167  
 Rayleigh, Lord 19  
 Reitwiesner, G. 199  
 Rényi, A. 140  
 Richtmyer, R. D. 204, 235, 237  
 Robinson, D. W. 188  
 Roos, P. 234  
 Rosenbluth, M. N. & A. W. 93, 114, 127  
 Rotenberg, A. 178  
 Roth, K. F. 220  
 Rubin, R. J. 106  
 Salem, R. 215  
 Salsburg, Z. W. 117, 119, 120  
 Schoenberg, I. J. 215  
 Shilov, G. E. 251  
 Shreider, Yu. A. 33, 51  
 Sibuya, M. 157  
 Sierpiński, W. 8  
 Slater, N. B. 215  
 Smith, E. B. 122, 129  
 Smith, G. B. 230  
 Sobol', I. M. 33, 51  
 Sós, V. T. 222, 223  
 Spanier, J. 105, 136, 247  
 Spaulding, A. D. 112  
 Sragovich, V. G. 33, 51  
 Steenberg, N. R. 87  
 Storm, M. 88  
 'Student' [Gosset] 20  
 Surányi, J. 224  
 Swann, J. 52  
 Świerczkowski, S. 225  
 Taussky, O. 32, 172  
 Teller, A. H. & E. 93  
 Theus, R. B. 32  
 Thomson, W. E. 168  
 Tocher, K. D. 28  
 Todd, J. 32, 172  
 Trotter, H. F. 32, 47, 48  
 Tukey, J. W. 32, 47, 48  
 Turkevich, A. 88  
 Ulam, S. M. 24, 25, 32, 174  
 Uspensky, J. V. 158  
 Van der Corput, J. G. 217, 244  
 Van Gelder, A. 198  
 Van Iterson, W. 87  
 Van Wijngarden, A. 179  
 Varga, R. S. 64  
 Vickery, C. W. 32  
 Vinson, J. 189  
 Volkman, B. 215  
 Von Neumann, J. 145, 199  
 Votaw, D. F., Jr. 147  
 Wainwright, T. E. 118  
 Wald, A. 76  
 Wall, D. D. 187  
 Wall, F. T. 106  
 Walsh, J. E. 32  
 Walther, A. 32  
 Wasow, W. R. 68, 69, 81, 82, 83  
 Wendel, J. G. 50  
 Wensrich, C. J. 34  
 Westlake, W. J. 182  
 Weyl, H. 216  
 Wheeler, D. J. 106  
 Wilkinson, J. H. 65, 66  
 Windwer, S. 106  
 Wood, W. W. 115, 116, 117, 119  
 Wright, E. M. 213  
 Yaglom, A. M. 132  
 Yosida, K. 56  
 Zaremba, S. K. 15, 53, 233, 238, 239  
 Zeidman, E. A. 246, 249  
 Zieliński, R. 139  
 Zoltukhin, V. G. 45

## LIST OF NOTATIONS

In the following list of notations, the numbers refer to page numbers of this survey.

$\mathbf{a}, a_r$	13	$p_{rsu}$	16	$Z_{rs}(\Gamma)$	17, 18
$a(\mathbf{q})$	39	$p_{rs}$	16, 17	$Z_{rst}(\Gamma)$	18
$\mathbf{A}, A_{rs}$	13	$p_r$	17	$\Gamma$	17
$\mathbf{b}, b_r$	13	$p_\mu$	5	$\delta_N(f)$	38
$b(\mathbf{p})$	39	$\mathbf{q}$	39	$\delta_z \phi(\mathbf{z})$	42
$c$	17	$q(n)$	3	$\delta_{z_1 z_2 \dots z_k}^k \phi(\mathbf{z})$	42
$c(\mathbf{p})$	39	$q(x)$	30	$\Delta_g$	10
$C$	11	$Q$	14	$\Delta_N(\boldsymbol{\alpha})$	37
$\mathbf{C}(s)$	11	$Q(\mathbf{x})$	4, 48	$\theta$	2
$\mathbf{d}, d_r$	25	$Q_{rm}(\Gamma)$	26	$\theta_h$	8
$d(\mathbf{q})$	39	$R$	3	$\lambda$	7, 14
$d_{\sigma_h}^h \mathbf{z}$	42	$R(\mathbf{q})$	40	$\lambda_D$	30
$D$	11, 25	$R_m$	26	$\lambda_x$	16
$D_{v,N}$	46	$s_M$	44	$\Lambda$	5
$\mathcal{D}_N$	37	$s^*$	12	$\Lambda_D$	29
$\mathcal{D}_{N,\sigma_h}$	42	$S$	3	$(\Lambda, \Psi)$	5
$E[\cdot]$	2	$\bar{S}$	17	$\mu$	2, 14, 26
$E(\boldsymbol{\alpha}) = E(\alpha_1, \alpha_2, \dots, \alpha_k)$	36	$S(t)$	12	$v_i(s)$	10
$f(s)$	2	$S(\mathbf{x})$	14	$v_N(E)$	36
$f(\mathbf{z}) = f(z_1, z_2, \dots, z_k)$		$S_h$	8	$v_N(\boldsymbol{\alpha})$	37
	37, 39	$S_m$	26	$\xi$	3
$f_{\sigma_h}$	42	$\mathbf{t}$	11		37
$F$	3	$\mathbf{t}_0$	12		42
$\mathbf{f}, f_u$	14	$T$	14		5
$F_n$	34	$\mathbf{T}$	11		43
$F_\phi$	7	$T_m$	26		43
$g(s)$	3	$\mathcal{T}_N$	38		43
$g(\xi)$	30	$\mathcal{T}_{N,\sigma_h}$	42		43
$g_{rsu}$	16	$u(s)$	7		45
$g_{ru}$	16	$U$	30		42
$g^*(s)$	12	$v(s)$	8		24
$G$	3, 25	$v_M$	46	$\rho(\mathbf{A})$	14
$G(\mathbf{A})$	15	$\text{var}[\tau]$	2	$\rho(\mathbf{g})$	40
$h(s)$	10	$V$	11	$\sigma_h$	42
$H$	4	$\mathbf{V}$	5	$\tau$	2
$\mathbf{H}, H_{rs}$	13	$V(f)$	42	$\phi$	4
$\mathbf{H}^+, H_{rs}^+$	17	$V(\boldsymbol{\alpha})$	37	$\phi^{-1}$	5
$k_{rs}$	16	$V^k(f)$	42	$\phi_{rs}(u_1, \dots, u_{k_{rs}})$	16
$k_r$	16	$w(s)$	9	$\phi_r(u_1, \dots, u_{k_r})$	16
$\mathbf{K}, K_{rs}$	17	$w_M$	46	$\phi_k(\zeta_1, \dots, \zeta_k)$	2
$\mathbf{L}, L_{us}$	14	$w^*(s)$	12	$\phi(\mathbf{z})$	42
$(L, \mathbf{L}, \lambda)$	6	$W(f)$	42	$\phi_R(n)$	43
$(L_D, \mathbf{L}_D, \lambda_D)$	29	$W_n(s_1, s_2, \dots, s_n)$	9	$\phi(s)$	7
$\mathbf{m}_2[\tau]$	2	$W^h(f_{\sigma_h})$	42	$\Phi$	5
$\mathbf{M}$	17	$\mathbf{x}, x_s$	13	$\Psi$	5
$\mathcal{M}_N$	37	$\mathbf{X}^{(s)}$	25	$\omega$	30
$(M, \mathbf{M}, \mu)$	2	$\mathbf{X}_m$	13	$\Omega$	5
$N$	2	$X_r(\Gamma)$	17, 18	$(\Omega, \Phi)$	5
$\mathcal{N}_N$	37	$X_{rl}(\Gamma)$	18	$\Omega, \omega_u$	14
$\mathbf{p}$	39	$\mathbf{y}^{(s)}$	25	$\ \mathbf{A}\ $	14
$p(s)$	3	$\mathbf{Y}^{(s)}$	25	$\ \mathbf{x}\ $	14
$p(E)$	36	$z_0$	10	$\ \dots\ _n$	48