Origins of Randomness in Physical Systems

Stephen Wolfram
The Institute for Advanced Study, Princeton, New Jersey 08540
(Received 4 February 1985)

Randomness and chaos in physical systems are ususally ultimately attributed to external noise. But it is argued here that even without such random input, the intrinsic behavior of many nonlinear systems can be computationally so complicated as to seem random in all practical experiments. This effect is suggested as the basic origin of such phenomena as fluid turbulence.

PACS numbers: 05.45.+b, 02.90.+p, 03.40.Gc

There are many physical processes that seem random or chaotic. They appear to follow no definite rules, and to be governed merely by probabilities. But all fundamental physical laws, at least outside of quantum mechanics, are thought to be deterministic. So how, then, is apparent randomness produced?

One possibility is that its ultimate source is external noise, often from a heat bath. When the evolution of a system is unstable, so that perturbations grow, any randomness introduced through initial and boundary conditions is transmitted or amplified with time, and eventually affects many components of the system.[1] A simple example of this "homoplectic" behavior occurs in the shift mapping $x_t = 2x_{t-1} \bmod 1$. The time sequence of bins, say, above and below $\frac{1}{2}$ visited by x_t is a direct transcription of the binary-digit sequence of the initial real number x_0.[2] So if this digit sequence is random (as for most x_0 uniformly sampled in the unit interval) then so will the time sequence be; unpredictable behavior arises from a sensitive dependence on unknown features of initial conditions.[3] But if the initial condition is "simple," say a rational number with a periodic digit sequence, then no randomness appears.

There are, however, systems which can also generate apparent randomness internally, without external random input. Figure 1 shows an example, in which a cellular automaton evolving from a simple initial state produces a pattern so complicated that many features of it seem random. Like the shift map, this cellular automaton is homoplectic, and would yield random behavior given random input. But unlike the shift map, it can still produce random behavior even with simple input. Systems which generate randomness in this way will be called "autoplectic."

In developing a mathematical definition of autoplectic behavior, one must first discuss in what sense it is "random." Sequences are commonly considered random if no patterns can be discerned in them. But whether a pattern is found depends on how it is looked for. Different degrees of randomness can be defined in terms of the computational complexity of the procedures used.

The methods usually embodied in practical physics experiments are computationally quite simple.[4,5] They correspond to standard statistical tests for randomness,[6] such as relative frequencies of blocks of elements (dimensions and entropies), correlations, and power spectra. (The mathematical properties of ergodicity and mixing are related to tests of this kind.) One characteristic of these tests is that the computation time they require increases asymptotically at most like polynomial in the sequence length.[7] So if in fact no polynomial-time procedure can detect patterns in a sequence, then the sequence can be considered "effectively random" for practical purposes.

Any patterns that are identified in a sequence can be used to give a compressed specification for it. (Thus, for example, Morse coding compresses English text by exploiting the unequal frequencies of letters of the alphabet.) The length of the shortest specification measures the "information content" of a sequence with respect to a particular class of computations. (Standard Shannon information content for a stationary process[8] is associated with simple statistical computations of block frequencies.) Sequences are predictable only to the extent that they are longer than their shortest specification, and so contain information that can be recognized as "redundant" or "overdetermined."

Sequences generated by chaotic physical systems often show some redundancy or determinism under simple statistical procedures. (This happens whenever measurements extract information faster than it can be transferred from other parts of the system.[1]) But, typically, there remain compressed sequences in which no patterns are seen.

A sequence can, in general, be specified by giving an algorithm or computer program for constructing it. The length of the smallest possible program measures the "absolute" information content of the sequence.[9] For an "absolutely random" sequence the program must essentially give each element explicitly, and so be close in length to the sequence itself. But since no computation can increase the absolute information content of a closed system [except for $O(\log t)$ from input of "clock pulses"], physical processes presumably cannot generate absolute randomness.[10] However, the numbers of possible sequences and programs both increase exponentially with length, so that all but an exponentially small fraction of arbitrarily chosen sequences must be absolutely random. Nevertheless, it

is usually undecidable what the smallest program for any particular sequence is, and thus whether the sequence is absolutely random. In general, each program of progressively greater length must be tried, and any one of them may run for an arbitrarily long time, so that the question of whether it ever generates the sequence may be formally undecidable.

Even if a sequence can ultimately be obtained from a small specification or program, and so is not absolutely random, it may nevertheless be effectively random if no feasible computation can recover the program.[11] The program can always be found by explicitly trying each possible one in turn.[12] But the total number of possible programs increases exponentially with length, and so such an exhaustive search would soon become infeasible. And if there is no better method the sequence must be effectively random.

In general, one may define the "effective information content" Θ of a sequence to be the length of the shortest specification for it that can be found by a feasible (say polynomial time) computation. A sequence can be considered "simple" if it has small Θ. Θ (often normalized by sequence length) provides a measurue of "complexity," "effective randomness," or "computational unpredictability."

Increasing Θ can be considered the defining characteristic of autoplectic behavior. Examples such as Fig. 1 suggest that Θ can increase through polynomial-time processes. The rule and initial seed have a short specification, with small Θ. But one suspects that no polynomial time computation can recover this specification from the center vertical sequence produced, or can in fact detect any pattern in it.[13] The polynomial-time process of cellular automaton evolution thus increases Θ, and generates effective randomness. It is phenomena of this kind that are the basis for cryptography, in which one strives to produce effectively random sequences whose short "keys" cannot be found by any practical cryptanalysis.[14]

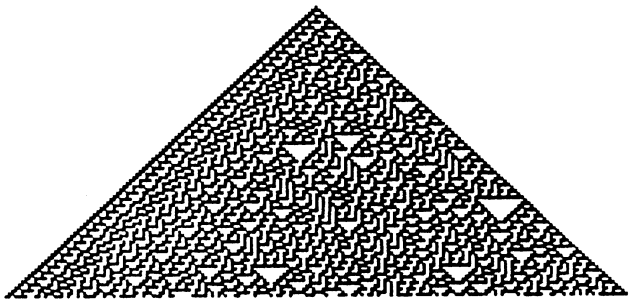

FIG. 1. Pattern generated by cellular automaton evolution from a simple initial state. Site values 0 or 1 (represented by white or black, respectively) are updated at each step according to the rule $a_i' = a_{i-1} \oplus (a_i \vee a_{i+1})$ ($\oplus$ denotes addition modulo 2, and $\vee$ Boolean disjunction). Despite the simplicity of its specification, many features of the pattern (such as the sequence of site values down the center column) appear random.

The simplest mathematical and physical systems (such as the shift mapping) can be decomposed into essentially uncoupled components, and cannot increase Θ. Such systems are nevertheless often homoplectic, so that they transfer information, and with random input show random behavior. But when their input is simple (low Θ), their behavior is correspondingly simple, and is typically periodic. Of course, any system with a fixed finite total number of degrees of freedom (such as a finite cellular automaton) must eventually become periodic. But the phenomena considered here occur on time scales much shorter than such exponentially long recurrences.

Another class of systems widely investigated consists of those with linear couplings between components [such as a cellular automaton in which $a_i^{(t+1)} = (a_{i-1}^{(t)} + a_{i+1}^{(t)}) \bmod 2$]. Given random input, such systems can again yield random output, and are thus homoplectic. But even with simple input, they can produce sequences which pass some statistical tests of randomness. Examples are the standard linear congruence and linear-feedback shift-register (or finite additive cellular automaton[15]) systems used for pseudorandom number generation in practical computer programs.[6,16]

Characteristic of such systems is the generation of self-similar patterns, containing sequences that are invariant under blocking or scaling transformations. These sequences are almost periodic, but may contain all possible blocks of elements with equal frequencies. They can be considered as the outputs of finite-state machines (generalized Markov processes) given the digits of the numerical positions of each element as input.[17] And although the sequences have certain statistical properties of randomness, their seeds can be found by comparatively simply polynomial-time procedures.[18] Such systems are thus not autoplectic (with respect to polynomial-time computations).

Many nonlinear mathematical systems seem, however, to be autoplectic, since they generate sequences in which no patterns have ever been found. An example is the sequence of leading digits in the fractional part of successive powers of $\frac{3}{2}$[19] (which corresponds to a vertical column in a particular $k = 6$, $r = 1$ cellular automaton with a single site seed).

Despite extensive empirical evidence, almost nothing has, however, been proved about the randomness of such sequences. It is nevertheless possible to construct sequences that are strongly expected to be effectively random.[20] An example is the lowest-order bits of $x_t = x_{t-1}^2 \bmod(pq)$, where p and q are large primes.[20] The problem of deducing the initial seed x_0, or of substantially compressing this sequence, is

equivalent to the problem of factoring large integers, which is widely conjectured to require more than polynomial time.[21]

Standard statistical tests have also revealed no patterns in the digit sequences of transcendental numbers such as[22] $\sqrt{2}$, e, and π [22] (or continued-fraction expansions of π or of most cubic irrational numbers). But the polynomial-time procedure of squaring and comparing with an integer does reveal the digits of, say, $\sqrt{2}$ as nonrandom.[23] Without knowing how the sequence was generated, however, such a very special "statistical test" (or program) can probably only be found by explicit enumeration of all exponentially many possible ones. And if a sequence passes all but perhaps exponentially few polynomial-time batteries of statistical tests, it should probably be considered effectively random in practice.

Within a set of homoplectic dynamical systems (such as class 3 or 4 cellular automata) capable of transmitting information, all but the simplest seem to support sophisticated information processing, and are thus expected to be autoplectic. In some cases (quite probably including Fig. 1[24]) the evolution of the system represents a "complete" or "universal" computation, which, with appropriate initial conditions, can mimic any other (polynomial-time) computation.[21] If short specifications for sequences generated by any one such computation could in general be found in polynomial time, it would imply that all could, which is widely conjectured to be impossible. (Such problems are called *NP*-complete.[21])

Many systems are expected to be computationally irreducible, so that the outcome of their evolution can be found essentially only by direct simulation, and no computational short cuts are possible.[25] To predict the future of these systems requires an almost complete knowledge of their current state. And it seems likely that this can be deduced from partial measurements only by essentially testing all exponentially many possibilities. The evolution of computationally irreducible systems should thus generically be autoplectic.

Autoplectic behavior is most clearly identified in discrete systems such as cellular automata. Continuous dynamical systems involve the idealization of real numbers on which infinite-precision arithmetic operations are performed. For systems such as iterated mappings of the interval there seems to be no robust notion of "simple" initial conditions. (The number of binary digits in images of, say, a dyadic rational grows like p^t, where p is the highest power of x in the map.) But in systems with many degrees of freedom, described for example by partial differential equations, autoplectism may be identified through discrete approximations.

Autoplectism is expected to be responsible for apparent randomness in many physical systems. Some features of turbulent fluid flow,[26] say in a jet ejected from a nozzle, are undoubtedly determined by details of initial or boundary conditions. But when the flow continues to appear random far from the nozzle, one suspects that other sources of effective information are present. One possibility might be thermal fluctuations or external noise, amplified by homoplectic processes.[1] But viscous damping probably allows only sufficiently large-scale perturbations to affect large-scale features of the flow. (Apparently random behavior is found to be almost exactly repeatable in some carefully controlled experiments.[27]) Thus, it seems more likely that the true origin of turbulence is an internal autoplectic process, somewhat like Fig. 1, operating on large-scale features of the flow. Numerical experiments certainly suggest that the Navier-Stokes equations can yield complicated behavior even with simple initial conditions.[28] Autoplectic processes may also be responsible for the widespread applicability of the second law of thermodynamics.

Many discussions have contributed to the material presented here; particularly those with C. Bennett, L. Blum, M. Blum, J. Crutchfield, P. Diaconis, D. Farmer, R. Feynman, U. Frisch, S. Goldwasser, D. Hillis, P. Hohenberg, E. Jen, R. Kraichnan, L. Levin, D. Lind, A. Meyer, S. Micali, J. Milnor, D. Mitchell, A. Odlyzko, N. Packard, I. Procaccia, H. Rose, and R. Shaw. This work was supported in part by the U. S. Office of Naval Research under Contract No. N00014-80-C-0657.

---

[1]For example, R. Shaw, Z. Naturforsch. **36A**, 80 (1981), and in *Chaos and Order in Nature,* edited by H. Haken (Springer, New York, 1981).

[2]An analogous cellular automaton [S. Wolfram, Nature (London) **311**, 419 (1984), and references therein] has evolution rule $a_i^{(t+1)} = a_i^{(t)} \oplus a_{i+1}^{(t)}$, so that with time the value of a particular site is determined by the value of progressively more distant initial sites.

[3]For example, *Order in Chaos,* edited by D. Campbell and H. Rose (North-Holland, Amsterdam, 1982). Many processes analyzed in dynamical systems theory admit "Markov partitions" under which they are directly equivalent to the shift mapping. But in some measurements (say of x_t with four bins) their deterministic nature may introduce simple regularities, and "deterministic chaos" may be said to occur. (This term would in fact probably be better reserved for the autoplectic processes to be described below.)

[4]This is probably also true of at least the lower levels of human sensory processing [for example, D. Marr, *Vision* (Freeman, San Francisco, 1982); B. Julesz, Nature (London) **290**, 91 (1981)].

[5]The validity of Monte Carlo simulations tests the random sequences that they use. But most stochastic physical processes are in fact insensitive to all but the simplest equidistribution and statistical independence properties.

(Partial exceptions occur when long-range order is present.) And in general no polynomial-time simulation can reveal patterns in effectively random sequences.

[6]For example, D. Knuth, *Seminumerical Algorithms* (Addison-Wesley, Reading, Mass., 1981).

[7]Some sophisticated statistical procedures, typically involving the partitioning of high-dimensional spaces, seem to take exponential time. But most take close to linear time. It is possible that those used in practice can be characterized as needing $O(\log^p n)$ time on computers with $O(n^q)$ processors (and so be in the computational complexity class *NC*) [cf. N. Pippenger, in *Proceedings of the Twentieth IEEE Symposium on Foundations of Computer Science* (IEEE, New York, 1979); J. Hoover and L. Ruzzo, unpublished].

[8]For example, R. Hamming, *Coding and Information Theory* (Prentice-Hall, Englewood Cliffs, 1980).

[9]G. Chaitin, J. Assoc. Comput. Mach. **13**, 547 (1966), and **16**, 145 (1969), and Sci. Am. **232**, No. 5, 47 (1975); A. N. Kolmogorov, Problems Inform. Transmission **1**, 1 (1965); R. Solomonoff, Inform. and Control **7**, 1 (1964); L. Levin, Soviet Math. Dokl. **14**, 1413 (1973). Compare J. Ford, Phys. Today **33**, No. 4, 40 (1983). Note that the lengths of programs needed on different universal computers differ only by a constant, since each computer can simulate any other by means of a fixed "interpreter" program.

[10]Quantum mechanics suggests that processes such as radioactive decay occur purely according to probabilities, and so could perhaps give absolutely random sequences. But complete quantum mechanical measurements are an idealization, in which information on a microscopic quantum event is spread through an infinite system. In finite systems, unmeasured quantum states are like unknown classical parameters, and can presumably produce no additional randomness. Suggestions of absolute randomness probably come only when classical and quantum models are mixed, as in the claim that quantum processes near black holes may lose information to space-time regions that are causally disconnected in the classical approximation.

[11]In the cases now known, recognition of any pattern seems to involve essentially complete reconstruction of the original program, but this may not always be so (L. Levin, private communication).

[12]In some cases, such as optimization or eigenvalue problems in the complexity class *NP* [e.g., M. Garey and D. Johnson, *Computers and Interactability: A Guide to the Theory of NP-Completeness* (Freeman, San Francisco, 1979)], even each individual test may take exponential time.

[13]The sequence certainly passes the standard statistical tests of Ref. 6, and contains all possible subsequences up to length at least 12. It has also been proved that only at most one vertical sequence in the pattern of Fig. 1 can have a finite period [E. Jen, Los Alamos Report No. LA-UR-85-1218 (to be published)].

[14]For example, D. E. R. Denning, *Cryptography and Data Security* (Addison-Wesley, Reading, Mass., 1982). Systems like Fig. 1 can, for example, be used for "stream ciphers" by adding each bit in the sequences produced with a particular seed to a bit in a plain-text message.

[15]For example, O. Martin, A. Odlyzko, and S. Wolfram, Commun. Math. Phys. **93**, 219 (1984).

[16]B. Jansson, *Random Number Generators* (Almqvist & Wiksells, Stockholm, 1966).

[17]They are one-symbol-deletion tag sequences [A. Cobham, Math. Systems Theory **6**, 164 (1972)], and can be represented by generating functions algebraic over $GF(k)$ [G. Christol, T. Kamae, M. Mendes France, and G. Rauzy, Bull. Soc. Math. France **108**, 401 (1980); J.-M. Deshouillers, Seminar de Theorie des Nombres, Université de Bordeaux Exposé No. 5, 1979 (unpublished); M. Dekking, M. Mendes France, and A. van der Poorten, Math. Intelligencer, **4**, 130, 173, 190 (1983)]. Their self-similarity is related to the pumping lemma for regular languages [e.g., J. Hopcroft and J. Ullman, *Introduction to Automata Theory, Languages and Computation* (Addison-Wesley, Reading Mass., 1979)]. More complicated sequences associated with context-free formal languages can also be recognized in polynomial time, but the recognition problem for context-sensitive ones is *P*-space complete.

[18]For example, A. M. Frieze, R. Kannan, and J. C. Lagarias, in *Twenty-Fifth IEEE Symposium on Foundations of Computer Science* (IEEE, New York, 1984). The sequences also typically fail certain statistical randomness tests, such as multidimensional spectral tests (Ref. 6). They are nevertheless probably random with respect to all *NC* computations [J. Reif and J. Tygar, Harvard University Computation Laboratory Report No. TR-07-84 (to be published)].

[19]For example, G. Choquet, C. R. Acad. Sci. (Paris), Ser. A **290**, 575 (1980); cf. J. Lagarias, Amer. Math. Monthly **92**, 3 (1985). (Note that with appropriate boundary conditions a finite-size version of this system is equivalent to a linear congruential pseudorandom number generator.)

[20]A. Shamir, Lecture Notes in Computer Science, **62**, 544 (1981); S. Goldwasser and S. Micali, J. Comput. Sys. Sci. **28**, 270 (1984); M. Blum and S. Micali, SIAM J. Comput. **13**, 850 (1984); A. Yao, in *Twenty-Third IEEE Symposium on Foundations of Computer Science* (IEEE, New York, 1982); L. Blum, M. Blum, and M. Shub, in *Advances in Cryptology: Proceedings of CRYPTO-82,* edited by D. Chaum, R. Rivest, and A. T. Sherman (Plenum, New York, 1983); O. Goldreich, S. Goldwasser, and S. Micali, in *Twenty-Fifth IEEE Synmposium on Foundations of Computer Science* (IEEE, New York, 1984).

[21]For example, M. Garey and D. Johnson, Ref. 12.

[22]For example, L. Kuipers and H. Niederreiter, *Uniform Distribution of Sequences* (Wiley, New York, 1974).

[23]A polynomial-time procedure is also known for recognizing solutions to more complicated algebraic or trigonometric equations (R. Kannan, A. K. Lenstra, and L. Lovasz, Carnegie-Mellon University Technical Report No. CMU-CS-84-111).

[24]Many localized structures have been found (D. Lind, private communication).

[25]S. Wolfram, Phys. Rev. Lett. **54**, 735 (1985).

[26]For example, U. Frisch, Phys. Scr. **T9**, 137 (1985).

[27]G. Ahlers and R. W. Walden, Phys. Rev. Lett. **44**, 445 (1980).

[28]For example, M. Brachet *et al.,* J. Fluid Mech. **130**, 411 (1983).