Random Generators and Normal Numbers

David H. Bailey[1] and Richard E. Crandall[2]
20 March 2003

Abstract

Pursuant to the authors' previous chaotic-dynamical model for random digits of fundamental constants [5], we investigate a complementary, statistical picture in which pseudorandom number generators (PRNGs) are central. Some rigorous results are achieved: We establish b-normality for constants of the form $\sum_i 1/(b^{m_i}c^{n_i})$ for certain sequences $(m_i), (n_i)$ of integers. This work unifies and extends previously known classes of explicit normals. We prove that for coprime $b, c > 1$ the constant $\alpha_{b,c} = \sum_{n=c,c^2,c^3,\ldots} 1/(nb^n)$ is b-normal, thus generalizing the Stoneham class of normals [49]. Our approach also reproves b-normality for the Korobov class [34] $\beta_{b,c,d}$, for which the summation index n above runs instead over powers $c^d, c^{d^2}, c^{d^3}, \ldots$ with $d > 1$. Eventually we describe an uncountable class of explicit normals that succumb to the PRNG approach. Numbers of the α, β classes share with fundamental constants such as π, $\log 2$ the property that isolated digits can be directly calculated, but for these new classes such computation tends to be surprisingly rapid. For example, we find that the googol-th (i.e. 10^{100}-th) binary bit of $\alpha_{2,3}$ is 0. We also present a collection of other results—such as digit-density results and irrationality proofs based on PRNG ideas—for various special numbers.

AMS 2000 subject classification numbers: 11K16, 11K06, 11J81, 11K45
Keywords: normal numbers, transcendental numbers, pseudo-random number generators

[1]Lawrence Berkeley National Laboratory, Berkeley, CA 94720, USA, dhbailey@lbl.gov. Bailey's work is supported by the Director, Office of Computational and Technology Research, Division of Mathematical, Information, and Computational Sciences of the U.S. Department of Energy, under contract number DE-AC03-76SF00098.

[2]Center for Advanced Computation, Reed College, Portland, OR 97202 USA, crandall@reed.edu.

1. Introduction

We call a real number b-normal if, qualitatively speaking, its base-b digits are "truly random." For example, in the decimal expansion of a number that is 10-normal, the digit 7 must appear 1/10 of the time, the string 783 must appear 1/1000 of the time, and so on. It is remarkable that in spite of the elegance of the classical notion of normality, and the sobering fact that almost all real numbers are absolutely normal (meaning b-normal for *every* $b = 2, 3, \ldots$), proofs of normality for fundamental constants such as $\log 2,\ \pi,\ \zeta(3)$ and $\sqrt{2}$ remain elusive. In [5] we proposed a general "Hypothesis A" that connects normality theory with a certain aspect of chaotic dynamics. In a subsequent work, J. Lagarias [37] provided some additional interesting viewpoints and analyses using the dynamical approach.

There is a fascinating historical thread in normality theory, from "artificial" or "unnatural" normals to "natural" normals. By the adjective "artificial" or "unnatural", we mean that a number's construction is relatively nonalgebraic and nonanalytic, in contrast to a "natural" normal number, which is given by some reasonably analytic formulation, such as a conveniently defined series. Such talk is of course qualitative and heuristic; yet, in the last few decades we have seen numbers, provably normal to some base, and via elegant series descriptions looking more like fundamental constants.

Since the 1930s we have known of artificial constructions, such as the 10-normal, binary Champernowne constant [16]:

$$C_{10} \;=\; 0.(1)(2)(3)(4)(5)(6)(7)(8)(9)(10)(11)(12)\cdots,$$

(or the 2-normal $C_2 = 0.(1)(10)(11)(100)(101)(110)(111)\cdots_2$), with the $(\cdot)$ notation meaning the expansion is constructed via mere *concatenation* of registers.

The migration toward more natural constructions was intensified by the work of Korobov and Stoneham from the 1950s into the 1990s, with Levin [38] and others working even more recently on statistical properties of normals. Those investigations were rooted in the recurring-decimal constructions of Good [26] (see, e.g., the interesting historical discussions in [52]). Let us now highlight what we shall call Korobov and Stoneham classes of normals, referring further details to the works of those authors [53] [48] [50] [51] [52] [33] [34] [35]. Although Korobov achieved normal number construction in the 1950s by parlaying Good's ideas [52], and Stoneham gave some explicit—yet rather recondite—series construction of normals in 1970 [48], an elegant and easily described representative class of "natural" normals was exhibited in 1973 by Stoneham [49]. We shall denote these Stoneham numbers by $\{\alpha_{b,c}\}$, with $b, c > 1$ coprime:

$$\alpha_{b,c} \;=\; \sum_{n=c^k>1} \frac{1}{b^n n} \;=\; \sum_{k=1}^{\infty} \frac{1}{b^{c^k} c^k}.$$

Stoneham proved that $\alpha_{b,c}$ is b-normal whenever c is an odd prime and b is a primitive root of c^2. We shall in the present paper generalize this class of normals by removing Stoneham's restrictions, demanding only coprime $b, c > 1$. Another class of normals we

shall be able to cover with the present techniques is the Korobov class whose members we denote (for $b, c > 1$ again coprime and $d > 1$):

$$\beta_{b,c,d} = \sum_{n=c,c^d,c^{d^2},c^{d^3},\ldots} \frac{1}{nb^n},$$

Korobov showed in 1990, via a clever combinatorial argument, that $\beta_{b,c,d}$ is b-normal [34]. We shall reprove this result, and do so with a general method that encompasses also the Stoneham class and generalizations. It should be remarked that these pioneers were not merely concerned with the aforementioned thread from artificial to natural constructions. For example, Stoneham used the representations

$$\sqrt{2} = 2 \prod_{d \text{ odd}} \left(1 - \frac{1}{4d^2}\right),$$
$$\pi = 4 \prod_{d \text{ odd } >1} \left(1 - \frac{1}{d^2}\right),$$

to creatively demonstrate (for either constant) that for a *fixed* number of multiplicands, certain digit strings must appear in the resulting rational period [52]. Unfortunately this does not on the face of it lead to rigorous results about the exact constants π and $\sqrt{2}$. (It is also puzzling, in that, whereas π falls squarely under the rubric of the present authors' Hypothesis A [5], the constant $\sqrt{2}$ does not, and one can only wonder whether the two constants should ultimately be treated in the same fashion as regards normality.) As for Korobov, his work actually included explicit continued fractions for the $\beta_{b,c,d}$ and related normals. For example,

$$\beta_{2,3,2} = \sum_{i \geq 0} \frac{1}{3^{2^i} 2^{3^{2^i}}} = \frac{1}{23 + \frac{1}{1 + \frac{1}{7 + \cdots}}},$$

with the precise algorithm for the fraction's ensuing elements given in the reference [34] (and note that the fraction elements soon grow extremely rapidly, the 11-th element being $2^{6399} - 1$).

In the present paper the way we generalize and extend such normality classes is to adopt a complementary viewpoint to Hypothesis A, focusing upon pseudorandom number generators (PRNGs), with relevant analyses of these PRNGs carried out via exponential-sum and other number-theoretical techniques. One example of success along this pathway is the establishment of large (indeed, uncountable) classes of "natural" normal numbers. Looking longingly at the fundamental constants

$$\log \frac{b}{b-1} = \sum_{n>0} \frac{1}{b^n n}$$

whose normality—for any $b \geq 2$ and to any base, b or not—remains to this day unresolved, we use PRNG concepts to prove b-normality for sums involving sparse filtering of the logarithms' summation indices. Of specific interest to us are sums

$$\alpha_{b,c,m,n} = \sum_{i \geq 1} \frac{1}{b^{m_i} c^{n_i}}$$

for certain integer pairs b, c and sequences $m = (m_i), n = (n_i)$ that enjoy certain growth properties. Note that our definition of Stoneham numbers $\alpha_{b,c}$ is the case $n_i = i,\ m_i = c^{n_i}$, while the Korobov numbers $\beta_{b,c,d}$ arise from sequence definitions $n_i = d^i,\ m_i = c^{n_i}$.

It is tantalizing that Stoneham and Korobov numbers both involve restrictions on the summation indices in the aforementioned logarithmic expansion, in the sense that numbers of either class enjoy the general form $\sum_{n \in S} 1/(nb^n)$ for some subset $S \subset Z^+$. Our generalizations include the sums

$$\sum_{n=c^{f(1)},c^{f(2)},\ldots} \frac{1}{nb^n},$$

for suitable integer-valued functions f; so again we have a restriction of a logarithmic sum to a sparse set of indices.

In addition to the normality theorems applicable to the restricted sums mentioned above, we present a collection of additional results on irrationality and b-density (see ensuing definitions), these side results having arisen during our research into the PRNG connection.

2. Nomenclature and fundamentals

We first give some necessary nomenclature relevant to base-b expansions. For a real number $\alpha \in [0, 1)$ we shall assume uniqueness of base-b digits, b an integer ≥ 2; i.e. $\alpha = 0.b_1b_2 \cdots$ with each $b_j \in [0, b-1]$, with a certain termination rule to avoid infinite tails of digit values $b-1$. One way to state the rule is simply to define $b_j = \lfloor b^j \alpha \rfloor$; another way is to convert a trailing tail of consecutive digits of value $b-1$, as in $0.4999 \cdots \rightarrow 0.5000 \cdots$ for base $b = 10$. Next, denote by $\{\alpha\}$, or $\alpha \bmod 1$, the fractional part of α, and denote by $||\alpha||$ the closer of the absolute distances of $\alpha \bmod 1$ to the interval endpoints $0, 1$; i.e. $||\alpha|| = \min(\{\alpha\}, 1-\{\alpha\})$. Denote by (α_n) the ordered sequence of elements $\alpha_0, \alpha_1, \ldots$. Of interest will be sequences (α_n) such that $(\{\alpha_n\})$ is equidistributed in $[0, 1)$, meaning that any subinterval $[u, v) \subseteq [0, 1)$ is visited by $\{\alpha_n\}$ for a (properly defined) limiting fraction $(v - u)$ of the n indices; i.e., the members of the sequence fall in a "fair" manner. We sometimes consider a weaker condition that $(\{a_n\})$ be merely dense in $[0, 1)$, noting that equidistributed implies dense.

Armed with the above nomenclature, we paraphrase from [5] and references [36] [28] [44] [33] in the form of a collective definition:

Definition 2.1 (Collection) The following pertain to real numbers α and sequences of real numbers $(\alpha_n \in [0, 1) : n = 0, 1, 2, \ldots)$. For any base $b = 2, 3, 4 \ldots$ we assume, as enunciated above, a unique base-b expansion of whatever real number is in question.

1. α is said to be b-dense iff in the base-b expansion of α every possible finite string of consecutive digits appears.

2. α is said to be b-normal iff in the base-b expansion of α every string of k base-b digits appears with (well-defined) limiting frequency $1/b^k$. A number that is b-normal for every $b = 2, 3, 4, \ldots$ is said to be absolutely normal. (This definition of normality differs from, but is provably equivalent to, other historical definitions [28] [44].)

3. The discrepancy of (α_n), essentially a measure of unevenness of the distribution in $[0,1)$ of the first N sequence elements, is defined (when the sequence has at least N elements) as

$$D_N \;=\; \sup_{0\le a<b<1}\left|\frac{\#(n<N:\alpha_n\in[a,b))}{N}-(b-a)\right|.$$

   One may also speak of a number α's b-discrepancy, as the discrepancy of the sequence $(b^n\alpha)$, which sequence being relevant to the study of b-normality.

4. The gap-maximum of (α_n), the largest gap "around the mod-1 circle" of the first N sequence elements, is defined (when the sequence has at least N elements) as

$$G_N = \max_{k=0,\ldots,N-1} ||\beta_{(k+1) \bmod N} - \beta_{k \bmod N}||,$$

   where (β_n) is a sorted (either in decreasing or increasing order) version of the first N elements of $(\alpha_n \bmod 1)$.

On the basis of such definition we next give a collection of known results in regard to b-dense and b-normal numbers:

Theorem 2.2 (Collection) In the following we consider real numbers and sequences as in Definition 2.1. For any base $b = 2, 3, 4\ldots$ we assume, as enunciated above, a unique base-b expansion of whatever number in question.

1. If α is b-normal then α is b-dense.

   Proof. If every finite string appears with well-defined, fair frequency, then it appears perforce.

2. If, for some b, α is b-dense then α is irrational.

   Proof. The base-b expansion of any rational is ultimately periodic, which means some finite digit strings never appear.

3. Almost all real numbers in $[0,1)$ are absolutely normal (the set of non-absolutely-normal numbers is null).

   Proof. See [36], p. 71, Corollary 8.2, [28].

4. α is b-dense iff the sequence $(\{b^n\alpha\})$ is dense.

   Proof. See [5].

5. α is b-normal iff the sequence $(\{b^n\alpha\})$ is equidistributed.

   Proof. See [36], p. 70, Theorem 8.1.

6. Let $m \neq k$. Then α is b^k-normal iff α is b^m-normal.

   Proof. See [36], p. 72, Theorem 8.2.

7. Let q, r be rational, $q \neq 0$. If α is b-normal then so is $q\alpha + r$, while if $c = b^q$ is an integer then α is also c-normal.

   Proof. The b-normality of $q\alpha$ is a consequence of the Birkoff ergodic theorem — see [3]; see also [36], p. 77, Exercise 8.9. For the additive $(+r)$ part, see end of the present section. For the c-normality see [36], p. 77, Exercise 8.5.

8. (Weyl criterion) A sequence $(\{\alpha_n\})$ is equidistributed iff for every integer $h \neq 0$

$$\sum_{n=0}^{N-1} e^{2\pi i h \alpha_n} \quad = \quad o(N).$$

   Proof. See [36], p. 7, Theorem 2.1.

9. (Erdős–Turan discrepancy bound) There exists an absolute constant C such that for any positive integer m the discrepancy of any sequence $(\{\alpha_n\})$ satisfies (again, it is assumed that the sequence has at least N elements):

$$D_N \quad < \quad C\left(\frac{1}{m} + \sum_{h=1}^{m} \frac{1}{h}\left|\frac{1}{N}\sum_{n=0}^{N-1} e^{2\pi i h \alpha_n}\right|\right).$$

   Proof. See [36], pp. 112-113, where an even stronger Theorem 2.5 is given.

10. Assume (x_n) is equidistributed (dense). If $y_n \to c$, where c is constant, then $(\{x_n + y_n\})$ is likewise equidistributed (dense). Also, for any nonzero integer d, $(\{dx_n\})$ is equidistributed (dense).

    Proof. For normality (density) of $(\{x_n + y_n\})$ see [5] [36], Exercise 2.11 (one may start with the observation that $(x_n + y_n) = (x_n + c) + (y_n - c)$ and $(\{x_n + c\})$ is equidistributed iff (x_n) is). The equidistribution of $(\{dx_n\})$ follows immediately from parts 5,8 above. As for density of $(\{dx_n\})$, one has $\{dx_n\} = \{d\{x_n\}\}$ for any integer d, and the density property is invariant under any dilation of the mod-1 circle, by any real number of magnitude ≥ 1.

11. Given a number α, define the sequence $(\alpha_n) = (\{b^n\alpha\})$. Then α is b-dense iff $\lim_{N\to\infty} G_N = 0$.

    Proof. The only-if is immediate. Assume, then, the vanishing limit, in which case for any $\epsilon > 0$ and any point in $[0, 1)$ some sequence member can be found to lie within $\epsilon/2$ of said point, hence we have density.

12. Consider α and the corresponding sequence (α_n) of the previous item. Then α is b-normal iff $\lim_{N\to\infty} D_N = 0$.

    Proof. See [36], p. 89, Theorem 1.1.

Some of the results in the above collection are simple, some are difficult; the aforementioned references reveal the difficulty spectrum. This collective Theorem 2.2 is a starting point for many interdisciplinary directions. Of special interest in the present treatment is the interplay between normality and equidistribution.

We focus first on the celebrated Weyl result, Theorem 2.2(8). Observe the little-o notation, essentially saying that the relevant complex vectors will on average exhibit significant cancellation. An immediate textbook application of the Weyl theorem is to show that for any irrational α, the sequence $(\{n\alpha\})$ is equidistributed. Such elementary forays are of little help in normality studies, because we need to contemplate not multiples $n\alpha$ but the rapidly diverging constructs $b^n\alpha$.

We shall be able to put the Weyl theorem to some use in the present treatment. For the moment, it is instructive to look at one nontrivial implication of Theorem 2.2(8). We selected the following example application of the Weyl sum to foreshadow several important elements of our eventual analyses. With Theorem 2.2(5,6,8) we can prove part of Theorem 2.2(7), namely: If α is b-normal and r is rational then $\alpha + r$ is b-normal. Let $r = p/q$ in lowest terms. The sequence of integers $(b^m \bmod q)$ is eventually periodic, say with period T. Thus for some fixed integer c and any integer n we have $b^{nT} \bmod q = c$. Next we develop an exponential sum, assuming nonzero h:

$$S \;=\; \sum_{n=0}^{N-1} e^{2\pi i h b^{nT}(\alpha+p/q)} \;=\; e^{2\pi i h c p/q} \sum_{n=0}^{N-1} e^{2\pi i h b^{nT}\alpha}.$$

Now a chain of logic finishes the argument: α is b-normal so it is also b^T-normal by Theorem 2.2(6). But this implies $S = e^{2\pi i h c p/q} o(N) = o(N)$ so that $\alpha + p/q$ is b^T-normal, and so by Theorem 2.2(6) is thus b-normal.

3. Pseudorandom number generators (PRNGs)

We consider PRNGs under the iteration

$$x_n \;=\; (b x_{n-1} + r_n) \mod 1,$$

which is a familiar congruential form, except that the perturbation sequence r_n is not yet specified (in a conventional linear-congruential PRNG this perturbation is constant). Much of the present work is motivated by the following hypothesis from [5].

Hypothesis A (Bailey–Crandall) If the perturbation $r_n = p(n)/q(n)$, a non-singular rational-polynomial function with $\deg q > \deg p \geq 0$, then (x_n) is either equidistributed or has a finite attractor.

It is unknown whether this hypothesis be true, however a motivation is this: The normality of many fundamental constants *believed* to be normal would follow from Hypothesis A. Let

us now posit an *unconditional* theorem that leads to both conditional and unconditional normality results:

Theorem 3.1 (Unconditional) Associate a real number

$$\beta \;=\; \sum_{n=1}^{\infty} \frac{r_n}{b^n}$$

where $\lim_{n\to\infty} r_n = c$, a constant, with a PRNG sequence (x_n) starting $x_0 = 0$ and iterating

$$x_n \;=\; (bx_{n-1} + r_n) \mod 1.$$

Then (x_n) is equidistributed (dense) iff β is b-normal (b-dense).

Proof. Write

$$\begin{aligned} b^d\beta - x_d &= \sum_{n=1}^{\infty} b^{d-n} r_n - (b^{d-1}r_1 + b^{d-2}r_2 + \cdots + r_d) \\ &= \frac{r_{d+1}}{b} + \frac{r_{d+2}}{b^2} + \cdots \;\to\; c', \end{aligned}$$

with c' a constant. Therefore by Theorem 2.2(10), (x_n) equidistributed (dense) implies β is b-normal (b-dense). Now assume b-normality (b-density). Then (x_d) is the sequence $(\{b^d\beta\})$ plus a sequence that approaches constant, and again by Theorem 2.2(10) (x_d) is equidistributed (dense).

In our previous work [5] this kind of theorem led to the following (conditional) result:

Theorem 3.2 (Conditional) On Hypothesis A, each of the constants

$$\pi,\;\; \log 2,\;\; \zeta(3)$$

is 2-normal. Also, on Hypothesis A, if $\zeta(5)$ be irrational then it likewise is 2-normal.

Theorem 3.2 works, of course, because the indicated fundamental constants admit of polylogarithm-like expansions of the form $\sum r_n b^{-n}$ where r_n is rational-polynomial. The canonical example is

$$\log 2 \;=\; \sum_{n=1}^{\infty} \frac{1}{n2^n}$$

and 2-normality of $\log 2$ comes down to the question of whether (for $x_0 = 0$)

$$x_n \;=\; \left(2x_{n-1} + \frac{1}{n}\right) \mod 1$$

gives rise to an equidistributed (x_n). The main results of the present paper will be to establish equidistribution for generators reminiscent of, but not quite the same as, this one for $\log 2$.

With a view to ultimate achievement of normality results, let us take a brief tour of some other (not rational-polynomial) perturbation functions. The iteration

$$x_n \;=\; \left(2x_{n-1} + \frac{n}{2^{n^2-n}}\right) \bmod 1$$

is associated with the constant

$$\beta \;=\; \sum_{n\geq 1} \frac{n}{2^{n^2}},$$

which is 2-dense but *not* 2-normal, as we establish later. Another rather peculiar perturbation, for base $b = 4$, is

$$r_n \;=\; \frac{1}{(2n)!}\frac{4n+1}{4n+2}.$$

If the associated PRNG is equidistributed, then $1/\sqrt{e}$ is 2-normal. Likewise, and again for base $b = 4$, a result of equidistribution for a perturbation

$$r_n \;=\; \frac{(2n-3)!!}{n!} \;=\; \frac{(2n-3)(2n-5)\cdots 3\cdot 1}{n(n-1)(n-2)\cdots 2\cdot 1}$$

would prove that $\sqrt{2}$ is 4-normal, hence 2-normal. It might have seemed on the face of it that the decay rate of the perturbation r_n has something to do with normality. But the conditional results on Hypothesis A involve only polynomial-decay perturbations, while the r_n assignments immediately above involve rapid, factorial decay. On the other hand there are very slowly-decaying perturbation functions for which one still embraces the likelihood of normality. For example, the mysterious Euler constant γ can be associated with the base $b = 2$ and perturbation function r_n that decays like $n^{-1/2}$ (see Section 5 and [5]).

In a spirit of statistical investigation let us revisit once again the canonical case of the number $\beta = \log 2$ and base $b = 2$. For the purpose of discussion we write out for $d = 1, 2, 3, \ldots$ an iterate as assembled from d explicit terms:

$$x_d \;=\; \left(\frac{2^{d-1} \bmod 1}{1} + \frac{2^{d-2} \bmod 2}{2} + \frac{2^{d-3} \bmod 3}{3} + \ldots + \frac{2}{d-1} + \frac{1}{d}\right) \bmod 1.$$

and remind ourselves that

$$2^d \log 2 \;=\; x_d + t_d,$$

where t_d is a "tail" term that vanishes in the limit, but is also a kind of source for subsequent generator iterates. (Note that the first term always vanishes modulo 1; we include that term for clarity.) One can think of such a PRNG as a "cascaded" random number generator, in which distinct generators $(2^{d-m} \bmod m)/m$ are added together, with the number of moduli m steadily diverging.

There are difficult aspects of the PRNG analysis for $\log 2$. First, the theory of cascaded PRNGs appears difficult; even the class of generators with *fixed* numbers of summands are

not completely understood. Second, even if we succeeded in some form of equidistribution theorem for cascaded generators, we still have the problem that the tail t_d is to be added into the final segment of the generator that has just been started with its power-of-two numerators.

These difficulties may be insurmountable. Nonetheless, there are two separate approaches to altering the $\log 2$ PRNG such that density and normality results accrue. These separate modifications are:

- Arrange for some kind of synchronization, in which iterates change number-theoretic character on the basis of a "kicking" pertubation that emerges only at certain iterates.
- Arrange somehow for the tail t_d to be so very small that meaningful statistical properties of the first $d + d'$ generator terms are realized before t_d is significantly magnified via d' multiplies by b.

We shall be able to apply both of these qualitative alterations. For the first case (kicking/synchronization) we shall finally achieve normality proofs. For the second kind of alteration (small tail) we shall be able to effect some proofs on density and irrationality.

4. PRNGs admitting of normality proofs

Herein we exhibit a class of generators—we shall call them (b, c, m, n)-PRNGs, for which normality proofs can be achieved due to the special synchronization such generators enjoy. We begin with some necessary nomenclature (we are indebted to C. Pomerance for his expertise, ideas and helpful communications on nontrivial arithmetic modulo prime powers).

Definition 4.1 We define a (b, c, m, n)-PRNG sequence $x = (x_0, x_1, x_2, \ldots)$ for coprime integers $b, c > 1$ and strictly increasing sequences $m = (0, m_1, m_2, \ldots), n = (0, n_1, n_2, \ldots)$ as follows: Set $x_0 = 0$ and for $k > 0$ iterate:

$$x_k \;=\; (bx_{k-1} + r_k) \mod 1,$$

with the perturbation given by

$$r_{m_i} \;=\; \frac{1}{c^{n_i}}$$

with all other r_k vanishing.

Knowing the parameters (b, c, m, n) determines the PRNG sequence x. The perturbation is of the "kicking" variety, not happening unless the index j on r_j is one of the exponents m_i. So the PRNG runs like so (we denote simply by $\equiv$ an equality on the

mod-1 circle):

$$\begin{aligned}
x_0 &\equiv 0,\\
&\cdots,\\
x_{m_1} &\equiv b^{m_1}\cdot 0 + r_{m_1} \equiv \frac{1}{c^{n_1}},\\
x_{m_1+1} &\equiv \frac{b}{c^{n_1}},\\
&\cdots,\\
x_{m_2-1} &\equiv \frac{b^{m_2-m_1-1}}{c^{n_1}},\\
x_{m_2} &\equiv \frac{b^{m_2-m_1}}{c^{n_1}} + r_{m_2} \equiv \frac{b^{m_2-m_1}c^{n_2-n_1}+1}{c^{n_2}},\\
&\cdots,
\end{aligned}$$

and generally speaking,

$$x_{m_k} \equiv \frac{a_k}{c^{n_k}}.$$

where a_k is always coprime to c. It is evident that upon the $1/c^{n_k}$ perturbation, the x_k commence an orbit of length $\mu_{k+1} = m_{k+1} - m_k$ before the next perturbation. Therefore the first N terms of the sequence x can be envisioned like so. Observe $m_0 = 0$ and write $N = \mu_1 + \cdots + \mu_K + J$ where $J \in [1, \mu_{K+1}]$ is the (possibly partial) length of the last orbit. Then the first N terms of the (b, c, m, n)-PRNG sequence start with $\mu_1 = m_1$ zeros and appear:

$$\begin{aligned}
(x_n)|_{k=0}^{N-1} \equiv (&0, 0, \ldots, 0,\\
&\frac{a_1}{c^{n_1}}, \frac{ba_1}{c^{n_1}}, \frac{b^2a_1}{c^{n_1}}, \ldots, \frac{b^{\mu_2-1}a_1}{c^{n_1}},\\
&\cdots,\\
&\frac{a_k}{c^{n_k}}, \frac{ba_k}{c^{n_k}}, \frac{b^2a_k}{c^{n_k}}, \ldots, \frac{b^{\mu_{k+1}-1}a_k}{c^{n_k}},\\
&\cdots,\\
&\frac{a_K}{c^{n_K}}, \frac{ba_K}{c^{n_K}}, \frac{b^2a_K}{c^{n_K}}, \ldots, \frac{b^{J-1}a_K}{c^{n_K}}).
\end{aligned}$$

We intend to argue, for certain parameter sets (b, c, m, n), that $x = (x_k)$ is equidistributed. For this we shall require some resulus from the number theory of power moduli, and an important lemma on exponential sums. But first we give a general lemma useful for estimating the discrepancy of an ordered union of finite subsequences. We use notation reminiscent of that above for our (b, c, m, n)-PRNG sequences:

Lemma 4.2 For an infinite sequence (y_n) built as an ordered union

$$((y_0, \ldots, y_{N_1-1}), (y_{N_1}, \ldots, y_{N_1+N_2-1}), \cdots))$$

of subsequences of respective lengths N_i, we have, for $K > 0$, $N = N_1 + N_2 + \cdots + N_K + J$ with $J \in [1, N_{K+1}]$, a discrepancy bound

$$D_N \leq \sum_{i=1}^{K} \frac{N_i}{N} D_{N_i} + \frac{J}{N} D_J,$$

where D_{N_i} are the respective discrepancies of the finite subsequences and D_J is the discrepancy of the partial sequence $(y_{N_1+\cdots+N_K+j} : j = 0, 1, 2, \ldots, J-1)$.

Proof. This is proved simply, in [36], p. 115, Theorem 2.6.

Now we can focus upon number-theoretical ideas, in order to bound subsequence discrepancies. We shall make use of the following lemma which gives relations for the order of numbers modulo a given modulus c. We denote the multiplicative order of y modulo c by $\mathrm{ord}(y, c)$ in what follows.

Lemma 4.3 Let $b, c > 1$ be coprime with c having prime decomposition $c = p_1^{t_1} \cdots p_s^{t_s}$. Let $\tau_1(c) = \mathrm{ord}(b, p_1 \cdots p_s)$ and define β_i by:

$$p_i^{\beta_i} \parallel b^{(\mu+1)\tau_1} - 1$$

where $\mu = 1$ if c is even and τ_1 is odd and $b \equiv 3 (\mathrm{mod} 4)$; otherwise $\mu = 0$. Define further

$$c_1(c) = \prod_{k=1}^{s} p_k^{\min(t_k, \beta_k)}.$$

Then

$$\mathrm{ord}(b, c) = \frac{c}{c_1} \tau',$$

where $\tau' = 2\tau_1$ if $\mu = 1$ and $c \equiv 0 (\mathrm{mod} 4)$; otherwise $\tau' = \tau_1$.

Proof. This lemma is proved in [35] and references therein.

These above order relations lead easily to a key lemma for our present treatment:

Lemma 4.4 Let $b, c > 1$ be coprime. Then there exist constants A_1, A_2 such that for sufficiently large n both of these conditions hold:

$$\begin{aligned} \mathrm{ord}(b, c^n) &= A_1 c^n, \\ \frac{\mathrm{ord}(b, c^n)}{c_1(c^n)} &= A_2 c^n \end{aligned}$$

Proof. The simple replacement $c \to c^n$ in Lemma 4.3 leaves the values of the β_i and τ_1 invariant. Thus for sufficiently large n, we have $c_1(c^n) = \prod p_i^{\beta_i}$ which is fixed, and both large-n results follow.

Next we state a lemma on exponential sums:

Lemma 4.5 (Korobov, Niederreiter) For $b, c > 1$ coprime, with $c_1(c)$ defined as in Lemma 4.3, and an integer h such that $d = \gcd(h, c) < c/c_1$, and an integer $J \in [1, \mathrm{ord}(b, c)]$ we have

$$\left| \sum_{j=0}^{J-1} e^{2\pi i h b^j / c} \right| \quad < \quad \sqrt{\frac{c}{d}} \left(1 + \log \frac{c}{d} \right).$$

Proof. The lemma is a direct corollary of results found in [33], e.g. p. 167, Lemma 32 for odd c, but (earlier) results of Korobov [35] are sufficiently general to cover all composite c. See also [41], pp. 1004-1008. A highly readable proof of a similar result and an elementary description of Niederreiter's seminal work on the topic can be found in [32], pp. 107-110. There are also enhancements on the theory of fractional parts for the exponential function, as in [38] and references therein.

Lemma 4.5 speaks to the distribution of powers of b modulo general c coprime to b. For our purposes we want to bound the magnitudes of exponential sums when the modulus is a pure power, say c^n. (Incidentally we shall not be needing the dependence of the lemma's bound on d.) To this end we establish a theorem. Note that in this theorem and thereafter, when we say constants exist we mean always positive constants depending only on b, c, therefore independent of any running indices or growing powers. The idea of the following theorem is not only to make the transition $c \to c^n$ for the exponential sum, but also to unrestrict J:

Theorem 4.6 For $b, c > 1$ coprime, there exist constants A, B, D such that for any positive integer J and sufficiently large n, the condition $\gcd(H, c^n) < Dc^n$ implies

$$\left| \sum_{j=0}^{J-1} e^{2\pi i H b^j / c^n} \right| \quad < \quad B \left(A c^{n/2} + J c^{-n/2} \right) \log c^n.$$

Proof. Substituting $c \to c^n$ in Lemma 4.5, and using Lemma 4.4, we establish that for sufficiently large n, the indicated exponential sum of the theorem, for any H as indicated, is less in magnitude than a bound $E c^{n/2} \log c^{n/2}$, where E is constant, as long as J does not exceed $\mathrm{ord}(b, c^n)$. But for larger J we have at most $\lceil J/\mathrm{ord}(b, c^n) \rceil$ copies of the exponential sum, and this ceiling is bounded by $1 + J/(A_1 c^n)$, so the result follows.

We are aware that one could start from Theorem 4.6 and apply the Weyl criterion (Theorem 2.2 (8)) to establish equidistribution for certain (b, c, m, n)-PRNG sequences. We shall prove a little more, by virtue of discrepancy formulae. Again consider the first N terms of the sequence $x = (x_n)$, where $N = N_0 + \mu_{k_1} + \cdots + \mu_K + J$, where $J \in [1, \mu_{K+1}]$ as before, but k_1 is chosen so that the powers c^n for any $n > n_{k_1 - 1}$ are sufficiently large,

as in Lemma 4.4 and Theorem 4.6, and so N_0 is constant. Then the discrepancy of the first J' elements of an orbit, namely of the subsequence

$$\left(\frac{a_k}{c^{n_k}}, \frac{ba_k}{c^{n_k}}, \frac{b^2a_k}{c^{n_k}}, \ldots, \frac{b^{J'-1}a_k}{c^{n_k}}\right)$$

for $k \geq k_1$ is bounded according to the Erdős–Turan Theorem 2.2(9) like so:

$$D_{\mu_{k+1}} \;<\; C_1\left(\frac{1}{M} + \sum_{h=1}^{M}\frac{1}{h}\left|\frac{1}{J'}\sum_{j=0}^{J'-1} e^{2\pi i h a_k b^j/c^{n_k}}\right|\right),$$

where we are at liberty to chose $M = \lfloor Dc^{n_k/2}\rfloor$ with the constant D from Theorem 4.6, so that the exponential sum appearing in the discrepancy bound is covered by said theorem—recall a_k and c are coprime so that $\gcd(ha_k, c^{n_k}) = \gcd(h, c^{n_k}) \leq h \leq M < Dc^{n_k}$. We then get, for an orbit's discrepancy for J' terms of that orbit,

$$D_{J'} \;<\; B'\left(A'\frac{c^{n_k/2}}{J'} + c^{-n_k/2}\right)\log^2 c^{n_k},$$

where A', B' are constants, and we shall take $J' = \mu_{k+1}$ for each complete orbit and observe $J' = J$ in our last orbit (the orbit in which lies the last element x_{N-1}). Now using Lemma 4.2 we can obtain an overall discrepancy formula for the N sequence terms, N sufficiently large:

$$\begin{aligned} D_N \;<\; & \frac{N_0}{N} + \frac{B'}{N}\sum_{k=k_1}^{K}\left(A'c^{n_{k-1}/2} + \frac{\mu_k}{c^{n_{k-1}/2}}\right)\log^2 c^{n_{k-1}} \\ & + \frac{B'}{N}\left(A'c^{n_K/2} + \frac{J}{c^{n_K/2}}\right)\log^2 c^{n_K}. \end{aligned}$$

We can weaken this bound slightly, in favor of economy of notation, by observing that $N\mu_K$, $J < N$, and the powers c^{n_i} are monotonic in i, so that the following result is thereby established (note that we allow ourselves to rename constants with previously used names when such nomenclature is not ambiguous):

Lemma 4.7 For the (b, c, m, n)-PRNG sequence $x = (x_n)$, the discrepancy is bounded for sufficiently large N as

$$\begin{aligned} D_N(x) \;<\; & \left(N_0 + Ac^{n_{K-1}/2} + B\sum_{k=1}^{K}\frac{\mu_k}{c^{n_{k-1}/2}}\right)\frac{\log^2 c^{n_{K-1}}}{\mu_K} \\ & + \left(A\frac{c^{n_K/2}}{\mu_K} + B\frac{1}{c^{n_K/2}}\right)\log^2 c^{n_K}, \end{aligned}$$

where $\mu_k = m_k - m_{k-1}$ and N is decomposed as $N = \mu_1 + \cdots + \mu_K + J$ with $J \in [1, \mu_{K+1}]$, with N_0, A, B constant.

It is now feasible to posit growth conditions on the m, n sequences of our PRNGs such that discrepancy vanishes as $N \to \infty$. One possible result is

Theorem 4.8 For the (b, c, m, n)-PRNG sequence $x = (x_k)$ of Definition 4.1, assume that the difference sequences $\mu_k = m_k - m_{k-1},\ \nu_k = n_k - n_{k-1}$ satisfy the following growth conditions:

(i) (ν_k) is nondecreasing,

(ii) There exists a constant $\gamma > 1/2$ such that for sufficiently large k

$$\frac{\mu_k}{c^{\gamma n_k}} \ \geq \ \frac{\mu_{k-1}}{c^{\gamma n_{k-1}}}.$$

Then x is equidistributed and the number

$$\alpha_{b,c,m,n} \ = \ \sum_{k=1}^{\infty} \frac{1}{b^{m_k} c^{n_k}}$$

is b-normal.

Proof. We bound contributions to the discrepancy bound of Lemma 4.7, using growth condition (ii) as follows:

$$\frac{1}{\mu_K} \sum_{k=1}^{K} \frac{\mu_k}{c^{n_{k-1}/2}} \ \leq \ \frac{1}{c^{n_{K-1}/2}} \sum_{L=0}^{K-1} \frac{c^{\gamma n_{K-L}}}{c^{\gamma n_K}} \frac{c^{n_{K-1}/2}}{c^{n_{K-L-1}/2}}.$$

Now

$$\gamma(n_K - n_{K-L}) + \frac{1}{2}(n_K - n_{K-1} - (n_{K-L} - n_{K-L-1})) \ \geq \ \left(\gamma - \frac{1}{2}\right) L,$$

this last inequality arising from growth condition (i) and the fact that the n_k are monotone increasing with $n_1 \geq 1$. Thus

$$\frac{1}{\mu_K} \sum_{k=1}^{K} \frac{\mu_k}{c^{n_{k-1}/2}} \ \leq \ \frac{1}{c^{n_{K-1}/2}} \left(\frac{1}{1 - c^{1/2-\gamma}}\right).$$

Actually this component is the only problematic part of the discrepancy bound in Lemma 4.7, and we quickly write, now with more conveniently labeled constants C_i, and for sufficiently large N,

$$D_N(x) \ < \ C_1 \frac{1}{c^{n_K \gamma}} + C_2 \frac{\log^2 c^{n_{K-1}}}{c^{n_{K-1}(\gamma - 1/2)}} + C_3 \frac{\log^2 c^{n_{K-1}}}{c^{n_{K-1}/2}} + C_4 \frac{\log^2 c^{n_K}}{c^{n_K(\gamma-1/2)}} + C_5 \frac{\log^2 c^{n_K}}{c^{n_K/2}}.$$

Being as $(\log^2 z)/z^\epsilon$ is, for any $\epsilon > 0$, eventually monotone decreasing as $z \to \infty$, it follows that for sufficiently large N

$$D_N(x) \ < \ C \frac{\log^2 c^{n_{K-1}}}{c^{n_{K-1} \min(\gamma - 1/2, 1/2)}}.$$

But this means $D_N \to 0$ as $N \to \infty$, so x is equidistributed by Theorem 2.2(12). Theorem 3.1 then establishes the number $\alpha_{b,c,m,n}$ as b-normal.

As we have said, equidistribution of sequences x as in Theorem 4.8 would also follow from simpler arguments involving the Weyl criterion. However, the discrepancy bound at the end of the above proof is interesting in its own right. For certain choices of the m, n sequences, such as $m_i = c^i, n_i = i$, we can easily relate the index N to the c^{n_K-1} to obtain a discrepancy bound

$$D_N(x) \ < \ C\frac{\log^2 N}{\sqrt{N}}.$$

Now such bounds (logarithmic numerator and square-root denominator) on classical PRNGs have been obtained in brilliant fashion by Niederreiter (see [41], p. 1009, and [42], pp. 169-170), who also gives arguments as to the best-possible nature of such bounds in the classical PRNG contexts. It is thus no surprise that our exponent factor $\min(\gamma - 1/2, 1/2)$ at the end of the above proof cannot exceed $1/2$ (however, we see later in this section that other constructions of normals involved number-discrepancies of somewhat lower magnitude).

The discrepancy approach, in yielding Theorem 4.8, leads us to specific classes of normals:

Corollary 4.9 In what follows we assume an underlying (b, c, m, n)-PRNG and so $b, c > 1$ are coprime.

(i) The generalized Stoneham numbers

$$\alpha_{b,c} \ = \ \sum_{i\geq 1} \frac{1}{c^i b^{c^i}}$$

are each b-normal.

(ii) The generalized Korobov numbers ($d > 1$):

$$\beta_{b,c,d} \ = \ \sum_{i\geq 1} \frac{1}{c^{d^i} b^{c^{d^i}}}$$

are each b-normal.

(iii) For positive integers $s < 2r$, each of the numbers

$$\sum_{i\geq 1} \frac{1}{c^{ir} b^{c^{is}}}$$

is b-normal. So for example,

$$\sum_{i\geq 1} \frac{1}{8^i 3^{32^i}}$$

is 3-normal.

(iv) If integer $d > \sqrt{c}$ then each of

$$\sum_{i\geq 1} \frac{1}{c^i b^{d^i}}$$

is b-normal. So for example,

$$\sum_{i\geq 1} \frac{1}{3^i 2^{2^i}}$$

is 2-normal.

(v) If the integer-valued function $f(i)$ is strictly increasing,
and $f(i) - f(i-1)$ is nondecreasing for sufficiently large n, then

$$\sum_{i\geq 1} \frac{1}{c^{f(i)} b^{c^{f(i)}}}$$

is b-normal. So for example,

$$\sum_{i\geq 1} \frac{1}{c^{i^2} b^{c^{i^2}}}$$

and

$$\sum_{i\geq 1} \frac{1}{c^{i!} b^{c^{i!}}}$$

are both b-normal.

Proof. Each of the results (i)-(v) follows easily from Theorem 4.8. For example, in case (iv) we have $d > \sqrt{c}$ so define δ by $d = c^{\delta+1/2}$ so that for a constant C_1

$$\frac{\mu_K}{c^{\gamma n_K}} \quad = \quad \frac{C_1 c^{(\delta+1/2)K}}{c^{\gamma K}} \tag{1}$$

which, for γ chosen between $1/2$ and $1/2 + \delta$, is monotone increasing. The rest of the results follow in similar fashion.

It is natural to ask whether a number $\alpha_{b,c,m,n}$ associated with a (b, c, m, n)-PRNGs is transcendental, which question we answer at least for some such numbers:

Theorem 4.11 Denote $\alpha_{b,c,m,n} = \sum_{i\geq 1} 1/(c^{n_i} b^{m_i})$ where (b, c, m, n) are as in Definition 4.1 but without the restriction of coprimality. Let $\lambda = \log b / \log c$ and assume that for some fixed $\delta > 2$ and sufficiently large K

$$\frac{n_{K+1} + \lambda m_{K+1}}{n_K + \lambda m_K} \quad > \quad \delta.$$

Then $\alpha_{b,c,m,n}$ is transcendental.

Remark. Some of the $\alpha_{b,c,m,n}$ appearing here are not in the class of b-normal constants relevant to Theorem 4.8, because of the coprimality requirement for our defined PRNGs. Conversely, some of the b-normals in question are not covered by Theorem 4.11; for example, the assignments $b = 3, c = 2, n_k = k, m_k = 2^k$ yield a b-normal but the inequality above involving δ fails (yet, the b-normal may well be transcendental; we are saying the following application of the Roth theorem is not sufficient).

Proof. For simplicity denote $\alpha = \alpha_{b,c,m,n}$. The celebrated Roth theorem states [47] [15] that if $|P/Q - \alpha| < 1/Q^{2+\epsilon}$ admits of infinitely many distinct rational solutions P/Q (i.e. if α is approximable to degree $2 + \epsilon$ for some $\epsilon > 0$), then α is transcendental. Write

$$\alpha \;=\; P/Q + \sum_{i>k} \frac{1}{c^{n_i} b^{m_i}},$$

where $\gcd(P, Q) = 1$ with $Q = c^{n_k} b^{m_k}$. The sum over i gives

$$|\alpha - P/Q| \;<\; \frac{2}{c^{n_{k+1}} b^{m_{k+1}}}.$$

But the right-hand side is, by virtue of the δ-inequality, less than $2/Q^{\delta}$ and transcendency follows.

Theorem 4.11 immediately repeats transcendency results on Stoneham and Korobov numbers, such results having been known to both of those authors, except for the former class when $c = 2$, as explained in the above Remark.

For a different research foray, consider the problem of specifying an uncountable collection of normals. One way to do this is surprisingly easy. In what follows we define the bits of a real number according to the no-trailer rule: Any infinite trailer of 1's is to be removed via carry; e.g., $0.01111\ldots \to 0.1$ in binary; and then when we ask for the k-th bit of a real number in $[0, 1)$ we shall mean the k-bit to the right of the decimal point.

Theorem 4.12 Let $b, c > 1$ be coprime and for each real $t \in [0, 1)$ denote by t_k the k-th binary bit of t. Then the collection of numbers

$$\alpha(t) \;=\; \sum_{i\geq 0} \frac{1}{c^i b^{c^i + t_i}},$$

is uncountable, and each is b-normal.

Remark. We are creating here what could be called "perturbed Stoneham numbers," yet we could just as easily perturb in this way other kines of normals.

Proof. That $\alpha(t)$ is always b-normal follows from Theorem 4.8—take $\gamma = 2/3$, say, so that the perturbation of adding t_i to m_i does not harm the required growth condition (ii) of that Theorem. It remains to show that the $\alpha(t)$ are all pairwise distinct. Indeed, let $s > t$, with the first occurrence of unequal corresponding bits between s and t being

$s_k = 1, t_k = 0$. Then

$$\begin{aligned}\alpha(t) - \alpha(s) &= \frac{1}{c^K}\frac{1}{b^{c^K}}\left(1 - \frac{1}{b}\right) + \sum_{i>k}\frac{1}{c^i}\left(\frac{1}{c^{c^i+t_i}} - \frac{1}{b^{c^i+s_i}}\right) \\ &> \frac{1}{c^K}\frac{1}{b^{c^K}}\left(1 - \frac{1}{b}\right)\left(1 - \sum_{i>k}\frac{1}{c^{i-k}}\frac{1}{b^{c^i-c^k}}\right) \\ &> 0.\end{aligned}$$

Inasmuch as this construction is fairly straightforward, one wonders whether there be other simple approaches. As a possible example, for the Champernowne C_{10} let (u_k) be the ordered set of *positions* of 0's, and likewise let (v_k) be the set of positions of 1's. Clearly, by 10-normality of C_{10}, these two sets are infinite. Now, based on some real number t as was used in Theorem 4.12, either swap (when $t_k = 1$) or do not swap the (0,1) digit pair from respective positions (u_k, v_k) depending on the k-th bit of t. So for $t = 0 = 0.000\ldots$, the Champernowne is left unchanged; while for any other real $t < 1$, the Champernowne is altered and may be 10-normal. We have not finished this argument; we mention it only to note that there may be other means of constructing an uncountable class of normal numbers.

Next we move to a computational issue: Can one efficiently obtain isolated digits of $\alpha_{b,c,m,n}$? It turns out that at least the Stoneham number $\alpha_{b,c}$ admits of an individual digit-calculation algorithm, as was established for π, $\log 2$ and some others in the original Bailey–Borwein–Plouffe (BBP) paper [4] — the same approach works for the new, b-normal and transcendental constants. Indeed, for $\alpha_{b,c}$ the BBP algorithm is extraordinarily rapid: the overall bit-complexity to resolve the n-th base-b digit of $\alpha_{b,c}$ is

$$O(\log^2 n \log\log n \log\log\log n),$$

which can conveniently be thought of as $O(n^\epsilon)$. By comparison, the complexity for the BBP scheme applied to fundamental constants such as π and $\log 2$ (in general, the constants falling under the umbrella of Hypothesis A) is $O(n^{1+\epsilon})$. As a specific example, in only 2.8 seconds run time on a modern workstation the authors were able to calculate binary bits of $\alpha_{2,3}$, beginning at position one googol (i.e. 10^{100}). The googol-th binary digit is 0; the first ten hexadecimal digits starting at this position are `2205896E7B`. In contrast, C. Percival's recent resolution of the quadrillionth (10^{15}-th) binary bit of π is claimed to be the deepest computation in history for a 1-bit result [45], finding said bit to be 0 but at the cost of over 10^{18} CPU clocks.

At this point one might look longingly at the b-normality of $\alpha_{b,p}$ and wonder how difficult it is to relax the constraint on summation indices in $\sum_{n\in S} 1/(nb^n)$ in order finally to resolve logarithmic sums. Some relaxations of the set $S \subset Z^+$ may be easier than others. We conjecture that

$$\alpha = \sum \frac{1}{p2^p},$$

where p runs through the set of Artin primes (of which 2 is a primitive root), is 2-normal. It is a celebrated fact that under the extended Riemann hypothesis (ERH) the Artin-prime set is infinite, and in fact—this may be important—has positive density amongst the primes. We make this conjecture not so much because of statistical evidence, but because we hope the fact of 2 being a primitive root for every index p might streamline any analysis. Moreover, any connection whatever between the ERH and the present theory is automatically interesting.

With these results in hand, let us sketch some alternative approaches to normality. We have mentioned in our introduction some of the directions taken by Good, Korobov, Stoneham et al. over the decades. Also of interest is the form appearing in [33, Theorem 30, p. 162], where it is proven that

$$\alpha \quad = \quad \sum_{n\geq 1} \frac{\lfloor b\{f(n)\}\rfloor}{b^n}$$

is b-normal for any "completely uniformly distributed" function f, meaning that for every integer $s \geq 1$ the vectors $(f(n), f(n+1), \ldots f(n+s))$ are, as $n = 1, 2, 3, \ldots$, equidistributed in the unit s-cube. (Korobov also cites a converse, that *any* b-normal number has such an expansion with function f.) Moreover, Korobov gives explicit functions such as

$$f(x) \quad = \quad \sum_{k=0}^{\infty} e^{-k^5} x^k,$$

for which the number α above is therefore b-normal. It is possible to think of some normals as being "more normal" than others, in the sense of discrepancy measures. We have seen that the normals of our Theorem 4.8 enjoy discrepancy no better than $D_N(x) = O\left(\log^2 N/\sqrt{N}\right)$, while on the other hand we know [38] that for almost all real x,

$$D_N\left(\{(b^n x)\}\right) = O\left(\left(\frac{\log\log N}{N}\right)^{1/2}\right).$$

Yet, researchers have done better than this. Levin gives [38] constructions of normals based on certain well-behaved sequences—such as quasi-Monte Carlo, low-discrepancy sequences or Pascal matrices—and derives discrepancy bounds as good as

$$D_N\left(\{(b^n \alpha)\}\right) = O\left(\frac{\log^k N}{N}\right)$$

for $k = 2, 3$.

For another research direction, there is another exponential-sum result of Korobov [33][Theorem 33, p. 171] that addresses the distribution of the powers $(b, b^2, b^3, \ldots b^m)$ modulo a prime power p^i, but where m is significantly less than $\sqrt{\text{ord}(b, p^i)}$. It may be possible to use such a result to establish normality of numbers such as $\sum 1/(p^i b^{m_i})$ where the m_i have different growth conditions than we have so far posited via Theorem 4.8.

One also looks longingly at some modern treatments of nonstandard exponential sums, such as the series of papers [23][24][25], wherein results are obtained for power generators, which generators having become of vogue in cryptography. The manner in which Friedlander et al. treat exponential sums—for their purposes the summands being such as $\exp(2\pi i g^{g^j}/c)$—is of interest not because of any direct connection to normality, but because of the bounding techniques used.

5. PRNGs leading to density and irrationality proofs

Independent of number theory and special primes, one could ask what is the statistical behavior of truly random points chosen modulo 1; for example, what are the expected gaps that work against uniform point density?

In view of Definition 2.1(4) and Theorem 2.2(11), it behooves us to ponder the expected gap-maximum for *random* points: If N random (with uniform distribution) points are placed in $[0,1)$, then the probability that the gap-maximum G_N exceeds x is known to be [30]

$$\text{Prob}(G_N \geq x) \;=\; \sum_{j=1}^{\lfloor 1/x \rfloor} \binom{N}{j} (-1)^{j+1} (1-jx)^{N-1}.$$

The expectation E of the gap-maximum can be obtained by direct integration of this distribution formula, to yield:

$$E(G_N) \;=\; \frac{1}{N}(\psi(N+1)+\gamma)$$

where ψ is the standard polygamma function Γ'/Γ. Thus for large N we have

$$\begin{aligned} E(G_N) &= \frac{\log N + \gamma - 1/2}{N} + O(\frac{1}{N^2}) \\ &\sim \frac{\log N}{N}. \end{aligned}$$

This shows that whereas the mean gap is $1/N$, the mean *maximum* gap is essentially $(\log N)/N$. In this sense, which remains heuristic with an uncertain implication for our problem, we expect a high-order cascaded PRNG to have gaps no larger than "about" $(\log P)/P$ where P is the overall period of the PRNG.

It turns out that for very specialized PRNGs we can effect rigorous results on the gap-maximum G_N. One such result is as follows:

Theorem 5.1. Let $1 = e_1 < e_2 < e_3 < \ldots < e_k$ be a set of pairwise coprime integers. Consider the PRNG with any starting seed $(s_1, \ldots, s_k)$:

$$x_d \;=\; \left(2^d \left(\frac{2^{s_1}}{2^{e_1}-1} + \frac{2^{s_2}}{2^{e_2}-1} \cdots \frac{2^{s_k}}{2^{e_k}-1}\right)\right) \bmod 1.$$

Then the generated sequence (x_d) has period $e_1 e_2 \cdots e_k$ and for sufficiently large N we have

$$G_N \;<\; 3/2^{\lfloor k/2 \rfloor}.$$

Proof. Each numerator 2^{d+s_i} clearly has period e_i modulo the respective denominator $2^{e_i} - 1$, so the period is the given product. The given bound on gaps can be established by noting first that the behavior of the PRNG defined by

$$y_{(f_i)} \;=\; \frac{2^{f_1}-1}{2^{e_1}-1} + \frac{2^{f_2}-1}{2^{e_2}-1} + \cdots + \frac{2^{f_k}-1}{2^{e_k}-1},$$

as each f_i runs over its respective period interval $[0, e_i - 1]$, is very similar to the original generator. In fact, the only difference is that this latter form has constant offset $\sum 1/(2^{e_i} - 1)$ so that the maximum gap around the mod 1 circle is unchanged. Now consider a point $z \in [0, 1)$ and attempt construction of a set (f_i) such that $y_{(f_i)} \approx z$, as follows. Write a binary expansion of z in the (non-standard) form:

$$z \;=\; \sum_{n=1} \frac{1}{2^{b_n}},$$

i.e., the b_n denote the positions of the 1 bits of z. Now set $f_i = e_i - b_i$ for i from k down to $k - K + 1$ inclusive. Using the following inequality chain for any real $0 < a < b > 1$:

$$\frac{a}{b} - \frac{1}{b} \;<\; \frac{a-1}{b-1} \;<\; \frac{a}{b},$$

it follows that we can find a PRNG value such that

$$||y_{(f_i)} - z|| \;<\; \left| -\frac{2}{2^{e_{k-K+1}}} + \sum_{j=1}^{K} \frac{1}{2^{b_k}} \right|.$$

Attention to the fact that the e_i are strictly increasing leads directly to the upper bound $3/2^{\lfloor k/2 \rfloor}$ on the maximum gap for the y, and hence the x generator.

Of course the maximum-gap theorem just exhibited is weaker than the statistical expectation of the maximum gap, roughly $(\log E)/E$ where $E = e_1 \cdots e_k$, but at least we finally have a rigorously vanishing gap and therefore, as we shall see, some digit-density, hence irrationality results.

Though the previous section reveals difficulties with the PRNG approach, there are ways to apply these basic ideas to obtain irrationality proofs for certain numbers of the form

$$x \;=\; \sum_{i} \frac{1}{m_i 2^{n_i}}.$$

for integers m_i and n_i. A first result is based on our rigorous PRNG gap bound, from Theorem 5.1, as:

Theorem 5.2. Let $1 = e_1 < e_2 < \ldots$ be a strictly increasing set of integers that are pairwise coprime. Let (d_i) be a sequence of integers with the growth property:

$$d_{k+1} \;>\; \prod_{i=1}^{k} d_i + \prod_{i=1}^{k} e_i.$$

Then the number:

$$\begin{aligned} x &= \sum_{m=1}^{\infty} \frac{1}{2^{d_m}(2^{e_m}-1)} \\ &= \frac{1}{2^{d_1}(2^{e_1}-1)} + \frac{1}{2^{d_2}(2^{e_2}-1)} + \dots \end{aligned}$$

is 2-dense and hence irrational.

Proof: Fix a k, define $D = \prod d_i,\ E = \prod e_i$, and for $0 \le g < E$ consider the fractional part of a certain multiple of x:

$$\{2^{g+D}x\} = \sum_{i=1}^{k} \frac{2^{f_i}-1}{2^{e_i}-1} + \sum_{i=1}^{k} \frac{1}{2^{e_k}-1} + T,$$

where $f_i = 2^{g+D-d_i}$ and error term $|T| < 1/2^{e_k}$. By the Chinese remainder theorem, we can find, in the stated range for g, a g such that the PRNG values of Theorem 5.1 are attained. Thus the maximum gap between successive values of the sequence $\{2^n x\}$ vanishes as $k \to \infty$, so the sequence is dense by Theorem 2.2(11) and desired results follow.

Of course there should be an alternative—even easy—means to establish such an irrationality result. In fact, there are precedents arising from disparate lines of analysis. Consider what we call the Erdős–Borwein number: The sum of the reciprocals of all Mersenne numbers, namely:

$$E = \sum_{n=1}^{\infty} \frac{1}{2^n - 1}.$$

This still-mysterious number is known to be irrational, as shown by Erdős [22] with a clever number-theoretical argument. More recently, P. Borwein [9] established the irrationality of more general numbers $\sum 1/(q^n - r)$ when $r \neq 0$, using Pade approximant techniques. Erdős also once showed that the sum of terms $1/(b_n 2^{2^n})$ is *always* irrational for any positive integer sequence (b_n). Such binary series with reciprocal terms have indeed been studied for decades.

The Erdős approach for the E number can be sketched as follows. It is an attractive combinatorial exercise to show that

$$E = \sum_{a=1}^{\infty}\sum_{b=1}^{\infty} \frac{1}{2^{ab}} = \sum_{n=1}^{\infty} \frac{d(n)}{2^n},$$

where $d(n)$ is the number of divisors of n (including 1 and n). To paraphrase the Erdős method for our present context, consider a relevant fractional part:

$$\{2^m E\} = \left(\frac{d(m+1)}{2} + \frac{d(m+2)}{2^2} + \frac{d(m+3)}{2^3} + \dots \right) \bmod 1$$

What Erdős showed is that one can choose any prescribed number of succesive integers $k+1, k+2, \ldots k+K$ such that their respective divisor counts $d(k+1), d(k+2), \ldots, d(k+K)$ are respectively divisible by increasing powers $2, 2^2, 2^3, \ldots, 2^K$; and furthermore this can be done such that the subsequent terms beyond the K-th of the above series for $\{2^k E\}$ are not too large. In this way Erdős established that the binary expansion of E has arbitrarily long strings of zeros. This proves irrationality (one also argues that infinitely many 1's appear, but this is not hard). We still do not know, however, whether E is 2-dense. The primary difficulty is that the Erdős approach, which hinges on the idea that if n be divisible by j distinct primes, each to the first power, then $d(n)$ is divisible by 2^j, does not obviously generalize to the finding of arbitrary d values modulo arbitrary powers of 2. Still, this historical foreshadowing is tantalizing and there may well be a way to establish that the E number is 2-dense.

As a computational matter, it is of interest that one can also combine the terms of E to obtain an accelerated series:

$$E \;=\; \sum_{m=1}^{\infty} \frac{1}{2^{m^2}} \frac{2^m+1}{2^m-1}.$$

Furthermore, the E number finds its way into complex analysis and the theory of the Riemann zeta function. For example, by applying the identity $\zeta^2(s) = \sum_{n\geq 1} d(n)/n^s$, one can derive

$$E \;=\; \frac{\gamma - \log\log 2}{\log 2} + \frac{1}{2\pi} \int_R \frac{\Gamma(s)\zeta^2(s)}{(\log 2)^s} dt,$$

where R is the Riemann critical line $s = 1/2 + it$. In this sophisticated integral formula we note the surprise appearance of the celebrated Euler constant γ. Such machinations lead one to wonder whether γ has a place of distinction within the present context. A possibly relevant series is [6]

$$\gamma \;=\; \sum_{k=1}^{\infty} \frac{1}{2^{k+1}} \sum_{j=0}^{k-1} \binom{2^{k-j}+j}{j}^{-1}.$$

If any one of our models is to apply, it would have to take into account the fairly slow convergence of the j sum for large k. (After $k = 1$ the j-sum evidently approaches 1 from above.) Still, the explicit presence of binary powers and *rational* multipliers of said powers suggests various lines of analysis. In particular, it is not unthinkable that the j-sum above corresponds to some special dynamical map, in this way bringing the Euler constant into a more general dynamical model.

It is of interest that a certain PRNG conjecture addresses directly the character of the expansion of the Erdős-Borwein number.

Conjecture 5.3 The sequence given by the PRNG definition

$$x_d \;=\; \left(\sum_{k=1}^{d} \frac{2^d - 1}{2^k - 1} \right) \bmod 1 \;=\; \left(\sum_{k=1}^{d} \frac{2^{d \bmod k} - 1}{2^k - 1} \right) \bmod 1$$

is equidistributed.

Remark. One could also conjecture that the sequence in Conjecture 5.3 is merely dense, which would lead to 2-density of E.

This conjecture leads immediately, along the lines of our previous theorems pertaining to specially-constructed PRNGs, to:

Theorem 5.4. The Erdős-Borwein number E is 2-normal iff Conjecture 5.3 holds.

Proof. For the PRNG of Conjecture 5.3, we have

$$x_d \;=\; (2^d-1)\left(E-\sum_{j>d}\frac{1}{2^j-1}\right) \bmod 1,$$

so that

$$\{x_d\} \;=\; \{\{2^dE\}+\{-E-1+t_d\}\},$$

where $t_d \to 0$. Thus $\{2^dE\}$ is equidistributed iff (x_n) is, by Theorem 2.2(10).

We believe that at least a weaker, density conjecture should be assailable via the kind of technique exhibited in Theorem 5.1, whereby one proceeds constructively, establishing density by forcing the indicated generator to approximate any given value in $[0,1)$.

P. Borwein has forwarded to us an interesting observation on a possible relation between the number E and the "prime-tuples" postulates, or the more general Hypothesis H of Schinzel and Sierpinski. The idea is — and we shall be highly heuristic here — the fractional part $d(m+1)/2+d(m+2)/2^2+\cdots$ might be quite tractable if, for example, we have

$$\begin{aligned} m+1 &= p_1,\\ m+2 &= 2p_2,\\ &\cdots\ ,\\ m+n &= np_n, \end{aligned}$$

at least up to some $n=N$, where the $p_i > N$ are all primes that appear in an appropriate "constellation" that we generally expect to live *very* far out on the integer line. Note that in the range of these n terms we have $d(m+j)=2d(j)$. Now if the tail sum beyond $d(m+N)/2^N$ is somehow sufficiently small, we would have a good approximation

$$\{2^mE\} \;\approx\; d(1)+d(2)/2+\cdots \;=\; 2E.$$

But this implies in turn that some iterate $\{2^mE\}$ revisits the neighborhood of an earlier iterate, namely $\{2E\}$. It is not clear where such an argument—especially given the heuristic aspect—should lead, but it may be possible to prove 2-density (i.e. all possible finite bitstrings appear in E) on the basis of the prime k-tuples postulate. That connection

would of course be highly interesting. Along such lines, we do note that a result essentially of the form: "The sequence $(\{2^m E\})$ contains a near-miss (in some appropriate sense) with any given element of $(\{nE\})$" would lead to 2-density of E, because, of course, we know E is irrational and thus $(\{nE\})$ is equidistributed.

6. Special numbers having "nonrandom" digits

This section is a tour of side results in regard to some special numbers. We shall exhibit numbers that are b-dense but not b-normal, uncountable collections of numbers that are neither b-dense nor b-normal, and so on. One reason to provide such a tour is to dispel any belief that, because almost all numbers are absolutely normal, it should be hard to use algebra (as opposed to artificial construction) to "point to" nonnormal numbers. In fact it is not hard to do so.

First, though, let us revisit some of the artificially constructed normal numbers, with a view to reasons why they are normal. We have mentioned the binary Champernowne, which can also be written

$$C_2 \;=\; \sum_{n=1}^{\infty} \frac{n}{2^{F(n)}}$$

where the indicated exponent is:

$$F(n) \;=\; n + \sum_{k=1}^{n} \lfloor \log_2 k \rfloor .$$

Note that the growth of the exponent $F(n)$ is slightly more than linear. It turns out that if such an exponent grows too fast, then normality can be ruined. More generally, there is the class of Erdős–Copeland numbers [17], formed by (we remind ourselves that the $(\cdot)$ notation means digits are concatenated, and here we concatenate the base-b representations)

$$\alpha \;=\; 0.(a_1)_b(a_2)_b\cdots$$

where (a_n) is *any* increasing integer sequence with $a_n = O(n^{1+\epsilon})$, any $\epsilon > 0$. An example of the class is

$$0.(2)(3)(5)(7)(11)(13)(17)\cdots_{10},$$

where primes are simply concatenated. These numbers are known to be b-normal, and they all can be written in the form $\sum G(n)/b^{F(n)}$ for appropriate numerator function G and, again, slowly diverging exponent F. We add in passing that the generalized Mahler numbers (for any $g, b > 1$)

$$M_b(g) \;=\; 0.(g^0)_b(g^1)_b(g^2)_b\cdots$$

are known at least to be irrational [43], [55], and it would be of interest to establish perturbation sums in regard to such numbers. Incidentally, it is ironic that some of the

methods for establishing irrationality of the $M_b(g)$ are used by us, below, to establish *nonnormality* of certain forms.

We have promised to establish that

$$\alpha \;=\; \sum_{n\geq 1} n/2^{n^2}$$

is 2-dense but not 2-normal. Indeed, in the n^2-th binary position we have the value n, and since for sufficiently large n we have $n^2-(n-1)^2 > 1+\log_2 n$, the numerator n at bit position n^2 will not interfere (in the sense of carry) with any other numerator. One may bury a given finite binary string in some sufficiently large integer n (we say buried because a string 0000101, for example, would appear in such as $n = 10000101$), whence said string appears in the expansion. Note that the divergence of the exponent n^2 is a key to this argument that α is 2-dense. As for the lack of 2-normality, it is likewise evident that almost all bits are 0's.

Let us hereby consider faster growing exponents, to establish a more general result, yielding a class of b-dense numbers none of which are b-normal. We start with a simple but quite useful lemma.

Lemma 6.1 For polynomials P with nonnegative integer coefficients, $\deg P > 0$, and for any integer $b > 1$, the sequence

$$(\{\log_b P(n)\} : n = 1, 2, 3, \ldots)$$

is dense in $[0, 1)$.

Proof. For $d = \deg P$, let $P(x) = a_d x^d + \ldots + a_0$. Then $\log_b P(n) = \log_b a_d + d(\log n)/\log b + O(1/n)$. Since $\log n = 1 + 1/2 + 1/3 + \ldots + 1/n - \gamma + O(1/n^2)$ diverges with n but by vanishing increments, the sequence $(\{d(\log n)/\log b\})$ and therefore the desired $(\{\log_b P(n)\})$ are both dense by Theorem 2.2(10).

Now we consider numbers constructed via superposition of terms $P(n)/b^{Q(n)}$, with a growth condition on P, Q:

Theorem 6.2 For polynomials P, Q with nonnegative integer coefficients, $\deg Q > \deg P > 0$, the number

$$\alpha \;=\; \sum_{n\geq 1} \frac{P(n)}{b^{Q(n)}}$$

is b-dense but not b-normal.

Proof. The final statement about nonnormality is easy: Almost all of the base-b digits are 0's, because $\log_b P(n) = o(Q(n) - Q(n-1))$. For the density argument, we shall show that for any $r \in (0, 1)$ there exist integers $N_0 < N_1 < \ldots$ and $d_1, d_2, \ldots$ with $Q(N_{j-1}) < d_j < Q(N_j)$, such that

$$\lim_{j\to\infty} \{b^{d_j}\alpha\} \;=\; r.$$

This in turn implies that $(\{b^d\alpha\}) : d = 1, 2, \ldots\})$ is dense, hence α is b-dense. Now for any ascending chain of N_i with N_0 sufficiently large, we can assign integers d_j according to

$$Q(N_j) \;>\; d_j \;=\; Q(N_j) + \log_b r - \log_b P(N_j) + \theta_j \;>\; Q(N_{j-1})$$

where $\theta_j \in [0, 1)$. Then

$$P(N_j)/b^{Q(N_j)-d_j} \;=\; 2^{\theta_j} r.$$

However, $(\{\log_b P(n)\})$ is dense, so we can find an ascending N_j-chain such that $\lim \theta_j = 0$. Since $d_j < Q(N_j)$ we have

$$\{b^{d_j}\alpha\} \;=\; \left(b^{\theta_j} r + \sum_{k>0} P(N_j + k)/b^{Q(N_j+k)-d_j} \right) \mod 1$$

and because the sum vanishes as $j \to \infty$, it follows that α is b-dense.

Consider the interesting function [36], p. 10:

$$f(x) \;=\; \sum_{n=1}^{\infty} \frac{\lfloor nx \rfloor}{2^n}.$$

The function f is reminiscent of a degenerate case of a generalized polylogarithm form—that is why we encountered such a function during our past [5] and present work. Regardless of our current connections, the function and its variants have certainly been studied, especially in regard to continued fractions [19] [20] [36] [10] [39] [7] [1] [11], [12]. If one plots the f function over the interval $x \in [0, 1)$, one sees a brand of "devil's staircase," a curve with infinitely many discontinuities, with vertical-step sizes occurring in a fractal pattern. There are so many other interesting features of f that it is efficient to give another collective theorem. Proofs of the harder parts can be found in the aforementioned references.

Theorem 6.3 (Collection) For the "devil's staircase" function f defined above, with the argument $x \in (0, 1)$,

1. f is monotone increasing.
2. f is continuous at every irrational x, but discontinuous at every rational x.
3. For rational $x = p/q$, lowest terms, we have

$$f(x) \;=\; \frac{1}{2^q - 1} + \sum_{m=1}^{\infty} \frac{1}{2^{\lfloor m/x \rfloor}}$$

but when x is irrational we have the same formula without the $1/(2^q - 1)$ leading term (as if to say $q \to \infty$).

4. For irrational $x = [a_1, a_2, a_3, \ldots]$, a simple continued fraction with convergents (p_n/q_n), we have:

$$f(x) \;=\; [A_1, A_2, A_3, \ldots].$$

where the elements A_n are:

$$A_n \;=\; 2^{q_{n-2}} \frac{2^{a_n q_{n-1}} - 1}{2^{q_{n-1}} - 1}.$$

Moreover, if (P_n/Q_n) denote the convergents to $f(x)$, we have

$$Q_n \;=\; 2^{q_n} - 1.$$

5. $f(x)$ is irrational iff x is.
6. If x is irrational then $f(x)$ is transcendental.
7. $f(x)$ is never 2-dense and never 2-normal.
8. The range $\mathcal{R} = f([0,1))$ is a null set (measure zero).
9. The density of 1's in the binary expansion of $f(x)$ is x itself; accordingly, f^{-1}, the inverse function on the range $\mathcal{R}$, is just 1's density.

Some commentary about this fascinating function f is in order. We see now how f can be strictly increasing, yet manage to "completely miss" 2-dense (and hence 2-normal) values: Indeed, the discontinuities of f are dense. The notion that the range $\mathcal{R}$ be a null set is surprising, yet follows immediately from the fact that almost all x have 1's density equal to 1/2. The beautiful continued fraction result allows extremely rapid computation of f values. The fraction form is exemplified by the following evaluation, where x is the reciprocal of the golden mean and the Fibonacci numbers are denoted F_i:

$$\begin{aligned} f(1/\tau) &= f\left(\frac{2}{1+\sqrt{5}}\right) \\ &= [2^{F_0}, 2^{F_1}, 2^{F_2}, \ldots] \\ &= \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{2\,\cfrac{1}{4 + \cfrac{1}{8 + \ldots}}}}}, \end{aligned}$$

It is the superexponential growth of the convergents to a typical $f(x)$ that has enabled transcendency proofs as in Theorem 6.2(6).

An interesting question is whether (or when) a companion function

$$g(x) \;=\; \sum_{n=1}^{\infty} \frac{\{nx\}}{2^n}$$

can attain 2-normal values. Evidently

$$g(x) \;=\; 2x - f(x),$$

and, given the established nonrandom behavior of the bits of $f(x)$ for any x, one should be able to establish a correlation between normality of x and normality of $g(x)$. One reason why this question is interesting is that g is constructed from "random" real values $\{nx\}$ (we know these are equidistributed) placed at unique bit positions. Still, we did look numerically at a specific irrational argument, namely

$$x \;=\; \sum_{n\geq 1} \frac{1}{2^{n(n+1)/2}}$$

and noted that $g(x)$ almost certainly is *not* 2-normal. For instance, in the first 66,420 binary digits of $g(x)$, the string '010010' occurs 3034 times, while many other length-6 strings do not occur at all.

7. Conclusions and open problems

Finally, we give a sampling of open problems pertaining to this interdisciplinary effort:

- We have shown that for (b, c, m, n)-PRNG systems, each associated constant $\alpha_{b,p,m,n}$—under the conditions of Theorem 4.8—is b-normal. What about c-normality of such numbers for c not a rational power of b?

- The generalized Stoneham numbers (case (i) of Corollary 4.9) might be generalizable in the following way: Instead of coprimality of b, c, just specify that neither integer divides the other. Can a result on b-normality then be effected? Presumably one would need some generalization of the exponential-sum lemmas.

- We have obtained rigorous results for PRNGs that either have a certain synchronization, or have extremely small "tails." What techniques would strike at the intermediate scenario which, for better or worse, is typical for fundamental constants; e.g., the constants falling under the umbrella of Hypothesis A?

- What are the fundamental connections between normality theory and automated sequences (for an excellent survey of the latter, see [2])? We have talked—albeit heuristically—about unnatural vs. natural constructions. Perhaps there are elegant, undiscovered ways to create new normals via automatic rules.

- Does polynomial-time (in $\log n$) resolution of the n-th digit for our $\alpha_{b,c}$ and similar constants give rise to some kind of "trap-door" function, as is relevant in cryptographic applications? The idea here is that it is so very easy to find a given digit even though the digits are "random." (As in: Multiplication of n-digit numbers takes polynomial time, yet factoring into multiples is evidently very much harder.)

8. Acknowledgments

The authors are grateful to J. Borwein, P. Borwein, D. Bowman, D. Broadhurst, J. Buhler, D. Copeland, H. Ferguson, M. Jacobsen, J. Lagarias, R. Mayer, H. Niederreiter, S. Plouffe, A. Pollington, C. Pomerance, M. Robinson, S. Wagon, T. Wieting and S. Wolfram for theoretical and computational expertise throughout this project. We thank, in particular, J. Shallit whose acute scholarship alerted us to the deeper history of normal numbers, allowing clutch corrections to an earlier draft of our work. A referee was kind to provide key corrections as well. We would like to dedicate this work to the memory of Paul Erdős, whose ingenuity on a certain, exotic analysis dilemma—the character of the Erdős–Borwein constant E—has been a kind of guiding light for our research. When we coauthors began—and this will surprise no one who knows of Erdős—our goals were presumed unrelated to the Erdős world. But later, his way of thinking meant a great deal. Such is the persona of genius, that it can speak to us even across rigid boundaries.

References

[1] W. W. Adams and J. L. Davison, "A Remarkable Class of Continued Fractions," *Proceedings of the American Mathematical Society*, vol. 65 (1977), 194-198.

[2] J.-P. Allouche and J. Shallit, *Automatic Sequences Theory, Applications, Generalizations*, manuscript 2002.

[3] David H. Bailey and Daniel J. Rudolph, "An Ergodic Proof that Rational Times Normal is Normal," manuscript, 2002, available at the URL `http://www.nersc.gov/~dhbailey/dhbpapers/ratxnormal.pdf`.

[4] David H. Bailey, Peter B. Borwein and Simon Plouffe, "On The Rapid Computation of Various Polylogarithmic Constants," *Mathematics of Computation*, vol. 66, no. 218, 1997, pp. 903–913.

[5] David H. Bailey and Richard E. Crandall, "On the Random Character of Fundamental Constant Expansions," *Experimental Mathematics*, vol. 10 (2001), 175-190.

[6] M. Beeler, et al., item 120 in M. Beeler, R. W. Gosper, and R. Schroeppel, "HAKMEM," Cambridge, MA: MIT Artificial Intelligence Laboratory, Memo AIM-239, 55, Feb. 1972.

[7] P. E. Böhmer,"Über die Transzendenz Gewisser Dyadischer Brüche," *Mathematische Annalen*, no. 96 (1926), 367-377; Erratum: vol. 96 (1926), 735.

[8] J. Borwein, D. Bradley and R. Crandall, "Computational Strategies for the Riemann Zeta Function," *Journal of Computational and Applied Mathematics*, vol. 121 (2000), 247-296.

[9] Peter Borwein, "On the Irrationality of Certain Series," *Mathematical Proceedings of the Cambridge Philosophical Society*, vol. 112 (1992), 141-146.

[10] Jonathan Borwein and Peter Borwein, "On the Generating Function of the Integer Part of $\lfloor n\alpha + \gamma \rfloor$," *Journal of Number Theory*, vol. 43 (1993), 293-318.

[11] Douglas Bowman, "Approximation of $\lfloor n\alpha + s \rfloor$ and the zero of $\{n\alpha + s\}$," *Journal of Number Theory*, vol. 50 (1995), 128-144.

[12] Douglas Bowman, "A New Generalization of Davison's Theorem," *Fibonacci Quarterly*, vol. 26 (1988), 40-45.

[13] David J. Broadhurst, "Polylogarithmic Ladders, Hypergeometric Series and the Ten Millionth Digits of $\zeta(3)$ and $\zeta(5)$," preprint, March 1998, available from the URL `http://xxx.lanl.gov/abs/math/9803067`.

[14] David J. Broadhurst, "Conjecture on Integer-Base Polylogarithmic Zeros Motivated by the Cunningham Project", manuscript, March 2000.

[15] J. W. S. Cassels, *An Introduction to Diophantine Approximations*, Cambridge Univ. Press, Cambridge, 1957.

[16] D. G. Champernowne, "The Construction of Decimals Normal in the Scale of Ten," *Journal of the London Mathematical Society*, vol. 8 (1933), 254-260.

[17] A. H. Copeland and P. Erdős, "Note on Normal Numbers," *Bulletin American Mathematical Society*, vol. 52 (1946), 857-860.

[18] R. Crandall, *Topics in Advanced Scientific Computation*, Springer-Verlag, 1996.

[19] L. V. Danilov, "Some Classes of Transcendental Numbers," *Matematicheskie Zametki*, vol. 12 (1972), 149-154; In Russian, English translation in *Mathematical Notes of the Academy of Science of the USSR*, vol. 12 (1972), 524-527.

[20] J. L. Davison, "A Series and Its Associated Continued Fraction," *Proceedings of the American Mathematical Society*, vol. 63 (1977), 29-32.

[21] Robert L. Devaney, *Complex Dynamical Systems: The Mathematics Behind the Mandelbrot and Julia Sets*, American Mathematical Society, Providence, 1995.

[22] P. Erdős. "On Arithmetical Properties of Lambert Series," *Journal of the Indian Mathematical Society (N.S.)*, vol. 12 (1948), 63-66.

[23] J. Friedlander; C. Pomerance; I. Shparlinski, "Period of the Power Generator and Small Values of Carmichael's Function," *Mathematics of Computation*, vol. 70 (2001), 1591-1605.

[24] J. Friedlander and I. Shparlinski, "On the Distribution of the Power Generator", *Mathematics of Computation*, vol. 70 (2001), 1575-1589.

[25] J. Friedlander and I. Shparlinski, "Some Double Exponential Sums over $\mathbf{Z}_m$", manuscript (2002).

[26] I. Good, "Normal Recurring Decimals," *Journal of the London Mathematical Society*, vol. 21 (1946), 167-169.

[27] Helaman R. P. Ferguson, David H. Bailey and Stephen Arno, "Analysis of PSLQ, An Integer Relation Finding Algorithm," *Mathematics of Computation*, vol. 68 (1999), no. 225, 351-369.

[28] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, Oxford University Press, 1979.

[29] Norbert Hegyvari, "On Some Irrational Decimal Fractions." *American Mathematical Monthly*, vol. 100 (1993), 779-780.

[30] Mark Jacobsen, private communication (2000). Jacobsen in turn references Herbert Solomon, *Geometric Probabilities*, SIAM, Philadelphia, 1978.

[31] A. Khinchin, *Continued Fractions*, Phoenix Books, Univ. of Chicago Press, 1964.

[32] Donald E. Knuth, *The Art of Computer Programming*, vol. 2, second edition, Addison-Wesley, Menlo Park, 1981.

[33] N. Korobov, *Exponential Sums and their Applications*, Kluwer Academic Publishers, 1992.

[34] N. Korobov, "Continued Fractions of Certain Normal Numbers," *Mathematik Zametki*, vol. 47 (1990), 28-33; in Russian; English translation in *Mathematical Notes of the Academy of Science USSR*, vol. 47 (1990), 128-132.

[35] N. Korobov, "On the Distribution of Digits in Periodic Fractions," *Mathematicheskie USSR Sbornik*, vol. 18 (1972), 659-676.

[36] L. Kuipers and H. Niederreiter, *Uniform Distribution of Sequences*, Wiley-Interscience, New York, 1974.

[37] J. Lagarias, "On the Normality of Fundamental Constants," *Experimental Mathematics*, vol. 10 (2001), no. 3, 353-366.

[38] M. Levin, "On the discrepancy estimate of normal numbers," *Acta Arithmetica*, LXXXVIII 2 (1999), 99-111.

[39] R. Mayer, private communication (2000).

[40] A. McD. Mercer, "A Note on Some Irrational Decimal Fractions," *American Mathematical Monthly*, vol. 101 (1994), 567-568.

[41] H. Niederreiter, "Quasi-Monte Carlo Methods and Pseudo-Random Numbers," *Bulletin of the American Mathematical Society*, vol. 84 (1978), no. 6, 957-1041.

[42] H. Niederreiter, "Random Number Generation and Quasi-Monte Carlo Methods," *CBMS-NSF Regional Conference Series in Applied Mathematics*, SIAM, 1992.

[43] H. Niederreiter, "On an Irrationality Theorem of Mahler and Bundschuh," *Journal of Number Theory*, vol. 24 (1986), 197-199.

[44] I. Niven, *Irrational Numbers*, Carus Mathematical Monographs, no. 11, Wiley, New York, 1956.

[45] C. Percival, "PiHex: A Distributed Effort to Calculate Pi," `http://www.cecm.sfu.ca/projects/pihex/index.html`.

[46] P. Ribenboim, *The New Book of Prime Number Records*, Springer-Verlag, New York 1996.

[47] K. Roth, "Rational Approximations to Algebraic Numbers," *Mathematika*, vol. 2 (1955), 1-20. Corrigendum, 168.

[48] R. Stoneham, "A General Arithmetic Construction of Transcendental Non-Liouville Normal Numbers from Rational Fractions," *Acta Arithmetica*, vol. 16 (1970), 239-253.

[49] R. Stoneham, "On Absolute (j, ϵ)-Normality in the Rational Fractions with Applications to Normal Numbers," *Acta Arithmetica*, vol. 22 (1973), 277-286.

[50] R. Stoneham, "On the Uniform Epsilon-Distribution of Residues Within the Periods of Rational Fractions with Applications to Normal Numbers," *Acta Arithmetica*, vol. 22 (1973), 371-389.

[51] R. Stoneham, "Some Further Results Concerning the (j, ϵ) Normality in the Rationals," *Acta Arithmetica*, vol. 26 (1974), 83-96.

[52] R. Stoneham, "Normal Recurring Decimals, Normal Periodic Systems, (j, ϵ)-Normality, and Normal Numbers," *Acta Arithmetica*, vol. 28 (1976), 349-361.

[53] R. Stoneham, "On a Sequence of (j, ϵ)-Normal Approximations to $\pi/4$ and the Brouwer Conjecture," *Acta Arithmetica*, vol. 42 (1983), 265-279.

[54] E. Weisstein, mathematics web site, `http://www.mathworld.com`.

[55] J. Zun, "A Note on Irrationality of Some Numbers," *Journal of Number Theory*, vol. 25 (1987), 211-212.