Random Generators and Normal Numbers

David H. Bailey[1] and Richard E. Crandall[2]
30 October 2001

Abstract

Pursuant to the authors' previous chaotic-dynamical model for random digits of fundamental constants [3], we investigate a complementary, statistical picture in which pseudorandom number generators (PRNGs) are central. Some rigorous results such as the following are achieved: Whereas the fundamental constant $\log 2 = \sum_{n \in Z^+} 1/(n2^n)$ is not yet known to be 2-normal (i.e. normal to base 2), we are able to establish b-normality (and transcendency) for constants of the form $\sum 1/(nb^n)$ but with the index n constrained to run over certain subsets of Z^+. In this way we demonstrate, for example, that the constant $\alpha_{2,3} = \sum_{n=3,3^2,3^3,\ldots} 1/(n2^n)$ is 2-normal. The constants share with π, $\log 2$ and others the property that isolated digits can be directly calculated, but for the new class such computation is extraordinarily 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 density results and irrationality proofs based on PRNG ideas — for various special numbers.

[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 $\log 2$, π, $\zeta(3)$ and $\sqrt{2}$ remain elusive. In [3] we proposed a general "Hypothesis A" that connects normality theory with a certain aspect of chaotic dynamics. In a subsequent work, J. Lagarias [28] provided interesting viewpoints and analyses on the dynamical concepts.

In the present paper we adopt a kind of complementary viewpoint, 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 as follows: Whereas the possible b-normality of the fundamental constant

$$\log 2 \;=\; \sum_{n \in Z^+} \frac{1}{n 2^n}$$

remains to this day unresolved (for any b), we prove that for certain subsets $S \subset Z^+$ and bases b, the sum

$$\sum_{n \in S} \frac{1}{n b^n}$$

is indeed b-normal (and transcendental). An attractive special case is a number we denote $\alpha_{2,3}$, obtained simply by restricting the indices in the $\log 2$ series definition to run over powers of 3:

$$\begin{aligned} \alpha_{2,3} &= \sum_{n=3^k>1} \frac{1}{n 2^n} \;=\; \sum_{k=1}^{\infty} \frac{1}{3^k 2^{3^k}} \\ &= 0.041883680831502985071252898624571682426096758465485 7\ldots_{10} \\ &= \texttt{0.0AB8E38F684BDA12F684BF35BA781948B0FCD6E9E06522C3F35B}\ldots_{16}\,, \end{aligned}$$

which number we now know to be 2-normal (and thus 16-normal as well; see Theorem 2.2(6)). It is of interest that until now, explicit b-normal numbers have generally been what one might call "artificial," as in the case of the 2-normal, binary Champernowne constant:

$$C_2 \;=\; 0.(1)(10)(11)(100)(101)(110)(111)\cdots_2\,,$$

with the $(\cdot)$ notation meaning the expansion is constructed via *concatenation* of registers. Now with numbers such as $\alpha_{2,3}$ we have b-normal numbers that are "natural" in the sense that they can be described via some kind of analytic formulation. Such talk is of course heuristic; the rigor comes in the theorems of the following sections.

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 have 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 α mod 1, the fractional part of α, and denote by $||\alpha||$ the closer of the absolute distances of α mod 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 [3] and references [27] [21] [33] [25] 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 [21] [33].)

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)

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

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)

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

where (β_n) is a sorted (either in decreasing or increasing order) version of the first N elements of (α_n)

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 [27], p. 71, Corollary 8.2, [21].

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

   Proof. See [3].

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

   Proof. See [27], p. 70, Theorem 8.1.

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

   Proof. See [27], 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. For the b-normality of $q\alpha$, see [27], p. 77, Exercise 8.9. For the additive $(+r)$ part, see end of the present section. For the c-normality see [27], 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 [27], 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 [27], 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 [3] [27], 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

$$\lim_{N\to\infty} G_N \quad = \quad 0.$$

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. Assume α and the corresponding sequence of the previous item. Then α is b-normal iff

$$\lim_{N\to\infty} D_N \quad = \quad 0.$$

Proof. See [27], 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 2.3 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 2.3(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 2.3(8). We selected the following example application of the Weyl sum to foreshadow several important elements of our eventual analyses. With Theorem 2.3(5,6,8) we can prove part of Theorem 2.3(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 2.3(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 2.3(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 [3].

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

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

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

Proof. Write

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

with c' being a constant. Therefore by Theorem 2.2(10) it follows that β is b-normal. Now assume b-normality. 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) iff β is b-normal (dense)..

In our previous work [3] this kind of unconditional 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 $x_0 = 0$)

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

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

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

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 statements 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 [3])..

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-theoretical 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,p)-PRNG systems, 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,p)-PRNG system, for base $b \geq 2$ and odd prime p coprime to b, as the sequence of iterates defined $x_0 = 0$ and

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

where the perturbation is given by

$$r_{p^{k-1}} \;=\; \frac{1}{p^k}$$

for $k \geq 1$, with all other $r_i = 0$.

Remark 1. Just knowing the pair (b,p) determines the PRNG and its properties. Consider the parameter a, defined by $p^a || (b^{\tau_1} - 1)$ with τ_1 being the order of b modulo p. It is known that the order, then, of b modulo p^k is given by

$$\tau_k \;=\; \tau_1 p^{\max(0,k-a)}.$$

For example, for $b = 2$ and $p = 7$ we have $2^3 - 1 = 7$, so $\tau_1 = 3$, $a = 1$ and the order of 2 modulo 7^k is thus $\tau_k = 3 \cdot 7^{k-1}$. For $b = 2$ again, and a Wieferich prime such as $p = 1093$ we have $\tau_1 = 364$ and $p^2 || (2^{364} - 1)$, so in this case $a = 2$, whence for $k > 1$ we have $\tau_k = 364 \cdot 1093^{k-2}$. (Thus for example the order of 2 modulo 1093^2 is also 364.)

Remark 2. One could attempt to expand the (b,p)-PRNG definition to include the even-modulus case $p^k = 2^k$, with odd $b \geq 3$, in which case the rules run like so: If $2^k | (b-1)$ then the order is $\tau_k = 1$, else if $2^k | (b^2 - 1)$ then $\tau_k = 2$, else define a by $2^a || (b^2 - 1)$, whence the order is $\tau_k = 2^{1+k-a}$. One expects therefore that normality results would accrue for a $(b,2)$-PRNG system, odd $b \geq 3$. However we do not travel this path in the present treatment; for one thing some of the lemmas from the literature are geared toward odd prime powers, so that more details would be required to include $p = 2$ systems.

The perturbation r_n for a (b,p)-PRNG system is thus of the "kicking" variety; happening indefinitely, but not on every iteration, and in fact, happening progressively rarely. Between the "kicks," iterates of the sequence are, in effect, repetitions of a certain type of

normalized linear congruential PRNG. This is best seen by examining a specific example. Consider successive iterates of the $(2,3)$-PRNG system, whose iterates run like so:

$$(x_0,\, x_1,\, \ldots,\, x_{26},\, \ldots) = (0,\, \frac{1}{3},\, \frac{2}{3},\, \frac{4}{9},\, \frac{8}{9},\, \frac{7}{9},\, \frac{5}{9},\, \frac{1}{9},\, \frac{2}{9},$$
$$\frac{13}{27},\, \frac{26}{27},\, \frac{25}{27},\, \frac{23}{27},\, \frac{19}{27},\, \frac{11}{27},\, \frac{22}{27},\, \frac{17}{27},\, \frac{7}{27},\, \frac{14}{27},\, \frac{1}{27},\, \frac{2}{27},\, \frac{4}{27},\, \frac{8}{27},\, \frac{16}{27},\, \frac{5}{27},\, \frac{10}{27},\, \frac{20}{27},$$
$$\frac{40}{81},\, \cdots)$$

A pattern is clear from the above: The entire sequence is merely (after the initial 0) a concatenation of subsequences of respective lengths $2 \cdot 3^{k-1}$, for $k = 1, 2, \ldots$. Each subsequence is the complete period of a certain linear congruential PRNG normalized by 3^k. Note that since 2 is a primitive root modulo 3^k, $k > 0$, each subsequence visits, exactly once, every integer in $[1, 3^k - 1]$ that is coprime to 3.

In general, we can write the following (for simplicity we use simply $\equiv$ to mean equality on the mod-1 circle):

$$\begin{aligned}
x_0 &\equiv 0, \\
x_1 &\equiv b \cdot 0 + r_1 \equiv \frac{1}{p}, \\
x_2 &\equiv \frac{b}{p}, \\
&\cdots , \\
x_{p-1} &\equiv \frac{b^{p-2}}{p}, \\
x_p &\equiv \frac{b^{p-1}}{p} + r_p \equiv \frac{p+1}{p^2}, \\
&\cdots , \\
x_{p^2-1} &\equiv \frac{b^{p^2-p-1}(p+1)}{p^2}, \\
x_{p^2} &\equiv \frac{b^{p(p-1)}(p+1)}{p^2} + r_{p^2} = \frac{p^2+p+1}{p^3}, \\
&\cdots ,
\end{aligned}$$

and generally speaking,

$$x_{p^{k-1}} \equiv \frac{(p^k-1)/(p-1)}{p^k}.$$

It is evident that upon the $1/p^k$ perturbation, the x_n commence a run of length $\varphi(p^k) = p^{k-1}(p-1)$ before the next perturbation, according to the following rule: The subsequence

$$(x_{p^{k-1}}, \ldots, x_{p^k-1})$$

runs from

$$\left(a_k b^0 \bmod p^k\right)/p^k$$

through

$$\left(a_k b^{p^{k-1}(p-1)-1} \bmod p^k\right)/p^k$$

inclusive, where

$$a_k \;=\; \frac{p^k-1}{p-1}$$

is coprime to p. One is aware that, in general, this subsequence will repeat — i.e., "walk on itself" — unless b is a primitive root of p^k. This phenomenon occurs, of course, because the powers of b modulo p^k have period τ_k which period can be less than $\varphi(p^k)$. Later we shall use the symbol M_k to be the multiplicity of these subsequence orbits; $M_k = \varphi(p^k)/\tau_k$. For the moment we observe that the M_k are bounded for all k, in fact $M_k < p^a$ always.

We need to argue that (x_n) is equidistributed. For this we shall require an important lemma on exponential sums, which lemma we hereby paraphrase using our (b,p)-PRNG nomenclature:

Lemma 4.2 (Korobov, Niederreiter) Given $b \geq 2$, $\gcd(b,p) = 1$, and p an odd prime (so that the order of b modulo p^k is τ_k of the text), assume positive integers k, H, J and $d = \gcd(H, p^k)$ with $J \leq \tau_k$ and $d < \tau_k/\tau_1$. Then

$$\left|\sum_{j=1}^{J} e^{2\pi i H b^j/p^k}\right| \;<\; \sqrt{\frac{\tau_k}{d}}\left(1+\log\frac{\tau_k}{d}\right).$$

Proof. The lemma is a direct corollary of results found in [25], e.g. p. 167, Lemma 32 (which Lemma in fact involves more general moduli than p^k—notably products of prime powers), plus (earlier) results of Korobov [26]. The corollary also follows from somewhat stronger variants for the moduli p^k of our present interest in [30], 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 [24], pp. 107-110.

Lemma 4.2 speaks to the distribution of powers of b modulo prime powers. We are aware that one could start from Lemma 4.2 and apply the Weyl criterion (Theorem 2.2(8)) to establish equidistribution of the (x_n). We shall prove a little more, starting from the following lemma:

Lemma 4.3 For a sequence (y_n) built as an ordered union $((y_1,\cdots,y_{N_1}),(y_{N_1+1},\cdots,y_{N_1+N_2}),\cdots)$ of subsequences of respective lengths N_i, we have for $N = N_1+N_2+\cdots+N_{k-1}+J$ with $0 \leq J < N_k$

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

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

Proof. This is proved simply, in [27], p. 115, Theorem 2.6.

Next we establish a lemma pertaining to the full subsequence of iterates occurring between two successive perturbations.

Lemma 4.4 For a (b,p)-PRNG system, and $k > 2a$, the subsequence

$$(x_{p^{k-1}}, \ldots, x_{p^k-1}),$$

having $\varphi = \varphi(p^k) = p^{k-1}(p-1)$ terms, has discrepancy satisfying

$$D_\varphi \;<\; C\frac{\log^2 \varphi}{\sqrt{\varphi}},$$

where C is a constant depending only on (b,p) (and thus k-independent).

Remark. Such $O(\log^2 N/\sqrt{N})$ results including some results on best-possibility of such bounds, have been achieved in brilliant fashion by Niederreiter (see [30], p. 1009 and [31], pp. 169-170). Such results have historically been applied to generators of long period, e.g. PRNGs that have long period for the given modulus. Evidently the only statistical drawback for the PRNGs of present interest is that the discrepancy-bound constant can be rather large (and, of course, we need eventually to chain our PRNG subsequences together to obtain an overall discrepancy).

Proof. By the Erdős–Turan Theorem 2.2(9), for any integer $m_k > 0$ we have

$$D_\varphi \;<\; C_1\left(\frac{1}{m_k} + \sum_{h=1}^{m_k}\frac{1}{h}\left|\frac{M_k}{\varphi}\sum_{j=0}^{\tau_k-1} e^{2\pi i h a_k b^j/p^k}\right|\right),$$

where M_k is the multiplicity φ/τ_k that describes how many complete cycles the given subsequence performs modulo p^k. When $h < \tau_k/\tau_1 = p^{k-a}$ the $|\cdot|$ term is, by Lemma 4.2, less than $C_2(1+\log\tau_k)/\sqrt{\tau_k}$. Choosing $m_k = \lfloor p^{k/2}\rfloor < p^{k-a}$ constrains the index h properly, and we obtain $D_\varphi < C_3(1/\sqrt{m_k} + (\log(m_k)\log\tau_k)/\sqrt{\tau_k})$. Now we recall that $M_k = \varphi/\tau_k$ is bounded and observe that $C_4\sqrt{\varphi} < m_k < C_5\sqrt{\varphi}$, and the desired discrepancy bound is met.

Finally we can address the issue of equidistribution of the (b,p)-PRNG system, by contemplating the chain of subsequences that constitute the full generator:

Theorem 4.5 For the full (b,p)-PRNG sequence (x_n), the discrepancy for $N > 1$ satisfies

$$D_N \;<\; C\frac{\log^2 N}{\sqrt{N}},$$

where C is independent of N, and accordingly, (x_n) is equidistributed.

Proof. Let $N = \varphi(p) + \varphi(p^2) + \cdots + \varphi(p^{k-1}) + J = p^{k-1} - 1 + J$ be the index into the full (x_n) sequence, where $0 < J < \varphi(p^k)$, so that we have $(k-1)$ complete mod-p^i

subsequences, then J initial terms from a last subsequence having denominator p^k. Also let $k > 2a+1$ so that Lemma 4.4 is effective. By Lemma 4.3 and the Erdős–Turan Theorem 2.2(9) we have for any positive integer m

$$D_N \;<\; \frac{2a}{N} + C_1 \sum_{i=2a+1}^{k-1} \frac{\varphi(p^i)}{N} \frac{\log^2 \varphi(p^i)}{\sqrt{\varphi(p^i)}} + C_2 \frac{J}{N} \left(\frac{1}{\sqrt{m}} + \sum_{h=1}^{m} \frac{1}{h} \left| \frac{1}{J} \sum_{j=1}^{J} e^{2\pi i h a_k b^j / p^k} \right| \right).$$

Now the $|\cdot|$ term involves J exponential summands, so that the number of complete cycles of b^j modulo p^k is $\lfloor J/\tau_k \rfloor$, so that this $|\cdot|$ term is bounded above by

$$\frac{1}{J} \left\lceil \frac{J}{\tau_k} \right\rceil \sqrt{\tau_k} \left(1 + \log^2 \tau_k\right),$$

where again we have used the Korobov–Niederreiter Lemma 4.2. On the basis of the relations $\varphi(p^i) = p^{i-1}(p-1)$ and $\tau_k = \tau_1 p^{k-a}$ (recall $k > 2a+1$) we have:

$$\begin{aligned} C_3 N \;&<\; p^k \;<\; N, \\ C_5 N^{i/k} \;&<\; \varphi(p^i) \;<\; C_6 N^{i/k}, \\ C_7 N \;&<\; \tau_k \;<\; C_8 N, \end{aligned}$$

where the various C_j here are k-and-i-independent, positive constants. Next, choose the parameter $m = \lfloor p^{k/2} \rfloor$. Now the desired discrepancy bound follows upon replacement of all p^k, $\varphi(p^i)$, τ_k terms with constants times powers of N. That (x_n) is equidistributed is a consequence of Theorem 2.2(12).

Now we can move to the main result

Theorem 4.6 For base $b > 1$ and odd prime p coprime to b, the number

$$\alpha_{b,p} \;=\; \sum_{n \geq 1} \frac{1}{p^n b^{p^n}}$$

is b-normal.

Remark. When b is a primitive root of p and $p || (b^{p-1} - 1)$, it is easy to show that this $\alpha_{b,p}$ is b-dense (the (b,p)-PRNG sequence becomes progressively finer in an obvious way).

Proof. For a (b,p)-PRNG system the associated constant as in Theorem 3.1 is $\beta = \sum_{k \geq 1} 1/(p^k b^{p^{k-1}})$ and this is a rational multiple of our $\alpha_{b,p}$. Theorem 2.2(7) finishes the argument.

Corollary 4.7 The number

$$\alpha_{2,3} \;=\; \sum_{n=3^k > 1} \frac{1}{n 2^n}$$

is 2-normal.

It is natural to ask whether $\alpha_{b,p}$ is transcendental, which question we answer in the positive with:

Theorem 4.8 The number $\alpha_{b,p}$ for any integers $b > 1, p > 2$ is transcendental.

Remark. Though $\alpha_{b,p}$ has been introduced for (b,p)-PRNG systems with $b > 1$, $\gcd(b,p) = 1$, p an odd prime, the transcendency result is valid for any integer pair (b,p) with $p > 2$ and $b > 1$.

Proof. The celebrated Roth theorem states [36] [13] that if $|P/Q - \alpha| < 1/Q^{2+\epsilon}$ admits of infinitely many rational solutions P/Q (i.e. if α is approximable to degree $2+\epsilon$ for some $\epsilon > 0$), then α is transcendental. We show here that $\alpha_{b,p}$ is approximable to degree $p - \delta$. Fix a k and write

$$\alpha_{b,p} \;=\; P/Q + \sum_{n>k} \frac{1}{p^n b^{p^n}},$$

where $\gcd(P,Q) = 1$ with $Q = p^k b^{p^k}$. The sum over n gives

$$|\alpha_{b,p} - P/Q| \;<\; \frac{2}{p^{k+1}(Q/p^k)^p} \;<\; \frac{p^{kp}}{Q^p}.$$

Now $p^k \log b + k \log p = \log Q$, so that $p^k < \log Q / \log b$, and we can write

$$p^{kp} \;<\; (\log Q / \log b)^p \;=\; Q^{p(\log\log Q - \log\log b)/\log Q}.$$

Thus for any fixed $\delta > 0$,

$$|\alpha_{b,p} - P/Q| \;<\; \frac{1}{Q^{p(1+\log\log b/\log Q - \log\log Q/\log Q)}} \;<\; \frac{1}{Q^{p-\delta}},$$

for all sufficiently large k.

Can one efficiently obtain isolated digits of $\alpha_{b,p}$? It turns out that $\alpha_{b,p}$ 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 [2] — the same approach works for the new, b-normal and transcendental constants. Indeed, for $\alpha_{b,p}$ the BBP algorithm is extraordinarily rapid: the overall bit-complexity to resolve the n-th base-b digit of $\alpha_{b,p}$ 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 [34], finding said bit to be 0 but at the cost of over 10^{18} CPU clocks.

The PRNG we have presented takes a more erudite form if we only run through single mod-p^k cycles when the iterate denominator is p^k. That would entail a perturbation

$$r_{1+\tau_1+\tau_2+\cdots+\tau_{k-1}} \quad = \quad \frac{1}{p^k},$$

with all other $r_i = 0$. The associated real number in question is then:

$$\beta_{b,p} \quad = \quad \sum_{k\geq 1} \frac{1}{p^k b^{1+\tau_1(p^k-1)/(p-1)}},$$

and each of these $\beta_{b,p}$ is provably b-normal. One might wonder why this more complicated form should be mentioned at all, what with the elegance of the $\alpha_{b,p}$ forms. The answer is, the PRNG is better, in the usual conventional senses. The discrepancy bound for this PRNG can generally be lowered below the bound for the $\alpha_{b,p}$ (but only in the overall constant), except that if b happens to be a primitive root of p, $\alpha_{b,p} = \beta_{b,p}$ and there is nothing new.

During this work it occurred to the authors that the uniform $(0,1)$ generator

$$y_n \quad = \quad \frac{z_n}{3^k},$$

where z_n is defined by the recursion $z_n = 2z_{n-1} \bmod 3^k$, is of a class (namely, long-period linear congruential generators) that is widely used in modern computing. One possible weakness is that the numerator omits multiples of three; such a defect might be uncovered in spectral tests, for example. The weakness can however be ameliorated to some degree by modifying the y sequence as follows:

$$y_n \quad = \quad \frac{z_n - \lfloor z_n/3 \rfloor}{2 \cdot 3^{k-1}},$$

in this way "contracting" the generator to render a uniformly spaced set of random values—the working denominator is now the period of the generator. The authors are not aware of statistical studies on "contracted" PRNGs of this form.

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

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

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 at all between the ERH and the present theory is automatically interesting.

With Theorem 4.6, we now have normal numbers defined with explicit algebra, as opposed to "artificial" constructions. In this light, of some interest is the form appearing in [25, Theorem 30, pg. 162], where it is proven that

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

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 an explicit function

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

for which the number α above is therefore b-normal. Indeed this work is the closest to ours that we have uncovered in the literature; witness that results of Korobov and Niederreiter have figured strongly into our proofs.

It may be possible to extend some of these ideas to handle even the artificially constructed normal numbers described in Sections 1 and 6.

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 [22]

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

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, y form has constant offset $\sum 1/(2^{e_i} - 1)$ so that the maximum gap around the mod 1 circle is the same. 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 $0 < a < b$:

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

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:

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

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 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 [19] with a clever number-theoretical argument. More recently, P. Borwein [7] 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:

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

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 [4]

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

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

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

where $t_d \to 0$. Thus $\{2^d E\}$ 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

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

But this implies in turn that some iterate $\{2^m E\}$ 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 is ruined. More generally, there is the

class of Erdős–Copeland numbers [14], 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 $g, h > 1$)

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

are known at least to be irrational [32], [38], and it would be of interest to establish perturbation sums in regard to such numbers. Incidentally, it is ironic that the 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 is 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 agrument, 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 [27], 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 [3] and present work. Regardless of our current connections, the function and its variants have certainly been studied, especially in regard to continued fractions [16] [17] [27] [8] [29] [5] [1] [17] [9], [10]. 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:

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

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,p)-PRNG systems, the numbers $\alpha_{b,p}$ are each b-normal. What about c-normality of such a number for c not a rational power of b?

- What techniques might allow is to relax the constraint of rapid growth $n = p^k$ in our sums $\sum 1/(nb^n)$, in order to approach the spectacular goal of resolving the suspected b-normality of $\log(b/(b-1))$? One promising approach is to analyze discrepancy for relatively short parts of PRNG cycles. In [25], p. 171, [26] there appear exponential sum bounds for relatively short indices J into the last cycle. It could be that such theorems can be used to slow the growth of the summation index n.

- It is clear that the discrepancy bound given in Theorem 4.5, based in turn on the Korobov–Niederreiter Lemma 4.2, is "overkill," in the sense that we only need show $D_N = o(N)$ to achieve a normality proof. Does this mean that the numbers $\alpha_{b,p}$ are somehow "especially normal"? For such a question one would perhaps need extra variance statistics of a normal number; i.e., some measures beyond the "fair frequency" of digit strings.

- 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?

- With our (b, p)-PRNG systems we have established a countable infinity of explicit b-normal numbers. What will it take to exhibit an uncountable, explicit collection?

- What are the properties of "contracted" PRNGs, as exemplified in Section 4?

- Does polynomial-time (in $\log n$) resolution of the n-th digit for our $\alpha_{b,p}$ 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, J. Shallit, S. Wagon, T. Wieting and S. Wolfram for theoretical and computational expertise throughout this project. 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 robust boundaries.

References

[1] W. W. Adams and J. L. Davison, "A remarkable class of continued fractions," *Proceedings of the American Mathematical Society*, **65**, 1977, 194-198.

[2] 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.

[3] David H. Bailey and Richard E. Crandall, "On the random character of fundamental constant expansions," *Experimental Mathematics*, 10, 2001, 175-190.

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

[5] P. E. Böhmer,"Über die Transzendenz gewisser dyadischer Brüche," *Mathematiche Annalen*, **96**, 1926, 367-377, Erratum: **96**, 1926, 735

[6] J. Borwein, D. Bradley and R. Crandall, "Computational Strategies for the Riemann Zeta Function," manuscript, Dec. 1998, www.cecm.sfu.ca/preprints/1998pp.html

[7] Peter Borwein, "On the irrationality of certain series," *Mathematical Proceedings of the Cambridge Philosophical Society*, vol. 112 (1992), pg. 141-146; MR 93g:11074.

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

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

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

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

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

[13] J. W. S. Cassels, *An introduction to diophantine approximations*, Cambridge Univ. Press, Cambridge, 1957.

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

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

[16] L. V. Danilov, "Some classes of transcendental numbers," *Matematicheskie Zametki*, **12**, 1972, 149-154; In Russian, English translation in *Mathematical Notes of the Academy of Science of the USSR* **12**, 1972, 524–527.

[17] J. L. Davison, "A series and its associated continued fraction," *Proceedings of the American Mathematical Society*, **63**, 1977, 29-32.

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

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

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

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

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

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

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

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

[26] N. Korobov, "On the distribution of digits in periodic fractions," *Matematicheskie USSR Sbornik*, 18, 1972, 659-676.

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

[28] J. Lagarias, "On the Normality of Fundamental Constants," Experimental Mathematics, Vol. 10, No. 3, 353–366 (2001).

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

[30] H. Niederreiter, "Quasi-Monte Carlo Methods and Pseudo-Random Numbers," Bull. Amer. Math. Soc. 84, 6, (1978).

[31] H. Niederreiter, "Random Number Generation and Quasi-Monte Carlo Methods," CBMS-NSF Regional Conference Series in Applied Mathematics, SIAM, 63, (1992).

[32] H. Niederreiter, "On an irrationality theorem of Mahler and Bundschuh," J. Number Theory 24, 197-199 (1986).

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

[34] C. Percival, "PiHex: A distributed effort to calculate Pi," `http://www.cecm.sfu.ca/projects/pihex/index.html`.

[35] P. Ribenboim, *The new book of prime number records*, Springer-Verlag, New York 1996.

[36] K. Roth, "Rational approximations to algebraic numbers," *Mathematika*, **2**, 1955, 1-20' Corrigendum, 168, **MR 17**, 242.

[37] E. Weisstein, mathematics web site, `http://www.mathworld.com` or `http://mathworld.pdox.net`.

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