On the Random Character of Fundamental Constant Expansions

David H. Bailey and Richard E. Crandall

CONTENTS

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.

We propose a theory to explain random behavior for the digits in the expansions of fundamental mathematical constants. At the core of our approach is a general hypothesis concerning the distribution of the iterates generated by dynamical maps. On this main hypothesis, one obtains proofs of base-2 normality—namely bit randomness in a specific technical sense—for a collection of celebrated constants, including π, $\log 2$, $\zeta(3)$, and others. Also on the hypothesis, the number $\zeta(5)$ is either rational or normal to base 2. We indicate a research connection between our dynamical model and the theory of pseudorandom number generators.

1. INTRODUCTION

It is of course a long-standing open question whether the digits of π and various other fundamental constants are "random" in an appropriate statistical sense. Informally speaking, we say that a number α is normal to base b if every sequence of k consecutive digits in the base-b expansion of α appears with limiting frequency b^{-k}. In other words, if a constant is normal to base 10, its decimal expansion would exhibit a "7" one-tenth of the time, the string "37" one one-hundredth of the time, and so on. It is widely believed that most, if not all, of the "fundamental" or might we say "natural" irrationals are not only normal to base 10, but are *absolutely* normal, meaning they are normal to every integer base $b \geq 2$. By "fundamental" or "natural" constants here we include π, e, $\log 2$, $\sqrt{2}$, the golden mean $\tau = (1+\sqrt{5})/2$, the Riemann zeta function evaluation $\zeta(3)$, and a host of others. In regard to algebraic numbers, one could further conjecture that *every* irrational algebraic number is absolutely normal, since there are no known counter-examples. Even suspected (but not yet proven) irrationals, such as

1058-6458/2001 $0.50 per page

the Euler constant γ, are generally expected to be absolutely normal.

It is well-known from measure theory that a "random" real number is absolutely normal with probability one. In spite of this result, not a *single* fundamental constant has been shown to be normal to base b for any b, much less for all bases simultaneously. Even the weaker assertion that every finite digit string appears in the expansion has not been established, to our knowledge, for any fundamental constant. We shall mention later some artificially constructed, provably normal numbers; yet the situation with respect to fundamental constants has remained bleak to the present day.

We discuss here a linkage between the normality of certain constants and a certain kind of dynamical mechanism. In a companion paper, we establish a relationship between the dynamical picture and the theory of pseudorandom number generators [Bailey and Crandall 2001]. Our present theory is based on the following general hypothesis:

Hypothesis A. *Denote by*

$$r_n = p(n)/q(n)$$

a rational-polynomial function, $p, q \in Z[X]$. *Assume further that* $0 \le \deg p < \deg q$, *with* r_n *nonsingular for positive integers* n. *Choose an integer* $b \ge 2$ *and set* $x_0 = 0$. *Then the sequence* $x = (x_0, x_1, x_2, \dots)$ *determined by the iteration*

$$x_n = (bx_{n-1} + r_n) \bmod 1 \qquad (1\text{–}1)$$

either has a finite attractor or is equidistributed in $[0, 1)$.

We shall precisely define "equidistributed" and "finite attractor" shortly, intending for the moment just to convey the spirit of this core hypothesis. The condition $0 \le \deg p$ is simply a convenience, to rule out the zero polynomial (on the mnemonic: $\deg 0 = -\infty$). Now, there is a striking consequence of Hypothesis A, namely that digits of the expansions of certain constants must be random in the following sense:

Theorem 1.1. *On Hypothesis A* (that is, assuming its validity), *each of the constants* π, $\log 2$, *and* $\zeta(3)$ *is normal to base* 2, *and* $\log 2$ *is normal to base* 3. *Furthermore*, *on the same hypothesis*, *if* $\zeta(5)$ *is irrational it too is normal to base* 2.

The particular set of constants appearing in Theorem 1.1 is merely representative, for as we shall see, numerous other constants could also be listed.

If even one particular instance of Hypothesis A could be established, the consequences would be remarkable. For example, if it could be established that the simple iteration given by $x_0 = 0$ and

$$x_n = \left(2x_{n-1} + \frac{1}{n}\right) \bmod 1 \qquad (1\text{–}2)$$

is equidistributed in $[0, 1)$, then it would follow that $\log 2$ is normal to base 2. In a similar vein, if it could be established that the iteration given by $x_0 = 0$ and

$$x_n = \left(16x_{n-1} + \frac{120n^2 - 89n + 16}{512n^4 - 1024n^3 + 712n^2 - 206n + 21}\right) \bmod 1 \qquad (1\text{–}3)$$

is equidistributed in $[0, 1)$, it would follow that π is normal to base 16 (and, as we shall see, it would follow easily that π is also normal to base 2).

The algorithmic motivation for our current treatment is the recent discovery of a simple algorithm by which one can rapidly calculate individual digits of certain polylogarithmic constants [Bailey et al. 1997]. This BBP algorithm (named after Bailey, P. Borwein and S. Plouffe) has already given rise to a small computational industry of sorts. For example, the quadrillionth binary digit of π, the billionth binary digit of $\log 2$ and the hundred-millionth binary digit of $\zeta(3)$ have been found in this fashion [Bailey et al. 1997; Borwein et al. 2000; Broadhurst 1998; Percival 2000]. Our intent here is not to present new computational results, but instead to pursue the *theoretical* implications of this algorithm.

We describe the BBP algorithm by way of example. We start with the well-known formula

$$\log 2 = \sum_{k=1}^{\infty} \frac{1}{k\, 2^k}.$$

Now for any $n \ge 1$ the fractional part

$$(2^n \log 2) \bmod 1$$

gives precisely that part of the expansion of $\log 2$ starting at location $n + 1$ inclusive in the binary expansion of $\log 2$. (Location 1 is the first binary digit to the right of the "decimal" point.) We have

$$
\begin{aligned}
&(2^n \log 2) \bmod 1 \\
&= \left(\sum_{k=1}^{\infty} \frac{2^{n-k}}{k} \right) \bmod 1 \\
&= \left(\sum_{k=1}^{n} \Big(\frac{2^{n-k} \bmod k}{k} \Big) \bmod 1 + \sum_{k=n+1}^{\infty} \frac{2^{n-k}}{k} \right) \bmod 1.
\end{aligned} \tag{1–4}
$$

We have parsed this last expression explicitly to indicate the algorithm in question: (1) compute each numerator of the first sum (having $k \in [1, n]$) using the well-known binary-ladder algorithm for exponentiation, reducing each intermediate product modulo k; (2) divide each numerator by its respective k using ordinary floating-point arithmetic; (3) sum the terms of the first series, discarding any integer parts; (4) compute the second sum (typically just a few terms are needed), and (5) add the two sum results, again discarding the integer part. The resulting fraction, when expressed in binary notation, gives the first few binary digits of $\log 2$ beginning at position $n + 1$. High-precision arithmetic software is not required for these operations — ordinary 64-bit or 128-bit floating-point arithmetic will suffice — and very little memory is required. A few hexadecimal digits of $\log 2$ beginning at the ten billionth position, which were computed using this formula, are given in [Bailey et al. 1997].

In a similar manner, one can compute arbitrary hexadecimal (or binary) digits of π by means of the formula

$$
\pi = \sum_{n=0}^{\infty} \frac{1}{16^n} \left(\frac{4}{8n+1} - \frac{2}{8n+4} - \frac{1}{8n+5} - \frac{1}{8n+6} \right).
$$

This can be done by simply writing this expression as a sum of four infinite series and then applying the scheme described above for $\log 2$ to each of these four series [Bailey et al. 1997].

Our theoretical approach here is to analyze this process of "digit extraction" to study the randomness of the digits produced. As we shall see, this inquiry leads into several disparate fields of inquiry, including algebraic number theory, chaotic dynamics, ergodic theory, pseudorandom number generation, probability and statistics. Some of these connections are explored in the companion paper [Bailey and Crandall 2001] and in [Lagarias 2001].

2. NOMENCLATURE AND FUNDAMENTALS

We denote by $\lfloor \alpha \rfloor$ and $\{\alpha\}$ respectively the usual floor and fractional-part extractions of a real α. In general we have $\alpha = \lfloor \alpha \rfloor + \{\alpha\}$, noting that the fractional part is always in $[0, 1)$. We can also say $\{\alpha\} = \alpha \bmod 1$, which is convenient given our opening remarks. We define the norm $\|\alpha\|$ for $\alpha \in [0, 1)$ as $\|\alpha\| = \min(\alpha, 1-\alpha)$. With this definition, $\|\alpha - \beta\|$ measures the shortest distance between α and β on the unit circumference circle in the natural way. A simple but useful rule that we will use in some of the ensuing analysis is what we call the dilated-norm rule: if $0 \le \delta \le 1/(2\,\|z\|)$ then, because $\|\delta z\|$ is now bounded above by $1/2$, we have $\|\delta z\| = \delta\,\|z\|$.

A base-b expansion, say

$$
\alpha = 0.\alpha_1 \alpha_2 \alpha_3 \ldots
$$

where each α_j is an integer in $[0, b-1]$, is taken to be unique for α. When competing expansions exist, as in decimal $0.1000\ldots = 0.0999\ldots$, we take the variant with trailing zeros. Now consider the frequency (when it exists) with which a given finite digit string $(d_1 d_2 \ldots d_k)$ appears in α. This is taken to be the limit as $N \to \infty$ of the number of instances where $\alpha_j = d_1,\ \alpha_{j+1} = d_2,\ \ldots,\ \alpha_{j+k-1} = d_k$ (for j ranging from 1 to $N+1-k$), divided by N. We now introduce a standard definition from the literature [Kuipers and Niederreiter 1974, pp. 69, 71].

Definition 2.1. A real number α is said to be normal to base b if every finite string of k digits appears in the base-b expansion of α with well-defined limiting frequency b^{-k}. A number that is normal to every integer base $b \ge 2$ is said to be absolutely normal.

We remarked earlier that almost all numbers are absolutely normal. This is intuitively evident, since a base-b expansion of $\alpha \in [0, 1)$ corresponds to an infinite game of flipping a fair, b-sided die, and thus we expect every k-long string of symbols to appear with the expected frequency b^{-k}, for almost all α (i.e., with probability one). For our present purposes, it will be useful to also adopt a second, somewhat weaker criterion of digit randomness, namely:

Definition 2.2. We say a number α is digit-dense to base b if every finite string of k consecutive base-b digits appears in the base-b expansion of α.

This definition implies that if α be digit-dense to base b every finite string appears not just once but infinitely often. This follows immediately upon the simple observation that every finite string is contained in an infinite number of longer finite strings.

Analogous to the notion of a digit-dense expansion is the notion of a dense sequence in $[0,1)$. A dense sequence visits every nonempty subinterval $[c,d)$ at least once (and hence infinitely often). A stronger notion is equidistribution, to which we now turn. For a sequence $x=(x_0,x_1,\dots)$ of real numbers in $[0,1)$, consider the counting function

$$C(x,c,d,N)=\#\{x_j\in[c,d):j<N\}.$$

This C function gives the count of the first N elements of the sequence x that lie in the interval $[c,d)$. Then the property of equidistribution is that elements of x lie in subregions of $[0,1)$ with a fair frequency, in the following exact sense:

Definition 2.3. A sequence x in $[0,1)$ is said to be equidistributed if for any $0\le c<d<1$ we have

$$\lim_{N\to\infty}\frac{C(x,c,d,N)}{N}=d-c.$$

This definition is identical to that of "uniform distribution modulo 1", as given in [Kuipers and Niederreiter 1974, p. 1].

In our development we shall need one (out of several) existing theorems on equidistribution, namely the following [Kuipers and Niederreiter 1974, p. 3], where we have added the simple extension that covers the weaker condition of density along with equidistribution:

Theorem 2.4. *Let (x_n) be equidistributed (alternatively, dense). If a sequence (y_n) has the property that $\{y_n\}\to C$ (constant C) as $n\to\infty$, then the sequence $(\{x_n+y_n\})$ is likewise equidistributed (alternatively, dense). In particular, if $y_n\to 0$, then $(\{x_n+y_n\})$ is equidistributed (alternatively, dense).*

There is a simple but beautiful connection between normality of a number and equidistribution of relevant fractional parts [Kuipers and Niederreiter 1974, p. 70]:

Theorem 2.5. *A number α is normal to base b if and only if the sequence $(\{b^n\alpha\}:n=1,2,3,\dots)$ is equidistributed.*

Corollaries of these last two theorems can be useful, even amusing. A typically curious side result is this: $\log 2$ is normal to base 2 if and only if the sequence $(\{\log F_n\})$ is equidistributed, where $F_n=2^{2^n}+1$ are the celebrated Fermat numbers. This result follows immediately by observing that $\lim_n(\log F_n-2^n\log 2)=0$.

It is straightforward to prove the following result, which will enjoy application to certain specific real numbers:

Theorem 2.6. *A number α is digit-dense to base b if and only if the sequence $(\{b^n\alpha\}:n=1,2,3,\dots)$ is dense in $[0,1)$.*

Proof. Any interval (r,s) in $[0,1)$ contains a base-b subinterval I of the form

$$[0.d_0d_1\dots d_{k-1},\ d_0d_1\dots(d_{k-1}{+}1)),$$

where the d_j represent base-b digits and $d_{k-1}<b-1$. If one assumes that α is digit-dense, then $\{b^n\alpha\}$ visits the interval I at least once, and thus visits (r,s) at least once. Conversely, if one assumes that the sequence $(\{b^n\alpha\})$ is dense in $[0,1)$, then any base-b string appears at least once, so that α is digit-dense to base b. $\square$

The theory of normal numbers is deep, and has a long history; we mention here just one of the deeper results relevant to our present treatment [Kuipers and Niederreiter 1974, p. 72]:

Theorem 2.7. *Assume α is normal to base b, and denote by r a nonzero rational number. Then $r\alpha$ is normal to base b; moreover α is also normal to any (integer) base $c=b^r$.*

The first part of this theorem tells us that if we establish the normality of say $(r/s)\zeta(5)$ for integers r,s, then $\zeta(5)$ is automatically normal. The second part tells us, for example, that if a number be normal to base 16 (i.e., every hexadecimal string appears with proper frequency), then the number is also normal to base 2, or for that matter to any power-of-two base. The wording of this latter part is critical: there exist numbers normal to some base b but not to some other base a that is not a rational power of b [Cassels 1959; Kuipers and Niederreiter 1974]. For example, the standard Cantor set has members that are normal to base 2, yet none of its members is normal to base 3. Moreover, there are results on the class of "absolutely abnormal" numbers, meaning numbers not normal to any base. Any rational number is of this class, of course, yet the class is uncountable, and there exist proven, constructive examples of absolutely abnormal irrationals [Martin 2000].

It is a celebrated theorem of Weyl that α is irrational if and only if the sequence $(\{n\alpha\} : n = 1, 2, 3, \dots)$ is equidistributed [Kuipers and Niederreiter 1974, p. 8]. Note, however, that in the present treatment we are not concentrating on multipliers n; rather we need the much sparser multiplier set of powers b^n in order to analyze base-b digits *per se*. For reader convenience we summarize thus: the sequence $(\{b^n\alpha\})$ is dense (alternatively, equidistributed) as α is respectively digit-dense to base b (alternatively, normal to base b).

We have mentioned the abject paucity of normality proofs for fundamental constants. The interesting but artificial Champernowne constant, which is the number

$$C_{10} = 0.123456789101112131415\dots$$

obtained by concatenation of the positive integers, is known to be normal to base 10, but existing proofs of even this are nontrivial [Champernowne 1933; Niven 1956]. One can, of course, construct a binary or ternary equivalent of this constant, by concatenating digits in such bases. In a separate treatise we touch upon the theory of continued fractions, noting for the moment that the Champernowne constant has some gargantuan elements in its simple continued fraction, as can be seen by simple numerical experiments. Another example of a concoction known to be normal to base 10 is the Copeland–Erdős number $0.23571113171923\dots$ [Copeland and Erdős 1946], in which the *primes* are concatenated; this concatenation game can be generalized yet further to more general integer sequences for the digit construction.

Theorem 2.8. *If α be normal to base b then α is digit-dense to base b. If α be digit-dense to some base b then α is irrational.*

Proof. Normality clearly implies the digit-denseness, by 2.1. If one assumes that α is digit-dense to some base b, then α cannot be rational, since it is well-known that the base-b expansion of any rational number repeats with a finite period after some initial digit string. This peridocity rules out the existence of arbitrary strings. □

Now we turn to some preliminary dynamical notions for the iterates involved in Hypothesis A. First off we owe the reader a definition of "finite attractor," and a related notion which we call "periodic attractor":

Definition 2.9. A sequence $x = (x_n)$ in $[0, 1)$ is said to have a finite attractor $W = (w_0, w_1, \dots, w_{P-1})$ if for any $\varepsilon > 0$ there is some $K = K(\varepsilon)$ such that for all $k \geq 0$, we have $\|x_{K+k} - w_{t(k)}\| < \varepsilon$, for some function $t(k)$, with $0 \leq t(k) < P$.

Definition 2.10. A sequence $x = (x_n)$ in $[0, 1)$ is said to have a periodic attractor $W = (w_0, w_1, \dots, w_{P-1})$ if for any $\varepsilon > 0$ there is some $K = K(\varepsilon)$ such that for any $k \geq 0$, we have $\|x_{K+k} - w_{k \bmod P}\| < \varepsilon$.

Two useful results along these lines are:

Theorem 2.11. *Assume a sequence (y_n) has the property that $y_n \to C$ (with C constant) as $n \to \infty$. Then a sequence (x_n) in $[0, 1)$ has a finite attractor (alternatively, a periodic attractor) if and only if $(\{x_n + y_n\})$ does.*

Theorem 2.12. *The sequence (x_n), as defined for Hypothesis A, has infinitely many distinct elements; thus this set of distinct elements has at least one limit point.*

Proof. Theorem 2.11 follows immediately from the ε-restriction in Definitions 2.9 and 2.10.

For Theorem 2.12, Consider the set D of all possible differences $\|x_n - bx_{n-1}\|$. If there are finitely many distinct elements in the full sequence (x_n), then D is a finite set so must have a least element. But the perturbation term r_n is arbitrarily close (but not equal) to zero for sufficiently large n, which is a contradiction. Thus (x_n) has infinitely many distinct elements, and it follows by elementary real analysis that these distinct elements have at least one limit point. □

We now show that in certain cases of interest here, the two notions of attractor set introduced above coincide:

Theorem 2.13. *Let α be real and assume an integer base $b \geq 2$. If the sequence $x = (\{b^n\alpha\})$ has a finite* *attractor W, then W is a periodic attractor, and the structure of the attractor W is necessarily*

$$W = (w_0,\ \{bw_0\},\ \{b^2w_0\},\ \ldots,\ \{b^{P-1}w_0\}),$$

for some period P. Moreover each $w_i \in W$ is rational.

Proof. Let $W = \{w_0, w_1, \ldots, w_{P-1}\}$ be the finite attractor for x. Let $d = \min_{0\le i,j<P}(\|w_i - w_j\|)$, and choose

$$\varepsilon < \frac{d}{4b}.$$

Let W_ε be the set of all z in $[0,1)$ such that $\|z - w_i\| < \varepsilon$ for some $0 \le i < P$. Then we know that there is some $K'(\varepsilon)$ such that for all $k > K'$ we have $x_k \in W_\varepsilon$. Let K be the first $k > K'$, such that $\|x_k - w_0\| < \varepsilon$. Then

$$\begin{aligned}\|x_{K+1} - bw_0\| &= \|bx_K - bw_0\| = b\|x_K - w_0\| \\ &< b\varepsilon < d/4,\end{aligned}$$

where the second equality follows from the dilated-norm rule enunciated at the start of this section.

It follows that x_{K+1} is within $b\varepsilon$ of $\{bw_0\}$, and similarly x_{K+k+1} is within $b\varepsilon$ of $\{bw_0\}$ whenever x_{K+k} is within ε of w_0, which must occur infinitely often. Since there can be at most one element of the attractor set W in the region of size $d/4$ about $\{bw_0\}$, and since the choice of ε above was arbitrary, we conclude that bw_0 must be the element of W in that region. We can for notational convenience assume that $w_1 = \{bw_0\}$. Then $\|x_{K+1} - w_1\| < \varepsilon$, and the argument can be repeated to show that x_{K+2} is close to $w_2 = \{b^2w_0\}$, etc., and finally that x_{K+P-1} is close to $w_{P-1} = \{b^{P-1}w_0\}$. It then follows that the member of W which x_{K+P} is close to must be w_0, since otherwise the ε region around w_0 would never be visited again by the x sequence and thus w_0 could not be a member of the attractor set. Therefore $W = (w_0, \{bw_0\}, \ldots, \{b^{P-1}w_0\})$, and W is a periodic attractor for the x sequence. Rationality of the attractor points is demonstrated by noting the periodicity condition $w_0 = \{b^P w_0\}$, which implies that for some integer m we have $w_0 = m/(b^P - 1)$, and similarly for the other $w_i \in W$. ☐

Theorem 2.14. *If the sequence (x_n) as defined for Hypothesis A has a finite attractor W, then W is a periodic attractor, and each element of W is rational.*

Proof. Here the sequence x is given by $x_0 = 0$, and $x_n = bx_{n-1} + r_n$, with $r_n \to 0$ (since $\deg p < \deg q$). Let $W = \{w_0, w_1, \ldots, w_{P-1}\}$ be the finite attractor for x. Let $d = \min_{0\le i,j<P}(\|w_i - w_j\|)$, and choose $\varepsilon < d/(4b + 4)$. Let W_ε be the set of all z in $[0,1)$ such that $\|z - w_i\| < \varepsilon$ for some $0 \le i < P$. Then we know that there is some $K'(\varepsilon)$ such that for all $k > K'$ we have $x_k \in W_\varepsilon$ and $|r_k| < \varepsilon$. Let K be the first $k > K'$, such that $\|x_k - w_0\| < \varepsilon$. We then have (again we use the dilated-norm rule from the start of the present section)

$$\begin{aligned}\|x_{K+1} - bw_0\| &= \|bx_K + r_{K+1} - bw_0\| \\ &\le b\|x_K - w_0\| + \varepsilon < (b+1)\varepsilon < d/4.\end{aligned}$$

The remainder of the proof of this result follows the second paragraph of the proof of Theorem 2.13. ☐

Now we are prepared to establish one final, important result for this stage of the analysis:

Theorem 2.15. *The sequence $(\{b^n\alpha\})$ has a finite attractor if and only if α is rational.*

Proof. Assume that the sequence $(\{b^n\alpha\})$ has a finite attractor. By Theorem 2.13 it then has a periodic attractor. In Definition 2.10 let K be the index corresponding to $\varepsilon = 1/(4b)$, and set $h = |x_K - w_0|$. Suppose $h > 0$. Then let $m = \lfloor \log_b(\varepsilon/h) \rfloor$, and note that $b^m h < \varepsilon < b^{m+1}h < b\varepsilon < 1/4$. Thus we can write (once again using the dilated-norm rule)

$$\begin{aligned}\|x_{K+m+1} - w_{m+1 \bmod P}\| &= \|b^{m+1}x_K - b^{m+1}w_0\| \\ &= b^{m+1}\|x_K - w_0\| \\ &= b^{m+1}h > \varepsilon.\end{aligned}$$

But this contradicts Definition 2.10. Thus we conclude that $h = 0$, so that $x_{K+k} = w_{k \bmod P}$ for all $k \ge 0$. In other words, after at most K initial digits, the base-b expansion of α repeats with period P, so that α is rational. As for the converse, $\alpha = p/q$ rational implies the sequence $(b^n p/q) = (((pb^n) \bmod q)/q)$ is periodic, having in fact the period 1 for $\alpha = 0$ and, for p/q in lowest terms, the period of the powers of b modulo q. ☐

3. THE DYNAMICAL PICTURE

Before giving a proof for Theorem 1.1, we prove:

Theorem 3.1. *Given $p, q \in Z[X]$, with q having no positive integer zeros and $0 \le \deg p < \deg q$, and* *given the integer $b \geq 2$, define a real number α via a generalized polylogarithm series*

$$\alpha = \sum_{k=1}^{\infty} \frac{1}{b^k} \frac{p(k)}{q(k)}.$$

Then α is rational if and only if the sequence (x_n), where

$$x_n = \left(bx_{n-1} + \frac{p(n)}{q(n)}\right) \bmod 1$$

has a finite (alternatively, periodic) attractor.

Proof. Theorem 2.15 we know that the sequence $(\{b^n\alpha\})$ has a periodic attractor if and only if α is rational. Following the BBP strategy, we can write

$$\{b^n\alpha\} = \left(\sum_{k=1}^{n} \frac{b^{n-k}p(k)}{q(k)} + \sum_{k=n+1}^{\infty} \frac{b^{n-k}p(k)}{q(k)}\right) \bmod 1$$
$$= (x_n + t_n) \bmod 1,$$

where x is defined by $x_0 = 0$ and the recursion

$$x_n = bx_{n-1} + \frac{p(n)}{q(n)},$$

with the "tail" sequence t given by

$$t_n = \sum_{k=1}^{\infty} \frac{1}{b^k} \frac{p(k+n)}{q(k+n)}.$$

Provided that $\deg p < \deg q$ as in Hypothesis A, given any ε there is some n such that

$$\left|\frac{p(k+n)}{q(k+n)}\right| < \varepsilon$$

for all $k \geq 1$. For such n, we have

$$|t_n| < \varepsilon \sum_{k\geq 1} b^{-k} = \varepsilon/(b-1) \leq \varepsilon.$$

Thus t_n converges to zero as $n \to \infty$. Hence it follows from Theorem 2.11 that (x_n) has a periodic attractor if and only if α is rational. □

Theorem 3.1 does not depend on Hypothesis A; we merely use the stated conditions of Hypothesis A in the exposition.

Proof of Theorem 1.1. The constants π, $\log 2$ and $\zeta(3)$ are known to be irrational. An infinite series formula of the form required in Theorem 3.1 exists for each of them (see equations (5–1)–(5–4)). The conclusions of Theorem 1.1 (assuming Hypothesis A) follow immediately. □

Further, as we will see in the next section, the conclusions of Theorem 1.1 apply to quite a few other generalized polylogarithmic constants.

We now lay out some preliminary observations on the kinds of chaotic dynamical maps under discussion. Equation (1–2) (see also (5–1)) gives the sequence $x = (x_n)$ for $\log 2$: $x_0 = 0$ and

$$x_n = 2x_{n-1} + \frac{1}{n}.$$

The first few iterates are

$$\left(0, 0, \tfrac{1}{2}, \tfrac{1}{3}, \tfrac{11}{12}, \tfrac{1}{30}, \tfrac{7}{30}, \tfrac{64}{105}, \tfrac{289}{840}, \ldots\right).$$

We remark that these numbers are precisely the (rational) coefficients in the Taylor expansion of

$$g(t) = \frac{-\log(1-t)}{1-2t},$$

reduced modulo 1. However, this observation evidently brings nothing new. Similarly, the dynamical $\log 2$ iteration can be modeled in terms of a "matrix-factorial" system. In fact, if we decompose $x_n = f_n/g_n$ then the iteration takes the form

$$n! \begin{bmatrix} f_n \\ g_n \end{bmatrix} = \begin{bmatrix} 2n & 1 \\ 0 & n \end{bmatrix}! \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

where the matrix-factorial is simply the left-right product of matrices with internal parameter n running down to 1, as with integer factorials. Though a theory of matrix-factorials might bring some insight, such algebra may merely be a symbolic reformulation.

Suppose one computes the binary sequence $y_n = \lfloor 2x_n \rfloor$, where (x_n) is the sequence associated with $\log 2$ (see above). Assuming Hypothesis A, Theorem 1.1 tells us, in effect, that (y_n) eventually agrees quite well with the true sequence of binary digits of $\log 2$ — so much so that properties such as density and equidistribution, if possessed by one sequence, are possessed by the other. In computations that we have done, we have found that the sequence (y_n) disagrees with 15 of the first 200 binary digits of $\log 2$, but in only one position over the range 5000 to 8000.

For the constant π, the associated sequence is given by $x_0 = 0$ and x_n as in (1–3); see also equation (5–2). As with $\log 2$, one can compute the hexadecimal digit sequence $y_n = \lfloor 16x_n \rfloor$. When this is done, a remarkable phenomenon is observed: the sequence (y_n) appears to perfectly (not just approximately) produce the hexadecimal digits of π. We have computed over 100,000 hexadecimal digits using this recursion, and have found no discrepancies with the true hexadecimal digits of π.

Conjecture 3.1. *The sequence $(\lfloor 16x_n \rfloor)$, where (x_n) is the sequence of iterates in the above dynamical map for π, yields the correct hexadecimal expansion. In other words, the ignored tail terms never change a digit.*

Evidently this phenomenon arises from the fact that in the sequence here associated with π, the perturbation term r_n is summable, whereas the corresponding expression for $\log 2$, namely $r_n = 1/n$, is not summable. In particular, the term t_n of the tail sequence for π is given by

$$\sum_{k=n+1}^{\infty} \frac{120k^2 - 89k + 16}{16^{k-n}(512k^4 - 1024k^3 + 712k^2 - 206k + 21)},$$

which is approximately equal to the first summand (for $k = n+1$); we have

$$\sum_{n=1}^{\infty} t_n \approx 0.01579\ldots.$$

This figure (multiplied by 16) can be thought of as an "expected value" of the total number of base-16 digit errors likely to be observed in the recursive sequence for π. The small value indicates it is unlikely that any carries or other errors will be observed. The comparable figure for $\log 2$ is infinite, indicating that discrepancies can be expected to appear indefinitely.

4. REMARKS ON HYPOTHESIS A

Now we turn to the question: "what motivates Hypothesis A in its particular form?" One may wonder to what extent the conditions of the hypothesis, and perforce Theorem 1.1, can be relaxed. For example, Hypothesis A allows only *rational* iterates (x_n). Consider again the dynamical sequence associated with $\log 2$, namely the sequence given by $x_0 = 0$, perturbation $r_n = 1/n$, and recursion

$$x_n = 2x_{n-1} + \frac{1}{n}$$

(see equations (1–1) and (5–1)). Now other rational choices of x_0 may well result in an equidistributed sequence (x_n). However, if one starts with x_0 set equal to the irrational number $1 - \log 2 = 0.3068\ldots$, then the sequence (x_n) converges to the single limit point zero, so that the full sequence (x_n) is in this case not even dense, much less equidistributed. This fact underscores the essentially chaotic nature of recursions of this form — an extreme sensitivity to initial conditions is definitely present.

Along such lines, suppose that the class of perturbation terms r_n in Hypothesis A were enlarged to include expressions such as $r_n = n/2^{n^2-n}$, which is not, of course, a rational-polynomial function. It turns out that in this case the associated constant, namely

$$\alpha = \sum_{n=1}^{\infty} \frac{n}{2^{n^2}},$$

is digit-dense to base 2 and hence irrational, yet *not* normal to base 2. This and some more general constants of the form $\sum P(n)/2^{Q(n)}$ with P, Q polynomial and $0 < \deg P < \deg Q$, are discussed in our separate paper [Bailey and Crandall 2001].

One might guess that it is the very fact of rapid decay in $r_n = n/2^{n^2-n}$ that causes a nonequidistributed sequence of dynamical iterates. But this line of thought is imperfect. Rapid decay can be expected (it is difficult to be rigorous here) to allow, in many cases, equidistribution of the iterates. One attractive example is

$$x_n = 4x_{n-1} + \frac{1}{(2n)!}\left(\frac{4n+1}{4n+2}\right),$$

whose equidistribution mod 1 would imply the base-4 normality of the transcendental $1/\sqrt{e}$; while an algebraic constant arises from the iterates

$$x_n = 4x_{n-1} + \frac{(2n-3)!!}{n!},$$

whose equidistribution mod 1 would establish base-4 normality of the constant $1 - 1/\sqrt{2}$ and hence that of $\sqrt{2}$ itself (by Theorem 2.5, α normal implies that each of $\pm\alpha \pm 1$ is normal). Given such examples of rapidly decaying perturbations, it is perhaps amusing that, evidently, one still cannot attempt to associate very rapidly decaying perturbation functions with normal numbers. Some of the (perhaps likely to be) abnormal numbers described in [Martin 2000], such as the Pomerance number

$$P = \sum_{n=1}^{\infty} \frac{1}{n!^{n!}}$$

can of course be generated on the basis of extremely rapidly decaying perturbation functions.

Again on the subject of the decay rate of perturbation, consider that the binary Champernowne

$$C_2 = 0.11011100101110111\ldots\ _2,$$

which is known to enjoy base-2 normality, can be written in the intriguing form

$$C_2 = \sum_{n=1}^{\infty} \frac{1}{2^n} r_n = \sum_{n=1}^{\infty} \frac{1}{2^n} \frac{n}{2^{f(n)}}$$

where the indicated exponent is

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

Thus the decay rate of the perturbation r_n is slightly faster than exponential, showing that at least this (admittedly artificial) constant C_2 has the normality property together with a decay more rapid than polynomial.

Thus the decay rate of the dynamical perturbation function r_n seems to be somewhat irrelevant. Still, if we could establish some results in regard to the character of dynamical sequences for certain perturbation functions outside the class of Hypothesis A, a beautiful vista could emerge. As just one example of an interesting departure from Hypothesis A, said departure involving a slowly decaying perturbation function, consider the following expansion for the Euler constant [Beeler et al. 1972, item 120, p. 55]:

$$\gamma - \frac{1}{2} = \sum_{k=1}^{\infty} \frac{1}{2^{k+1}} \left(-1 + \sum_{j=0}^{k-1} \binom{2^{k-j}+j}{j}^{-1} \right).$$

Here the relevant perturbation function is $r_k = (1/2)(-1+\sum)_k$ and exhibits a slow decay (evidently: $r_n \sim 1/\sqrt{n}$). Needless to say, any results on the distribution of the corresponding dynamical iterates would have application to the study of the still-mysterious γ.

5. GENERALIZED POLYLOGARITHM FORMS

We now discuss some specific examples of interesting constants belonging to the class of numbers relevant to Hypothesis A.

The BBP algorithm for resolving isolated digits of a constant works for constants defined by what could be called generalized polylogarithm forms. It turns out that the forms of interest can all be described as superpositions of the classical Lerch–Hurwitz zeta function, itself defined as

$$L(s, z, \delta) = \sum_{n=0}^{\infty} \frac{z^n}{(n+\delta)^s},$$

A special instance is the standard polylogarithm Li_s defined by

$$\mathrm{Li}_s(z) = \sum_{n=1}^{\infty} \frac{z^n}{n^s} = zL(s, z, 1),$$

for which a considerable literature has sprung over the years, notably in regard to integer indices s. To unify our approach to generalized polylogarithms, we next cite three expansion forms, each of which has appeared in the literature. The "rational-polynomial" or R-form is the generalized polylogarithm value

$$R(b, p/q) = \sum_{m=0}^{\infty} \frac{p(m)}{q(m)} \frac{1}{b^m}$$

for polynomials p, q. The notation $R'(b, p/q)$ will be used to denote this expression with the summation starting at $m = 1$. (Note that R' is the entity that figures naturally into Theorem 3.1 and accordingly into the proof of Theorem 1.1.) Then there is what we shall call a "periodic" or P-form,

$$P(s, b, d, A) = \sum_{n=0}^{\infty} \frac{1}{b^n} \sum_{c=1}^{d} \frac{A_c}{(dn+c)^s},$$

where $A = (A_c)$ is a finite sequence of d elements. A third form is what we shall call the "Broadhurst" or B-form [Broadhurst 1998]:

$$B(s, b, \rho, \bar{a}) = \sum_{n=1}^{\infty} \frac{1}{b^{\lfloor (n+1)\rho \rfloor}} \frac{a_n}{n^s},$$

where $\bar{a} = (a_n)$ is an infinite periodic sequence and ρ is positive real.

It is evident that these functions have at least some interrelations; for example when s is an integer we have

$$\begin{aligned}\mathrm{Li}_s\Big(\frac{1}{b}\Big) &= R'(b,1/n^s) = \frac{1}{b}R(b,1/(n+1)^s)\\ &= \frac{1}{b}P(s,b,1,(1)) = bB(s,b,1,(\overline{1})),\end{aligned}$$

where here and elsewhere $(\overline{a_1,a_2,\dots,a_P})$ denotes a periodic sequence with indicated pattern. However, it is an important observation with respect to our dynamical model that the R,P,B forms are well-connected even for very general parameters, in the following manner:

- We have in general
$$R\left(b,\frac{p(n)}{q(n)}\right) = bR'\left(b,\frac{p(n-1)}{q(n-1)}\right).$$
- A P-form can often be converted to an R-form. In particular, when s is a positive integer and the A sequence is nonvanishing, one can combine fractions in the P definition to produce a suitable rational-polynomial multiplier p/q in the R definition and this procedure gives rise to an admissible perturbation $r_n = p(n)/q(n)$ for Hypothesis A.
- Conversely, for $p,q\in Z[X]$ one can often split easily into partial fractions, to arrive at a P-form. Thus in many circumstances of interest P and R are interchangeable forms.
- When $\rho = e/f$ is rational the B-form can be cast as a P-form, via the basic relation
$$B(s,b,\rho,\bar a) = \sum_{n=0}^{\infty}\frac{1}{b^{ne}}\sum_{g=1}^{n}\frac{a_{nf+g}}{(nf+g)^s\, b^{\lfloor (g+1)e/f\rfloor}}.$$
- The connection back to the Lerch–Hurwitz function is best seen via the P-form; in fact,
$$P(s,b,d,A) = d^{-s}\sum_{c=1}^{d}A_c L\Big(s,\frac{1}{b},\frac{c}{d}\Big),$$
and this relation embodies the superposition effect to which we have alluded.

We now establish a compendium of generalized polylogarithm values, with a view to application of Hypothesis A. We have, as mentioned in Section 1, the classical expansion of $\log 2 = \mathrm{Li}_1(1/2)$:

$$\log 2 = \sum_{n=1}^{\infty}\frac{1}{n2^n} = R'(2,1/n) \tag{5–1}$$

With some simple algebraic manipulations, similar base 2 series, suitable for this analysis, can be given for $\log 3$, $\log 5$, $\log 7$, $\log 11$, $\log 31$ and other logarithms [Bailey et al. 1997]. Less trivial but well known higher-order polylogarithm evaluations include

$$\begin{aligned}\pi^2 - 6\log^2 2 &= 12R'(2,1/n^2),\\ -2\pi^2\log 2 + 4\log^3 2 + 21\zeta(3) &= 24R'(2,1/n^3).\end{aligned}$$

One of the historical driving relations for the original BBP algorithm development was the following [Bailey et al. 1997], for which we have intentionally written out some conversion steps to exemplify once again the interconnection of forms:

$$\begin{aligned}\pi &= 8B\big(1,2,\tfrac12,(\overline{1,0,0,-1,-1,-1,0,0})\big)\\ &= 8\sum_{n=1}^{\infty}\frac{1}{n}\frac{1}{2^{\lfloor (n+1)/2\rfloor}}(\overline{1,0,0,-1,-1,-1,0,0})\\ &= \sum_{n=0}^{\infty}\frac{1}{16^n}\left(\frac{4}{8n+1}-\frac{2}{8n+4}-\frac{1}{8n+5}-\frac{1}{8n+6}\right)\\ &= P\big(1,16,8,(4,0,0,-2,-1,-1,0,0)\big)\\ &= R(16,p/q),\end{aligned} \tag{5–2}$$

with the rational polynomial here defined as

$$\frac{p(n)}{q(n)} = \frac{47+151n+120n^2}{15+194n+712n^2+1024n^3+512n^4}.$$

The sequence for π given as (1–3) is obtained via the above translation rule for converting $R\to R'$.

Moreover, this simple, base-16 prescription for π is not unique — one also has the following equality, first discovered by Ferguson and Hales [1997] and independently by Adamchik and Wagon [1997]:

$$\pi = 4B\big(1,2,\tfrac12,(\overline{1,1,1,0,-1,-1,-1,0})\big)$$

This formula may be written in the P-form notation as

$$\pi = \tfrac14 P\big(1,16,8,(8,8,4,0,-2,-2,-1,0)\big).$$

Actually, various expansions for π arise from the following formal identity, valid for $t \in (0, \pi)$ [Crandall 1996]:

$$\frac{\pi}{2} - t = \sum_{n=1}^{\infty} \cos^n t \frac{\sin(nt)}{n}.$$

One may use rational multiples of π such as $t = \pi/3$ to achieve expressions such as

$$\begin{aligned}\pi &= 2\sqrt{27}\, B(1, 2, 1, (\overline{1, 1, 0, -1, -1, 0})) \\ &= \sqrt{27} R(64, p/q),\end{aligned}$$

where now the rational polynomial is

$$\frac{p(n)}{q(n)} = \frac{193+1188n+2097n^2+1134n^3}{320+3744n+14112n^2+20736n^3+10368n^4}.$$

This $t = \pi/3$ value thus yields a BBP scheme for extraction of individual base-64 digits; and perforce, includes $\pi\sqrt{3}$ in the galaxy of normal numbers under Hypothesis A. The use of $t = \pi/4$ gives a previous expansion of this section. The choice $t = \pi/5$ gives a peculiar expansion. Using the exact relation $\cos(\pi/5) = \tau/2$ with $\tau = (1 + \sqrt{5})/2$ the golden mean of antiquity, we find

$$\pi = \frac{5^{5/4}}{3\sqrt{\tau}} \sum_{n=1}^{\infty} \frac{1}{n} \left(\frac{\tau}{2}\right)^n (\overline{1, \tau, \tau, 1, 0, -1, -\tau, -\tau, -1, 0}).$$

Fascinating as this relation may be, it falls into the category of an irrational-base expansion (i.e., the BBP base would be $2/\tau = 1.23606\ldots$), and applications if any are unclear. Similarly, choosing $t = \pi/6$ results in a base-$\frac{4}{3}$ expansion, which likewise is of dubious benefit.

The more peculiar base expansions point to the open question of whether a BBP implementation for π can be performed in the culturally important base 10. The best we can seem to do in this regard was uncovered during the present work, and runs as follows. Choosing parameter $t = \cos^{-1}(1/\sqrt{20})$ one can derive

$$\frac{\pi}{2} = \sin^{-1} \tfrac{9}{10} + \sqrt{19} \sum_{n=1}^{\infty} D_{n-1} \frac{1}{n10^n},$$

with initial coefficients $D_0 = D_1 = 1$, and the rest determined via the recurrence $D_{n+1} = D_n - 5D_{n-1}$. It is intriguing that a variant of the original BBP algorithm can be fashioned on the idea that the D_n comprise a Lucas sequence, and as is known, evaluations of sequence elements mod n can be effected via exponential-ladder methods. Incidentally, there are other expansions that do involve the decimal base in a simpler fashion. One is

$$\log \tfrac{9}{10} = -\sum_{n=1}^{\infty} \frac{1}{n10^n},$$

which admits straightforward computation of isolated decimal digits [Bailey et al. 1997]. Thus, on Hypothesis A, $\log \frac{9}{10}$ is normal to base 10, since it is known to be irrational. More exotic base-10 relations include

$$\log \tfrac{1111111111}{387420489} = 10^{-8} \sum_{n=0} \frac{1}{10^{10n}} \left(\frac{10^8}{10n+1} + \frac{10^7}{10n+2} + \cdots + \frac{1}{10n+9} \right),$$

which we found during the course of the present research, as explained later.

In regard to π expansions, it is also known that

$$\pi^2 = 32B(2, 2, \tfrac{1}{2}, (\overline{1, -1, -1, -2, -1, -1, 1, 0})),$$

and

$$\pi^2 = \tfrac{9}{8} P(2, 16, 6, (16, -24, -8, -6, 1, 0)),$$

and thus one may address π^2 itself within the theory. We should add that a base 3 series is known for π^2, due to Broadhurst [1999]:

$$\pi^2 = \tfrac{2}{27} P\big(2, 729, 12, (243, -405, -81, -27, -72, -9, -9, -5, 1)\big).$$

Similar high-order generalizations can be given for $\log^2 2$ and for the Catalan constant G, as in

$$G - \tfrac{1}{8}\pi \log 2 = B\big(2, 2, \tfrac{1}{2}, (\overline{1, 1, 1, 0, -1, -1, -1, 0})\big).$$

Broadhurst [1998] also developed forms for $\zeta(3)$ and $\zeta(5)$, for example

$$\begin{aligned}\zeta(3) = \tfrac{48}{7} B\big(3, 2, \tfrac{1}{2}, (\overline{1, -7, -1, 10, -1, -7, 1, 0})\big) \\ + \tfrac{32}{7} B\big(3, 2, \tfrac{3}{2}, (\overline{1, 1, -1, -2, -1, 1, 1, 0})\big).\end{aligned}$$

However, recall the convenient result that any superposition of B functions (with appropriate, rational "ρ" parameters and integer power arguments s) can be cast as a single R function. With this in mind we achieve, after suitable symbolic manipulation, a base-4096 expansion

$$\zeta(3) = R(4096, p/q), \tag{5–3}$$

where the specific rational function is defined by the formidable expression

$$\begin{aligned}\frac{7p(m)}{8q(m)} &= \frac{3}{(1+24m)^3}-\frac{21}{(2+24m)^3}+\frac{12}{(3+24m)^3}+\frac{15}{(4+24m)^3}-\frac{3}{4(5+24m)^3}+\frac{3}{2(6+24m)^3}\\ &\quad+\frac{3}{8(7+24m)^3}-\frac{3}{2(9+24m)^3}-\frac{21}{16(10+24m)^3}-\frac{3}{32(11+24m)^3}-\frac{3}{4(12+24m)^3}-\frac{3}{64(13+24m)^3}\\ &\quad-\frac{21}{64(14+24m)^3}-\frac{3}{16(15+24m)^3}+\frac{3}{256(17+24m)^3}+\frac{3}{128(18+24m)^3}-\frac{3}{512(19+24m)^3}\\ &\quad+\frac{15}{256(20+24m)^3}+\frac{3}{128(21+24m)^3}-\frac{21}{1024(22+24m)^3}+\frac{3}{2048(23+24m)^3}.\end{aligned}$$

For $\zeta(5)$ one ends up working with yet a larger base ($b = 2^{60}$):

$$\begin{aligned}\zeta(5) &= \tfrac{18432}{62651}B(5,2,\tfrac{1}{2},(\overline{31,-1614,-31,-6212,-31,-1614,31,74552}))\\ &\quad+\tfrac{14336}{62651}B(5,2,\tfrac{3}{2},(\overline{173,284,-173,-457,-173,284,173,-111}))\\ &\quad-\tfrac{1511424}{62651}B(5,2,\tfrac{5}{2},(\overline{1,0,-1,-1,-1,0,1,1}))\\ &= R(2^{60},p/q),\end{aligned} \tag{5–4}$$

for a certain rational perturbation p, q with $\deg p = 590$ and $\deg q = 595$. Nevertheless these machinations reveal that $\zeta(3)$ and $\zeta(5)$ can be written in terms of R-function values appropriate to Hypothesis A.

No eventually periodic sequence can be uniformly distributed mod 1, so this case must be treated separately in Hypothesis A. So one might ask under what conditions, if any, on $p(n)$, $q(n)$, and $b \geq 2$ is $\sum p(n)/q(n)b^{-n}$ rational? We now describe two different classes of generalized series that turn out to be rational.

The first case can be called the "telescoping" phenomenon. For example, any sum of the form

$$\sum_{n=1}^{\infty}\frac{1}{b^n}\left(\frac{b^m}{n}-\frac{1}{n+m}\right),$$

where m is a fixed positive integer, has a rational value due to elementary telescoping. For such sums, the corresponding dynamical iterations of Hypothesis A, with perturbation function $p(n)/q(n) = (b^m(n+m)-n)/(n(n+m))$, result in a periodic attractor. One could fashion a theory in which telescoping amounted to the formal relation

$$0 = \oint_C b^{-z}\frac{p(z)}{q(z)}\,dz,$$

where C is a contour starting at $+\infty + i$, circling the origin counterclockwise, and ending at $+\infty - i$. Unfortunately, this kind of formalism is only effective for telescoping *per se*. There is a different kind phenomenon that yields rational R-forms.

This second, and more profound class of exceptions we call the "Ferguson anomalies," involving a fascinating and evidently rare phenomenon. These anomalies are also known as "Zagier zeros," which involve polylogarithmic ladders [Broadhurst 2000]. We only know of a few genuinely different examples (note that mere translation of indices can turn one example, say a zero sum, into a rational sum giving nothing new). Here are three, where we write out the explicit partial fraction decomposition for the first example only:

$$\begin{aligned}0 &= P(1,16,8,(-8,8,4,0,8,2,-1,0))\\ &= \sum_{n=0}^{\infty}\frac{1}{16^n}\left(\frac{-8}{8n+1}+\frac{8}{8n+2}+\frac{4}{8n+3}+\frac{8}{8n+5}+\frac{2}{8n+6}-\frac{1}{8n+7}\right),\end{aligned}$$

$$0 = P(1,64,6,(16,-24,-8,-6,1,0)),$$

$$0 = P\big(1,4096,24,(0,0,0,0,-256,256,128,0,128,-128,-64,-64,0,-16,0,24,4,-4,-2,-2,-2,-3,1,0)\big).$$

David Broadhurst [2000] has enumerated several other anomalies of this type, some involving base 3.

The iterates for the above anomalies, with their rational polynomials as exhibited, are rapidly attracted to the single limit point zero. If one trivially translates such anomalous sums (for example by leaving off the leading term of the first case above, which results in the sum 97/105) then the dynamical iterates will become pseudoperiodic in the long run (in this example, the attractor set has 12 points, since 2 has order 12 modulo 105). In summary, under Hypothesis A, our generalized polylogarithmic constants tend to be either normal or rational, the latter instance covering the telescoping and Ferguson anomalies.

During the course of this work, and due mainly to theoretical attempts to resolve the Ferguson anomalies, we developed a procedure for analyzing certain generalized polylogarithms. Some of our results echo formulae found in the original BBP-algorithm work [Bailey et al. 1997] but tend to lead one into different research directions, for example into symbolic as opposed to numerical processing. To convey an idea of the kind of new relation we have in mind, we give some examples:

$$\tan^{-1}\tfrac{1}{2} = \frac{1}{8}\sum_{n=0}^{\infty} 16^{-n}\left(\frac{4}{4n+1} - \frac{1}{4n+3}\right),$$

which is not especially profound — it is the way this was derived that may be of interest. Then we have

$$\log 2 = \tfrac{2}{27}\sum_{n=0}^{\infty} 81^{-n}\left(\frac{9}{4n+1} + \frac{1}{4n+3}\right),$$

which conveniently enough will establish, on Hypothesis A, that $\log 2$ is normal to base 3. Alternatively, such a base-3 result can be gleaned from the simple formula

$$\log 2 = 6\sum_{n=1}^{\infty} \frac{1}{9^n(2n-1)}.$$

These relatively simple new examples all arose in our work not from PSLQ numerical experiments, but from a certain form for a specific polylogarithmic construction. First one obtains a closed form, involving base b and any positive integers d, c, for a typical component of the P-form:

$$\sum_{n=0}^{\infty} \frac{1}{b^n}\,\frac{1}{dn+c} = -\frac{1}{d}\, b^{c/d}\sum_{a=0}^{d-1} e^{-2\pi i a c/d}\log\left(1 - \frac{1}{b^{1/d}}e^{2\pi i a/d}\right),$$

which we call closed because the a sum is finite. But it is not the derivation (as foreshadowed in [Crandall 1996]) of this result that presents difficulty. It is what we do with this closed form that is the challenging epistemological issue. One success achieved by symbolic processing is the formula

$$\sum_{n=0}^{\infty} \frac{1}{b^{3n}}\left(\frac{b}{3n+1} + \frac{1}{3n+2}\right) = \tfrac{1}{3}b^2\log\frac{b^2+b+1}{b^2-2b+1},$$

which differs from most other formulae thus far, in that arbitrary bases b are here involved. Under Hypothesis A, every style of logarithm on the right for base $b \ge 2$ is normal to base b. Our procedure for moving from the finite, logarithmic sum to such results involved symbolic processing in the following way. Since the a sum above is patently real, one may split everything into real, imaginary parts and discard the latter. Then one may exploit exact trigonometric evaluations to arrive at new relations. Some selected examples of what this symbolic procedure can uncover are the following. For the peculiar base $b = 5^5$ we have

$$P\big(1, 5^5, 5, (0,5,1,0,0)\big) = \sum_{n=0}^{\infty} \frac{1}{5^{5n}}\left(\frac{5}{5n+2} + \frac{1}{5n+3}\right) = \tfrac{25}{2}\log\left(\tfrac{781}{256}\left(\frac{57-5\sqrt{5}}{57+5\sqrt{5}}\right)^{\sqrt{5}}\right).$$

This dampens the hope that a purely experimental mathematics approach (such as the use of PSLQ-based numerics: see [Ferguson et al. 1999]) will resolve any polylogarithm form; indeed, to discover the above example one would need to have in one's basis of possible terms not only quadratic surds as coefficients but also logarithms of such surds. By certain manipulations on the c-index of the logarithmic a-sum one can establish other relations such as the following, valid for integer $m \ge 2$:

$$P\big(1, m^m, m, (m^{m-2}, m^{m-3}, \ldots, m, 1, 0)\big) = \sum_{n=0}^{\infty} \frac{1}{m^{mn}}\sum_{c=1}^{m-1}\frac{m^{m-1-c}}{nm+c} = m^{m-2}\log\left(\frac{m^m-1}{(m-1)^m}\right).$$

It is this formula that yields, for $m = 10$, our aforementioned expansion for $\log((10^{10}-1)/9^{10})$. By adjusting the weights of the partial fraction components, one may also arrive at some obscure $\tan^{-1}$ evaluations. We have given one of the simpler cases (for $\tan^{-1}(1/2)$); yet one can also derive

$$P\big(1,3^3,3,(3,-1,0)\big) = \sum_{n=0}^{\infty} \frac{1}{27^n}\left(\frac{3}{3n+1} - \frac{1}{3n+2}\right) = 6\sqrt{3}\tan^{-1}\frac{\sqrt{3}}{7},$$

as well as $\tan^{-1}$ forms such as a curious construct that involves *quartic* irrationals:

$$P\big(1,5^5,5,(5^3,-5^2,5,-1,0)\big) = 2\cdot 5^{13/4}\left(\frac{1}{\sqrt{\tau}}\tan^{-1}\Big(\frac{5^{1/4}}{\sqrt{\tau}}\frac{233-329\sqrt{5}}{5938}\Big) + \sqrt{\tau}\tan^{-1}\Big(\frac{5^{1/4}}{\sqrt{\tau}}\frac{939+281\sqrt{5}}{5938}\Big)\right).$$

Whatever be the implications of such machinations, this construct is, on Hypothesis A, either rational (unlikely) or normal to base 5.

6. CONNECTION WITH PSEUDORANDOM NUMBER GENERATORS

We revisit once again what has been our canonical constant for present purposes, namely $\alpha = \log 2$. As in equation (1–4), we can write

$$\begin{aligned}\{2^n \log 2\} &= \left(\sum_{k=1}^{\infty}\frac{2^{n-k}}{k}\right) \bmod 1 \\ &= \left(\sum_{k=1}^{n}\Big(\frac{2^{n-k} \bmod k}{k}\Big) \bmod 1 + \sum_{k=n+1}^{\infty}\frac{2^{n-k}}{k}\right) \bmod 1 \\ &= (x_n + t_n) \bmod 1,\end{aligned}$$

where x_n and t_n denote the two sums as shown. Recall that our proof of Theorem 3.1 (and perforce, Theorem 1.1) depends on the fact that tail terms such as t_n vanish as $n \to \infty$. In this light, the sequence x can be considered to be a pseudorandom number generator (PRNG), with values in $[0,1)$:

$$x_n = \left(\frac{2^{n-1} \bmod 1}{1} + \frac{2^{n-2} \bmod 2}{2} + \frac{2^{n-3} \bmod 3}{3} + \cdots + \frac{1}{n}\right) \bmod 1.$$

(The first term vanishes; we include it only for notational completeness.) One can think of this as a cascaded PRNG, in which an ever-increasing number of distinct linear congruential PRNGs, namely the terms $(2^{n-m} \bmod m)/m$, are summed together mod 1. We might then attempt to characterize the behavior of the sequence (x_n) in terms of the generator's properties. For example, we can investigate the period of this type of cascaded generator.

There are difficulties with this approach, not the least of which is the fact that a theory of cascaded PRNGs is not commonly discussed, and upon preliminary investigation it is evident that open problems abound. For one thing, there are questions about *fixed* sums of PRNGs that are yet open, such as the precise statistics of the sum of just two standard PRNGs. Moreover, whereas for fixed, large n the initial terms corresponding to $(2^{n-m} \bmod m)/m$ may well be on their way into stable statistical cycles, the latter terms ending $4/(n-2) + 2/(n-1) + 1/n$ are "just getting started," as it were. So the cascaded PRNG does, in some sense, continue to "seed itself" as n increments. These difficulties may be insurmountable. Nevertheless, some partial results pertaining to random generators are obtained in [Bailey and Crandall 2001], where we investigate a statistical picture as a kind of complement to the present, dynamical one.

7. CONCLUSIONS AND OPEN PROBLEMS

We have outlined above what we believe to be some new approaches to the age-old question of the statistical randomness of the digits in the expansions of several well-known mathematical constants. We acknowledge that our analysis may have raised more questions than it has answered, and we do not expect that the open hypotheses and conjectures will be quickly or easily resolved. We only hope that these results will stimulate further research in the field and lead to a greater understanding of the issues. Here is a sampling of the open problems in this arena:

1. Is there a natural, or even believable, generalization of the perturbation function r_n in Hypothesis A? We saw at the end of Section 3 that the particular decay rate of r_n does not have an obvious connection with the normality properties of the as-

sociated constants. This subject is taken up further in [Bailey and Crandall 2001].

2. Is there a way to connect the dynamical picture, as embodied in Hypothesis A and our various observations thereupon, with the celebrated Weyl theorem that (x_n) is equidistributed if and only if

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=0}^{N-1} e^{2\pi i h x_n} = 0$$

for every integer $h \neq 0$? That the x_n contain powers b^n for base b prevents any easy manipulation of the exponential sum.

3. How does one bring to bear all of the historical achievements from ergodic theory and the theory of chaotic-dynamical maps? We have barely touched upon a few isolated connections. Everything from Lyapunov exponents to fractal dimension has, let us say *a priori*, a possible role. Along this line, J. Lagarias [2001] has recently demonstrated intriguing connections between our theory, ergodic theory, the theory of G-functions and a conjecture by Furstenberg.

4. Can one develop a satisfactory theory of "Ferguson anomalies," namely those instances in which a generalized polylogarithm series has a rational sum, and yet elementary telescoping does not occur?

5. Can we obtain formal bounds on the lengths of periods produced by cascaded PRNGs, even for the special case of $\log 2$? Can we obtain further results on the statistics of PRNG sequences, such as limits on the deviations of frequencies of digit strings from their expected values? Again this is touched upon in a companion paper [Bailey and Crandall 2001].

6. Is there cryptographic significance to the present notion of digit randomness? It is well known in cryptographic circles that chaos generators are highly (and rightfully) suspect as random generators, and also that linear-congruential generators have been "broken" (in fact, many polynomial-recursive generators have been broken as well). Still, do we not believe that the hexadecimal digits of π should be cryptographically secure (given an unknowable starting position, say), and if yes, then does not Conjecture 3.1 imply that a fairly simple dynamical map should produce secure digits? We do admit that in this regard one must recognize precision issues; i.e., to go very far out in a π expansion, nonlinear — albeit efficient in the sense of the BBP algorithm — work must be expended. Still, one might contemplate the notion of taking the rational dynamical iterates x_k and reducing both numerator and denominator modulo p for large prime p, in this way maintaining linear control over precision for all iterates. Then again, one could "seed" such a cryptographic generator with an adroitly obscure choice of rational perturbation r_k, and so on.

ACKNOWLEDGMENTS

We are grateful to J. Borwein, P. Borwein, K. Briggs, D. Broadhurst, J. Buhler, D. Copeland, M. Jacobsen, J. Lagarias, R. Mayer, S. Plouffe, A. Pollington, C. Pomerance, J. Shallit, M. Trott, S. Wagon, T. Wieting and S. Wolfram for theoretical and computational expertise throughout this project.

We would like to express our delight at discovering just how far one may push a state-of-the-art symbolic processor of today to aid in algebraic development; we were enormously impressed with the powers of Mathematica for that purpose, and hereby thank all of the mathematicians and engineers who have made that comprehensive package available. We also wish to acknowledge H. Ferguson for his amazing PSLQ integer relation algorithm, which we used heavily in our investigations.

We thank a reviewer for incisive remarks of such quality that the very design of this and subsequent papers was positively affected.

REFERENCES

[Adamchik and Wagon 1997] V. Adamchik and S. Wagon, "A simple formula for π", *Amer. Math. Monthly* **104**:9 (1997), 852–855.

[Bailey and Crandall 2001] D. H. Bailey and R. E. Crandall, "Random generators and normal numbers", preprint, 2001.

[Bailey et al. 1997] D. Bailey, P. Borwein, and S. Plouffe, "On the rapid computation of various polylogarithmic constants", *Math. Comp.* **66**:218 (1997), 903–913.

[Beeler et al. 1972] M. Beeler, R. W. Gosper, and R. Schroeppel, "HAKMEM", Memo AIM-239, Mass. Inst. Technology AI Lab, Cambridge (MA), 1972.

[Borwein et al. 2000] J. M. Borwein, D. M. Bradley, and R. E. Crandall, "Computational strategies for the Riemann zeta function", *J. Comput. Appl. Math.* **121**:1-2 (2000), 247–296. See http://www.cecm.sfu.ca/preprints/1998pp.html.

[Broadhurst 1998] D. J. Broadhurst, "Polylogarithmic ladders, hypergeometric series and the ten millionth digits of $\zeta(3)$ and $\zeta(5)$", preprint, 1998. See http://arxiv.org/abs/math/9803067.

[Broadhurst 1999] D. J. Broadhurst, "Massive 3-loop Feynman diagrams reducible to SC* primitives of algebras of the sixth root of unity", *Eur. Phys. J. C Part. Fields* **8**:2 (1999), 313–333. See http://arxiv.org/abs/hep-th/9803091.

[Broadhurst 2000] D. J. Broadhurst, "Conjecture on integer-base polylogarithmic zeros motivated by the cunningham project", preprint, 2000.

[Cassels 1959] J. W. S. Cassels, "On a problem of Steinhaus about normal numbers", *Colloq. Math.* **7** (1959), 95–101.

[Champernowne 1933] D. G. Champernowne, "The construction of decimals normal in the scale of ten", *J. London Math. Soc.* **8** (1933), 254–260.

[Copeland and Erdős 1946] A. H. Copeland and P. Erdős, "Note on normal numbers", *Bull. Amer. Math. Soc.* **52** (1946), 857–860.

[Crandall 1996] R. E. Crandall, *Topics in advanced scientific computation*, Springer, New York, 1996.

[Ferguson et al. 1999] H. R. P. Ferguson, D. H. Bailey, and S. Arno, "Analysis of PSLQ, an integer relation finding algorithm", *Math. Comp.* **68**:225 (1999), 351–369.

[Kuipers and Niederreiter 1974] L. Kuipers and H. Niederreiter, *Uniform distribution of sequences*, Wiley-Interscience, New York, 1974.

[Lagarias 2001] J. C. Lagarias, "On the normality of fundamental constants", *Experiment. Math.* **10**:2 (2001).

[Martin 2000] G. Martin, "Absolutely abnormal numbers", preprint, 2000. See http://arxiv.org/abs/math/0006089/.

[Niven 1956] I. Niven, *Irrational numbers*, Math. Assoc. of America and Wiley, New York, 1956.

[Percival 2000] C. Percival, "The quadrillionth bit of pi is '0"', preprint, 2000. See http://cecm.sfu.ca/pihex/announce1q.html.

David H. Bailey, Lawrence Berkeley National Laboratory, Berkeley, CA 94720, United States (dhbailey@lbl.gov)

Richard E. Crandall, Center for Advanced Computation, Reed College, Portland, OR 97202, United States (crandall@reed.edu)

Received March 17, 2000; accepted in revised form October 4, 2000