JOURNAL OF COMPUTATIONAL PHYSICS 49, 394–419 (1983)

The Simulation of Random Processes on Digital Computers: Unavoidable Order*

T. ERBER AND T. M. RYNNE

Department of Physics, Illinois Institute of Technology, Chicago, Illinois 60616

AND

W. F. DARSOW AND M. J. FRANK

Department of Mathematics, Illinois Institute of Technology, Chicago, Illinois 60616

Received April 21, 1982

Nonrandom features of pseudorandom number generators are usually regarded as defects which may be minimized by improving the algorithms or resorting to larger computers. There are, however, certain elements of order which cannot be avoided even on digital devices of arbitrarily large capacity. For instance, on an N-state machine, pseudorandom number generators will terminate on fixed points or fall into loops after approximately $\sqrt{N}$ steps. Combinatorial arguments then can be used to show that for any given algorithm and any finite device it is highly improbable that there are more than three or four distinct terminal loops. All pseudorandom sequences merging into these loops can be traced backwards to their initial numbers; and the resulting pattern of "ancestor numbers" can be charted in detail for any computer, even for noninvertible algorithms. The conflicting requirements of randomness and finite numerical precision lead to an ordered distribution of the set of initial numbers. In this sense neither the initial nor the final states of a simulation of chaotic behavior can ever be random. The "few loop" constraint could generate patterns of self-organization in non-equilibrium systems. Experimental evidence from the hysteresis of Ewing arrays supports this conjecture.

1. INTRODUCTION

Since the original work of Hopf and Krylov there has been a growing interest in applying deterministic simulations of random processes, such as mixing transformations, to problems in statistical physics [1, 2]. Computer modeling has played an important role in interpolating between the tentative theoretical schemes—for instance the iteration of quadratic maps on the interval [3]—and the experimental situations which they are supposed to represent.

* Dedicated to K. Menger on his 80th birthday.

0021-9991/83 $3.00

Copyright © 1983 by Academic Press, Inc.
All rights of reproduction in any form reserved.

The successive links in the chain

$$\begin{matrix}\text{random} \\ \text{process}\end{matrix} \leftrightarrow \begin{matrix}\text{deterministic} \\ \text{simulation}\end{matrix} \leftrightarrow \begin{matrix}\text{computer} \\ \text{modeling}\end{matrix} \leftrightarrow \begin{matrix}\text{physical} \\ \text{system}\end{matrix} \tag{1.1}$$

must, however, be treated with the utmost care: "... pseudo-random numbers form the backbone of computer simulation and Monte Carlo analysis, yet there are essentially no known theorems which make explicit the sense in which pseudo-random numbers are replacements for random numbers" [4]. Moreover, the realization of any pseudorandom number algorithm on a computer is basically an experimental problem since digital networks are restricted to processing finite sets whereas the theoretical schemes promise random behavior only on sets of positive, nonatomic measure. Finally, in order to ensure that the discrete models give a faithful representation of the behavior of the associated continuous systems, it is also necessary to check the numerical criteria of consistency, convergence, and stability [5, 6].

Fortunately there are examples which show that the entire sequence (1.1) can in fact be realized. If the physical systems are either harmonic oscillators or cascades of biased product detectors, their stochastic behavior can be simulated with Chebyshev mixing transformations [7, 8]. Extensive trials have also confirmed that the Chebyshev mixing can be approximated with excellent statistical fidelity on a wide variety of digital devices. Similar results have been obtained for other mixing processes which are conjugate transforms of the Chebyshev polynomials [9]. In all cases the computer-generated sequences continue to imitate the "right" pseudorandom features even after the cumulative roundoff and truncation errors have been amplified by the iterations to the point where they dominate the numerical aspects of the calculations. Here and subsequently, a sequence of digits qualifies as being pseudorandom if it satisfies the usual criteria involving equidistributivity and normality; and has auto- and cross-correlations equivalent to those of white noise [7, 10]. Computer simulations of these mixing transformations can also be adapted to imitate various physical aspects of irreversible and disordered systems: ergodicity, fading memory (relaxation), instability, and the irreversible dispersal of any set of positive measure throughout the domains of the mixing processes [2, 11, 12].

In general the pseudorandom sequences generated by mixing transformations can be visualized as extending indefinitely far into the "past" and the "future" without ever encountering a repetition. For instance, in the Chebyshev case the set of points which will eventually recur under iteration—the cyclic points—can be enumerated explicitly. This set is dense, but countably infinite, and therefore of measure zero [7, Eqs. (3.7a)–(3.7c)]. Thus if a Chebyshev mixing sequence is constructed starting with any number, the probability of having selected one of the pseudorandom but periodic sequences is zero. It is precisely this perpetual wandering which cannot be imitated on any finite digital device because every computer-generated sequence necessarily terminates in a cycle. Specifically, for any mapping $\mathscr{M}: x_i \to x_j$ of a finite set of N distinct objects, $x_1, x_2, ..., x_N$, to itself, each sequence of iterates

$$\mathscr{M}(x_i), \mathscr{M}^2(x_i), ..., \mathscr{M}^f(x_i), ..., \mathscr{M}^l(x_i), ..., \mathscr{M}^m(x_i) \tag{1.2}$$

must contain at least two identical elements, say $\mathcal{M}^f(x_i)$ and $\mathcal{M}^l(x_i)$, whenever $m > N$, irrespective of the choice of the initial "seed" x_i (pigeonhole principle [13]). In computing terminology this implies that (1.2) consists of a "free-running" subsequence $\mathcal{M}(x_i),\ldots,\mathcal{M}^{f-1}(x_i)$ containing no repetitions, and a contiguous subsequence $\mathcal{M}^f(x_i),\ldots,\mathcal{M}^l(x_i)$ which constitutes a terminal loop with $l-f$ distinct elements. Physically this means simply that all iterative processes on finite sets eventually degenerate into clocks.

These obvious distinctions between infinite strings of nonrecurrent numbers and sequences which ultimately become periodic have drastic consequences. For if the computer-generated sequences are also intended to imitate chaotic behavior, we encounter the paradoxical situation that it is precisely the simulation of *disorder* which imposes a high degree of *order* on the initial and final states of any pseudorandom algorithm. In Section 2 we analyze this point by introducing a combinatorial lemma concerning the likelihood of coincidences in random sequences. The results enable us to show that for any pseudorandom number algorithm and any digital network it is highly improbable that the sequences (1.2) will terminate in more than three or four distinct terminal cycles *regardless* of the choice of the initial seed x_i. Furthermore, the distribution of the numbers on all these terminal loops cannot be completely uncorrelated.

The limited ability of computers to simulate pseudorandom behavior also influences another aspect of the structure of the sequences (1.2). Observe that for any mapping $\mathcal{M}$, it is possible, at least in principle, to trace back all of the preimages, or ancestor points, of any element. For instance, the quadratic Chebyshev polynomial $C_2(x) = x^2 - 2$ is mixing on the interval $[-2, 2]$ and noninvertible, but the entire set of preimages for any element x can be explicitly constructed with the help of the simple scheme [7, (6.2)]

$$
\begin{array}{l}
\cdots \\
\quad \nearrow + [(x+2)^{1/2}+2]^{1/2} \\
\cdots \\
\cdots \\
\quad \searrow - [(x+2)^{1/2}+2]^{1/2} \\
\cdots \\
\cdots \\
\quad \nearrow + [-(x+2)^{1/2}+2]^{1/2} \\
\cdots \\
\cdots \\
\quad \searrow - [-(x+2)^{1/2}+2]^{1/2} \\
\cdots
\end{array}
\qquad
\begin{array}{l}
\\
\quad \searrow + (x+2)^{1/2} \\
\\
\\
\quad \nearrow - (x+2)^{1/2} \\
\\
\end{array}
\qquad
\begin{array}{l}
\\
\\
\quad x \to x^2 - 2 \to \cdots . \\
\\
\\
\end{array}
\tag{1.3}
$$

If this fan-out of preimages is followed on a computer, the finite precision of the calculations leads to a progressive extinction of all ancestral lines. In other words, each machine-generated sequence (1.2) has a definite "age" corresponding to the number of iterations linking its "oldest" starting element (i.e., a number having *no* preimages on the computer) to $\mathscr{M}^f(x)$, where the sequence merges into a terminal cycle. In Section 4 we discuss this behavior in quantitative detail using the Chebyshev mixing as a specific example. We shall see that the statistical properties of the entire set of sequences (1.2) permit us to assign an average age to the mixing so that the Chebyshev simulations in effect display a time evolution. One consequence is that computer simulations of mixing processes cannot be strictly ergodic.

All results of this kind concerning the existence of latent, ineluctable patterns of order may be interpreted in at least two different ways. If one is mainly interested in perfecting the computer simulations of chaotic behavior, then the essential precaution which emerges from this work is to rely only on those portions of the machine-generated sequences (1.2) that are "free-running" and not too "young"—in other words, avoid the structure inherent in the initial and final states. With these safeguards most of the existing schemes for modeling chaos are left intact, and one can wring out still more of the latent correlations. On the other hand, the appearance of patterns of order in pseudorandom processes can also reflect the actual behavior of physical systems—particularly the tendency for self-organization in nonequilibrium systems. We shall see in Section 3 that the long-time or asymptotic response of some large scale hysteresis systems corresponds precisely to the limiting behavior predicted by the "few loop" principle. In this sense the study of the terminal states of discrete finite systems evolving under pseudorandom laws is a useful extension of the scope of statistical physics. We also touch on some implications for encryption and information compression in Section 3.

2. The Few Loop Principle

A. *The Double Birthday Lemma*

A random string of n binary numbers is said to contain a maximal, or irreducible, amount of information because approximately n bits of information are required to specify its construction [14, 15]. In contrast, a pseudorandom string generated by a given mapping $\mathscr{M}$ contains relatively little information since in principle the entire string is completely determined by the initial number. For example, if one programs the algorithm $\mathscr{M}$: $x \mapsto x^2 - 2$ (the simple mixing transformation C_2), then all successive elements $\mathscr{M}^m(x_i)$, $m = 1, 2,...,$ are determined by the choice of x_i. Now in practical computations the actual values of the numbers $\mathscr{M}^m(x_i)$ will be affected by cumulative roundoff and truncation errors, but this does not alter the basic information mismatch between random processes and pseudorandom simulations (cf. [15, Theorem 21.4]). The equivalence of computational complexity, information content, and degree of disorder is based on the familiar notion that an n-bit string of random

numbers ought to pass at least n tests of randomness. A pseudorandom sequence of course is likely to fail at least some of these tests. Every such failure is indicative of a trace of regularity, and as we shall see, a suitable series of randomness tests applied to computer models of chaos can actually be used to infer the existence of pervasive patterns of order. To this end, we derive a combinatorial result related to the well-known "birthday" problem [16].

LEMMA [17]. *From an urn containing N distinguishable objects, observer $\mathscr{R}$ draws one object at a time, at random with replacement, until a repetition occurs. A similar set of draws is made by another observer $\mathscr{B}$. The probability P_N^1 that $\mathscr{R}$ and $\mathscr{B}$ have selected at least one object in common is then given by*

$$P_N^1 = \frac{2}{3} + \frac{(N-1)!}{6N^N} \sum_{k=0}^{N} \frac{N^k}{k!}, \tag{2.1a}$$

and

$$P_N^1 = \tfrac{2}{3} + \tfrac{1}{12}\sqrt{2\pi/N} + (1/9N) + O(1/N^{3/2}). \tag{2.1b}$$

Proof. Suppose $\mathscr{R}$ has drawn i distinct objects, and $\mathscr{B}$ has drawn j distinct objects; then there are $ijN!/(N-i-j)!$ distinct sequences of draws in which $\mathscr{R}$ and $\mathscr{B}$ have *not* selected any object in common. Since $\mathscr{R}$ and $\mathscr{B}$ together have made $i+j+2$ draws, the corresponding total number of possible sequences is N^{i+j+2}. Therefore, if p_N^0 is the probability that $\mathscr{R}$ and $\mathscr{B}$ have not selected any object in common, then P_N^1 is given by

$$1 - P_N^1 = p_N^0 = N! \sum_{i+j \leqslant N} \frac{ij}{(N-i-j)!\, N^{i+j+2}}. \tag{2.2}$$

The summation terminates at the indicated limit because for $i+j > N$ it is certain that $\mathscr{R}$ and $\mathscr{B}$ must have made a common choice (pigeonhole principle once again [13]!).

With $k = i+j$, (2.2) can be rewritten as

$$\begin{aligned} p_N^0 &= N! \sum_{k=2}^{N} \left\{ \sum_{i=1}^{k-1} i(k-i) \right\} \Big/ ([N-k]!\, N^{k+2}) \\ &= \frac{(N-1)!}{6} \sum_{k=0}^{N} \frac{(k^2-1)\,k}{(N-k)!\, N^{k+1}}. \end{aligned} \tag{2.3}$$

The last expression can be simplified:

$$\begin{aligned} \sum_{k=0}^{N} \frac{(k^2-1)\,k}{(N-k)!\, N^{k+1}} &= \sum_{k=0}^{N-1} (k^2-1) \left[\frac{1}{(N-k)!\, N^k} - \frac{1}{(N-k-1)!\, N^{k+1}} \right] + \frac{N^2-1}{N^N} \\ &= \sum_{k=0}^{N-1} \frac{k^2-1}{(N-k)!\, N^k} - \sum_{k=1}^{N} \frac{(k-1)^2-1}{(N-k)!\, N^k} + \frac{N^2-1}{N^N} \end{aligned}$$

$$= \sum_{k=1}^{N-1} \frac{2k-1}{(N-k)!\,N^k} - \frac{1}{N!} - \frac{N^2-2N}{N^N} + \frac{N^2-1}{N^N}$$

$$= \sum_{k=0}^{N} \frac{2k-1}{(N-k)!\,N^k}. \tag{2.4}$$

By similar means the remaining linear term in k in (2.4) can also be removed:

$$\sum_{k=0}^{N} \frac{2k-1}{(N-k)!\,N^k} = 2N \sum_{k=0}^{N-1} \left[\frac{1}{(N-k)!\,N^k} - \frac{1}{(N-k-1)!\,N^{k+1}} \right] + \frac{2N}{N^N} - \sum_{k=0}^{N} \frac{1}{(N-k)!\,N^k}$$

$$= \frac{2}{(N-1)!} - \sum_{k=0}^{N} \frac{1}{(N-k)!\,N^k}$$

$$= \frac{2}{(N-1)!} - \frac{1}{N^N} \sum_{k=0}^{N} \frac{N^k}{k!}. \tag{2.5}$$

By combining (2.2)–(2.5) we obtain the first part of the lemma, Eq. (2.1a). Since the sum in (2.1a) can be expressed in terms of the incomplete gamma function,

$$\sum_{k=0}^{N} \frac{x^k}{k!} = e^x \left(1 - \frac{\gamma(N+1, x)}{N!} \right),$$

standard asymptotic results, such as [18]

$$\sum_{k=0}^{N} \frac{N^k}{k!} = e^N \left\{ \frac{1}{2} + \frac{1}{3} \sqrt{\frac{2}{\pi N}} + O\left(\frac{1}{N} \right) \right\},$$

and Stirling's approximation may be used to reduce (2.1a) to (2.1b).

The numerical comparisons given in Table I indicate that the $O(N^{-3/2})$ terms in

TABLE I

Exact and Approximate Values of the Coincidence Probability P_N^1

N	P_N^1 exact, Eq. (2.1a)	P_N^1 approximate, Eq. (2.1b)
10	0.744 337	0.743 833
10^2	0.688 683	0.688 663
10^3	0.673 384	0.673 383
10^4	0.688 768	0.688 766
10^5	0.667 329	0.667 328
10^6	0.666 876	0.666 875
10^7	0.666 733	0.666 732
∞	$\frac{2}{3}$	—

(2.1b) are negligible for $N \gtrsim 10$. An auxiliary calculation also yields an estimate of the average number of draws made by $\mathscr{R}$ and $\mathscr{B}$ in order to obtain a match. This number can be inferred from the ratio

$$F_N(t) = \frac{(N-1)!}{6p_N^0} \sum_{k=0}^{[tN^{1/2}]} \frac{(k^2-1)\,k}{(N-k)!\,N^{k+1}}, \tag{2.6}$$

where $[tN^{1/2}]$ is the largest integer contained in $tN^{1/2}$. By (2.3), this is the conditional probability that the total number of distinct objects drawn by $\mathscr{R}$ and $\mathscr{B}$ does not exceed $tN^{1/2}$, given that no objects were selected in common. When $N \gtrsim 10^2$, the ratio $F_N(t)$ is essentially independent of N, so it suffices to consider the asymptotic approximation $F_N(t) \to_{N \gg 1} F(t)$. This function is plotted in Fig. 1 and partially tabulated in Table II. Note that most of the contributions to the sum (2.3) originate in the narrow range $1.03 \lesssim t \lesssim 2.79$, and that the median value $F(t) \sim 50\%$ occurs at $t \sim 1.83$. Consequently, the median of the sum of the draws made by $\mathscr{R}$ and $\mathscr{B}$ in the event that both find repetitions without selecting a common object is

$$\langle i + j \rangle \simeq 1.83 N^{1/2}. \tag{2.7a}$$

An independent calculation of the median of the sum of the draws made by $\mathscr{R}$ and $\mathscr{B}$ in the case that both find repetitions but without any coincidence constraints leads to a somewhat higher value [19, 35]

$$\langle i + j \rangle \simeq 2.44 N^{1/2}. \tag{2.7b}$$

A distributional analysis of the urn drawing model also confirms the intuitive expec-

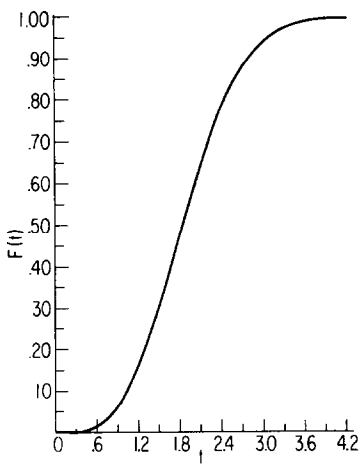

FIG. 1. Contributions to the noncoincidence probability p_N^0. The graph indicates that most of the contribution to the sum (2.3) originates in the narrow range $1.0N^{1/2} \lesssim k \lesssim 2.8N^{1/2}$. The variable t is defined in Eq. (2.6).

TABLE II

Values of the Ratio $F(t)$

t	0.40	0.48	0.53	0.57	0.61	0.64	0.69	0.71
$F(t)$	0.003	0.006	0.009	0.012	0.015	0.018	0.024	0.027
t	0.73	0.82	0.89	1.00	1.09	1.17	1.24	1.30
$F(t)$	0.030	0.045	0.060	0.090	0.120	0.150	0.180	0.210
t	1.37	1.48	1.59	1.70	1.80	1.90	2.01	2.13
$F(t)$	0.240	0.300	0.360	0.420	0.480	0.540	0.600	0.660
t	2.25	2.39	2.56	2.79	2.86	2.95	3.06	3.18
$F(t)$	0.721	0.781	0.841	0.901	0.912	0.931	0.950	0.962
t	3.38	3.50	3.70	3.80	3.90	4.27	4.74	5.00
$F(t)$	0.980	0.986	0.992	0.994	0.996	0.999	0.9998	0.99996

Note. $F(t) \approx F_N(t)$, $N \gg 1$, cf. (2.6); the exact values of $F_N(t)$ differ from the table entries by less than 10^{-3} for $N = 10^4$.

tation that longer series of draws increase the probability of finding coincidences. For instance, given a series of draws by $\mathscr{R}$ and $\mathscr{B}$—each terminating in a repetition as in the Lemma—in about 7.6% of the cases the sum of the draws will exceed the estimate (2.7a) by a factor of two, i.e.,

$$\langle i + j \rangle \sim 3.6N^{1/2}. \tag{2.7c}$$

In these "long" draws the probability of obtaining at least one coincidence between the objects drawn by $\mathscr{R}$ and $\mathscr{B}$ has risen to 94%.

Of course if $\mathscr{R}$ and $\mathscr{B}$ sample from an urn as indicated in the Lemma it is also possible for multiple coincidences to occur between the two series of draws. Let p_N^m be the probability that $\mathscr{R}$ and $\mathscr{B}$ have selected exactly m distinct objects in common. Then we already know that

$$p_N^0 = \tfrac{1}{3} + O(N^{-1/2}). \tag{2.8}$$

The single and higher order coincidences can then be obtained from expressions analogous to (2.2). In particular the next four probabilities are [19]

$$\begin{aligned} p_N^1 &= \tfrac{4}{15} + O(N^{-(\frac{1}{2}+\varepsilon_1)}), & p_N^2 &= \tfrac{6}{35} + O(N^{-(\frac{1}{2}+\varepsilon_2)}), \\ p_N^3 &= \tfrac{32}{315} + O(N^{-(\frac{1}{2}+\varepsilon_3)}), & p_N^4 &= \tfrac{40}{693} + O(N^{-(\frac{1}{2}+\varepsilon_4)}), \end{aligned} \tag{2.9}$$

where $\varepsilon_i > 0$. Evidently the probability p_N^1 of finding a single match does not nearly exhaust the total probability P_N^1 of finding coincidences. This leads to the curious result that even the probability of finding *three* or more common elements in an independent series of draws made by $\mathscr{R}$ and $\mathscr{B}$ is not negligible, for

$$P_N^3 = 1 - (p_N^0 + p_N^1 + p_N^2) \to \tfrac{8}{35} \qquad (N \gg 1). \tag{2.10}$$

B. *The Few Loop Principle*

The results of the "double birthday" lemma imply severe constraints on the behavior of the terminal loops of computer simulations of chaotic systems. To be specific, let us suppose that $\mathscr{M}_u(x)$ is a uniform pseudorandom number generator that maps the unit interval onto itself; the piecewise linear mixing transformation $\mathscr{M}_{h(2)}(x) = |2x - 1|$, $x \in [0, 1]$, is a simple example (cf. (A6)). Another type often encountered in practice is the RANDU algorithm [36]. If $\mathscr{M}_u$ is programmed to run on a machine that effectively operates with q digits to the base 10, then the accessible universe $\mathscr{N}$ of numbers in $[0, 1]$ consists of

$$N_q = 10^q + 1 \tag{2.11a}$$

distinct fixed point displays including all the digit combinations ranging from

$$0.0_1 0_2 \cdots 0_q \quad \text{to} \quad 0.9_1 9_2 \cdots 9_q, \quad \text{and} \quad 1.0_1 0_2 \cdots 0_{q-1}. \tag{2.11b}$$

The computer may then be regarded as an "urn" containing the N_q distinct elements of the set $\mathscr{N}$ which can be "drawn" or sequentially displayed by running the $\mathscr{M}_u$ program. In particular, we can start with a number $\bar{x}_0$ arbitrarily chosen from $\mathscr{N}$ (2.11b) and form a sequence of pseudorandom numbers simply by iterating the program for calculating $\mathscr{M}_u(\bar{x}_0)$. Upon setting $\mathscr{M}_u(\bar{x}_0) = \bar{x}_1$, $\mathscr{M}_u(\bar{x}_1) = \bar{x}_2$, and so forth, we can rewrite the pseudorandom sequence (1.2) in the parallel form

$$\begin{array}{ccccccccccc} \bar{x}_0, & \bar{x}_1, & & \bar{x}_2, & \cdots, & \bar{x}_f, & & \bar{x}_{f+1}, & \cdots, & \bar{x}_l, & \bar{x}_{l+1}, & \cdots \\ & \updownarrow & & \updownarrow & & \updownarrow & & \updownarrow & & \updownarrow & \updownarrow & \\ \bar{x}_0 \to & \mathscr{M}_u^1(\bar{x}_0) & \to & \mathscr{M}_u^2(\bar{x}_0) & \to \cdots \to & \mathscr{M}_u^f(\bar{x}_0) & \to & \mathscr{M}_u^{f+1}(\bar{x}_0) & \to \cdots \to & \mathscr{M}_u^l(\bar{x}_0) & \to \mathscr{M}_u^{l+1}(\bar{x}_0) \to & \cdots . \end{array} \tag{2.12}$$

The numbers indicated by the special symbols $\bar{x}_f$ and $\bar{x}_l$ then represent elements with a dual significance. First of all, if the sequence $\{\bar{x}_i\}$ actually imitates random behavior, it must also simulate the "single birthday" situation: after approximately $N_q^{1/2}$ iterations it should then become likely that two elements, say $\bar{x}_f$ and $\bar{x}_l$, represent the same computer display. Extensive numerical experiments with the Chebyshev mixing transform C_2 and its conjugate image $\mathscr{M}_{h(2)}$ confirm that the average running length l required for encountering a repetition is of the order of $N_q^{1/2}$, in agreement with (2.7b). The pigeonhole principle also guarantees that some value of the index $l \leqslant N_q + 1$ *forces* a repetition in the selection of the elements and ensures that the sequence (2.12) merges into a terminal loop. Both these aspects of $\bar{x}_f$ and $\bar{x}_l$ are illustrated by the diagram in Fig. 2a.

The constraints of the "double birthday" lemma appear when we repeat this procedure. Suppose we choose a different initial element, say $\bar{y}_0$, from the set (2.11b) and construct another pseudorandom sequence analogous to (2.12):

$$\begin{array}{ccccccc} \bar{y}_0, & \bar{y}_1, & \cdots, & \bar{y}_{f'}, & \cdots, & \bar{y}_{l'}, & \cdots \\ \bar{y}_0 \to & \mathscr{M}_u(\bar{y}_0) \to \cdots \to & \mathscr{M}_u^{f'}(\bar{y}_0) & \to \cdots \to & \mathscr{M}_u^{l'}(\bar{y}_0) & \to \cdots . & \end{array} \tag{2.13}$$

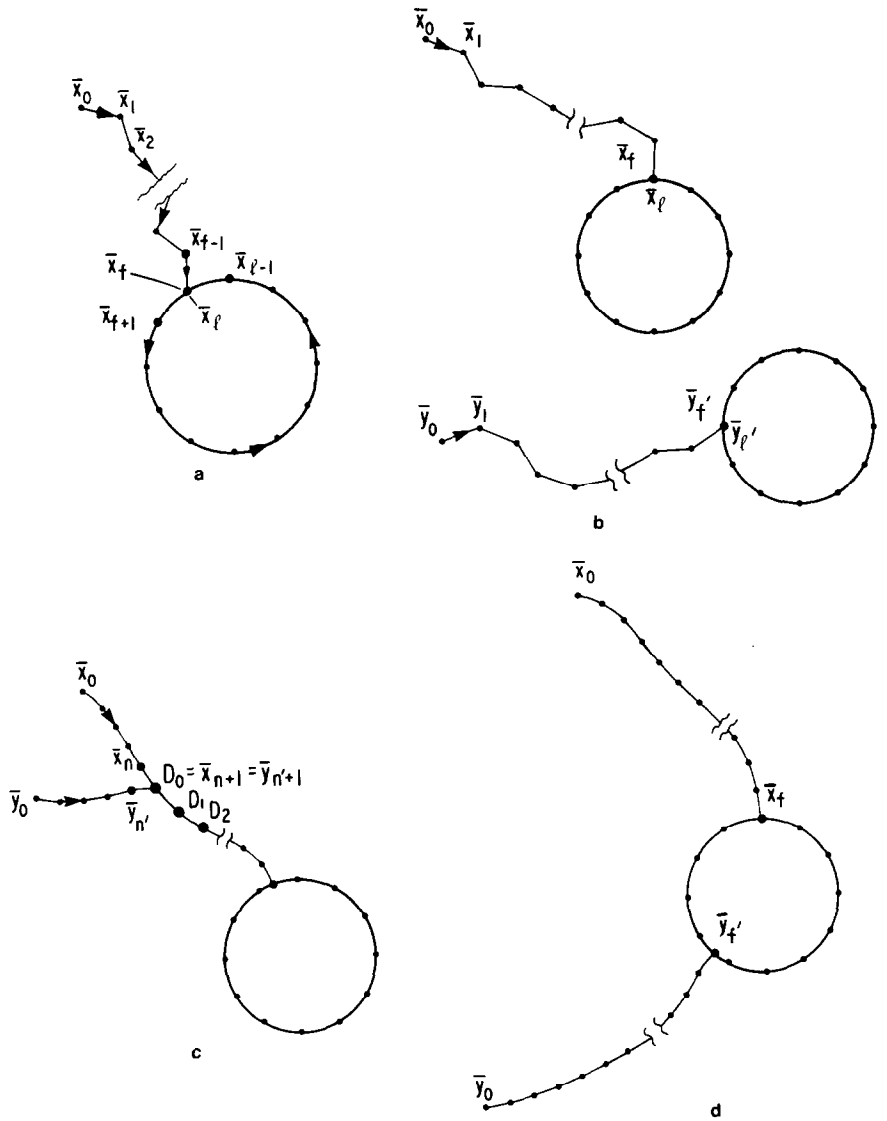

FIG. 2. (a) Flow network or de Bruijn diagram [20] for the pseudorandom sequence (2.12). The chain of points begins with the initial seed $\bar{x}_0$ and eventually enters a terminal loop at $\bar{x}_f$. There are $l-f$ distinct points in the loop which form a cycle under the action of $\mathcal{M}_u$. According to a "single birthday" estimate [19, 35] the magnitude of l is approximately $1.2N_q^{1/2}$, where N_q is the number of points in the computer universe (2.11a). The diagram reflects the conventions adopted in (1.2) and (2.12): the elements $\bar{x}_f$ and $\bar{x}_l$ represent identical computer displays. (b) Flow networks for two pseudorandom sequences merging into disjoint terminal loops. Computer trials confirm that statistical tests for random behavior are satisfied on large loops, i.e., $l-f \sim O(N_q^{1/2}) \gg 1$ [7, 19, 35]. (c) Flow network for two pseudorandom sequences that join before entering the terminal loop. All elements beginning with D_0 are identical for both sequences (cf. (3.1)). (d) Flow network for two pseudorandom sequences with a common terminal loop.

By convention the elements $\bar{y}_{f'}$ and $\bar{y}_{l'}$ again represent identical computer displays —the object drawn twice from the urn—and as before, this repetition becomes likely when $l' \sim N_q^{1/2}$.

If the two pseudorandom sequences $\{\bar{x}_t\}$ and $\{\bar{y}_j\}$ do *not* have any common elements, the corresponding computer runs will merge into different terminal loops as shown in Fig. 2b. The double birthday lemma, however, indicates that this is not the most favored situation. If one constructs many pairs of pseudorandom strings, like (2.12) and (2.13), each time beginning with numbers drawn from the set (2.11b), then the coincidence probability P_N^1 (2.1a), (2.1b) implies that in about 67% of the cases the two sequences will merge. The corresponding flow diagrams are shown in Figs. 2c and 2d. Note that the two sequences may join either before or after they have entered a terminal loop. We shall say more about these possibilities in Section 4.

By a slight extension of these arguments it is then possible to estimate the average number of terminal cycles associated with any uniform pseudorandom number generator $\mathscr{M}_u$. Begin with the sequence (2.12), and consider the set

$$\bar{\mathscr{X}} = \{\bar{x}\colon \mathscr{M}_u^m(\bar{x}) = \bar{x}_f \text{ for some } m \geqslant 0\}. \tag{2.14}$$

Here $\bar{\mathscr{X}}$ is one computer orbit of $\mathscr{M}_u$; it consists of all numbers in $\mathscr{N}$ which eventually end up in the loop $\bar{x}_f, \ldots, \bar{x}_{l-1}$ by repeated application of $\mathscr{M}_u$. The explicit enumeration of all the preimages, or ancestor numbers, of the loop can be quite laborious (cf. Section 4). Suppose now that the loop $\bar{y}_{f'}, \ldots, \bar{y}_{l'-1}$ in (2.13) is not contained in $\bar{\mathscr{X}}$; this is the situation shown in Fig. 2b. We can then form its orbit $\bar{\mathscr{Y}}$, i.e.,

$$\bar{\mathscr{Y}} = \{\bar{y}\colon \mathscr{M}_u^m(\bar{y}) = \bar{y}_{f'} \text{ for some } m \geqslant 0\}. \tag{2.15}$$

Note that $\bar{\mathscr{X}}$ and $\bar{\mathscr{Y}}$ are disjoint. By continuing this procedure we can in principle identify all the terminal loops of $\mathscr{M}_u$ on any particular computer $\mathscr{C}$ and construct the associated orbits. The end result is a partition of all the computer displays $\mathscr{N}$ (2.11b) among the various orbit sets, i.e.,

$$\mathscr{N} = \bar{\mathscr{X}} + \bar{\mathscr{Y}} + \bar{\mathscr{Z}} + \cdots. \tag{2.16}$$

If there are τ loops in all, and we imagine for convenience that each orbit is color coded—say all the $\bar{x} \in \bar{\mathscr{X}}$ are "red" numbers, all the $\bar{y} \in \bar{\mathscr{Y}}$ are "blue" numbers, and so on—then (2.16) is simply a summation over τ distinct color sets.

So now we can repeat the "double birthday" question with a new twist: Suppose that we choose any two numbers $\bar{s}_1$ and $\bar{s}_2$ from $\mathscr{N}$ and construct the pseudorandom strings $\mathscr{M}_u^m(\bar{s}_1)$ and $\mathscr{M}_u^{m'}(\bar{s}_2)$, where $m, m' = 1, 2, 3, \ldots$. Then clearly the probability $p_\tau(\mathscr{M}_u, \mathscr{C})$ that $\bar{s}_1$ and $\bar{s}_2$ belong to the same orbit of $\mathscr{M}_u$ is given by

$$p_\tau(\mathscr{M}_u, \mathscr{C}) = [N_q(N_q - 1)]^{-1} \sum_{t=1}^{\tau} n_t(n_t - 1), \tag{2.17}$$

where n_t is the number of elements in the tth orbit of $\mathscr{M}_u$. For any computer $\mathscr{C}$ these weight factors n_t can be found explicitly (Section 4). However, to expedite the arguments leading to the "few loop" estimate we introduce a plausible shortcut: *assume that in first approximation every uniform pseudorandom algorithm $\mathscr{M}_u$ generates an equipartition of the computer numbers $\mathscr{N}$ among its orbit sets*, i.e.,

$$n_1 \approx n_2 \approx n_3 \approx \cdots \approx n_\tau \approx N_q/\tau. \tag{2.18}$$

Indeed if there were some definite ranking of the orbit sizes, then the favored "colors" would represent a departure from random behavior (see below). Of course this ansatz ignores the presence of "small" orbits whose terminal states have comparatively few preimages. The multiplicity of these small orbits is discussed in [7, Sect. 5]. Since in all practical cases $N_q \gg 1$, Eqs. (2.17) and (2.18) imply that

$$p_\tau(\mathscr{M}_u, \mathscr{C}) \simeq 1/\tau, \tag{2.19}$$

independently of the pseudorandom algorithm $\mathscr{M}_u$ and the computer $\mathscr{C}$.

It is really not surprising that this matching probability p_τ differs from the coincidence probability P_N^1 (2.1b) of the double birthday lemma; after all, the underlying combinatorial problems are quite different. Both problems, however, were deliberately set up to model the *same* physical situation—the confluence of pairs of pseudorandom sequences—and therefore we can reasonably expect that the two probabilities will be similar even if they are not identical. One way of ensuring this consistency is to require

$$P_N^1 \simeq \tfrac{2}{3} \sim 1/\tau \simeq p_\tau(\mathscr{M}_u, \mathscr{C}), \qquad N_q \gg 1; \tag{2.20}$$

and clearly this implies that τ cannot be a large number. The entire chain of argument can then be summarized by way of the following *Few Loop Principle*:

> Let $\mathscr{M}_u$ be any uniform pseudorandom number algorithm programmed to run on a digital computer $\mathscr{C}$ capable of N_q ($\gg 1$) displays. Suppose that $\mathscr{M}_u$ generates an approximate equipartition of N_q among its orbit sets. Then it is unlikely that $\mathscr{M}_u$ has more than three or four distinct orbits or terminal loops on $\mathscr{C}$.

Inasmuch as estimates expressed in terms of "likely" or "unlikely" hardly qualify as theorems, we shall refer to this conclusion as the few loop principle. If there is ever a need to find the actual probabilities for the confluence of more pseudorandom number strings, the combinatorics of the double birthday lemma can be extended and the few loop arguments upgraded to the level of a theorem. For instance, the analogue of (2.2) for the "triple" birthday lemma is

$$q_N^0 = N! \sum_{i+j+k \leqslant N} \frac{ijk}{(N-i-j-k)!\, N^{i+j+k+3}}, \tag{2.21}$$

where q_N^0 denotes the probability of not selecting any object in common in three independent series of draws each terminating in a repetition. It can be shown that

$$q_N^0 = \tfrac{1}{15} - \tfrac{1}{24}\sqrt{2\pi/N} - (1/45N) + O(1/N^{3/2}), \tag{2.22}$$

and this result is also consistent with the few loop principle [19].

All the available evidence from trials with a variety of machines, including programmable calculators, indicates that uniform mixing transformations like $\mathcal{M}_{h(2)}$ and $\mathcal{M}_{h(3)}$ (cf. Appendix), as well as multiplicative congruence algorithms of the RANDU type (cf. [7, Table III]), have no more than three significant terminal cycles. One precaution which is essential for the computer experiments is that the capacity N_q must be sufficiently large so that the randomizing action of the iterations is not throttled by combinatorial constraints. This point is discussed in detail in [7, Sect. 5]. Furthermore [7, Table II(a)] shows that the three loop limit also appears in computer simulations of the quadratic Chebyshev polynomial C_2, even though this is a *nonuniform* mixing transformation [8].

The few loop principle can be placed into a larger context. Suppose we consider the set $\mathcal{S}$ comprising all possible mappings of N_q (cf. (2.11a)) into itself: evidently there are a total of $N_q^{N_q}$ such mappings. It has been shown by Kruskal [37] and Harris [38] that if one selects a function at random from the set $\mathcal{S}$, then the mean number of terminal loops is of the order

$$n(\mathcal{S}) \sim \tfrac{1}{2}(\ln N_q + \ln 2 + \gamma), \qquad N_q \gg 1, \tag{2.23}$$

where $\gamma \simeq 0.577...$ is Euler's constant. The weak dependence of $n(\mathcal{S})$ on N_q is already symptomatic of a "not very many loops" principle for computers of any practical size. Clearly, many of the mappings included in $\mathcal{S}$ correspond to ordered transpositions of the elements N_q and therefore escape the restrictions of the double birthday lemma and other tests of pseudorandom behavior. The few loop principle appears if we narrow the choice of functions in $\mathcal{S}$ to those which simulate random number generators under iteration.

Some of the combinatorial arguments leading to the few loop principle can be inverted to yield information on the orbit sizes n_t, cf. (2.17). Suppose for example that we drop equipartition hypothesis (2.18) and instead *assume* that the uniform pseudorandom number generator $\mathcal{M}_u$ has only two or three significant terminal loops. Then the results of the double and triple birthday lemmas, Eqs. (2.2) and (2.21), can be combined with combinatorial expressions such as (2.17) to derive constraints on the relative orbit sizes. One finds a considerable deviation from equipartition; both in the two and three loop cases about 80% of the computer numbers N_q belong to a single orbit [19]! This trend is consistent with the limited statistical evidence available in [7, Tables II(a) and III].

Finally, the fact that pairs of random sequences can have unintuitively high coincidence probabilities is the basis of a well-known card trick. Some years ago M. Kruskal found a simple method for selecting sequences of cards from a shuffled

deck with the surprising property that the face value of the last card is *insensitive* to the choice of initial card with a probability of 80% [21]. It is conceivable that both the few loop principle and Kruskal's algorithm are merely precursors of a large class of methods for forcing chaotic systems towards small sets of ordered final states.

3. Extensions and Applications

A. *Memory Dependent Feedback*

The correspondence between urn drawing models and pseudorandom computer simulations breaks down at once if we consider multiple coincidences. This becomes evident if we recall the two pseudorandom sequences (2.12) and (2.13) and adjust the notation to show the confluence indicated in Fig. 2c. The pattern of iterations can then be written in the parallel form

$$\begin{array}{lllllll}
\bar{x}_0, & \bar{x}_1, & \cdots, & \bar{x}_n, & \bar{x}_{n+1}, & \bar{x}_{n+2}, & \cdots \\
\bar{x}_0 \to \mathcal{M}_u^1(\bar{x}_0) \to \cdots \to \mathcal{M}_u^n(\bar{x}_0) \to & \mathcal{M}_u^{n+1}(\bar{x}_0) \to & \mathcal{M}_u^{n+2}(\bar{x}_0) \to \cdots & & & & \\
 & & \| & \| & & & \\
 & & D_0, & D_1, & D_2, D_3, \ldots & & \\
 & & \| & \| & & & \\
\bar{y}_0 \to \mathcal{M}_u^1(\bar{y}_0) \to \cdots \to \mathcal{M}_u^{n'}(\bar{y}_0) \to & \mathcal{M}_u^{n'+1}(\bar{y}_0) \to & \mathcal{M}_u^{n'+2}(\bar{y}_0) \to \cdots & & & & \\
\bar{y}_0, & \bar{y}_1, & \cdots, & \bar{y}_{n'}, & \bar{y}_{n'+1}, & \bar{y}_{n'+2}, & \cdots,
\end{array} \tag{3.1}$$

where the new symbol D_0 denotes the first common element. Clearly, if $\mathcal{M}_u$ represents *any* state-determined algorithm, then the occurrence of even a single coincidence

$$\mathcal{M}_u^{n+1}(\bar{x}_0) = D_0 = \mathcal{M}_u^{n'+1}(\bar{y}_0) \tag{3.2}$$

automatically ensures that all subsequent iterates follow a common track. In this case the idealization that the sequences $\{\bar{x}_i\}$, $i > n$, and $\{\bar{y}_j\}, j > n'$, represent independent random drawings becomes nonsensical, and it is pointless to check whether the multiple coincidence probabilities (2.9) are satisfied. However, this kind of degeneracy is not an inherent limitation of deterministic simulations. One remedy which is easy to implement on computers is to scramble the regular iterative patterns of (3.1) with memory dependent feedback. Specifically, if we have arrived at the $(n+2)$th term of the sequence $\{\bar{x}_i\}$, it is possible to associate a "memory" with the values of the preceding m terms by forming the product

$$\prod_{n+2-m}^{n+1} \bar{x}_i = p_m(\bar{x}_{n+2}). \tag{3.3}$$

The iteration of any uniform pseudorandom algorithm $\mathcal{M}_u$ can then be altered by adding increments proportional to $p_m(\bar{x}_{n+2})$, e.g.,

$$\cdots \to \mathcal{M}_u[\bar{x}_{n-1} + \delta p_m(\bar{x}_n)] \to \mathcal{M}_u[\bar{x}_n + \delta p_m(\bar{x}_{n+1})] \to \mathcal{M}_u[\bar{x}_{n+1} + \delta p_m(\bar{x}_{n+2})] \to \cdots, \tag{3.4}$$

where δ is a constant that is adjusted to be small enough so that the perturbations do not spoil the statistical properties of the sequences [7].

This procedure can be used to postpone the lockstep situation shown in Fig. 2c and by Eq. (3.1). Since we have assumed that neither of the sequences $\{\bar{x}_i\}$, $i \leqslant n$, nor $\{\bar{y}_j\}$, $j \leqslant n'$, contains any repetitions or common elements, the two memory factors $\delta p_m(\bar{x}_{n+2})$ and $\delta p_m(\bar{y}_{n+2})$, which enter into the computation of the terms beyond D_0, will generally be different for $m \geqslant 2$. The pseudorandom iterations can then be rewritten in the form

$$\begin{array}{ccccccc}
\bar{x}_{n-1}, & & \bar{x}_n, & & \bar{x}_{n+1}, & & \bar{x}_{n+2}, \\
\cdots & \to \mathcal{M}_u[\bar{x}_{n-1}+\delta p_m(\bar{x}_n)] \to & & \mathcal{M}_u[\bar{x}_n+\delta p_m(\bar{x}_{n+1})] & & \to \mathcal{M}_u[\bar{x}_{n+1}+\delta p_m(\bar{x}_{n+2})] \to & \cdots \\
 & & & \| & & & \\
 & & & D_0 & & & \\
 & & & \| & & & \\
\cdots & \to \mathcal{M}_u[\bar{y}_{n'-1}+\delta p_m(\bar{y}_{n'})] \to & & \mathcal{M}_u[\bar{y}_{n'}+\delta p_m(\bar{y}_{n'+1})] & & \to \mathcal{M}_u[\bar{y}_{n'+1}+\delta p_m(\bar{y}_{n'+2})] \to & \cdots \\
\bar{y}_{n'-1}, & & \bar{y}_{n'}, & & \bar{y}_{n'+1}, & & \bar{y}_{n'+2},
\end{array} \tag{3.5}$$

where it is evident that $\{\bar{x}_i\}$ and $\{\bar{y}_j\}$ usually diverge after the initial coincidence at $\bar{x}_{n+1} = D_0 = \bar{y}_{n'+1}$. In particular if $\mathcal{M}_u$ is a mixing transformation, the next terms, $\bar{x}_{n+2}$ and $\bar{y}_{n'+2}$, are likely to have quite different values—even if the perturbations are of the same order of magnitude, i.e., $\delta p_m(\bar{x}_{n+2}) \approx \delta p_m(\bar{y}_{n'+2})$—because it is known that mixing sequences are totally unstable [22]. When pseudorandom processes are scrambled by memory dependent feedback or the interleafing of mixing transforms, the resulting sequences should be sufficiently irregular so that multiple coincidences occur with the expected frequencies (2.9).

Of course none of these modifications can sustain the computer randomizations indefinitely: the pigeonhole principle also applies to the sequences (3.5), so they must eventually merge into terminal loops; according to our previous arguments there should be no more than three or four of these. The only practical difference is that the memory dependence has made the computers appear to be larger. For instance, if each term of the sequence $\{\bar{x}_i\}$ in (3.5) represents a q-digit number, cf. (2.11a) and (2.11b), and the memory factors $\delta p_m(\bar{x}_m)$ carry forward the information from $\tilde{q}$ additional places, then the effective computer size is increased to $10^{q+\tilde{q}}$ displays. It is interesting that the memory is also associated with an ageing process induced by imperfect information: The longer the $\{\bar{x}_i\}$ and $\{\bar{y}_j\}$ iterations continue past the initial

coincidence, the more likely it becomes that several elements on each string will resemble each other. When this "cross-matching" becomes sufficiently accurate so that the memory factors cannot distinguish any further differences, then the two sequences will finally enter a common track.

B. *Applications to Physics*

If for the moment we strip away the computer-oriented language of the preceding sections, we can restate the basic assumptions leading to the few loop principle as follows:

(1) There is a system $\mathscr{S}$ which may appear in any one of a finite number of states C_i, $i = 1,..., N$.

(2) There is a transformation $\mathscr{E}_{p(m)}$ which can be applied to $\mathscr{S}$ in any of its states. This transform has two essential properties:

(a) Transformation $\mathscr{E}_{p(m)}$ is *deterministic* in the sense that given any state C_i, the transform $\mathscr{E}_{p(m)}$ leads to a unique successor, i.e.,

$$\mathscr{E}_{p(m)} : C_i \to C_j[i, p(m)]. \tag{3.6}$$

(b) Transformation $\mathscr{E}_{p(m)}$ depends on a *stochastic* parameter $p(m)$. This means that if we extend (3.6) to a succession of transformations analogous to (2.12), i.e.,

$$\begin{array}{ccccccc} C_i, & C_{i+1}, & & C_{i+2}, & & C_{i+3}, & \cdots, \\ & \updownarrow & & \updownarrow & & \updownarrow & \\ C_i \to & \mathscr{E}_{p(i)}(C_i) & \to & \mathscr{E}_{p(i+1)}(C_{i+1}) & \to & \mathscr{E}_{p(i+2)}(C_{i+2}) & \to \cdots, \end{array} \tag{3.7}$$

the sequence of parameter values $\{p(i)\}$ *is random or pseudorandom.*

There are a variety of physical systems that appear to evolve according to this scheme, and whose long-time or asymptotic behavior is described by the few loop principle. We shall give a few illustrations—progressing from the literal to the speculative.

A simple class of physical objects that have properties corresponding to the $\mathscr{S}$-systems are Ewing arrays. These are well known classical models for cooperative magnetic interactions. Ewing arrays are usually constructed with sets of precisely magnetized permanent magnets, each mounted on a nearly frictionless vertical pivot and free to rotate in a horizontal plane without mutual mechanical obstruction. If the pivots are arranged in the form of a square lattice, then extensive observations show that the set of individual magnet orientations does not form an amorphous "spin glass," but rather that the entire array exhibits a regular domain structure [23, 24]. It is natural to identify these magnetic patterns with the C_j states of Eq. (3.6). Specifically, in a square array of $s \times s$ magnets, let us denote the orientation of the

magnet in the ρth row and κth column by $\theta_{\rho\kappa}$, $1 \leqslant \rho, \kappa \leqslant s$. Then the C_j's simply represent a particular set of these orientations for any locally stable state,

$$\theta_{11}, \theta_{12}, ..., \theta_{1s}, \theta_{21}, ..., \theta_{ss} \Rightarrow C_j. \tag{3.8}$$

The number of distinct configurations (apart from degeneracies due to array rotation, pole reversal, etc.) is a rapidly increasing function of the total number of magnets. For instance in a 9×9 array, statistical estimates indicate that the total number of C_j states is in the range 10^4–10^5.

It is known that the dominant magnetic interactions in these Ewing arrays are due to dipole and octupole forces [25]; therefore the potential energy E_j associated with each configuration C_j can be computed exactly. Since nearest-neighbor approximations are inadequate, these calculations must include all $s^2(s^2-1)/2$ pair-wise interactions. In particular, for a 9×9 array the energy of the anti-ferromagnetic state $C_{AF} \to \theta_{1\kappa} \cong 0$, $\theta_{2\kappa} \cong \pi, ...,$ $\theta_{8\kappa} \cong \pi$, $\theta_{9\kappa} \cong 0$, is given by

$$E_{AF} \cong (387.2 \pm 0.2)(\mu^2/a^3), \tag{3.9}$$

where a is the lattice spacing and μ is the magnetic dipole moment of a single magnet [26]. Although C_{AF} is presumably the lowest energy state of this system, it has a negligible statistical weight. Experimentally this can be verified by randomizing or "melting" the domain patterns with fluctuating external magnetic fields and then allowing the arrays to freeze or recrystallize by dissipating their kinetic energy in internal magnetic friction. The anti-ferromagnetic state never appears spontaneously from the melt.

This "irrelevance" of the ground state is not surprising: One can check explicitly that most of the 10^4 metastable C_j states are densely spaced in energy and grouped in degenerate clusters. Furthermore, the state-area or capture probability for each state is extremely small [27]. Under these circumstances equilibrium statistical mechanics is inapplicable. Nevertheless, Ewing arrays can be stabilized by procedures which mimic the shake-down of real structures—such as portal frames or pipelines—or the annealing of glassy materials. The existence of asymptotic sets of "attractor" states is then a direct consequence of the few loop principle. This connection can be demonstrated with the help of the following experiments [26]:

Suppose a 9×9 array is "melted" and then allowed to congeal into a state $C_0^{(T)}$ —this is the analog of choosing an arbitrary starting element for the pseudorandom sequences (2.12) or (2.13). Now let us attempt to transform the system by selecting a particular magnet, say the $\rho\kappa$th, turning it slowly by 360° ($\theta_{\rho\kappa} \to \theta_{\rho\kappa} + 360°$), and then releasing the magnet. If we have *not* supplied sufficient energy to boost the system over the lowest saddle-point, or "activation-complex" [27], separating $C_0^{(T)}$ from some other locally stable state on the energy surface, then nothing will happen. We can indicate this by rewriting (3.6) in the form

$$\mathscr{E}_{\rho(1)\kappa(1)} : C_0^{(T)} \to C_0^{(T)}, \tag{3.10}$$

where $\mathscr{E}_{\rho\kappa}$ simply represents the rotation of the $\rho\kappa$th magnet. Clearly, we can now go on to twist a sequence of magnets—$\rho(2)\,\kappa(2)$, $\rho(3)\,\kappa(3)$, etc.—until we finally find one whose rotation results in a change of pattern. If this happens on the mth step, then

$$\mathscr{E}_{\rho(m)\kappa(m)}: C_0^{(T)} \to C_1^{(T)}, \tag{3.11}$$

where $C_1^{(T)}$ denotes the next pattern. *This "twist and shift" procedure will correspond precisely to the general iterative scheme of* (3.7) *if the rotated magnets are selected by pseudorandom number generators.* In this case the stochastic parameter $p(m)$ represents a pair of (pseudo) random indices

$$p(m) \to \rho(m)\,\kappa(m), \qquad 1 \leqslant \rho, \kappa \leqslant 9, \quad m = 1, 2, 3, \ldots \tag{3.12}$$

specifying locations in the 9×9 array.

One series of experiments was carried out by randomizing a 9×9 array ten times. After each "melt," the array was allowed to freeze. In this way we obtained ten distinct initial configurations $C_0^{(T)}$, $T = 1, \ldots, 10$. Starting with *each* of these configurations we then prodded the array along a sequence of patterns in the C_j-space $(1 \leqslant j \lesssim 10^4)$ by turning randomly chosen magnets:

$$\begin{array}{cccc} C_0^{(1)} \to & C_1^{(1)} \to & C_2^{(1)} \to & \cdots, \\ \vdots & \vdots & \vdots & \vdots \\ C_0^{(10)} \to & C_1^{(10)} \to & C_2^{(10)} \to & \cdots. \end{array} \tag{3.13}$$

It is striking that nine of these sequences merged into the *same* set of four final states after approximately 80–130 steps. These four states formed a cluster rather than a loop because the $\mathscr{E}_{\rho\kappa}$ transforms can interconnect patterns in a variety of ways. But the physical situation in all essentials resembles the capture processes shown in Figs. 2c and d: once the array reaches this 4-cluster it cannot escape to any of the other C_j states by further magnet rotations. The average energy of this terminal cluster is $(375.6 \pm 0.2)\,\mu^2/a^3$, and all 4 states lie within 0.5% of this value. In other words, this set of attracting states is actually poised on a flat energy ledge about 3.1% above the anti-ferromagnetic ground state (3.9), but it is *not metastable* in the usual sense of the word.[1] It is suggestive that the average number of steps between the "melt" and this terminal cluster is of the order of the square root of the total number of C_j states (cf. (2.7a)).

Finally we note that we also found a short sequence of 26 steps leading to a 2-cluster: this consisted of the ground state C_{AF} and another pattern lying 1.7% higher

[1] In this connection it is interesting to recall Bohr's remarks on stability: "In Nature there is a general tendency to form certain structures ... and if these are perturbed or destroyed, then they are always recreated.... All of this is certainly not self-evident; on the contrary it appears to be quite incomprehensible from the standpoint of Newtonian physics: By this I mean the presumption of a strict causal determinism of events ... where every state is uniquely and solely determined by its immediate predecessor" [28].

in energy. The association of short sequences with small orbits conforms to the distributional analysis underlying (2.7a), (2.7c). Although we cannot rule out the existence of other attractive clusters, all the additional evidence available from simple variants of these experiments is consistent with the ordering behavior expected from the few loop principle [26].

The stochastic parameter $p(m)$ of course need not be associated with random or pseudorandom processes in the simple and literal way indicated by Eq. (3.12). In the technically important case of hysteresis systems, this parameter may be identified with the random location of discontinuities in the phase spaces of these systems. The physical relevance of the few loop principle then is connected with the fact that nearly all hysteresis systems evolve from virgin to asymptotic hysteresis, and that the asymptotic regime is comprised of cycles over a relatively small number of states. These assertions can also be checked directly with Ewing arrays.

A convenient method for generating hysteresis in Ewing arrays is to mount the magnet supports on deformable rhombohedral lattices [29, 30]. In practice the vertex angle of the rhombuses is varied through the range $20° \leqslant \phi \leqslant 90°$, where 90° corresponds to a square lattice. Most magnet orientations $\theta_{\rho\kappa}$ are then *not* single valued functions of ϕ. We can take this multiplicity into account by rewriting (3.8) in the form $C_j[\theta_{\rho\kappa}(\phi)]$, where the index j numbers all the locally stable magnet patterns for a given value of ϕ. As the hysteresis coordinate is cycled back and forth over the physically accessible range, $20° \to 90° \to 20°$, the locally stable magnet patterns $C_j[\theta_{\rho\kappa}(\phi)]$ move along corresponding trajectories on a foliated energy surface. In a 2×2 array there are essentially only two trajectories and the situation is sufficiently simple so that it can be shown graphically—for example, in [29, Fig. 5]. However, the complexity of the hysteresis increases rapidly as the Ewing arrays are enlarged. For instance, a 6×6 array has at least 256 distinct trajectories linked together in the form of an intricate hysteresis network. An additional complication stems from the fact that as ϕ is varied *smoothly*, there are discontinuous jumps from pattern to pattern. The hysteresis network of a 6×6 array has at least 1245 such jump discontinuities, or an average of 4.86 transitions per trajectory [31].

These jump discontinuities are responsible for the irreversible energy dissipation in hysteresis [29, 30], and are also useful for partitioning the hysteresis network into finite sets. Specifically, if we regard each continuous portion of every trajectory as a single state, then the associated set of $C_j[\theta_{\rho\kappa}(\phi)]$ patterns is discrete and finite. Since the cyclic variations of ϕ also generate discrete jumps *between* these states, the correspondence between hysteresis and the general iterative scheme of (3.7) is almost complete. The random character of the hysteresis then depends on two supplementary conditions:

(α) The distribution of jump discontinuities on the energy surfaces must be uniform but irregular. Statistical studies confirm that this condition is indeed satisfied by 6×6 arrays [31].

(β) The sequence of states traversed during hysteresis should be dispersed throughout the entire hysteresis network. This kind of "mixing" criterion is more

difficult to check in practice, but it is consistent with the observed behavior of the arrays.

With all this information at hand, it is now a straightforward matter to apply the few loop principle to the Ewing hysteresis. Specifically, for an N state system with an average of d discontinuities or transitions per hysteresis cycle, the estimate (2.7a) indicates that the total number of cycles required to reach asymptotic hysteresis is

$$n_{\text{asympt}} \sim (0.9N)^{1/2}/d \xrightarrow[6\times 6]{} (0.9 \times 1245)^{1/2}/(2 \times 4.86) \approx 3.5. \tag{3.14}$$

The numerical values given in this example are derived from statistical trials with a 6×6 array. Despite the fact that the 6×6 hysteresis network includes more than 100 different loops, experiments showed that most arbitrarily chosen starting configurations merged into a *unique* terminal loop after only 2–4 hysteresis cycles. This surprising result is in full accord with the few loop estimate (3.14). Similar trends appear in the hysteresis of complex structures subjected to mechanical loading cycles [30]. In this case the determination of the technically important shakedown load is facilitated by the rapid evolution of virgin to asymptotic hysteresis [32]. The shakedown results are also consistent with a simple extension of (3.14). Suppose that the amplitude of the hysteresis excursions were lowered by a fractional amount $\tilde{\rho}$ $(0 < \tilde{\rho} < 1)$: if the hysteresis over this restricted subspace retains its random character, then (3.14) implies that the approach to the asymptotic states requires more cycles, i.e., $n_{\text{asympt}} \sim \tilde{\rho}^{-1/2}$.

The magnetic hysteresis of Ewing arrays and the mechanical hysteresis of structural panels can become extremely complex, yet both types of systems are basically determinate. It is therefore not at all obvious why the few loop principle should have any more than a fortuitous connection with the description of their behavior. In particular, for the Ewing arrays, we can check in detail that the randomness criteria (α) and (β) *happen* to be satisfied, but we do not have any basis for asserting beforehand that the location of the discontinuities—which can all be obtained from classical magnetostatics [29]—will turn out to be uniformly distributed over the hysteresis energy surface. In essence this problem is an echo of our previous discussion of what makes a string of numbers random or pseudorandom, cf. Section 2A. According to Kolmogorov and Chaitin, the generation of random numbers requires tremendous computational complexity [14], i.e.,

$$\begin{matrix}\text{random} \\ \text{strings}\end{matrix} \rightarrow \begin{matrix}\text{maximal} \\ \text{information} \\ \text{content}\end{matrix} \rightarrow \begin{matrix}\text{algorithms of} \\ \text{irreducible} \\ \text{complexity.}\end{matrix} \tag{3.15}$$

Obviously it is possible to extend these equivalences to include *physical* systems if we recall that complicated physical systems generally require complicated computer programs to describe their behavior. It is then plausible to read Kolmogorov–Chaitin in reverse order,

$$\begin{matrix}\text{complex}\\ \text{physical}\\ \text{systems}\end{matrix} \rightarrow \begin{matrix}\text{complex}\\ \text{computational}\\ \text{algorithms}\end{matrix} \rightarrow \begin{matrix}\text{maximal}\\ \text{information}\\ \text{content}\end{matrix} \rightarrow \begin{matrix}\text{pseudorandom}\\ \text{strings.}\end{matrix} \tag{3.16}$$

This does not mean that all complicated systems behave like fluids, spin glasses, or roulette wheels; but the Ewing example clearly shows that in the midst of ordered patterns there may be at least one variable with a pseudorandom distribution. Physical processes which correspond to iterations of this special variable should lead to small sets of asymptotic attractor states in accordance with the few loop principle.

C. *Terminal Loops on Different Computers*

The few loop principle is a nonconstructive statement concerning the existence of terminal cycles. Different pseudorandom algorithms programmed for the same computer and ostensibly the same algorithm run on different computers will generally lead to different sets of terminal cycles. The dependence of these cycles on the truncation conventions and programming of various machines has been studied with the aid of variable precision simulations [7]. For instance, if the Chebyshev mixing transformation $C_2(x) = x^2 - 2$ is iterated in 3 place accuracy on programmable calculators such as an HP-25 (10 digits + 1 guard) or an SR-52 (10 digits + 3 guard), then the same terminal loops appear on both machines. This example is trivial, however, because the statistical features of the mixing are suppressed by the combinatorial regularities arising from the underlying arithmetic "lattice." In the Chebyshev case, the randomization of the mixing begins to dominate the iterations when the computations are carried out with more than 6 significant figures. Beyond the transition to this statistical regime the terminal loops also become device-dependent; cf. [7, Tables V–VII].

Since mixing transformations are not only chaotic but totally unstable, the sensitive dependence of the terminal loops on the truncation conventions and microprograms is quite natural. In principle this feature is useful for adapting mixing transformations to cryptographic purposes. In this context any "key" which can convert lengthy ciphertext into intelligible plaintext represents an enormous amount of information compression. The few loop principle indicates that keys of this type can be constructed for cryptosystems based on uniform mixing algorithms. Specifically, given a computer $\mathscr{C}$ together with its truncation algorithms and a mixing transformation $\mathscr{M}$, all that one needs in order to reconstruct completely the entire set of orbits (2.16) is one number from each terminal loop. Our estimates show that all of this information is usually provided by just 2 to 4 numbers!

4. The Reconstruction of Orbits

Suppose that the transformation $\mathscr{M}$ is mixing on the interval I with respect to Lebesgue measure. Then for all elements $x_0 \in I$—except for those drawn from a set of

measure zero—the sequences of iterates $\{\mathscr{M}^m(x_0)\}$ will extend indefinitely far into the "future" in a perpetual pseudorandom wandering. If, however, I is mapped into a finite set (e.g., the set of computer displays $\mathscr{N}$ (2.11a), (2.11b)) by some truncation procedure, then the initial elements x_0 will be replaced by the machine entries $\bar{x}_0$, and the computer sequences $\{\mathscr{M}^m(\bar{x}_0)\}$ will terminate as indicated in (1.2). In this situation the pigeonhole and few loop principles ensure that the "future" will not be pseudorandom: all the machine simulations are bound to terminate on a relatively small set of ordered states.

A complementary ordering appears if the computer sequences are traced back into the "past." In this event the gaps between the various processes shown in (1.1) can become even more drastic. For instance, the "past" of a mixing transformation may be inaccessible; this follows from the

THEOREM [33]. *It is impossible for any one-dimensional transformation to be simultaneously continuous, mixing, and invertible.*

Since on physical grounds it is preferable to idealize mixing transformations as being continuous, this theorem shows that the corresponding physical processes must be irreversible [2, 22].

The asymmetry between past and future appears in a somewhat different form in discrete models of mixing. For example, the continuous Chebyshev transformation $C_2(x) = x^2 - 2$ is noninvertible, but as indicated by (1.3) all preimages of any given point can in principle be determined. This suggests that the numerical reversions

$$\begin{array}{l} \bar{x}_{-1} = +(\bar{x}_0 + 2)^{1/2} \\ \qquad\qquad\qquad\qquad \nwarrow \\ \qquad\qquad\qquad\qquad\quad \bar{x}_0 \\ \qquad\qquad\qquad\qquad \swarrow \\ -\bar{x}_{-1} = -(\bar{x}_0 + 2)^{1/2} \end{array} \tag{4.1}$$

could actually be carried out on a computer because there are only a finite number of machine entries $\bar{x}_0$. By continuing these reversions into the "past" it should then be possible to compile an inventory of all iteration sequences leading to a particular elements $\bar{x}_0$. This still does not permit us, however, to retrodict the pseudorandom sequences that include $\bar{x}_0$ because we lack a definite rule for selecting a *unique* preimage at each step back in time.

The nonrandom features of the past can be studied by tracing every element of all terminal loops backwards in time. In particular, if we follow the iterative scheme (1.3) for g steps, every element should have approximately 2^g distinct preimages. From (1.2) and the few loop principle we then infer that the total number of "ancestors" up to the gth generation is of the order of $\sim 4(n_l - n_f)\, 2^g$. Since (2.7a) indicates that the average number of generations is proportional to $N^{1/2}$, where N is the total number of computer displays, it would appear that the number of preimages

preimages are included among the set of computer displays, then evidently they would have to satisfy the bound

$$N^{1/2} \ln 2 < \ln N, \tag{4.2}$$

and this is impossible. The flaw of the argument lies in the presumption that the preimage chain (1.3) can be simulated on a computer [7]. It is easy to check that for any digital device the limited accuracy of the machine arithmetic entails the existence of gaps so that numerical reversions such as (4.1) may not be feasible. Suppose for example that we set $\bar{x}_0 = 1.823\ 645\ 3$. Then on an electronic "slide rule" such as the TI-30 the operations indicated in (4.1) will result in $\pm\bar{x}_{-1} = \pm 1.955\ 414\ 4$. However, if we go forward in time by computing $C_2(\pm\bar{x}_{-1})$, we find

$$(\bar{x}_{-1}) \times (\bar{x}_{-1}) - 2 = 1.823\ 645\ 5 \neq \bar{x}_0; \tag{4.3}$$

and a little further experimentation will show that no matter how $\bar{x}_{-1}$ is varied it is impossible to recover $\bar{x}_0$. In this precise sense $\bar{x}_0$ does not have any ancestors on the TI-30. A similar thinning out prevails on larger machines. Quite generally, estimates of the maximum number of preimages must be modified by some extinction factor in order to avoid contradictions like (4.2). This extinction factor degrades the pseudorandom behavior of the computer simulations when they are extended into the past.

The extinction factor for $C_2(\bar{x})$ can be determined explicitly for arbitrarily large but finite machines. Suppose that the arithmetic precision is Δ. Then for the neighboring pair, $\bar{x}_0$ and $\bar{x}_0 + \Delta$, reversion (4.1) can be written in the parallel form

$$\delta \simeq \frac{\Delta}{2(\bar{x}_0 + 2)^{1/2}} \begin{Bmatrix} (\bar{x}_0 + \Delta + 2)^{1/2} \leftarrow \bar{x}_0 + \Delta \\ (\bar{x}_0 + 2)^{1/2} \quad\quad \leftarrow \bar{x}_0 \end{Bmatrix} \Delta, \tag{4.4}$$

where δ is the difference between adjacent preimages. Clearly, if $\delta > \Delta$, it is likely that $\bar{x}_0$ will have preimages among the set of computer displays. On the other hand, if

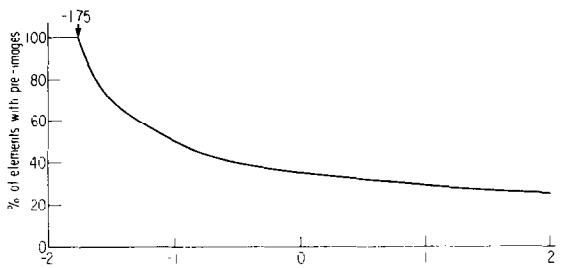

FIG. 3. Preimages of the Chebyshev mixing transformation $x \mapsto x^2 - 2$, $x \in [-2, 2]$. The ordinate indicates the percentage of points that have preimages. The curve is not a plot of (4.5), but represents the results of computer trials with $N = 400{,}001$ displays, and bin widths of 0.01.

$\delta < \Delta$, then the arithmetic mesh is too coarse, and it is likely that $\bar{x}_0$ will not have any ancestors. Since the ratio δ/Δ is proportional to the fraction of elements that have preimages, (4.4) implies that this factor is given by

$$\begin{aligned} f(\bar{x}) &= 1, && \text{if} \quad -2 < \bar{x} < -\tfrac{7}{4}, \\ &= \tfrac{1}{2}(\bar{x}+2)^{-1/2}, && \text{if} \quad -\tfrac{7}{4} \leqslant \bar{x} \leqslant 2. \end{aligned} \tag{4.5}$$

Figure 3 shows an approximate form of this function derived from an experimental "ancestor hunt." By averaging (4.5) over the mixing interval $[-2, 2]$, it is easy to check that the average number of preimages per element is $\frac{7}{8}$ instead of 2. This rapid extinction of ancestral lines avoids the contradictions represented by (4.2). It is then also feasible to associate an "age" with the simulations by starting the clock or the calendar with the oldest ancestor, i.e., the longest string of reversions. Finally, we note that the statistical differences arising from the asymmetric distribution (4.5) and the symmetric Chebyshev density $[4 - x^2]^{-1/2}$ of (A2) provide a definite direction for time's arrow in computer simulations of Chebyshev "chaos."

APPENDIX: Uniform Mixing Transformations

Computer trials indicate that mixing transformations can be employed as practical random number generators [7]. For instance, if I_1 is the interval $[-2, 2]$, then the Chebyshev polynomials

$$C_m(x) = 2\cos[m \cos^{-1}(x/2)], \qquad m \geqslant 2, \quad \text{principal } \cos^{-1}, \tag{A1}$$

are mixing on I_1 with respect to the probability measure

$$P_C(S) = \frac{1}{\pi}\int_S (4 - x^2)^{-1/2}\, dx. \tag{A2}$$

In many applications it is necessary to construct pseudorandom number generators with preassigned distributions over given intervals. Mixing simulations can often be adjusted to produce pseudorandom sequences with the desired properties by means of conjugacy transformations. In particular, if we want to modify the Chebyshev polynomial C_m to generate a uniform distribution over $[0, 1]$, then it can be shown that the mixing transformation

$$\mathscr{M}_{h(m)}(x) = (F_C \circ C_m \circ F_C^{-1})(x) \tag{A3}$$

has this property [9, 34]. Here "$\circ$" indicates functional composition; F_C is the distribution function of P_C, i.e.,

$$F_C(x) = (1/\pi)\cos^{-1}(-x/2), \qquad x \in [-2, 2]; \tag{A4}$$

and F_C^{-1} denotes the inverse,

$$F_C^{-1}(x) = -2\cos(\pi x), \qquad x \in [0, 1]. \tag{A5}$$

Two special cases of (A3) are

$$\mathcal{M}_{h(2)}(x) = |1 - 2x|, \qquad x \in [0, 1], \tag{A6}$$

and

$$\begin{aligned} \mathcal{M}_{h(3)}(x) &= 3x, && \text{if} \quad 0 \leqslant x < \tfrac{1}{3}, \\ &= 2 - 3x, && \text{if} \quad \tfrac{1}{3} \leqslant x < \tfrac{2}{3}, \\ &= 3x - 2, && \text{if} \quad \tfrac{2}{3} \leqslant x \leqslant 1. \end{aligned} \tag{A7}$$

Both $\mathcal{M}_{h(2)}$ and $\mathcal{M}_{h(3)}$ perform well on computers, but precautions are necessary. For instance, on a machine operating in binary arithmetic, $\mathcal{M}_{h(2)}$ will eventually collapse to $\frac{1}{2}$ upon iteration.

ACKNOWLEDGMENTS

We are grateful to D. J. Costello, P. C. Deliyannis, P. Everett, D. Graupe, H. Rubin, and A. Sklar for helpful conversations and critical remarks. It is also a pleasure for T. E. to acknowledge the hospitality of the Department of Physics at the University of California, Los Angeles.

REFERENCES

1. E. HOPF, *J. Math. Phys.* **13** (1934), 51.
2. N. S. KRYLOV, "Works on the Foundations of Statistical Physics," Princeton Univ. Press, Princeton, N.J., 1979.
3. P. COLLET AND J. P. ECKMANN, "Iterated Maps on the Interval as Dynamical Systems," Birkhäuser, Boston, 1980.
4. A. DEL JUNCO AND J. M. STEELE, *Ann. Probab.* **7** (1979), 267.
5. M. MÄKELÄ, O. NEVANLINNA, AND A. H. SIPILÄ, *Numer. Math.* **22** (1974), 261.
6. R. ANSORGE, "Differenzenapproximationen Partieller Anfangswertaufgaben," Teubner, Stuttgart, 1978.
7. T. ERBER, P. EVERETT, AND P. W. JOHNSON, *J. Comput. Phys.* **32** (1979), 168.
8. T. ERBER, P. W. JOHNSON, AND P. EVERETT, *Phys. Lett. A* **85** (1981), 61.
9. T. ERBER, T. M. RYNNE, AND A. SKLAR, *Acta Phys. Austriaca* **53** (1981), 145.
10. D. E. KNUTH, "The Art of Computer Programming, Vol. 2, Seminumerical Algorithms," Addison–Wesley, Reading, Mass., 1969.
11. T. ERBER, B. SCHWEIZER, AND A. SKLAR, *Commun. Math. Phys.* **29** (1973), 311.
12. R. E. RICE, *Aequationes Math.* **17** (1978), 104.
13. K. R. REBMAN, *Two-Year College Math. J.* **10** (1979), 3.
14. G. J. CHAITIN, *J. Assoc. Comput. Mach.* **21** (1974), 403.
15. C. P. SCHNORR, "Zufälligkeit und Wahrscheinlichkeit—Eine algorithmische Begründung der Wahrscheinlichkeitstheorie," Springer–Verlag, Berlin/New York, 1971.

16. W. FELLER, "Introduction to Probability Theory and Its Applications," Vol. 1, 3rd ed., Wiley, New York, 1967.
17. W. F. DARSOW, T. ERBER, AND M. J. FRANK, *Amer. Math. Soc. Abstr.* **3** (1) (1982), 140.
18. F. G. TRICOMI, *Math. Z.* **53** (1950), 136.
19. W. F. DARSOW, T. ERBER, AND M. J. FRANK, to appear.
20. N. G. DE BRUIJN, *K. Ned. Akad. Wet., Proc.* **49**, (2) (1946), 758.
21. M. GARDNER, *Sci. Amer.* **238** (2) (February 1978), 27.
22. T. ERBER AND A. SKLAR, *in* "Modern Developments in Thermodynamics" (B. Gal-Or, Ed.), pp. 281–301, Israel Univ. Press and Wiley, Jerusalem/New York, 1974.
23. J. A. EWING, "Magnetic Induction in Iron and Other Metals," Electrician Printing and Publ., London, 1894.
24. T. ERBER, G. R. MAROUSEK, AND G. K. FORSBERG, *Acta Phys. Austriaca* **30** (1969), 271.
25. T. ERBER AND H. G. LATAL, *Acta Phys. Austriaca* **34** (1971), 313.
26. T. ERBER, H. G. LATAL, AND C. R. WILLCOX, unpublished, 1977.
27. T. ERBER AND H. G. LATAL, *Acad. R. Belg. Bull. Cl. Sci. 5* **53** (1967), 1019.
28. W. HEISENBERG, "Der Teil und das Ganze," p. 52, Deutscher Taschenbuch Verlag, Munich, 1973.
29. T. ERBER, B. N. HARMON, AND H. G. LATAL, *Advan. Chem. Phys.* **20** (1971), 71.
30. T. ERBER, S. A. GURALNICK, AND H. G. LATAL, *Ann. Phys. (N.Y.)* **69** (1972), 161.
31. G. B. BAUMGARTNER, JR., T. ERBER, H. G. LATAL, AND J. E. NUTI, unpublished, 1973.
32. S. SINGH, "Shakedown Load and Hysteresis Phenomena of Portal Frames," Ph.D. Thesis, Illinois Institute of Technology, Chicago, 1982.
33. A. SKLAR, private communication.
34. R. L. ADLER, A. G. KONHEIM, AND M. H. MCANDREW, *Trans. Amer. Math. Soc.* **114** (1965), 309.
35. I. M. SOBOL, *Theory Probab. Its Appl.*, **9** (1964), 333.
36. "Random Number Generation and Testing," IBM Manual C20-8011.
37. M. D. KRUSKAL, *Amer. Math. Monthly* **61** (1954), 392.
38. B. HARRIS, *Ann. Math. Stat.* **31** (1960), 1045.