Proc. Natl. Acad. Sci. USA
Vol. 95, pp. 10367–10372, September 1998
Mathematics

A recipe for randomness

(normal numbers/maximally irregular/approximate entropy/deficit from equidistribution/combinatorial)

STEVE PINCUS[†‡] AND BURTON H. SINGER[§]

[†]990 Moose Hill Road, Guilford, CT 06437; and [§]Office of Population Research, Princeton University, Princeton, NJ 08544

Contributed by Burton H. Singer, July 7, 1998

ABSTRACT **Despite many diverse theories that address closely related themes—e.g., probability theory, algorithmic complexity, cryptoanalysis, and pseudorandom number generation—a near-void remains in constructive methods certified to yield the desired "random" output. Herein, we provide explicit techniques to produce broad sets of both highly irregular finite and normal infinite sequences, based on constructions and properties derived from approximate entropy (ApEn), a computable formulation of sequential irregularity. Furthermore, for infinite sequences, we considerably refine normality, by providing methods for constructing diverse classes of normal numbers, classified by the extent to which initial segments deviate from maximal irregularity.**

There is a critical and ubiquitous need for general techniques to produce broad sets of both highly irregular finite and putatively "random" infinite sequences. Early this century, Borel (1) introduced the notion of normal number, whose base b expansions are equidistributed in the limit, for all individual digits, pairs of digits, triples, . . . As such, the sequences of digits of normal numbers have often been viewed (2, 3) as reasonable candidates for broad collections of "random sequences." However, demonstrations of the existence of uncountably many normal numbers (1, 4) and of the fact that they constitute a set of Lebesgue measure 1 in the unit interval have been unaccompanied by general methods to explicitly construct them. Indeed, the difficulty of proving normality for any specific number is remarkably severe. Among the very few sets of known explicitly computable normal numbers, probably best known is Champernowne's number 0.1234567891011. . . (5), which was thematically generalized by Copeland and Erdös (6).

A primary step toward filling this near-void was the introduction of the notion of a C-random (computationally random) sequence (7), an equivalent characterization of normality based on a measure of irregularity among successive digits, approximate entropy (ApEn). Applying this formulation, in ref. 7 we presented a perturbation strategy for generating large sets of normal numbers, starting from one such number.

Two advantages accrue from the ApEn formulation: an ability to identify finite maximally irregular sequences as fundamental building blocks for construction of normal numbers; and subsequently, an ability to quantify the magnitude of deviation of any sequence from maximal irregularity.

The purposes of this paper are specifications of constructive methods for generating: (*i*) large classes of finite maximally irregular sequences; (*ii*) large classes of normal numbers by appropriate concatenations of finite maximally irregular sequences; and (*iii*) diverse classes of normal numbers, classified by the (asymptotic behavior of the) extent to which initial segments deviate from maximal irregularity.

We emphasize that herein, we focus on equidistribution as the central notion of "randomness," discussed further in endnote 1 below. The extreme limitations in attempting to utilize algorithmic complexity (an alternative notion of "randomness") for actual constructions of highly irregular sequences have been previously described (7, 8).

The central result below is *Theorem 10*, our recipe for constructing normal sequences, with the next section, *Varieties of Normal Numbers*, indicating how to apply *Theorem 10* to refine normal numbers into the aforementioned subclasses. The primary results that lead directly to *Theorem 10* are (*i*) *Theorem 1*, relating maximal irregularity to most equidistributed; (*ii*) *Theorem 3* and *Algorithm 1*, providing means to realize maximally irregular finite sequences; and (*iii*) *Theorems 8* and *9*, reconsidering and merging poignant, yet nonconstructive (abstract theoretical), developments by Besicovitch and Hanson with the present context of maximally irregular sequences to achieve the desired constructive methodology.

In the core text, we primarily analyze binary sequences; generalizations to the k-state alphabet are straightforward.

Approximate Entropy (ApEn) and Wrap-Around ApEn. We quantify irregularity utilizing approximate entropy, ApEn, formally defined in refs. 7 and 8. The intuitive idea is that for a sequence of real numbers $\underline{u} := (u(1), u(2), \ldots u(N))$, ApEn$(m, r, N)(\underline{u})$ measures the logarithmic frequency with which *blocks* (subsequences of contiguous sequence points) of length m that are close together—i.e., within a tolerance range r—remain close together for blocks augmented by one position. Larger values of ApEn imply greater irregularity in $\underline{u}$, while smaller values correspond to more instances of recognizable patterns in the sequence. Further intuition about ApEn, as quantifying degrees of irregularity, can be obtained by reviewing binary sequences of lengths 5 and 6, a comparison of two binary sequences of length $N = 20$, and the first N digits (for large values of N) in the binary and decimal expansions of e, π, $\sqrt{3}$, and $\sqrt{2}$ (7, 9).

Formally, we have

Definition 1: Given a positive integer N and nonnegative integer m, with $m \leq N$, a positive real number r and a sequence of real numbers $\underline{u} := (u(1), u(2), \ldots u(N))$, let the distance between two blocks $\underline{x}(i)$ and $\underline{x}(j)$, where $\underline{x}(i) = (u(i), u(i+1), \ldots u(i+m-1))$, be defined by $d(\underline{x}(i), \underline{x}(j)) = \max_{k=1,2,\ldots,m}(|u(i+k-1) - u(j+k-1)|)$. Then let $C_i^m(r) =$ (number of $j \leq N - m + 1$ such that $d(\underline{x}(i), \underline{x}(j)) \leq r)/(N - m + 1)$. Now define

$$\Phi^m(r) = \frac{1}{N-m+1} \sum_{i=1}^{N-m+1} \log C_i^m(r), \text{ and}$$

$\text{ApEn}(m, r, N)(\underline{u}) = \Phi^m(r) - \Phi^{m+1}(r), m \geq 1$; $\text{ApEn}(0, r, N)(\underline{u}) = -\Phi^1(r)$.

While restricting attention to binary sequences of 0s and 1s, we set $r < 1$ as our measure of resolution. Thus we are

The publication costs of this article were defrayed in part by page charge payment. This article must therefore be hereby marked "*advertisement*" in accordance with 18 U.S.C. §1734 solely to indicate this fact.

Abbreviations: ApEn, approximate entropy; LIL, law of the iterated logarithm.

[‡]To whom reprint requests should be addressed.

monitoring precise matches in the blocks $\underline{x}(i)$ and $\underline{x}(j)$. In this setting we suppress the dependence of ApEn on r below.

A length N sequence $\underline{u}$ is defined as $\{m, N\}$-*irregular* if it achieves the maximal ApEn(m, N) value among all sequences of length N; and it is defined as N-*irregular* (N-*random*) if it is $\{m, N\}$-irregular for $m = 0, 1, 2, \ldots, m_{\text{crit}}(N)$. In ref. 7, we employed the choice $m_{\text{crit}}(N) = \max(m: 2^{2^m} \leq N)$, motivated by the methods of Ornstein and Weiss (10), which can be used to show that for $\underline{u}_N = (u(1), u(2), \ldots u(N))$, $N \geq 1$, a so-called "typical realization" of a Bernoulli process, then $\lim_{N\to\infty}$ ApEn$(m_{\text{crit}}(N), N)$ $(\underline{u}_N) = h$ = entropy of the process. Super-exponential growth of N as a function of $m_{\text{crit}}(N)$ thus is a useful criterion for aligning maximally irregular finite sequences with ergodic theory technology. However, our normal number constructions require tighter control over irregularity in blocks of length m for more values of m than is imposed by $m_{\text{crit}}(N) = \max(m: 2^{2^m} \leq N)$. For all developments below, we specify $m_{\text{crit}}(N) = \max(m: 2^m < N)$.¶ Both choices of $m_{\text{crit}}(N)$ are consistent with the idea of finite "random sequence," as exemplified by the following theorem, proved in ref. 9:

THEOREM 1. *A sequence* $\underline{u}$ *is* N-random *if and only if for* $1 \leq m \leq m_{\text{crit}}(N) + 1$, *the expression*

$$\max_{\{v1, v2, \ldots, vm\}} \left| \frac{1}{N - m + 1} (\text{no. of } \{v1, v2, \ldots, vm\} \text{ blocks in the sequence } \underline{u}) - 1/2^m \right| \quad \textbf{[1]}$$

is a minimum (among length-N *sequences), where the max is evaluated over all blocks* $\{v1, v2, \ldots, vm\}$ *where* $vi = 0$ *or* 1 *for all* $1 \leq i \leq m$.

Thus maximal ApEn agrees with intuition for maximally equidistributed sequences, while allowing us to grade the remaining sequences in terms of proximity to maximality.

For infinite sequences $\underline{u} = (u(1), u(2), \ldots)$ and $r < 1$, define $\underline{u}^{(N)} = (u(1), u(2), \ldots, u(N))$, ApEn$(m, N)(\underline{u})$:= ApEn$(m, N)(\underline{u}^{(N)})$, and ApEn$(m)(\underline{u})$:= $\lim_{N\to\infty}$ ApEn$(m, N)(\underline{u}^{(N)})$. Asymptotic ApEn$(m)$ values converge to log 2 along maximally irregular binary sequences (7). This fact motivates the following formulation of an infinite "random sequence."

Definition 2: An infinite binary sequence $\underline{u}$ is called computationally random, denoted as C-random, if and only if ApEn$(m)(\underline{u}) = \log 2$ for all $m \geq 0$.

As pointed out in ref. 7, joint independence in probability theory for binary random variables reduces to C-randomness of realizations with probability one.

Our constructions of C-random sequences are facilitated by introducing a wrap-around version of approximate entropy, denoted by ApEn$_w$. The intuitive idea is to consider sequences of length N in a circular arrangement. Then for all m, blocks of length m are defined beyond the end of the original sequence by periodic extension. Thus averages in the calculation of ApEn$_w$ are always over N consecutive blocks. Formally, we introduce

Definition 3: Given a positive integer N, a nonnegative integer m, a positive real number r, and a sequence of real numbers $\underline{u} := (u(1), u(2), \ldots u(N))$, define the block $\underline{x}_w(i) = (u(i), u(i + 1), \ldots u(i + m - 1))$, with $u(N + k) := u(k)$ for $1 \leq k \leq N$. For all $1 \leq i, j \leq N$, define the distance between two blocks by $d(\underline{x}_w(i), \underline{x}_w(j)) = \max_{k=1,2,\ldots,m} (|u(i + k - 1) - u(j + k - 1)|)$. Then let $C^m_{i,w}(r) =$ (number of $j \leq N$ such that $d(\underline{x}_w(i), \underline{x}_w(j)) \leq r)/N$. Now define $\Phi^m_w(r) = 1/N \sum_{i=1}^N \log C^m_{i,w}(r)$, and ApEn$_w(m, r, N)(\underline{u}) = \Phi^m_w(r) - \Phi^{m+1}_w(r)$, $m \geq 1$; $ApEn_w(0, r, N)(\underline{u}) = -\Phi^1_w(r)$.

¶However, despite the utility seen herein, it would be unwise to employ this choice of $m_{\text{crit}}(N)$ in general *statistical* analyses of length-N data sets. The "curse of dimensionality" would be manifested in estimations of underlying length $\log_2 N$ joint frequencies, many of which would have 0 or 1 observed occurrences.

Here we again set $r < 1$ and suppress the dependence of ApEn$_w(m, r, N)$ on r, and simply write it as ApEn$_w(m, N)$.

Analogous to the original ApEn setting, for binary sequences of length N, we define $\{m, N\}$ *wr-random* (*wr-irregular*) sequences as those that achieve max ApEn$_w(m, N)(\underline{u})$ where the maximum is evaluated over the set of all binary sequences of length N. Corresponding definitions ensue for N wr-random and C$_w$-random.

Some properties are now noted regarding ApEn$_w$.

(*i*) Virtually the same criterion as that given by *Theorem 1* characterizes the maximally wr-irregular ApEn$_w$ sequences, via the same proof—-the only changes in the wrap-around setting are that all sums go from 1 to N (not $N - m + 1$), since evaluation of the number of $\{v1, v2, \ldots, vm\}$ blocks in the sequence u includes consideration of the wrap-around subblocks. Accordingly, in the expression corresponding to Eq. **1**, we average by dividing by N, rather than $N - m + 1$.

(*ii*) For any sequence, ApEn and ApEn$_w$ values will be reasonably close—i.e., $O(\log N/N)$, as their definitions differ only in the treatment of endpoint effects. Precisely, we have:

THEOREM 2. *For any length* N *sequence* $\underline{u}$,

$$|\text{ApEn}(m)(\underline{u}) - \text{ApEn}_w(m)(\underline{u})| \leq 2^{m+2}\left(\frac{m}{N - m}\right)\log N.$$

Proof: First, we recast $\Phi^m(0)$ in the ApEn definition in an alternative form, based on state space frequencies. Let $X(m)$:= {all blocks $\{v1, v2, \ldots, vm\}$ where $vi = 0$ or 1 for all $1 \leq i \leq m$}; and define $f_{v1,v2,\ldots,vm}$ as the frequency of occurrences of $\{v1, v2, \ldots, vm\}$ in $\underline{u}$—i.e., (no. of such occurrences)/(N − $m + 1$). Then it is straightforward to see that $\Phi^m(0) = \Sigma_{X(m)} f_{v1,v2,\ldots,vm} \log f_{v1,v2,\ldots,vm}$. Similarly, we have $\Phi^m_w(0) = \Sigma_{X(m)} f^w_{v1,v2,\ldots,vm} \log f^w_{v1,v2,\ldots,vm}$, where $f^w_{v1,v2,\ldots,vm}$ = (no. of occurrences, including wrap-around instances, of $\{v1, v2, \ldots, vm\})/N$.

Then $|\text{ApEn}(m)(\underline{u}) - \text{ApEn}_w(m)(\underline{u})| \leq |\Phi^m(0) - \Phi^m_w(0)| + |\Phi^{m+1}(0) - \Phi^{m+1}_w(0)| \leq \Sigma_{X(m)} |f_{v1,v2,\ldots,vm} \log f_{v1,v2,\ldots,vm} - f^w_{v1,v2,\ldots,vm} \log f^w_{v1,v2,\ldots,vm}| + \Sigma_{X(m+1)} |f_{v1,v2,\ldots,vm+1} \log f_{v1,v2,\ldots,vm+1} - f^w_{v1,v2,\ldots,vm+1} \log f^w_{v1,v2,\ldots,vm+1}|$. We bound all terms on the right side of this inequality by the mean value theorem, applied to $f(x) = x \log x$, observing that $|f(x) - f(x^*)| \leq \max_{t\in[x,x^*]} |(x - x^*)(1 + \log t)|$. Applied to the above, for $x = f_{v1,v2,\ldots,vk}$ and $x^* = f^w_{v1,v2,\ldots,vk}$, we deduce that $|\text{ApEn}(m)(\underline{u}) - \text{ApEn}_w(m)(\underline{u})| \leq 2^m [(m - 1)/(N - m + 1)] \log N + 2^{m+1}[m/(N - m)] \log N \leq 2^{m+2}[m/(N - m)] \log N$, which completes the proof.

In particular, for large N, N-wr-irregular ApEn$_w$ sequences will be nearly N-irregular ApEn sequences, and conversely.

(*iii*) ApEn$_w$ is $\underline{u}$-shift invariant (mod N)—i.e., for any $\underline{u} := (u(1), u(2), \ldots u(N))$ and any $k \leq N$, ApEn$_w(\underline{u})$ = ApEn$_w(\underline{v})$, where $\underline{v} := (v(1), v(2), \ldots v(N)) = (u(1 + k(\text{mod } N)), (u(2 + k(\text{mod } N)), \ldots, u(N + k \text{ (mod } N)))$. The proof of this observation is straightforward.

(*iv*) Given this shift invariance, as well as ApEn$_w$ invariance to sequence negation and reversal, the number of distinct equivalence classes comprising *all* N-wr-irregular sequences appears to be relatively small, an important property. For example, a single generator suffices to produce all *N-wr-irregular* sequences for $N = 4$ (4 maximal sequences) and $N = 5$ (10 maximal sequences), and all 18 6-wr-irregular sequences come from the above actions applied to 2 generators (e.g., {1, 1, 1, 0, 0, 0} and {1, 1, 0, 1, 0, 0}).

Construction of Highly Irregular Sequences. We first consider the 2^k-wr-irregular sequences, since they have an elegant characterization and are central to our other constructions. For this case, some directly transferable theory has been developed, in the study of shift registers, which have been extensively applied to communications and coding problems (11–13). One class of shift register sequences that has received special focus is full-length nonlinear shift register sequences

("full cycles")—i.e., periodic sequences of length 2^k such that all different binary k-tuples appear exactly once in a periodic portion of a sequence (14). The existence of full cycles for all k was shown by Good (15) and deBruijn (16). For one period $\underline{u}$ of a full cycle, it is immediate upon aggregation that any length-m block with $m \leq k$ occurs precisely 2^{k-m} times in $\underline{u}$. Thus, by the wrap-around version of *Theorem 1*, we infer that the periods of full cycles constitute the 2^k-wr-irregular sequences, restated as

THEOREM 3. *For any 2^k-wr-irregular sequence $\underline{u}$, each binary k-tuple occurs as a length-k block precisely once in $\underline{u}$.*

We next resolve whether any given length k sequence can be the initial segment of some wr-irregular sequence.

THEOREM 4. *Given any length k sequence $\underline{v} := \{v(1), v(2), \ldots, v(k)\}$, there exists a 2^k-wr-irregular sequence $\underline{u}$ for which the initial segment of $\underline{u}$ is $\underline{v}$—i.e., $u(i) = v(i)$ for $1 \leq i \leq k$.*

Proof: Choose an arbitrary 2^k-wr-irregular sequence $\{s(i)\}$. By *Theorem 3*, the block $\{v(i)\}_{1 \leq i \leq k}$ occurs precisely once in $\{s(i)\}$. Define $\{u(i)\}$ as the result of successive 1-shifts of $\{s(i)\}$ that leaves $\{v(i)\}$ as the initial block in $\{u(i)\}$. Since ApEn_w is shift-invariant, we infer the 2^k-wr-irregularity of $\{u(i)\}$.

Notably, deBruijn (16) showed that the number of full 2^k-length cycles $N(k) := 2^{2^{k-1}-k}$. Upon recognizing that all 2^k translations of one period of a full cycle are distinct from one another and from any period from another full cycle, we infer

THEOREM 5. *There are precisely $2^k N(k) = 2^{2^{k-1}} 2^k$-wr-irregular sequences.*

Thus for $N = 2^k$, precisely $1/\sqrt{\text{no. length-}N\text{ sequences}} = 1/\sqrt{2^N}$ are N-wr-irregular. Also, note that this fraction of N-wr-irregular sequences is much smaller than the coarse upper bound given in ref. 7, p. 2085, of $1/\sqrt{\pi N/2}$.

Moreover, the proofs of both Good and deBruijn provide a direct bridge to the combinatorial study of rooted trees, directed graphs, and necklaces. However, these proofs were nonconstructive, so the need remained for algorithmic "recipes" to construct full cycles. An outstanding source for many such algorithms is Fredricksen (ref. 14, section 3). We now briefly describe the two best-known such algorithms. Also readily usable from ref. 14 are the algorithms given by "prefer same," by "cross-join pairs," and by the method of appropriately splicing mirrored full cycles of span $k-1$ to generate full cycles of span k (ref. 14, section 3e).

(*i*) Linear shift registers are sequences defined by a recurrence relation of order n, $s(i+n) = \sum_{j=0}^{n-1} c(j)s(i+j)$. Associated is a characteristic polynomial $f(x) = 1 + c(1)x + \ldots + c(n-1)x^{n-1} + x^n$. If $f(0) \neq 0$, f has exponent k if $f(x) \mid x^k + 1$ but $f(x) \nmid x^j + 1$ for any $0 < j < k$ (where $\mid$ denotes divides). It is known from Galois theory (13) that [over the 2 element field GF(2)] if $f(x)$ has degree k, then $f(x)$ has an exponent $\leq 2^k - 1$. An irreducible polynomial of degree k is called primitive if its exponent $= 2^k - 1$. Primitive polynomials exist for all degrees k (ref. 13). The key result is that for a linear shift register corresponding to a primitive polynomial of degree k, the output sequence is an "$m(k)$-sequence"—i.e., the shift register goes through each of its $2^k - 1$ nonnull states before it repeats (11). Upon insertion of a 0 prior to the unique k block $\{0\,0\,0 \ldots 0\,1\}$ in one period of an $m(k)$-sequence, the resultant length 2^k sequence is directly seen to be a full cycle.

Tables of primitive polynomials exist—e.g., appendix C of ref. 13 for degree ≤ 34. However, the set of primitive polynomials supplies us with only some, but not nearly all, 2^k-wr-irregular sequences. Indeed, there are $\phi(2^k - 1)/k$ primitive polynomials of degree k over GF(2), for $\phi(m)$ the Euler ϕ-function (12). Thus, e.g., there are 2 primitive polynomials of degree 4 over GF(2), $f_1 = 1 + x + x^4$ and $f_2 = 1 + x^3 + x^4$, in contrast to 16 full cycles of length 16.

(*ii*) *"Prefer 1" Algorithm*: (*A*) Write k 0s. (*B*) For the nth sequence bit, $n > k$, write 1 if the newly formed k-tuple has not previously appeared in the sequence. Increase n and repeat *B*; otherwise (*C*) for the nth sequence bit, write 0. If the newly formed k-tuple has not previously appeared, increase n and go to *B*; otherwise stop.

This algorithm produces a full cycle. Notably, *all* full cycles can be generated by using "Prefer 1" repeatedly via "backtracking" (14); i.e., after we have generated the Prefer 1 sequence, succeeding sequences are determined by changing the final 1 to 0, and by using the algorithm, electing to place a 1 if the k-tuple formed is new but placing a 0 if 1 is prohibited. In this mode, the algorithm may terminate before the sequence is full length. If it terminates early, continue by again changing the final 1 to 0, proceeding as above.

For $N \neq 2^k$, both a theoretical description of and constructive algorithms for N-wr-irregular sequences appear to be much less elegant and relatively less straightforward, compared with the $N = 2^k$ setting. Insight into some of the complications are apparent from considering the 12-wr-irregular sequence $\underline{u} := \{1\,1\,0\,1\,1\,1\,0\,0\,1\,0\,0\,0\}$. It can be readily seen that (*i*) no length-4 block can be inserted into $\underline{u}$ to form a 16-wr-irregular sequence; (*ii*) $\underline{u}$ cannot be produced by insertion of a length-4 block to some 8-wr-irregular sequence; and notably, (*iii*) $\underline{u}$ provides a counterexample to the conjecture that each N-wr-irregular sequence can be derived from some $(N-1)$-wr-irregular sequence by appropriate insertion of a 0 or 1.

Point (*iii*) suggests that producing recursive techniques to generate (all) N-wr-irregular sequences for $N \neq 2^k$ may be quite challenging. Below, we give a recursive procedure that is part of a general strategy of building up longer N-wr-irregular sequences from shorter such sequences via concatenation. First, we formalize concatenation by

Definition 4: Given finite sequences $\underline{a} := (a(1), \ldots a(d))$ and $\underline{b} := (b(1), \ldots b(e))$, the concatenated sequence, of length $d + e$, is $\underline{a} \vee \underline{b} := (a(1), \ldots a(d), b(1), \ldots b(e))$.

Given a set of 2^k-wr-irregular sequences, *Algorithm 1* below generates $\{m, N\}$-wr-irregular sequences for $2^k < N < 2^{k+1}$, for all $m < k$. Within a general protocol of building up via concatenation, two points are critical to achieving maximality: (*i*) at least one concatenate should have length 2^k (so that slight excesses of particular blocks are not augmented); (*ii*) final segments of the concatenates must match exactly. To illustrate the need for *i*, consider $\underline{z} := \underline{v} \vee \underline{v}$, for $\underline{v} := \{0\,0\,1\,1\,1\} - \underline{z}$ is not even $\{0, 10\}$-wr-irregular, with 6 1s and 4 0s. To illustrate *ii*, let $\underline{v}$ be as above, with $\underline{w} := \{1\,1\,1\,0\,0\,0\,1\,0\}$. Then $\underline{z} := \underline{v} \vee \underline{w}$ is not $\{1, 13\}$-wr-irregular, with 5 (1, 1) occurrences, yet 2 occurrences each of both (1, 0) and (0, 1). However, upon translating $\underline{w}$ by successive 1-shifts to $\underline{w}' := \{0\,0\,0\,1\,0\,1\,1\,1\}$, matching a final 3-block to $\underline{v}$, we deduce that $\underline{z}' := \underline{v} \vee \underline{w}'$ is $\{m, 13\}$-wr-irregular, for all $m < 3$. More generally, we have

Algorithm 1: Given $2^k < N < 2^{k+1}$, let $t := N - 2^k$. Choose any t-wr-irregular sequence $\underline{w}$. We break the construction into two subcases: (I) $t \geq k$; (II) $t < k$. In the primary case (I), consider the end portion of $\underline{w}$, the length k block wend $:= (w(t-k+1), w(t-k+2), \ldots w(t))$. Choose any 2^k-wr-irregular sequence $\underline{s}$. By *Theorem 3*, $\underline{s}$ contains one occurrence of wend. Define $\underline{x} := (x(1), x(2), \ldots, x(2^k))$ as a shift of $\underline{s}$, so that the block wend is final in $\underline{x}$. By shift-invariance, $\underline{x}$ is 2^k-wr-irregular, and by the above, any length-m block with $m \leq k$ occurs precisely 2^{k-m} times in $\underline{x}$. Consider the length-N sequence $\underline{u} := \underline{w} \vee \underline{x}$: a straightforward counting argument then establishes that $\underline{u}$ is $\{m, N\}$-wr-irregular for all $m < k$.

In Case II, with $t < k$, a slightly modified construction is required. Given the t-wr-irregular sequence $\underline{w}$, let $\underline{y} := \underbrace{\underline{w} \vee \underline{w} \vee \ldots \underline{w}}_{[k/t]+1 \text{ times}}$, and let $\underline{z} :=$ the length k segment of the final k digits of $\underline{y}$. Choose a 2^k-wr-irregular sequence $\underline{x}$ such that $\underline{z}$ is final in $\underline{x}$, then define $\underline{u} := \underline{w} \vee \underline{x}$. A virtually identical counting argument to Case I establishes the result in this case as well.

The output of *Algorithm 1* is thus a selective list of highly irregular sequences. We then extract N-wr-irregular sequences

from this list by direct evaluation of each sequence for {k, N}-wr-irregularity. This final step provides functional triage; e.g., {1 1 0 1 0 0} $\vee$ {0 1 0 1 1 1 0 0} is {3, 14}- and thus 14-wr-irregular; whereas {1 1 0 1 0 0} $\vee$ {0 1 1 1 0 1 0 0} is not {3, 14}-wr-irregular, as some 4-blocks occur twice, others not at all.

Finally, our normal number constructions below require some bounds on the distribution of m-blocks for N-wr-irregular and N-irregular sequences. First, given a sequence $\underline{u}$, let $\mathbf{N}_w(\underline{u}, v1v2 \ldots vk) :=$ no. of occurrences of the block {$v1, v2, \ldots, vk$} in $\underline{u}$, including wrap-around instances; and let $\mathbf{N}(\underline{u}, v1v2 \ldots vk) :=$ no. of occurrences of the block {$v1, v2, \ldots, vk$}, excluding wrap-around instances. Two coarse inequalities, sufficient for our purposes, are as follows:

THEOREM 6. *Choose an N-wr-irregular sequence $\underline{u}$. Then for any $k \le [\log N]$ and any k-block {$v1, v2, \ldots, vk$},*

$$|\mathbf{N}_w(\underline{u}, v1v2 \ldots vk) - [N/2^k]| \le 2^k. \qquad \textbf{[2]}$$

Proof: We need only show that for any given k, there exists at least one length-N sequence $\underline{v}$ satisfying Eq. **2** for all k-blocks, by the wrap-around version of *Theorem 1*, in conjunction with the all-sequence minimality imposed by the wrap-around analog of Eq. **1**. We do so constructively. Choose a 2^k-wr-irregular $\underline{w}$ with {1 1 ... 1} as the initial length k segment. Let $P := \left[\frac{N}{2^k}\right]$ and let $\underline{w}^*(P) := \underbrace{\underline{w} \vee \underline{w} \vee \ldots \underline{w}}_{P \text{ times}}$. As above, for any $P \ge 1$, $\underline{w}^*(P)$ is seen to be {$k, P2^k$}-wr-irregular, indeed exactly equidistributed for all r-blocks, $r \le k$. Now define $\underline{v} := \underline{w}^*(P) \vee \underline{x}$, where $\underline{x}$ is a length $N - P2^k$ sequence of all 1s. It follows at once that $\underline{v}$ satisfies Eq. **2**, as desired.

THEOREM 7. *Choose an N-irregular sequence $\underline{u}$. Then for any $k \le [\log N]$ and any k-block {$v1, v2, \ldots, vk$}, $|\mathbf{N}(\underline{u}, v1v2 \ldots vk) - [(N - k + 1)/2^k]| \le 2^k + k$.*

Proof: This estimate follows at once by mimicking the proof of *Theorem 6* (again comparing to $\underline{v}$), in conjunction with two arithmetic observations. First, $|\mathbf{N}(\underline{u}, v1v2 \ldots vk) - \mathbf{N}_w(\underline{u}, v1v2 \ldots \text{vk})| \le k - 1$. Second, $|[N/2^k] - [(N - k + 1)/2^k]| \le 1$.

Normal Numbers. Our objective is to provide explicit rules for concatenating maximally irregular sequences of increasing length such that the limiting infinite sequences are normal numbers. *A priori* it seems plausible that the length of the ith concatenate should increase very rapidly (e.g., superexponentially) as a function of i (7, 10). However, we demonstrate via a counterexample that concatenating N-wr-irregular sequences with very rapidly growing lengths can lead to sequences where the frequency of occurrences of special blocks of digits is badly skewed over arbitrarily long segments, thus violating normality. Subtle restrictions on growth lengths of concatenates are necessary to ensure that the resulting infinite sequence is a normal number.

A Counterexample: Let $\mathrm{Lt}(\underline{v})$ denote the length of sequence $\underline{v}$. For a concatenated sequence $v_1 \vee v_2 \vee \ldots v_m$, let $\mathrm{Lcat}(m) = \Sigma_{i=1}^m \mathrm{Lt}(v_i)$. Now define $v_1 = (1, 0, 0, 1)$. Recursively, starting with $v_1 \vee v_2 \vee \ldots v_m$ of length $\mathrm{Lcat}(m)$, define s_m to be a sequence of 1s of length $(\mathrm{Lcat}(m))^2$. Then apply *Theorem 4* to obtain v_{m+1} as a $2^{(\mathrm{Lcat}(m))^2}$-wr-irregular sequence with s_m as an initial segment. Finally, define $\underline{u} := \lim_{m\to\infty} v_1 \vee v_2 \vee \ldots v_m$. Intuitively, in this construction, we are imposing intermediate biasing runs (via the $\underline{s}$-blocks) of exponentially increasing length.

Now consider the subsequences $\underline{u}_m^* := \{u(1), u(2), \ldots, u((\mathrm{Lcat}(m))^2 + \mathrm{Lcat}(m))\}$. Clearly, the fraction of 1s in $\underline{u}_m^* \ge \mathrm{Lcat(m)}^2/(\mathrm{Lcat}(m)^2 + \mathrm{Lcat}(m))$, which converges to 1 as $m \to \infty$. Thus $\underline{u}$ is not a normal number, for if it were, then $\lim_{m\to\infty}$ [fraction of 1s in $\underline{u}_m^*$] = 1/2.

The goal of concatenating maximally irregular sequences to produce normal numbers can be realized by bringing in two additional results. These are as follows:

THEOREM 8. *Given any positive integer k and any $\varepsilon > 0$, there exists $N_{k,\varepsilon}$ such that for all $N > N_{k,\varepsilon}$, the N-wr-irregular and N-irregular binary sequences are all (k, ε)-normal in the sense of Besicovitch (17).*

THEOREM 9. *Let $\{a_n\}$ be a nondecreasing sequence of positive integers having the property that, for any given k and $\varepsilon > 0$, all but finitely many a_n are (k, ε)-normal in the base b. If the lengths of the base b representations satisfy $n\mathrm{Lt}(a_n) = O(\Sigma_{i=1}^n \mathrm{Lt}(a_i))$, then the number $x = .a_1a_2a_3\ldots$ is normal in base b.*

Observe that in base 2, if we define the binary representations of $a_1, a_2, \ldots$ as the finite sequences $v_1, v_2, \ldots$, then x is just $v_1 \vee v_2 \vee \ldots$.

Theorem 8, a critical observation central to our constructive approach, provides the essential link between (k, ε)-normal integers and N-irregular sequences. *Theorem 9* is a minor adaptation of a little known theorem of Hanson (18). It provides necessary restrictions on the lengths of N-irregular sequences v_i to ensure that $\underline{u} := \lim_{m\to\infty} v_1 \vee v_2 \vee \ldots v_m$ is normal. To formalize these ideas we first require

Definition 5: (Besicovitch, ref. 17) An integer $t = a_{\mu\text{-}1}\, a_{\mu\text{-}2} \ldots a_1\, a_0$ ($a_{\mu\text{-}1} \ne 0$), where the a_i are digits of some base b, is *(k, ε)-normal* in base b for a given positive integer k and real $\varepsilon > 0$, if for every k-digit sequence $c_1c_2 \ldots c_k$, we have $\left|\frac{\mathbf{N}(t, c_1c_2\ldots c_k)}{\mu - k + 1} - \frac{1}{b^k}\right| < \varepsilon$, where $\mathbf{N}(t, c_1c_2 \ldots c_k)$ is the number of occurrences of $c_1c_2 \ldots c_k$ in t.

Specializing to base 2, we bring in

Proof of Theorem 8: Given k and ε, set $N_{k,\varepsilon} := \max(8{\cdot}2^k/\varepsilon, 2^{2k} + 1)$.

wr-Irregular case. For $N \ge N_{k,\varepsilon}$, choose any N-wr-irregular sequence $\underline{u}$ and any k-block {$v1, v2, \ldots, vk$}. Recall the notation $\mathbf{N}(\underline{u}, v1v2 \ldots vk)$ and $\mathbf{N}_w(\underline{u}, v1v2 \ldots vk)$ from *Theorems 6* and *7*, which we presently abbreviate by $\mathbf{N}(\underline{u})$, and $\mathbf{N}_w(\underline{u})$, respectively. Now $|\mathbf{N}(\underline{u})/(N - k + 1) - 1/2^k| \le |\mathbf{N}(\underline{u})/(N - k + 1) - \mathbf{N}_w(\underline{u})/(N - \mathrm{k} + 1)| + |\mathbf{N}_w(\underline{u})/(N - k + 1) - \mathbf{N}_w(\underline{u})/\mathrm{N}| + |\mathbf{N}_w(\underline{u})/N - 1/2^k|$. To estimate the first term on the right side of this inequality, since $|\mathbf{N}(\underline{u}) - \mathbf{N}_w(\underline{u})| \le k - 1$, it follows that $|\mathbf{N}(\underline{u})/(N - k + 1) - \mathbf{N}_w(\underline{u})/(N - k + 1)| \le |(k - 1)/(N - k + 1)| \le 2k/N \le \varepsilon/4$, from the definition of $N_{k,\varepsilon}$. To estimate the second term, since $k < \log N$, by *Theorem 6* and Eq. **2**, $\mathbf{N}_w(\underline{u}) \le N/2^k + 2^k$, thus $|\mathbf{N}_w(\underline{u})/(N - k + 1) - \mathbf{N}_w(\underline{u})/N| \le \mathbf{N}_w(\underline{u})|(k - 1)/[N(N - k + 1)]| \le (N/2^k + 2^k)(2k/N^2) \le (2N/2^k)(2k/N^2) = 4k/(N2^k) \le 2/N \le \varepsilon/4$. To estimate the third term, from Eq. **2**, $|\mathbf{N}_w(\underline{u})/N - 1/2^k| \le 2^k/N \le \varepsilon/4$. Combining these estimates, $|\mathbf{N}(\underline{u})/(N - k + 1) - 1/2^k| < \varepsilon/4 + \varepsilon/4 + \varepsilon/4 < \varepsilon$. Thus $\underline{u}$ is (k, ε)-normal in base 2.

Irregular case. For $N \ge N_{k,\varepsilon}$, choose any N-irregular sequence $\underline{u}$ and k-block {$v1, v2, \ldots, vk$}. By *Theorem 7*, since $k < \log N$, $|\mathbf{N}(\underline{u})/(N - k + 1) - 1/2^k| \le (2^k + k + 1)/(N - k + 1) < (4{\cdot}2^k/N) \le \varepsilon$, we conclude that $\underline{u}$ is (k, ε)-normal in base 2.

With this machinery established, we invoke Hanson's Theorem as adapted to *Theorem 9* to immediately deduce

THEOREM 10. *Define the base 2 sequence $\underline{u} := lim_{m\to\infty} v_1 \vee v_2 \vee \ldots \mathrm{v}_m$, with $\mathrm{Lt}(v_i)$ a nondecreasing integer-valued function of i. Let $S_n := \Sigma_{i=1}^n \mathrm{Lt}(v_i)$. If for all i, (i) v_i is either $\mathrm{Lt}(v_i)$-irregular or $\mathrm{Lt}(v_i)$-wr-irregular, (ii) $lim_{i\to\infty} \mathrm{Lt}(v_i) \to \infty$, and (iii) $n\mathrm{Lt}(v_n) = O(S_n)$, then $\underline{u}$ is normal in base 2.*

Theorem 10 provides a means to produce large collections of normal numbers, since diverse classes of functions $f(i) := \mathrm{Lt}(v_i)$ satisfy the conditions of the theorem. These include all polynomials with nonnegative integer coefficients; $f(i) = [A \log i]$, for $A > 0$; and $f(i) = [ki^\alpha]$ for positive k and α. We can extend these classes by observing that if f satisfies condition *iii*, and if there exist positive c and K such that $c \le |f(i)/g(i)| \le K$ for all i, then g also must satisfy *iii*—e.g., if $ci^\alpha < g(i) < Ki^\alpha$ for all i, where c, K, and $\alpha > 0$. Basically, functions that violate *iii* are either globally exponential or have locally, increasingly long exponentially growing segments.

Varieties of Normal Numbers. The length restrictions imposed by *Theorem 10*, while ensuring that limiting concatenations are normal numbers, nevertheless allow for considerable variation in sequence structure. We facilitate sequence assessment by introducing the functions $\text{def}_m[\underline{u}^{(N)}] := \max_{|v|=N} \text{ApEn}(m, N)(v) - \text{ApEn}(m, N)(\underline{u}^{(N)})$. For infinite sequences $\underline{u}$ these functions measure how close an initial segment, $\underline{u}^{(N)}$, of length N is to being $\{m, N\}$-irregular (or wr-irregular when ApEn_w is utilized). Normality reduces to the condition that $\lim_{N\to\infty} \text{def}_m[\underline{u}^{(N)}] = 0$ for all $m \geq 0$ (ref. 7). Restricting primary attention herein to $m = 0$, we can already demonstrate sharp distinctions among normal numbers.

We illustrate this perspective by comparing $\text{def}_0(N)$ for several sequences. The binary sequences are (*i*) base 2 expansion of *e*; (*ii*) the binary version of Champernowne's number 0.1234567891011. . . , denoted by BinChamp := 0.11011100101110111000. . . ; (*iii*) a perturbation of BinChamp (denoted as pert-BinChamp) that imposes a bias of excess 1s to BinChamp that decreases sufficiently rapidly with increasing sequence length so that limiting frequencies are unchanged; and (*iv*) a sequence denoted $\text{Seq}(F_{\text{IterLog-3}})$, defined below, where $\text{def}_0[\underline{u}^{(N)}]$ is extremely rapidly convergent to 0—i.e., $\text{def}_0[\underline{u}^{(N)}] \leq (\log\log\log N)^2/4N^2$ for sufficiently large N. Fig. 1 shows $\text{def}_0[\underline{u}^{(N)}]$ vs. N for values of N up to 300,000, with considerable differences among the sequences quite apparent.

Further analytic insight is gained by evaluation of asymptotic behavior of the sequences, and by comparison to the LIL asymptotic rate of convergence for $\text{def}_0(N)$. The LIL, an "almost sure" property of sums of independent, identically distributed (i.i.d.) binary random variables, interpreted for individual sequences, requires the following: Let $X_i = 1$ if the ith digit is 1, 0 otherwise, and let the partial sums $S_n = \Sigma_{i=1}^n X_i$ = (no. 1s among the first n digits). Then $\limsup_{n\to\infty} (S_n - n/2)/\sqrt{(n/2)\log\log n} = 1$. In ref. 7 we showed that the LIL holds for binary sequences $\underline{u}$ if and only if $\limsup_{N\to\infty} \text{def}_0[\underline{u}^{(N)}]/[(\log\log N)/N] = 1$.

Importantly, sequences *ii*, *iii*, and *iv*, all constructively defined, are normal, yet each has considerably different one-dimensional asymptotic behavior than the LIL mandate (as indicated below). These examples clarify the diversity of possible specifications of what one might mean by "random" (or highly irregular) sequence.

BinChamp is normal (5); yet observe a pronounced bias of excess 1s in BinChamp; e.g., $\{4, 5, 6, 7\}_{\text{base 2}} = \{\underline{1}00, \underline{1}01, \underline{1}10, \underline{1}11\}$. Formally, integers $\{2^k, 2^k + 1, \ldots, 2^{k+1} - 1\}_{\text{base 2}}$ produce 2^k segments, each length $k + 1$, headed by 1, followed, in aggregate, by all possible k-tuples of 1s and 0s. Thus

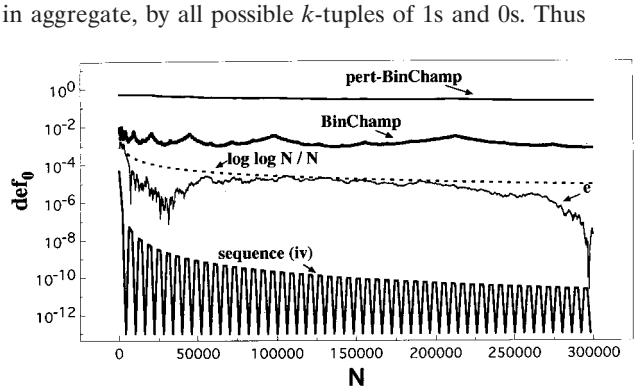

FIG. 1. One-dimensional deficit $\text{def}_0(N)$ from maximal irregularity for base 2 sequence expansions of *e* and for the binary sequences BinChamp (binary version of 0.1234567. . .), pert-BinChamp, and sequence $iv := \text{Seq}(F_{\text{IterLog-3}})$, all compared with $\log\log N/N$, where this last function is the asymptotic convergence rate of def_0 for sequences satisfying the law of the iterated logarithm (LIL).

$$\{\text{fraction of 1s in the first } \sum_{k=0}^{N} (k+1)2^k \text{ digits of BinChamp}\} \geq 1/2 + 1/2(N+1). \quad \textbf{[3]}$$

Now recall from ref. 7 the following definition of *excess*, for a binary sequence $\underline{u}$: {excess of "0" over "1"}$_N$ ($\underline{u}$) = max(0, no. 0s in $\underline{u}^{(N)}$ − no. 1s in $\underline{u}^{(N)}$), and symmetrically for {excess of "1" over "0"}$_N$ ($\underline{u}$). Let $\text{EXC}_N(\underline{u}) = \max(\{\text{excess of "0" over "1"}\}_N(\underline{u})\}$, {excess of "1" over "0"}$_N(\underline{u})\}$). In ref. 7, p. 2086, we established an easily derived relationship between def_0 and EXC (for small values of def_0) given by $\text{def}_0[\underline{u}^{(N)}] \approx \frac{1}{2}\left(\frac{\text{EXC}_N(\underline{u}^{(N)})}{N}\right)^2$. Upon translating Eq. **3** to a statement on EXC, we readily derive that for $\underline{u} :=$ BinChamp, $\limsup_{N\to\infty} \text{def}_0[\underline{u}^{(N)}] \geq 1/(5\log^2 N)$. This convergence rate for $\text{def}_0(N)$ thus quantifies the very slow extent to which the bias of excess 1s in BinChamp decreases toward asymptotic equidistribution.

We now specify sequences *iii* and *iv*. This also provides explicit constructions of special classes of normal numbers. We note as well that constructions similar to that of *Theorem 11* below, obtained by suitably controlling the length function $\text{Lt}(v_i)$ in the concatenations of finite maximally wr-irregular sequences, will yield yet further classes of normal numbers with prescribed asymptotic characteristics.

For sequence *iii* we perturb BinChamp, here denoted as $\underline{u} := (u(1), u(2), \ldots)$, according to the following algorithm (a specialization of theorem 3 in ref. 7):

Set $v(1) = u(1)$. Given $v(1), \ldots, v(N-1)$, set $v(N) = u(N)$ if $u(N) = 1$; set $v(N) = 1$ if $u(N) = 0$ and $\text{diff}_1(N-1)(\underline{u}, \underline{v}) \leq f(N) - 1$, where $\text{diff}_1(N)(\underline{u}, \underline{v}) :=$ the number of $i \leq N$ such that $u(i) \neq v(i)$, with $f(N) := [2N\sqrt{g(N)}]$, for $g(N) := N^{-0.3}$; otherwise set $v(N) = u(N)$ if $u(N) = 0$.

Then define pert-BinChamp := $\underline{v}$. By theorem 3 of ref. 7, pert-BinChamp is normal, and $\limsup_{N\to\infty} \text{def}_0[\underline{v}^{(N)}] > N^{-0.3}$, quantifying its very slow convergence of def_0 to 0.

Sequence *iv* is $\text{Seq}(F_{\text{IterLog-3}})$, a special case of the general construction in *Theorem 11*, below. First, we require

Definition 6: Fix n. Define $f_n(N) := \underbrace{\log(\log(\log \ldots (N)) \ldots)}_{n \text{ times}}$ for $N \geq \underbrace{\exp(\exp(\exp \ldots (1)) \ldots)}_{n \text{ times}}$; $f_n(N) := 0$ otherwise. Define $g_n(N)$ as the greatest even integer $\leq f_n(N)$. Then define $F_{\text{IterLog-}n}(N) := \max(6, g_n(N))$.

Next, for all i, select a maximally wr-irregular sequence v_i of length $F_{\text{IterLog-}n}(i)$. Let $\text{Seq}(F_{\text{IterLog-}n}) := \lim_{m\to\infty} w_m$, where $w_m = v_1 \vee v_2 \vee \ldots v_m$. From the construction of $F_{\text{IterLog-}n}(N)$, it follows from *Theorem 10* that $\text{Seq}(F_{\text{IterLog-}n})$ is normal in base 2. We now establish our fine-tuned result:

THEOREM 11. *Define* $k(N) := (1/4N^2)(F_{\text{IterLog-}n}(N))^2$. *Then for* $\underline{u} := \text{Seq}(F_{\text{IterLog-}n})$, *for all sufficiently large N,* $\text{def}_0[\underline{u}^{(N)}] \leq k(N)$.

Proof: Fix N. We will show that for all $p \leq \text{Lt}(w_N)$, $\text{EXC}_p(\underline{u}) \leq \frac{1}{2}(F_{\text{IterLog-}n}(N))$. Observe that $\underline{u}$ returns to precise 1-dimensional equidistribution at the cutpoints $p(k) := \{\text{Lt}(w_k)\}$ for all k—i.e., for all k, $\text{EXC}_{p(k)}(\underline{u}) = 0$. This is immediate, since v_i is $\{0, \text{Lt}(v_i)\}$-wr-irregular for all i (recalling that $F_{\text{IterLog-}n}(i)$ adopts only even values). Therefore $\max_{p\leq \text{Lt}(w_N)} \text{EXC}_p(\underline{u}) = \max_{1\leq i\leq N} \max_{p\leq \text{Lt}(v_i)} \text{EXC}_p(v_i) \leq \max_{1\leq i\leq N} \max(\text{no. 0s in } v_i, \text{no. 1s in } v_i) = \frac{1}{2}(F_{\text{IterLog-}n}(N))$.

Since $N < \text{Lt}(w_N)$, it then follows that $\text{EXC}_N(\underline{u}) \leq \frac{1}{2}(F_{\text{IterLog-}n}(N))$. Since $\underline{u}$ is normal, $\lim_{N\to\infty} \text{def}_0[\underline{u}^{(N)}] = 0$, hence for all sufficiently large N, $\text{def}_0[\underline{u}^{(N)}] \leq \left(\frac{\text{EXC}_N(\underline{u}^{(N)})}{N}\right)^2 \leq (1/4N^2)(F_{\text{IterLog-}n}(N))^2 = k(N)$, which completes the proof.

Thus for any $n \geq 1$, for $\underline{u} := \text{Seq}(F_{\text{IterLog-}n})$, $\limsup_{N\to\infty} \text{def}_0[\underline{u}^{(N)}]$ provides a much faster rate of convergence to 0 than that for the LIL of $(\log\log N)/N$.

Finally, observe that these Seq($F_{\text{IterLog-}n}$) provide a nearly "best possible" class of normal numbers, insofar as rapidity of convergence of $\lim \sup_{N\to\infty} \text{def}_0$ to 0. By the same argument as in the proof of theorem 1 of ref. 7, for any binary normal sequence $\underline{u}$, there exists arbitrarily large k for which $\underline{u}^{(2k)}$ fails to have precisely k 0s and k 1s. For such k, $\text{EXC}_{2k}(\underline{u}) \geq 2$; since $\text{def}_0[\underline{u}^{(N)}] \geq 0.4\left(\frac{\text{EXC}_N(\underline{u}^{(N)})}{N}\right)^2$ for sufficiently large N, we conclude that $\text{def}_0[\underline{u}^{(N)}] \geq 0.4/N^2$ for any such $N = 2k$—i.e., $\lim \sup_{N\to\infty} \text{def}_0[\underline{u}^{(N)}]$ must infinitely often be at least as large as the order of $1/N^2$. By comparison, $\lim \sup_{N\to\infty} \text{def}_0[\underline{u}^{(N)}]$ for Seq($F_{\text{IterLog-}n}$) is bounded above by $1/N^2$ times a function that can be chosen to increase arbitrarily slowly.

Endnotes. (*i*) In a vast preponderance of applications, the requirement of a "random" sequence reduces to (for either finite or infinite sequences) approximate equidistribution of m-blocks for all m. Our primary goal herein, met above, was to produce explicit sets of recipes to realize such sequences. Furthermore, the construction of normal numbers via concatenation of maximally irregular sequences, in conjunction with both the capability to impose length restrictions on the concatenates and the technology to assess resultant sequences via $\text{def}_m[\underline{u}^{(N)}]$, provides the basis for understanding irregularity and "randomness" in a previously unaddressed manner. The demonstration of pronounced qualitative differences among normal numbers above reinforces the perspective that grouping all normal numbers into a single asymptotically equidistributed category is often inadequately nonspecific, for both theoretical mathematical and applications-oriented considerations.

As well, a more subtle, yet arbitrary question concerns the choice of *a priori* constraints beyond normality that one might impose to designate a sequence as "random." For instance, to interpret a normal sequence as a typical realization of i.i.d. or weakly dependent binary random variables, one might mandate that the sequence satisfy the "almost sure" laws of axiomatic probability theory (19)—e.g., the LIL, and possibly a Gaussian distribution of 1-blocks. However, such mandates lead to conundrums; e.g., via *Theorem 11*, we now see that sequences satisfying the LIL are, in fact, more regular (*less* asymptotically equidistributed) than some classes of normal numbers. Additionally, recall that as $n \to \infty$ the proportion of binary sequences of length n that are maximally irregular converges to 0 (7). In contrast, a basic desideratum in Kolmogorov's algorithmic probability theory (20) is that the set of sequences called "random" should comprise a majority of the possible sequences. Thus the challenge is exposed, namely, how to balance the somewhat conflicting constraints imposed by maximal irregularity, typicality, and satisfaction of almost sure properties, to achieve a single well-defined class of constructable infinite "random" sequences.

(*ii*) Our explicit construction of normal numbers above is critically dependent on two ideas that had not previously been algorithmically formulated. First, the notion of (k, ε) normal number, as put forth by Besicovitch (17), was unaccompanied by any methods to actually produce them. Second, Hanson's Theorem (18) specifying length restrictions on $\text{Lt}(v_i)$ to ensure normality in a concatenation $\lim_{m\to\infty} v_1 \vee v_2 \vee \ldots v_m$ was not carried further to identify explicitly how to sequentially generate appropriate concatenates.

Among the very few previously constructed normal numbers not indicated above, perhaps most striking are those given by Stoneham (21, 22), who builds up transcendental non-Liouville normal numbers via controlled sums of expansions of reciprocals of powers of ergodic primes. Also notable in this development are some theorems concerning the distribution of residues within the periods of the summands. However, the considerable technologic effort required to achieve these specialized results underscores the need for broadly applicable methods to produce general classes of normal numbers.

(*iii*) In choosing normal sequences as specified by *Definition 6*, there is a tradeoff between limiting analytic excellence and appropriateness of application. To vividly clarify this, while Seq($F_{\text{IterLog-4}}$) produces asymptotically superb one-dimensional equidistribution, by *Theorem 11*, note that the first 6,000,000 digits of Seq($F_{\text{IterLog-4}}$) is a single fixed length-6 block concatenated 1,000,000 times, with a glaring and, for most applications, very much undesired periodicity. While the above technology refines the notion of normality, to our sensibilities, the present example highlights that the deficit from maximal equidistribution $\text{De}[\underline{u}^{(N)}] := \max_{m\leq \text{mcrit}(N)}(\text{def}_m[\underline{u}^{(N)}])$ is a preferred quantity to minimize, compared with def_0, in determining "limiting analytic excellence." For Seq($F_{\text{IterLog-4}}$), once N were sufficiently large so that $m_{\text{crit}}(N) \geq 5$, this sequence would be flagged as suboptimal, based on the lack of near-equidistribution of 6-blocks in long initial segments.

(*iv*) Symbolic dynamics (the study of maps on the space of infinite, typically binary sequences) has been extremely useful in advancing dynamical systems theory. It would seem natural, and highly worthwhile, to determine relationships between degrees of irregularity and classes of (binary sequence) maps and of dynamical systems. Such relationships may also provide a complementary perspective to and abet understanding of some "pathologies" within celestial mechanics—e.g., the existence of noncollision singularities in the Newtonian 5-body (and n-body) problem—i.e., Painlevé's conjecture (23). In particular, Xia's constructive proof of this (24), which critically utilizes symbolic dynamics, bears at least a thematic resemblance to the above counterexample, in which differing subsequences exhibit qualitatively dramatically different behavior, at times showing wild oscillations from equilibrium (equidistribution), at other times settling down to realize arbitrarily close approximation to a collision.

1. Borel, E. (1909) *Rendiconti del circolo matematico di Palermo* **27,** 247–271.
2. Franklin, J. N. (1963) *Math. Comput.* **17,** 28–59.
3. Knuth, D. E. (1981) *Seminumerical Algorithms: The Art of Computer Programming* (Addison–Wesley, Reading, MA), 2nd Ed., Vol. 2, Chap. 3.
4. Hardy, G. H. & Wright, E. M. (1983) *An Introduction to the Theory of Numbers* (Clarendon, Oxford), 5th Ed., pp. 125–128.
5. Champernowne, D. G. (1933) *J. London Math. Soc.* **8,** 254–260.
6. Copeland, A. H. & Erdös, P. (1946) *Bull. Amer. Math. Soc.* **52,** 857–860.
7. Pincus, S. & Singer, B. H. (1996) *Proc. Natl. Acad. Sci. USA* **93,** 2083–2088.
8. Pincus, S. M. (1991) *Proc. Natl. Acad. Sci. USA* **88,** 2297–2301.
9. Pincus, S. & Kalman, R. E. (1997) *Proc. Natl. Acad. Sci. USA* **94,** 3513–3518.
10. Ornstein, D. S. & Weiss, B. (1990) *Ann. Probab.* **18,** 905–930.
11. Beker, H. & Piper, F. (1982) *Cipher Systems, The Protection of Communications* (Wiley, New York), pp. 169–198.
12. Golomb, S. W. (1967) *Shift Register Sequences* (Holden-Day, San Francisco).
13. Peterson, W. & Weldon, E. (1972) *Error-Correcting Codes* (MIT Press, Cambridge, MA), 2nd Ed.
14. Fredricksen, H. (1982) *SIAM Rev.* **24,** 195–221.
15. Good, I. J. (1946)*J. London Math. Soc.* **21,** 167–169.
16. deBruijn, N. G. (1946) *Nederl. Akad. Wetensch. Proc.* **49,** 758–764.
17. Besicovitch, A. S. (1934) *Math. Z.* **39,** 146–156.
18. Hanson, H. A. (1954) *Can. J. Math.* **6,** 477–485.
19. Kolmogorov, A. N. (1933) *Grundbegriffe der Wahrscheinlichkeitsrechnung* (Springer, Berlin).
20. Kolmogorov, A. N. & Uspenskii, V. A. (1987) *Theory Probab. Its Appl. Eng. Trans.* **32,** 389–412.
21. Stoneham, R. G. (1973) *Acta Arith.* **22,** 371–389.
22. Stoneham, R. G. (1976) *Acta Arith.* **28,** 349–361.
23. Painlevé, P. (1897) *Leçons sur la Théorie Analytique des Équations Differentielles* (Hermann, Paris).
24. Xia, Z. (1992) *Ann. Math.* **135,** 411–468.