DYNAMICAL SYSTEMS AND NORMAL NUMBERS:

QUALITATIVE AND COMPUTATIONAL ASPECTS

DOCTORAL THESIS
ADRIAN-MARIA SCHEERER

Für meine Familie

I am indebted to:

Prof. Robert Tichy
Hermine Panzenböck
Irene Wilfinger
the FWF

Verónica Becher
Mike Bennett
Yann Bugeaud
Manfred Madritsch
Uri Shapira
Theodore Slaman

Christian Elsholtz
Wolfang Steiner
Thomas Stoll
Jörg Thuswaldner
Joseph Vandehey
Johannes Wallner

Alina
Clara
Edith
Karin
Molly
Rafaelis
Robert
Wilhelm

Contents

Introduction

This thesis deals with real numbers whose expansions to a base are random (in a sense made precise below). The introduction is aimed at giving a short overview over the field and an outline of our work in that area. We do not wish to give an exhausting review of all existing literature but rather refer to the books [42, 59, 82] for further reference. We devote two small sections to normal numbers in the theory of computing as well as to a fractal-geometric perspective on normal numbers as an invitation for the reader to further pursue these topics.

In Chapter 2, I briefly describe the results I have obtained. This is followed by the original research papers [18, 25, 91, 113–115].

1.1. **Definition and first results.** Normal numbers have been defined by Borel in 1909. His original definition is as follows. A real number $x \in [0, 1)$ is called *simply normal to base* b, $b \geqslant 2$ an integer, if in its b-ary expansion

$$x = \sum_{n \geqslant 1} a_n b^{-n},\ a_n \in \{0, \ldots, b-1\}$$

every digit $d \in \{0, 1, \ldots b-1\}$ appears with the expected frequency $\frac{1}{b}$. The number x is called *normal to base* b if each of x, bx, b^2x, ... is simply normal to every base b, b^2, b^3, ...

We will work the following equivalent definition (for these formulations see e.g. Bugeaud's book [42, Chapter 4]).

The number x is called *normal to base* b, $b \geqslant 2$ an integer, if in its b-ary expansion all finite combinations of digits appear with the expected frequency, i.e. if for all $k \geqslant 1$ and all $d \in \{0, \ldots, b-1\}^k$,

$$\lim_{N \to \infty} \frac{1}{N} |\{1 \leqslant n \leqslant N : (a_n, \ldots, a_{n+k-1}) = d\}| = \frac{1}{b^k}. \tag{1.1}$$

Another equivalent formulation is due to Pillai [107] who showed that x is normal to base b if and only if it is simply normal to every base b, b^2, b^3, ...

A real number is called *absolutely normal*, if it is normal to all integer bases $b \geqslant 2$. Borel showed that almost all real numbers (with respect to Lebesgue measure) are simply normal to all bases $b \geqslant 2$, thus absolutely normal.

The two main problems on normal numbers are the following.

(1) Find explicit examples of absolutely normal real numbers.
(2) Show that explicit numbers such as $\sqrt{2}$, $\ln 2, e, \pi, \ldots$ are normal.

Only little progress has been made on the second question. This thesis constitutes a modest contribution to the first question.

Question (1) has been solved if asked for normality to only one base. The first explicit example of a normal number is due to Champernowne in 1935 [47]. He showed that the real number constructed by concatenating the expansions in base 10 of the positive integers, i.e.

$$0,1\,2\,3\,4\,5\,6\,7\,8\,9\,10\,11\ldots, \tag{1.2}$$

is normal to base 10. This construction has been extended in various directions (including, but not limited to, Besicovitch [29], Erdős and Davenport [53], Copeland and Erdős [48] Schiffer [116], Nakai and Shiokawa [98], Madritsch, Thuswaldner and Tichy [92]).

Most of these and other constructions of numbers normal to one base essentially depend on the choice of the base and therefore no immediate information on the digital expansions of the produced number to other bases is available. It is however unknown whether for example Champernowne's number (1.2) is normal to bases other than powers of 10 or not.

All known examples of absolutely normal numbers have been established in the form of algorithms that output the digits of this number to some base one after the other. The first such constructions are due to Sierpinski [123] (from 1917) and Lebesgue [83] (which appeared in 1917 but dates back to 1909). Sierpinski's construction was made computable by Becher and Figueira [11] who gave a recursive formulation of his construction. Other constructions of absolutely normal numbers in the form of algorithms are due to Turing [128] (see also Becher, Figueira and Picchi [13]), Schmidt [117], Levin [84] (see also Alvarez and Becher [2]), Becher, Heiber and Slaman [17], Figueira and Nies [64] and Lutz and Mayordomo [88].

Exceptions to this scheme are numbers in the spirit of Chaitin's constant arising as halting probabilities in the theory of Turing machines. These numbers are almost by definition absolutely normal, but non-computable. See Section 1.4.

1.2. **Generalizatons of normality.** The concept of normality can be generalized in many ways as it is in principle the same as the concept of genericity of dynamics: A point is generic if it satisfies a given almost-everywhere property in a dynamical system. However, being motivated by representations of numbers by a sequence of digits having dynamical origins, the most natural generalizations of normality we deal with in this thesis are with respect to expansions to non-integer bases, and to continued fractions.

1.2.1. *Normality for expansions to non-integer bases.* As initiated by Rényi [112] and Parry [103], it is possible to represent real numbers $x \in [0, 1)$ to a base β that is not necessarily integer by expanding x as a power series

$$\sum_{n=1}^{\infty} a_n \beta^{-n}$$

where the digits $0 \leqslant a_n < \beta$ are chosen in increasing order of n as large as possible.

We say x is *β-normal* or *normal to base β* if the orbit of x under the map $T_\beta : x \mapsto \beta x$ (mod 1) is uniformly distributed with respect to the unique T_β-invariant entropy maximizing measure μ_β. In case β is an integer larger than or equal to 2, the β-expansion is just the expansion of x to base b, and equidistribution is with respect to Lebesgue measure.

The most well-studied case in the theory of β-expansions is if β is a *Pisot number.* These are real algebraic integers $\beta > 1$ such that all its conjugates lie inside the open unit disc. We call a real number *absolutely Pisot normal* if it is normal to all bases that are Pisot numbers. Since there are only countably many Pisot numbers, the Birkhoff ergodic theorem implies that almost all real numbers are in fact absolutely Pisot normal.

Normal numbers to non-integer bases have been constructed in [78] and [28].

A number absolutely normal with respect to a countable set of real numbers has been constructed by Levin using Weyl's theorem for equidistribution. We contribute with our constructions in [115] and [91] to this topic and obtain some ancillary results on β-expansions that might be of independent interest. See Section 2.2.

1.2.2. *Normality for continued fraction expansions.* A real number $x \in [0, 1)$ is called *continued fraction normal* if the orbit $\{T_G^n(x)\}_{n\geqslant 0}$ of x under the Gauss map

$$T_G : [0, 1) \to [0, 1), \quad x \mapsto \frac{1}{x} \pmod 1, \; x > 0, \quad x \mapsto 0, \; x = 0,$$

is equidistributed with respect to the Gauss-Kuzmin measure μ_G on $[0, 1)$, given by

$$\mu_G(A) = \int_A \frac{1}{\log 2} \frac{1}{1 + x} dx$$

for any Borel set of $[0, 1)$.

Equivalently, x is continued fraction normal, if and only if in its continued fraction expansion

$$x = [a_0; a_1, a_2, \ldots]$$

all finite blocks of positive integers $d_1 \dots d_k$ appear with asymptotic frequency

$$\mu_G(\{x \in [0,1) : a_1(x) = d_1, \dots, a_k(x) = d_k\}).$$

Explicit examples of continued fraction normal numbers have been given by Postnikov and Pyateckiĭ [109], Adler, Keane and Smorodinsky [1], Madritsch and Mance [90] and Vandehey [129] by concatenating suitable strings of partial quotients. For example, in [1] it is shown that the number with continued fraction expansion

$$[0; 2, 3, 1, 2, 4, 2, 1, 3, 5, \dots]$$

is continued fraction normal. This number is obtained by concatenating the (finite) expansions of the positive rational numbers, when ordered according to denominator.

In [114] I give a solution to an open problem by Bugeaud and Queffélec [42, Ch. 10] and [110] by giving a construction of an absolutely normal number that is also continued fraction normal. My construction is based on ideas of Sierpinski [123] and Becher and Figueira [11] and gives rational approximations to such a number by giving its digits to base 2 one after the other. However, to obtain a more explicit example of such a number is desirable and continues to be an open problem.

1.2.3. *Generic points in dynamical systems.* Let X be a topological space, $\mathcal{B}$ a Borel σ-algebra, μ a probability measure on $(X, \mathcal{B})$ and $T : X \to X$ a map, ergodic and measure-preserving with respect to μ. Then Birkhoff's point-wise ergodic theorem can be applied and we call $x \in X$ *generic* if the conclusion of Birkhoff's theorem is satisfied, i.e. if for all compactly supported continuous functions f on X,

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=0}^{N-1} f(T^n(x)) = \int_X f(x) d\mu(x). \tag{1.3}$$

If T is uniquely ergodic then 1.3 holds for all x, so there is no problem in finding generic points. The maps $\times b$, $\times\beta$ and $x \mapsto \{\frac{1}{x}\}$ are all examples of measure-preserving ergodic transformations on the unit interval that are not uniquely ergodic. For all of them there is a natural choice of measure with respect to which one defines normality. In these cases points satisfying (1.3) can thus all be seen as natural generalizations of the terminology of being normal.

1.3. **Discrepancies of normal numbers.** The *discrepancy* of a sequence $(x_n)_{n\geqslant 1}$ of real numbers is defined as

$$D_N(x_n) = \sup_I \left| \frac{1}{N} \sharp\{1 \leqslant n \leqslant N : x_n \bmod 1 \in I\} - \lambda(I) \right|,$$

where the supremum is extended over subintervals $I \subseteq [0,1)$ and where λ denotes the Lebesgue measure. A sequence is *uniformly distributed modulo* 1 if its discrepancy tends to zero as $N \to \infty$.

Wall [130] showed that x is normal to base b if and only if the sequence $(b^n x)_{n \geqslant 1}$ is uniformly distributed modulo 1, i.e. if $D_N(b^n x) \to 0$ as $N \to \infty$.

In this thesis we are interested in quantitative estimates of $D_N(b^n x)$ for absolutely normal numbers x.

Gaal and Gál [69] and Philipp [106] showed that for almost every $x \in [0,1)$, for every integer $b \geqslant 2$, $D_N(b^n x) = O(\sqrt{\log\log N/N})$. Fukuyama [67] completed this study by explicitly giving the implied constants, i.e. he showed that

$$\limsup_{N \to \infty} \frac{D_N(b^n x)\sqrt{N}}{\sqrt{\log\log N}} = c(b)$$

for almost every x for some explicit positive constant c depending on b.

For the case of general sequences of real numbers, Schmidt [119] showed that there is an absolute constant $c > 0$ such that for any sequence $(x_n)_{n \geqslant 1}$, $D_N(x_n) \geqslant c\frac{\log N}{N}$ holds for infinitely many N. Schiffer [116] showed that the discrepancies of constructions of normal numbers in the spirit of Champernowne satisfy bounds of order $\Omega(\frac{1}{\log N})$. Levin [85] constructed for any integer $b \geqslant 2$ a real number α such that $D_N(b^n \alpha) = O(\frac{(\log N)^2}{N})$. It is an open question whether there exist an integer $b \geqslant 2$ and a real number x with optimal discrepancy bound $D_N(b^n x) = O(\frac{\log N}{N})$.

For absolute normality there seems to be a trade-off between the complexity of the algorithms and the speed of convergence of the corresponding discrepancies. The discrepancies satisfy upper bounds of the order $O(N^{-1/6})$ (Sierpinski), $O(N^{-1/16})$ (Turing), $O(\frac{1}{(\log N)})$ (Schmidt) and $O(N^{-1/2}(\log N)^3)$ (Levin). All algorithms, except the one due to Schmidt, need double exponential many mathematical operations to output the first N digits of the produced absolutely normal number. Schmidt's algorithm requires exponentially many mathematical operations. Becher, Heiber and Slaman's construction [17] is polynomial in time and of discrepancy $O(\frac{1}{\log N})$.

No construction of an absolutely normal number x is known such that the discrepancy $D_N(b^n x)$ for some $b \geqslant 2$ decays faster than what one would expect for almost all x.

However, together with Verónica Becher and Theodore Slaman we were able to construct an absolutely normal number with discrepancy to each base as good as almost any number, including Philipp's constants. This slightly improves Levin's work. See Section 2.1.2.

1.4. **Normal numbers in the theory of computing.** A real number in called *random* when its expansion to each integer base b is unpredictable by any program running on a

Turing machine. The original definition of randomness for real numbers is due to Martin-Löf [94] and has several equivalent formulations.

The area of studying random numbers is now known as *algorithmic randomness* and the two very reference books are [57, 102].

The concepts of randomness and normality do not coincide. Randomness implies normality [7, 45], but normality does not imply randomness: Random numbers are by definition not computable, i.e. their fractional expansion is not obtainable by a computer program. In contrast, there are evidently computable normal numbers (e.g. Champernowne's number is in fact given by a computable construction). In particular, there exist computable absolutely normal numbers as mentioned above.

Another way of seeing that randomness and normality do not coincide is with a result from descriptive set theory. The set of random numbers as a subset of all real numbers is $\mathbf{\Pi^0_2}$-complete while the set of absolutely normal numbers is $\mathbf{\Pi^0_3}$ and also Π^0_3-complete [16, 19] (see also [81] for base 2).

Random real numbers can be characterized as being precisely those numbers whose sequences representing its expansions to integer bases can not be compressed by any algorithm run on a Turing machine [46] (see also [57, 102] and the references therein). A similar characterization theorem in terms of incompressibility holds for normal numbers. Instead of using Turing machines it uses finite-state automata which are the simplest possible computing machines. This result follows from a seminal paper by Schnorr and Stimm [120] from the early 1970's. They show that a real number is normal to a given base if and only if every martingale definable with a finite-state automata only takes bounded function values on the prefixes of the expansion of the number to this base. Martingales are functions on finite sequences whose function values depend in a natural way on the prefixes of the sequence and can be understood as 'betting strategies' on infinite sequences.

Schnorr and Stimm's result was generalized in [51] where degrees of profits obtainable by finite-state martingales were considered (this is known as the theory of *finite-state dimension*). The results of [51] together with the work of [35] connect unpredictability by finite-state martingales with incompressibility by finite-state automata. A direct proof of the characterization of normal numbers as being precisely those whose expansions are incompressible by finite-state automata was given by Becher and Heiber in [15]. This characterization is robust in the sense that it remains true even if we consider non-deterministic finite-state automata or add a counter [9].

Since randomness implies normality, every random number is an example of an absolutely normal number. One family of random numbers is given by Chaitin's Omega numbers [46]. These are halting probabilities of universal Turing machines and are as such defined as the limit of an infinite sum involving non-computable values. Other relevant works in this direction include [10, 12, 14, 43].

As indicated above, progress has recently been made on the fast computation of absolutely normal numbers. In particular, polynomial-time constructions have been given by Becher, Heiber and Slaman [17] using elementary methods and Figueira and Nies [64] and Lutz and Mayordomo [88] using martingale methods. It is as of yet unclear whether Lutz and Mayordomo's construction can be used for practical implementation.

With the analysis of the constructions of absolutely normal numbers by Schmidt, Turing and Becher, Heiber and Slaman and with our algorithm with Becher and Slaman, we contribute in this thesis to the open question whether good convergence to normality (for every base) necessarily implies large complexity.

Some early analysis of the space and time complexity of computing normal numbers was made by Strauss [126].

Martin Epszteyn [63] has carried out computer simulations and computed discrepancies of classical normal numbers expressed in bases multiplicatively independent to the base in which the number was constructed. His results clearly indicate that for example Champernowne's number when constructed to base 10 shows in fact the worst random behaviour to base 10, but behaves very random when the same real number is expressed e.g. to base 2. He also implemented Becher, Heiber and Slaman's polynomial-time algorithm to output an absolutely normal number.

Other digit-statistics experiments can be found in [6, 101].

1.5. **Normal numbers in fractals.** In this section we give an overview of existence results of normal numbers in fractals. We focus on normal numbers to base r with missing digits in base s, where r and s are multiplicatively independent; normal numbers with missing continued fraction digits; and continued fraction normal numbers with missing digits to integer bases. There has been recent progress, notably by Hochman and Shmerkin [76] and by Simmons and Weiss [124], such that we now know that in each of these cases almost all numbers (with respect to the corresponding natural Cantor measure) are normal.

In this section the following notation is used.

Let $\Lambda \subset \mathbb{N}_{\geqslant 2}$ be set. Denote by $C_\Lambda = \{x \in [0,1) : a_i(x) \in \Lambda, i \geqslant 1\}$ the set of real numbers in $[0,1)$ whose partial quotients only lie in Λ. Let $BA = \bigcup_{\Lambda \subset \mathbb{N}_{\geqslant 2} \text{ finite}} C_\Lambda$ be the set of badly approximable numbers and let $WA = [0,1) \setminus BA$ be the set of well approximable numbers, i.e. the set of real numbers whose continued fraction expansion has unbounded partial quotients.

Let $b \geqslant 2$ be an integer. For a subset $B \subset \{0, 1, \ldots, b-1\}$, let $C_B^{(b)} = \{x \in [0, 1) :$ the base-b expansion of x has digits only in $B\}$. For example, $C_{0,2}^{(3)}$ is the standard middle third Cantor set.

1.5.1. *Normal numbers to base r in $C_S^{(s)}$.* Going back to works of Cassels [44], Schmidt [117, 118], Pearce and Keane [104], Brown, Moran and Pearce [39–41], Pollington [108], Host [77], Becher and Slaman [19], Becher, Bugeaud and Slaman [8] and others, we know that normality (or simple normality) to base s and normality (or simple normality) to base r are completely independent, in the sense that as long as there is no multiplicativity relation between the bases, the set of numbers normal (or simply normal) to bases s in a set $\mathcal{S}$ and not normal (or simply normal) to bases r in a set $\mathcal{R}$ has full Hausdorff dimension.

Methods involve constructing measures with quickly decaying Fourier-transformation (see next section), methods from ergodic theory and Schmidt games. See [42, Ch. 4-7].

1.5.2. *Normal numbers to base b in C_Λ, Fourier-techniques.* Let μ be a probability measure on $\mathbb{R}$. The Fourier transform of μ is

$$\hat{\mu}(\zeta) = \int_{\mathbb{R}} e^{-2\pi i \zeta x} d\mu(x)$$

for $\zeta \in \mathbb{R}$.

If μ is such that $\hat{\mu}(\zeta) \ll |\zeta|^{-\alpha}$ for some $\alpha > 0$, then μ-almost any $x \in \mathbb{R}$ is absolutely normal.

Theorem 1.1 (Daveport, Erdős, LeVeque [54]). *Let μ be a probability measure on $[0, 1)$ and $(s_n)_{n \geqslant 1}$ a sequence of natural numbers. If*

$$\sum_{N=1}^{\infty} \frac{1}{N^3} \sum_{n,m=1}^{N} \hat{\mu}(k(s_m - s_n)) < \infty$$

for any $k \in \mathbb{Z} \smallsetminus \{0\}$, then $(s_n x)_{n \geqslant 1}$ equidistributes modulo 1 with respect to μ for μ-almost every x.

If $\hat{\mu}(\zeta) \ll |\zeta|^{-\alpha}$ for some $\alpha > 0$ then μ-almost every x is absolutely normal.

For example, there is such a measure with polynomial decay on the set of well-approximable numbers. However, the existence of such a measure on a set implies that this set has dimension at least $2\alpha > 0$. Hence e.g. there can not be any such measure on the set of Liouville numbers, as they have dimension 0.

Let $B_N = C_{\{1,2,\ldots,N\}}$ be the set of real numbers in $[0, 1)$ with partial quotients bounded by N.

Theorem 1.2 (Kaufman [80] ($N \geqslant 3$), Queffélec and Ramaré [111] ($N \geqslant 2$)). *There is a probability measure μ on B_N with polynomial decay of $\hat{\mu}(\zeta)$ as $|\zeta| \to \infty$.*

Furthermore, Queffélec and Ramaré showed the existence of a probability measure whose Fourier-transformation decays polynomially on C_Λ for any $|\Lambda| \geqslant 2$ provided the dimension of C_Λ is larger than $\frac{1}{2}$. Hensley [74] calculated the corresponding Hausdorff dimensions, but for example $\dim C_{\{5,6\}} < \frac{1}{2}$.

For a good review of these techniques, and a very interesting paper in general, see Jordan and Sahlsten [79]. Note that it seems to be an intrinsic obstruction of these techniques that they do not extend beyond dimension $\frac{1}{2}$. This seems to be a summability condition to achieve convergence. Jordan and Sahlsten [79] comment on this issue.

However, using different techniques, it has been shown by Hochman and Shmerkin [76] that almost all numbers in C_Λ are absolutely normal, for any $\Lambda \subset \mathbb{N}_{\geqslant 2}$, provided it has at least two elements.

1.5.3. *Normal numbers to base b in C_Λ, approach and solution by Hochman and Shmerkin.* Hochman and Shmerkin [76] use the so-called *scaling flow* as developed by Furstenberg. The scaling flow can be thought of as a continuous sequence (i.e. a flow) of probability measures supported on smaller and smaller neighbourhoods of a point x. Typical results on the scaling flow establish ergodic properties along the continuous variable for almost all points x. The scaling flow goes back to Furstenberg [68] and has for example been studied in several works by Hochman.

Hochman and Shmerkin's results apply to more general fractals and in fact include the results by Cassels and Schmidt on normal numbers in integer-base Cantor sets, as well as the Fourier-technique results by Kaufman and others on normal numbers in continued fraction Cantor sets. However, Hochman and Shmerkin point out that their techniques do not yield almost everywhere continued fraction normality in integer-base Cantor sets due to the non-linearity of the Gauss-map. They proved among other things the following result.

Theorem 1.3 (Hochman, Shmerkin [76]). *Let $\Lambda \subset \mathbb{N}$ be a finite set with at least two elements and let μ be the natural Hausdorff measure on C_Λ. Then μ-almost all numbers in C_Λ are absolutely normal.*

Sketch of proof. The proof uses a certain measure classification theorem, just as the approaches by Einsiedler, Fishman and Shapira, and Simmons and Weiss do (see next sections). Let $n \geqslant 2$ be an integer. Hochman and Shmerkin take a μ-generic point, look at its forward orbit under T_n (the multiplication by n map on $[0, 1)$) and look at the sequence of normalized counting measures supported at the first N points of this orbit. Since we are working on the compact unit interval, there will be a weak* convergent subsequence of the sequence of these measures and the limit measure ν will automatically be T_n-invariant.

Hochman and Shmerkin show that this limit measure ν has to have Hausdorff dimension 1 which implies that it is the Lebesgue measure since this is the unique T_n-invariant measure of maximal dimension.

The proof uses the concept of *resonance* of measures. Two Borel probability measures on $\mathbb{R}$ are said to resonate, if $\dim \mu * \nu < \min(1, \dim \mu + \dim \nu)$, and dissonate, if $<$ is replaced by $\geqslant$. Here, the convolution of measures can be thought of as the probability distribution of the sum of two random variables whose probability distributions are μ and ν, respectively.

Hochman and Shmerkin proceed by means of contradiction. They show by construction that any T_n-invariant measure other than the Lebesgue measure λ resonates with measures of arbitrary large dimension (this step uses the piece-wise linearity of T_n and according to Hochman and Shmerkin seems to fail for the Gauss map T_G). Then they show that if a μ-generic x distributes along a subsequence with respect to a measure ν, then ν in fact dissonates with all measures of sufficiently large dimension. Furthermore, they show that any such limit measure must have positive dimension (this step uses results on the scaling flow). This implies that ν must have dimension 1, hence ν has to be the Lebesgue measure. □

1.5.4. *Almost all points in the middle third Cantor set are well-approximable.* Einsiedler, Fishman and Shapira [61] show that almost all numbers in base-b fractals (for the natural Hausdorff measure) are in WA and in fact have continued fraction expansions in which all finite patterns appear.

Theorem 1.4 (Einsiedler, Fishman, Shapira)**.** *With respect to the natural Hausdorff measure, almost every number in the middle third Cantor set $C_{0,2}^{(3)}$ contains all finite patterns in its continued fraction expansion.*

Central to the considerations both by Einsiedler, Fishman and Shapira and Simmons and Weiss is a classical correspondence between geodesics in the hyperbolic upper half-plane (which are either vertical lines or half-circles orthogonal to the real line) and the continued fraction expansion of the base-points at which the geodesics intersect the real line. Since $\mathrm{Sl}_2(\mathbb{Z})$ acts by Mobius transformation on the upper half-plane, geodesics can naturally be lifted to the standard fundamental domain for this action (the strip of complex number with real part between $-\frac{1}{2}$ and $\frac{1}{2}$ from which the disc of radius 1 around 0 has been removed). Any geodesic in the upper half-plane corresponds under this lift to a set of geodesic pieces in the fundamental domain. Since there is a natural probability measure on the (tangent space of the) fundamental domain when viewed as a (non-compact) manifold, one can speak of *equidistribution* of a geodesic in the fundamental domain. Note that the tangent space to this manifold can be identified with $\mathrm{PGl}_2(\mathbb{R}) / \mathrm{PGl}_2(\mathbb{Z})$.

These considerations lead to the following theorem as taken from Simmons and Weiss [124] that goes back to Artin [3] (see also Series [121]) that constitutes the fundamental link between homogeneous dynamics and diophantine approximation.

Theorem 1.5. *Let $x \in [0,1)$ and suppose that the geodesic corresponding to x is equidistributed in $\mathrm{PGl}_2(\mathbb{R})/\mathrm{PGl}_2(\mathbb{Z})$ with respect to Haar measure. Then the orbit $\{T_G^n(x)\}_{n\geqslant 1}$ is equidistributed with respect to the Gauss measure.*

Note that it does not matter which geodesic ending in x one takes. Two different such geodesics approach each other towards x and thus have the same asymptotic behaviour. The converse of this theorem is not true. By changing the continued fraction expansion of a normal continued fraction on a subsequence of digits of zero density, one can allow for very large partial quotients without affecting the normality property. The corresponding geodesic will reflect this behaviour by visiting ∞ too long and will consequently not be equidistributed with respect to Haar measure on $\mathrm{PGl}_2(\mathbb{R})/\mathrm{PGl}_2(\mathbb{Z})$.

Sketch of proof of Theorem 1.4. Note that if a geodesic is dense in $\mathrm{PGl}_2(\mathbb{R})/\mathrm{PGl}_2(\mathbb{Z})$ (as opposed to equidistributed), then the continued fraction expansion of the endpoint contains all finite patterns (as denseness implies that any finite geodesic piece can be approximated arbitrarily closely which corresponds to finite patterns in the continued fraction expansion).

The main idea is to lift the natural measure on the middle-third Cantor set via the above described correspondence to $\mathrm{PGl}_2(\mathbb{R})/\mathrm{PGl}_2(\mathbb{Z})$ and then even further to an adelic extension of this group. In this situation it is possible to apply a deep measure classification theorem by Lindenstrauss concerning measures invariant under the geodesic flow. By a construction, this measure classification theorem can be used to give a contradiction to the assumption that the set of points in the middle-third Cantor set with non-dense orbits under the Gauss map had less than full measure. □

1.5.5. *Continued fraction normality in Cantor sets.* Using different methods, Simmons and Weiss [124] recently completed this study by showing that well-approximability in Einsiedler, Fishman and Shapira's theorem can be replaced by normality.

Theorem 1.6 (Simmons, Weiss)**.** *Almost every real number in the middle-thirds Cantor set is continued fraction normal.*

Their proof uses results from the theory of random walks on groups by Benoist and Quint [26]. Such a random walk can for example be thought of as fixing a set of, say, two elements of a group G and assigning them both a probability (such as $\frac{1}{2}$). Then one observes the trajectory of an element of the group if one repeatedly multiplies it from the left with one of those two elements as drawn according to the probabilities assigned to them.

In this context, one studies *stationary* measures (see e.g. [61, p. 272]). Such measures should be thought of as being invariant under the 'random walk' on the group. Any G-invariant measure is stationary. Invariant measures need not always exist but stationary measures do.

Sketch of proof of Theorem 1.6. As before, we work in $\mathrm{PGl}_2(\mathbb{R})/\mathrm{PGl}_2(\mathbb{Z})$. We let

$$g_0 = \begin{pmatrix} \sqrt{3} & 0 \\ 0 & 1/\sqrt{3} \end{pmatrix} \text{ and } g_2 = \begin{pmatrix} \sqrt{3} & 2\sqrt{3} \\ 0 & 1/\sqrt{3} \end{pmatrix}$$

be two elements of this space and wish to multiply the unit element of $\mathrm{PGl}_2(\mathbb{R})/\mathrm{PGl}_2(\mathbb{Z})$ repeatedly with one of each of g_0 or g_2, drawn with equal probability. The first part of the main theorem of Simmons and Weiss asserts that in this situation for almost any sequence of g_i's (according to the product measure on the space of all such sequences), for *any* element x of the group, the trajectory of the random walk $g_n g_{n-1} \dots g_1 x$ will be distributed according to a stationary measure. The second part of their theorem says that there is only one such stationary measure - the natural Haar measure. Simmons and Weiss' work goes back to work of Benoist and Quint, which by my understanding greatly extends a classical theorem by Breiman [37].

We write $g_0 = au_0$, $g_2 = au_2$ where

$$a = \begin{pmatrix} \sqrt{3} & 0 \\ 0 & 1/\sqrt{3} \end{pmatrix} \text{ and } u_x = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}.$$

Let $i = (i_1, i_2, \dots)$ be a random sequence of indices $i_n \in \{0, 2\}$ and denote by e the unit in $\mathrm{PGl}_2(\mathbb{R})/\mathrm{PGl}_2(\mathbb{Z})$. We have $g_{i_1} e = a u_{i_1} e$ and

$$g_{i_2} g_{i_1} e = a u_{i_2} a u_{i_1} e = a^2 \begin{pmatrix} 1 & i_1 + i_2/3 \\ 0 & 1 \end{pmatrix} e.$$

Note that $i_1 + i_2/3$ with $i_1, i_2 \in \{0, 2\}$ already resembles the ternary expansion of a number in the middle-third Cantor set. Inductively,

$$g_{i_n} \cdot \ldots \cdot g_{i_1} e = a^n u_{s|_n} e$$

where $s|_n$ are the first n digits of the base 3 expansion of a real number $s = i_1 + i_2/3 + i_3/3^2 + \dots$. We have

$$a^n u_{s|_n} = a^n u_{s|_n - s} u_s = a^n u_{s|_n - s} a^{-n} a^n u_s = \begin{pmatrix} 1 & (\sqrt{3})^{2n}(s|_n - s) \\ 0 & 1 \end{pmatrix} = u_{O(1)} a^n u_s.$$

This is because $s|_n - s = O(3^{-n})$. By construction, s lies in $C^3_{0,2}$, and the probability measure on the sequence space $\{0,1\}^{\mathbb{N}}$ corresponds exactly to the natural measure on the middle third Cantor set. The statement in the theorem follows if we establish that equidistribution of $\{u_{O(1)}a^n u_s e\}_{n\geqslant 0}$ implies equidistribution of the full diagonal action of $\{\mathrm{diag}(e^t, e^{-t})\}_{t\geqslant 0}$ on $\{u_{O(1)}u_s e\}$ which is corresponds to the geodesic starting at s and thus implies the theorem in view of Theorem 1.5. $\square$

Description of my Work

2.1. **Absolutely normal numbers.**

2.1.1. *Quantitative simultaneous equidistribution.* In [114], I solved a question by Bugeaud and Queffélec [42, Chapt. 10] on absolutely normal well-approximable numbers. In fact, I showed that there is a computable absolutely normal number that is also continued fraction normal. The construction is based on ideas of Sierpinski [123] and Becher and Figueira [11].

A sequence of digits ω of length n is called (ε, k)-normal or (ε, k, μ)-normal, if for all sequences d of length k, the number of times d appears in ω lies between $n(\mu(d) - \varepsilon)$ and $n(\mu(d) + \varepsilon)$. If the measure μ is ergodic with respect to underlying the shift map, the Shannon-McMillan-Breimann theorem implies that the μ-measure of the set of non-(ε, k)-normal numbers of length n decays exponentially in n. This consequence is not explicit, in the sense that one has no information on the magnitude of the implied constants. However, using a large deviation theorem for mixing random variables, I could give explicit estimates of these constants. This is necessary to establish a completely deterministic construction.

In the context of β-expansions for β a Pisot number, together with Manfred Madritsch and Robert Tichy [91], we also could make these constants completely explicit. This allowed us to give an algorithmic construction, realizable only with elementary mathematical operations, of a real number simultaneously normal to every Pisot number.

2.1.2. *Speed of computation and convergence to normality.* In [113] I showed that work by Schmidt [117] on numbers normal to multiplicatively independent bases can be made effective to yield an algorithmic construction of an absolutely normal number. I furthermore showed that this algorithm can be optimized with respect to speed of convergence to normality to generate an absolutely normal number that in each base converges faster to normality than all known constructions by concatenation of blocks of numbers normal only to a single base.

To make Schmidt's algorithm fully explicit, I gave explicit upper bounds for constants appearing in an exponential sum estimate in his work. This is of independent interest for applications to problems involving digital representations to multiplicatively independent bases.

In [113] and [91], we analyzed the computable versions of constructions of Sierpinski, Turing, and the algorithm of Becher, Heiber, Slaman and my explicit version of the construction of Schmidt. Our main conclusion is that the faster an algorithm computes the digits of the absolutely normal number that it outputs, the slower convergence to normality seems to be. In particular, the polynomial time algorithm by Becher, Heiber and Slaman [17] is as fast as other constructions by concatenation of blocks of digits. It is still unclear whether this trade-off is a defect of the existing constructions so far or if this is a natural behaviour to expect.

Together with Verónica Becher and Theodore Slaman we showed that it is possible to adapt Sierpinski's ideas to give a constructive proof of Philipp's result. This allows to compute an absolutely normal number, digit-by-digit, with discrepancy to each base as good as almost any number, including Philipp's constants. This improves Levin's construction in terms of rate of convergence to normality (and also in terms of computability - our construction is elementary and does not use exponential sums). We are however not sure whether or not it is possible to give this construction in linear time, or how to extend it to include the optimal constants as given by Fukuyama.

2.2. β-expansions.

2.2.1. *On expansions to Pisot bases.* Much of the arithmetic properties of β-expansions are encoded in the orbit of 1 under the map T_β. This is a finite set when β is a Pisot number. In [91] we obtained an upper bound for the number of points in this orbit. This is also an upper bound for the number of zeros occurring in the modified β-expansion of 1 and as such gives quantitative information about the specification property of the underlying dynamical system (T_β, μ_β). The proof uses some basic algebraic number theory and a result from the geometry of numbers.

Applying similar methods, in [115] I could give an estimate for the length of the β-expansion of a positive real number.

2.2.2. *β-normal numbers from polynomials along primes.* It was known that the most basic construction of numbers normal to an integer base, namely Champernowne's number, has analogues for β-numeration systems. However, it was not known whether or under which assumptions on the base other constructions of normal numbers have an analogue to real bases. I was especially interested in polynomial constructions: real numbers whose expansion to base β is obtained by concatenating the β-expansions of values of a non-constant positive integer-valued polynomial along the natural numbers or the primes, i.e.

$0, f(1)f(2)f(3)\ldots$ or $0, f(2)f(3)f(5)\ldots$. In [115] I proved that under natural finiteness assumptions on the base these constructions in fact do yield normal numbers.

The proof is based on a combinatorial cutting and pasting trick together with results on normal numbers to real bases by Bertrand-Mathis and Volkmann [27].

2.3. **Diophantine equations.**

2.3.1. *On squares with three non-zero digits.* A classical result of Besicovitch [29] that the concatenation of squares is normal implies that in an average sense only few integer squares have few non-zero digits. I was interested in 'local' results, i.e. in this case to classify explicitly which squares have few digits. My work with Michael Bennett can be seen as a study of local techniques for polynomial sequences. This continues work on the digital representation of perfect powers as initiated by Bennett, Bugeaud, Mignotte, Corvaja and Zannier and others. In particular, we determined all integers n such that n^2 has at most three digits in base b for $b \in \{2, 3, 4, 5, 8, 16\}$. More generally, we showed that all solutions to equations of the shape

$$Y^2 = t^2 + M \cdot q^m + N \cdot q^n,$$

where q is an odd prime, $n > m > 0$ and $t^2, |M|, |N| < q$, either arise from 'obvious' polynomial families or satisfy $m \leqslant 3$. Our arguments rely upon Padé approximants to the binomial function, considered q-adically.

Normality in Pisot Numeration Systems

Adrian-Maria Scheerer[1]

Abstract. Copeland and Erdős [48] showed that the concatenation of primes when written in base 10 yields a real number that is normal to base 10. We generalize this result to Pisot number bases in which all integers have finite expansion.

1. Introduction

Let x be a real number and $b \geqslant 2$ a positive integer. Then x has a b-adic representation of the form

$$x = \lfloor x \rfloor + \sum_{i=1}^{\infty} \varepsilon_i b^{-i}$$

where $\varepsilon_i \in \{0, 1, \dots b-1\}$ are the digits of x and $\lfloor x \rfloor$ is the integer part of x, the biggest integer less than or equal to x. We call x *normal to base* b, if any block $d = d_1 d_2 \dots d_k$ of $k \geqslant 1$ digits occurs with the expected frequency in the b-adic representation of x. This means that

$$\lim_{n \to \infty} \frac{1}{n} N_d(x, n) = \frac{1}{b^k},$$

where $N_d(x, n)$ counts the occurrences of the block d within the first n digits of x. A real number x is called *absolutely normal* if it is normal to every base $b \geqslant 2$.

The terminology of a normal number can be extended to the context when the underlying base is no longer an integer. Rényi [112] introduced and Parry [103] studied numeration systems with respect to real bases $\beta > 1$. Each real number x has a representation of the form

$$x = \sum_{i=L}^{-\infty} \varepsilon_i \beta^i,$$

with digits $\varepsilon_i \in \{0, 1, \dots, \lceil \beta \rceil - 1\}$. One way to produce the digits is the so-called *greedy algorithm* using the transformation $T_\beta : x \mapsto \beta x \pmod 1$ on the unit-interval. In a natural way, T_β corresponds to the shift-operator on the set W^∞ of right-infinite sequences over $\{0, 1, \dots, \lceil \beta \rceil - 1\}$ and each x corresponds to its sequence of digits. A sequence ω in W^∞ is called *μ-normal* for a given shift-invariant measure μ on W^∞, if all possible finite patterns of digits occur in ω with asymptotic frequency given by μ. Consequently, the real x is called

[1] This article appeared in [115]

μ-*normal* if its sequence of digits is μ-normal. Details will be made clear in the next section.

From a modern approach, using Birkhoff's point-wise ergodic theorem, it is immediate that almost all numbers are normal to a fixed[2] base b. The map $T_b : x \mapsto bx \pmod 1$ on the unit-interval is the underlying ergodic transformation which preserves Lebesgue-measure. Knowing this, the existence of normal numbers to base b is in a certain sense not very surprising. However, in this context, there are two observations that make the study of normal numbers interesting.

First: The explicit construction of normal numbers. The study of normal numbers dates back to Borel [34], who in 1909 showed that Lebesgue-almost all numbers are absolutely normal. However, the first explicit example of a normal number is due to Champernowne [47] in 1933. He showed that the concatenation of integers, when written in base 10,

$$0,1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12\ 13\ldots,$$

is normal to base 10. Copeland and Erdős [48] showed that

$$0,2\ 3\ 5\ 7\ 11\ 13\ 17\ 19\ldots,$$

i.e. the concatenation of primes in base 10 is normal to base 10. Besicovitch [29] showed that the decimal formed by concatenation of the squares in base 10 is normal to base 10. This construction was extended to general integer-valued polynomials by Davenport and Erdős [53] and by Schiffer [116] and Nakai and Shiokawa [98], [99] to more general polynomial settings. Nakai and Shiokawa [100] also evaluated polynomials at primes, and Madritsch [89] showed that numbers generated by pseudo-polynomial sequences along the primes are normal. Further constructions of normal numbers in the spirit of Copeland and Erdős and Erdős and Davenport include [93] and [92].

These constructions, most notably the one due to Champernowne, have subsequently been generalized to other number systems. To mention are the works by Ito and Shiokawa [78] who generalized the Champernowne-construction to real bases $\beta > 1$, and by Madritsch and Mance [90] who modified the construction to produce normal sequences in general symbolic dynamical systems. Bertrand-Mathis and Volkmann [27] give a generalized Copeland-Erdős construction to symbolic dynamical systems.

In this paper we prove a polynomial Copeland-Erdős-construction to bases which are not integers. We use results from the work of Bertrand-Mathis and Volkmann [27] which

[2] Borel's result also follows, but for the moment we want to restrict the discussion to one single base.

in turn is extending the original work of Copeland and Erdős [48].

Second: Not *all* numbers are normal (almost all cannot be improved to all, hence T_b is not uniquely ergodic), so the ergodic theorem is strict. This can be seen in context of the following 'test' for ergodicity.

Theorem 1.1 (See Theorem 1.4 in [32])**.** *Let $\mathcal{F}_0$ be a field*[3] *generating $\mathcal{F}$. If T respects*[4] *every A in $\mathcal{F}_0$, then T is ergodic.*

Hence normal numbers, or rather the existence of non-normal numbers, can be used to test the underlying transformation for unique ergodicity. Although the Lebesgue-measure is not the only T_b-invariant probability measure on the unit-interval, it is the only one that maximizes entropy (see the following section). Accepting this for the moment as a definition of uniqueness, it is possible to study normality in greater generality with respect to a given transformation that can be different from T_b.

2. Preliminaries

In the following we present a condensed introduction to β-expansions, Pisot numbers and symbolic dynamical systems - the context in which we want to state our result.

Let $\beta > 1$ be a fixed real number. A *β-expansion* of a non-negative real number x is a representation of x as a sum of integer powers of β of the form

$$x = \sum_{i=L}^{-\infty} \varepsilon_i \beta^i, \tag{2.1}$$

where the digits $\varepsilon_i \in \{0, 1, \dots \lceil\beta\rceil - 1\}$ are obtained by the following *greedy algorithm.* Let $L \in \mathbb{Z}$ such that $\beta^L \leqslant x < \beta^{L+1}$ and put $\varepsilon_L = \lfloor x/\beta^L \rfloor$ and $r_L = \{x/\beta^L\}$. For $L \geqslant i > -\infty$, define recursively $\varepsilon_i = \lfloor \beta r_{i+1} \rfloor$ and $r_i = \{\beta r_{i+1}\}$. β-expansions have been introduced and studied by Rényi [112] and Parry [103].

Let T_β be the *β-transformation* $T_\beta : [0, 1) \to [0, 1)$, $x \mapsto \{\beta x\}$. The digits in the β-expansion 2.1 are given by $\varepsilon_i = \lfloor \beta T_\beta^{i-1}(x) \rfloor$. Rényi [112] showed that there is a unique normalized measure μ_β on $[0, 1)$ that is invariant under T_β and equivalent to the Lebesgue measure. This measure also maximizes the entropy of the corresponding symbolic dynamical system and we use it to define normal numbers in base β, see below.

[3] The underlying sigma-field $\mathcal{F}$ is in our case the Borel sigma-algebra which is generated by b-adic intervals.

[4] Almost every orbit under T visits A with the expected asymptotic frequency.

A *Pisot number* β is a real algebraic integer $\beta > 1$ such that all its conjugates have absolute value less than 1. For a Pisot number of degree d, we denote its conjugates by β_i, $i = 2, \dots, d$, and the corresponding conjugations by σ_i.

We work with Pisot numbers such that every positive integer has finite β-expansion. A criterion for when this is the case can for example be found in [65].

In our notation concerning symbolic dynamical systems we follow Bertrand-Mathis and Volkmann [27].

Let A be a finite alphabet. A^* is the set of all finite (possibly empty) words over A and $A^{\mathbb{N}}$ is the set of all (right-)infinite words over A. We call a subset L of A^* a language. L^* denotes the set of all finite concatenations of words from L. Let $W(L^*)$ be the set of all non-empty factors of words in L^*. For a finite word ω we let $\|\omega\|$ be its length. A language L is said to be connecting[5] of order $j \geqslant 0$ if for any two words $a, b \in W(L^*)$ there is a word $u = u(a, b) \in W(L^*)$ of length j such that $aub \in W(L^*)$. For each $a, b \in W(L^*)$ we choose one $u = u(a, b)$ and introduce the notation $a \oplus b := aub$. In the applications we have in mind, this intermediary word will simply consist of 0's. We write $W(L^*) = \bigcup_{n \geqslant 1} L_n$ where L_n is the subset of words in $W(L^*)$ of length n. Also denote by L'_n the subset of $W(L^*)$ of words of length less or equal to n. For a language L we denote by $W^\infty = W^\infty(L)$ the set of all infinite words generated by L, i.e. the set of all $\omega = a_1 a_2 \dots$ such that $a_i a_{i+1} \dots a_k \in L$ for all $1 \leqslant i < k < \infty$.

We introduce the discrete topology on the alphabet A and the corresponding product topology on the set of sequences $A^{\mathbb{N}}$. With each language L we associate the symbolic dynamical system

$$S_L = (W^\infty, \mathcal{B}, T, I),$$

where $W^\infty = W^\infty(L)$; $\mathcal{B}$ is the σ-algebra generated by all cylinder sets of $A^{\mathbb{N}}$, i.e. sets of the form

$$c(\omega) = \{a_1 a_2 \ldots \in A^{\mathbb{N}} \mid a_1 a_2 \ldots a_n = \omega\}$$

for some word $\omega \in A^*$ of length n. T is the shift operator and I is the set of all T-invariant probability measures μ on $\mathcal{B}$. We will write $\mu(\omega)$ instead of $\mu(c(\omega))$ for a finite word ω.

With each symbolic dynamical system S_L we associate the entropy

$$h(W^\infty) = \sup_{\mu \in I} h(\mu),$$

[5] A symbolic dynamical system having a connecting language is also said having the *specification property.*

where $h(\mu)$ denotes the entropy of the measure μ (cf. Chapter 2 of Billingsley [32]). In the context of the symbolic dynamical system generated by a β-expansion the measure μ_β is precisely the (unique) measure with maximum entropy equal to $\log\beta$ (cf. [75] and the work by Bertrand-Mathis and Volkmann [27]). In the following, we will work with this maximal measure.

For an infinite word $\omega = \omega_1\omega_2\ldots \in W^\infty$ and a block $d = d_1d_2\ldots d_k \in L$ we denote with $N_d(\omega, n)$ the number of occurrences of d within the first n letters of ω. If the word ω is finite, we denote by $N_d(\omega)$ the occurrences of d in it. An infinite word $\omega \in W^\infty$ is called *μ-normal* or *μ-normal sequence* if for all $d \in W(L^*)$

$$\lim_{n\to\infty} \frac{1}{n} N_d(\omega, n) = \mu(d).$$

We note that a non-negative real number x is *μ_β-normal* if and only if the sequence of digits in its β-expansion is a μ_β-normal sequence.

In this terminology, the main result of Bertrand-Mathis and Volkmann [27] is the following

Theorem 2.1. *Let L be a connecting language and $a_1, a_2, \ldots$ a sequence of different elements of $W(L^*)$, $\|a_1\| \leqslant \|a_1\| \leqslant \ldots$, satisfying the generalised Copeland-Erdős condition:*

$$\forall\varepsilon > 0\ \exists n_0(\varepsilon)\ \forall n \geqslant n_0\ \sharp\{a_\nu \mid \|a_\nu\| \leqslant n\} > |L'_n|^{1-\varepsilon}.$$

Then the infinite word $a = a_1a_2\ldots \in W^\infty$ is normal.

The symbolic dynamical system *generated by the β-shift* (or *corresponding to the β-expansion*) arises naturally when viewing the β-expansions of real numbers $x \in [0, 1)$ as infinite words over the alphabet $\{0, 1, \ldots \lceil\beta\rceil\}$. W^∞ is the set of these right-infinite sequences, $\mathcal{B}$ the σ-algebra generated by all cylinder sets, T the shift operator (it corresponds to the β-transformation T_β), and I the set of all T-invariant probability measures on $\mathcal{B}$. We work with the unique entropy-maximizing measure μ in I. It corresponds to μ_β on $[0, 1)$ in the sense that for a finite word ω the measure of the cylinder set $\mu(\omega)$ is the same as the measure $\mu_\beta(\tilde{\omega})$ of the set $\tilde{\omega}$ of all real numbers in $[0, 1)$ whose β-expansion starts with ω. We allow us to speak of these two concepts interchangeably.

For a given Pisot number β, denote by $(n)_\beta$ the word over $\{0, 1, \ldots \lceil\beta\rceil - 1\}$ that corresponds to the β-expansion of the positive integer n. We prove the following polynomial generalization of [48].

Theorem 2.2. *Let β be a Pisot number such that all integers have finite β-expansion and let the measure μ_β be as before. Let f be a polynomial of degree g that maps positive integers to positive integers. Then*

$$(f(2))_\beta \oplus (f(3))_\beta \oplus (f(5))_\beta \oplus (f(7))_\beta \oplus (f(11))_\beta \oplus \dots$$

is a μ_β-normal sequence.

In the context of the dynamical system generated by the β-shift, the entropy is $\log \beta$. Hence by Lemma 2 of [27], we have bounds on the number of words of length n in $W(L^*)$. For n sufficiently large we have $\beta^n \ll |L_n| \ll \beta^n$, where the implied constants do not depend on n. Therefore

$$|L'_n| = \sum_{\nu=1}^{n} |L_\nu| \ll \beta^n \tag{2.2}$$

for all large n.

3. General Case

First we need upper and lower bounds of the length of the β-expansion of integers. Under the assumption of β being a Pisot number such that all integers have finite β-expansions we can in fact show that the lengths of these expansions are asymptotically of logarithmic order of magnitude.

Note that if $n = \sum_{i=L(n)}^{-R(n)} \varepsilon_i \beta^i$ we call $\sum_{i=0}^{L(n)} \varepsilon_i \beta^i$ its integer part and $\sum_{i=-1}^{-R(n)} \varepsilon_i \beta^i$ its fractional part. In the following we will think of n as fixed and omit writing the dependency on it in the lengths L and R.

Lemma 3.1. *Let β be a Pisot number of degree d such that all natural numbers have finite β-expansion. For the length $R(n)$ of the fractional part of n upper and lower bounds of the following form hold, for sufficiently large n:*

$$\delta \log n \leqslant R(n) \leqslant \delta' \log n$$

where δ is a positive constant (specified in the proof) and the difference $\delta' - \delta > 0$ can be chosen to be arbitrarily small.

Proof. We have $\frac{n}{\beta^{L+1}} \in [0,1)$. Following an argument of Proposition 3.5 Frougny and Steiner [66], for a certain number k the number $T_\beta^k(\frac{n}{\beta^{L+1}})$ is an element of the finite set

$$Y = \{y \in \mathbb{Z}[\beta] \cap [0,1) \mid |\sigma_j(y)| < 1 + \frac{\lfloor \beta \rfloor}{1 - |\sigma_j(\beta)|} \quad \text{for} \quad 2 \leqslant j \leqslant d\}.$$

To see this, let the β-expansion of n for the moment be $\varepsilon_1\varepsilon_2\dots$ and put $z := \frac{n}{\beta^{L+1}}$. Then for all $k \geqslant 0$,

$$T_\beta^k(z) = \beta T_\beta^{k-1}(z) - \varepsilon_k = \ldots = \beta^k z - \sum_{l=1}^{k} \varepsilon_l \beta^{k-l}.$$

Hence for all $k \geqslant 0$ and $2 \leqslant j \leqslant d$,

$$|\sigma_j(T_\beta^k(z))| = |\sigma_j(\beta)^k \sigma_j(z) - \sum_{l=1}^{k} \varepsilon_l \sigma_j(\beta)^{k-l}| < |\sigma_j(\beta)|^k |\sigma_j(z)| + \frac{\lfloor \beta \rfloor}{1 - |\sigma_j(\beta)|}.$$

Let k be equal to

$$\max_{2\leqslant j\leqslant d} \left\lceil -\frac{\log|\sigma_j(\frac{n}{\beta^{L+1}})|}{\log|\sigma_j(\beta)|} \right\rceil = L + 1 + \max_{2\leqslant j\leqslant d} \left\lceil \frac{\log n}{\log|\sigma_j(\beta)^{-1}|} \right\rceil$$

which we write as

$$k = L + 1 + \delta \log n + O(1), \quad \text{where} \quad \delta := \max_{2\leqslant j\leqslant d} \frac{1}{\log|\sigma_j(\beta)^{-1}|}.$$

Note that the $O(1)$ constant coming from the ceiling lies in $[0,1)$. For this choice of k, $T_\beta^k(\frac{n}{\beta^{L+1}}) \in Y$.

Let W be the maximum length of the β-expansions of the elements in Y. We therefore obtain asymptotic bounds of R,

$$\delta \log n \leqslant R \leqslant W + 1 + \delta \log n \leqslant \delta' \log n,$$

where $\delta' > \delta$ can be chosen arbitrarily close. □

In the course of the proof of Theorem 2.2 we deal with a problem caused by a constant coming from the length of the words we want to patch together. This issue can be circumvented by dividing the words into smaller subwords and glueing them back together afterwards. The following lemma ensures normality of the resulting word when patched back together.

Lemma 3.2. *Let $v = v_1v_2v_3\dots$ and $w = w_1w_2w_3\dots$ be μ-normal words such that $\|v_i\| = \|w_i\|$, $\|v_i\| \to \infty$ and assume that the quantities $\frac{\|v_{N+1}\|}{\|v_1\|+\ldots+\|v_N\|}$ and $\frac{N}{\|v_1\|+\ldots+\|v_N\|}$ tend to zero as N tends to infinity. Then the word*

$$u = v_1w_1v_2w_2v_3w_3\dots$$

is μ-normal.

Proof. We work with a fixed finite string $d = d_1 \dots d_k$ of length k. Since v is μ-normal, we have

$$N_d(v,n) = \sum_{i=1}^{N} N_d(v_i) + O(N) + O(\|v_{N+1}\|) \longrightarrow \mu(d)n$$

as $n \to \infty$, where N is chosen such that $\|v_1\| + \ldots + \|v_N\| \leqslant n < \|v_1\| + \ldots + \|v_{N+1}\|$. The $O(N)$ contribution comes from possible occurrences in-between two words v_i and v_{i+1}. Hence by the assumptions

$$\sum_{i=1}^{N} N_d(v_i) \longrightarrow \mu(d)n$$

as $n \to \infty$. Then, by arguing similarly,

$$N_d(u,n) = \sum_{i=1}^{N} N_d(v_i) + \sum_{i=1}^{N} N_d(w_i) + O(N) + O(\|w_{N+1}\|) = \mu(d)\frac{n}{2} + \mu(d)\frac{n}{2} + o(n).$$

Here, N is chosen such that $\|v_1\| + \|w_1\| + \ldots + \|v_N\| + \|w_N\| \leqslant n < \|v_1\| + \|w_1\| + \ldots + \|v_{N+1}\| + \|w_{N+1}\|$. This shows the normality of u. □

To verify the conditions of Lemma 3.2 in our application, we need some basic number theoretic input.

Lemma 3.3. *Denote by p_N the N-th prime number. We have for $N \to \infty$*

$$(1) \quad \frac{\log p_{N+1}}{\log p_1 + \ldots + \log p_N} \longrightarrow 0, \quad \textit{and} \quad (2) \quad \frac{N}{\log p_1 + \ldots + \log p_N} \longrightarrow 0.$$

Proof. This is a consequence of the prime number theorem. We have

$$\sum_{i=1}^{p_N} \log p_i = \theta(p_N) \sim p_N \sim N \log N.$$

□

With these preliminaries we can prove our theorem.

Proof of Theorem 2.2. The polynomial $f(n) = a_g n^g + \ldots + a_1 n + a_0$ behaves asymptotically like $a_g n^g$. Hence for any $\varepsilon > 0$ and any n large enough

$$f(n) \leqslant (1+\varepsilon)a_g n^g \quad \text{and} \quad f(n) \geqslant (1-\varepsilon)a_g n^g.$$

Thus a consequence of Lemma 3.1, we have the upper bounds

$$\begin{aligned} R(f(n)) &\leqslant R((1+\varepsilon)a_g n^g) \\ &\leqslant \delta'(\log(1+\varepsilon) + \log a_g + g\log n) \\ &\leqslant C' \log n \end{aligned}$$

for some constant $C' > \delta' g$ arbitrarily close and n large enough. Similarly we obtain lower bounds of the form

$$R(f(n)) \geqslant C \log n,$$

where $C < \delta g$ is a positive constant and can be chosen arbitrarily close if n is assumed to be large enough.

A direct consequence is an asymptotic upper bound for the total length of $f(n)$ when written in base β:

$$\begin{aligned}\|(f(n))_\beta\| &= L(f(n)) + 1 + R(f(n))\\ &\leqslant L((1+\varepsilon)a_g n^g) + 1 + R((1+\varepsilon)a_g n^g)\\ &\leqslant \frac{g\log n + \log a_g}{\log\beta} + O(1) + C'\log n\\ &\leqslant C\frac{\log n}{\log\beta},\end{aligned}$$

for some (other) constant C. Note that C only depends of f and β.

However, applying Theorem 2.1 directly does not work as we do not have control of the size of the constant C. This can be avoided by choosing an integer $m \geqslant 0$ such that $C/2^m \leqslant 1$ and dividing the words $(f(n))_\beta$ in 2^m words of (almost) equal length. Then we can apply Theorem 2.1 to show normality of the concatenations of those shorter words. They can subsequently be patched back together applying Lemma 3.2 multiple times. Note that the lower bounds for R enable us to use Lemma 3.2.

For a prime number p we have $\|(f(p))_\beta\| \leqslant C\frac{\log p}{\log\beta}$, so $\|(f(p))_\beta\| \leqslant N$ is implied by $C\frac{\log p}{\log\beta} \leqslant N$. This is equivalent to

$$p \leqslant \beta^{N/C}.$$

Thus, counting primes below $\beta^{N/C}$,

$$\pi(\beta^{N/C}) \sim \frac{\beta^{N/C}}{N/C\log\beta} \geqslant \frac{C}{\log\beta}\beta^{N(C^{-1}-\varepsilon)},$$

for any $\varepsilon < 1$ arbitrarily close and N large enough. Here we see why we require $C \leqslant 1$, namely so that the condition of Theorem 2.1,

$$\pi(\beta^{N/C}) \geqslant (\beta^N)^{1-\varepsilon}$$

for any $\varepsilon' > 0$, is implied by $\beta^{N(C^{-1}-\varepsilon)}$ being eventually greater than $(\beta^N)^{1-\varepsilon}$. Inserting the intermediary word to obtain admissibility in base β does not destroy the normality of the sequence since we are inserting a word of constant length. □

4. Final Remarks

Let $\varphi = \frac{1+\sqrt{5}}{2}$ be the golden ratio, i.e. the dominating root of the polynomial $x^2 - x - 1$. All positive integers have finite φ-expansion (see for example Theorem 2 of [65]). Considering this special case is interesting insofar that we can provide an *exact* formula on the length of the fractional part. Let n be a positive integer and denote by $L+1$ and R the lengths of its integer and fractional part when written in base φ. From the greedy algorithm we already know that

$$\varphi^L \leqslant n < \varphi^{L+1} \Rightarrow L = \lfloor \frac{\log n}{\log \varphi} \rfloor .$$

In [70] it is proved that the fractional part R of n satisfies $R = L$ or $R = L+1$, depending on whether L is even or odd. However, even with such an exact formula it is not possible to establish the normality to base φ of the word

$$(2)_\varphi 0 (3)_\varphi 0 (5)_\varphi 0 \ldots$$

by directly applying the generalized Copeland-Erdős criterion Theorem 2.1. Moreover, the method employed in [70] does not seem to yield an exact formula for the length of the fractional part when the underlying base is a Pisot-number of degree greater than two. It seems to be an interesting open problem to obtain such a formula.

Acknowledgements: The author would like to thank Robert Tichy and Manfred Madritsch for their support, supervision and discussions about the subject. Special thanks to Tomáš Vávra who showed me [70] and to Wolfgang Steiner who very patiently explained to me the proof of Proposition 3.5 in [66]. Part of this research was carried out at the Université de Lorraine in Nancy and at the Max-Planck Institute for Mathematics in Bonn and the author would like to thank these institutions for their hospitality. The author also would like to thank the anonymous referee for his/her useful comments. The author was supported by the Austrian Science Fund (FWF): I 1751-N26; W1230, Doctoral Program "Discrete Mathematics"; and SFB F 5510-N26.

Computable Absolutely Normal Numbers and Discrepancies

Adrian-Maria Scheerer[6]

Abstract. We analyze algorithms that output absolutely normal numbers digit-by-digit with respect to quality of convergence to normality of the output, measured by the discrepancy. We consider explicit variants of algorithms by Sierpinski, by Turing and an adaption of constructive work on normal numbers by Schmidt. There seems to be a trade-off between the complexity of the algorithm and the speed of convergence to normality of the output.

1. Introduction

A real number is *normal* to an integer base $b \geqslant 2$ if in its expansion to that base all possible finite blocks of digits appear with the same asymptotic frequency. A real number is *absolutely normal* if it is normal to every integer base $b \geqslant 2$. While the construction of numbers normal to one base has been very successful, no construction of an absolutely normal number by concatenation of blocks of digits is known. However, there are a number of algorithms that output an absolutely normal number digit-by-digit. In this work, we analyze some of these algorithms with respect to the speed of convergence to normality.

The *discrepancy* of a sequence $(x_n)_{n\geqslant 1}$ of real numbers is the quantity

$$D_N(x_n) = \sup_{I\subset[0,1)} \left| \frac{\sharp\{1 \leqslant n \leqslant N \mid x_n \bmod 1 \in I\}}{N} - |I| \right|,$$

where the supremum is over all subintervals of the unit interval. A sequence is *uniformly distributed modulo one*, or equidistributed, if its discrepancy tends to zero as N tends to infinity.

The *speed of convergence to normality* of a real number x (to some integer base $b \geqslant 2$) is the discrepancy of the sequence $(b^n x)_{n\geqslant 0}$. A real x is normal to base b if and only if $(b^n x)_{n\geqslant 0}$ is uniformly distributed modulo one [130]. Consequently, x is absolutely normal if and only if the orbits of x under the multiplication by b map are uniformly distributed modulo one for every integer $b \geqslant 2$. It is thus natural to study the discrepancy of these sequences quantitatively as a measure for the speed of convergence to normality.

[6] This article appeared in [113]

A result by Schmidt [119] shows that the discrepancy $D_N(x_n)$ of any sequence $(x_n)_{n\geqslant 1}$ of real numbers satisfies $D_N(x_n) \geqslant c\frac{\log N}{N}$ for infinitely many N, where c is some positive absolute constant. The study of sequences whose discrepancy satisfies an upper bound of order $O(\frac{\log N}{N})$, so-called low-discrepancy sequences, is a field in its own right. It is an open problem to give a construction of a normal number to some base that attains discrepancy this low. The best result in this direction is due to Levin [85] who constructed a number normal to one base with discrepancy $O(\frac{\log^2 N}{N})$. It is known [69], that for almost every real number (with respect to Lebesgue measure), for every integer base b, the sequence $(b^n x)_{n\geqslant 0}$ has discrepancy $D_N(b^n x) = O(\frac{\sqrt{\log\log N}}{N^{1/2}})$. For more on normal numbers, discrepancies and uniform distribution modulo one see the books [42], [59] and [42].

A construction for absolutely normal numbers was given by Levin [84] where he constructs a real number α normal to countably many specified real bases $\lambda_i > 1$, $i \geqslant 1$, such that the discrepancy of $(\lambda_i^n\alpha)_{n\geqslant 0}$ satisfies $D_N(\lambda_i^n\alpha) = O(\frac{(\log N)^2\omega(N)}{N^{1/2}})$. The implied constant depends on λ_i and ω is a function that can grow very slowly (it determines the bases to be considered at each step of the construction). Recently, Alvarez and Becher [2] analyzed Levin's work with respect to computability and discrepancy. They show that Levin's construction can yield a computable absolutely normal number α with discrepancy $O(\frac{(\log N)^3}{N^{1/2}})$. To output the first N digits of α, Levin's algorithm takes exponentially many (expensive) mathematical operations. Alvarez and Becher also experimented with small modifications of the algorithm.

In this work the following algorithms are investigated.

Sierpinski. Borel's original proof [34] that almost all real numbers with respect to Lebesgue measure are absolutely normal is not constructive. Sierpinski [123] gave a constructive proof of this fact. Becher and Figueira [11] gave a recursive reformulation of Sierpinski's construction. The resulting algorithm outputs the digits to some specified base b of an absolutely normal number ν, depending on b, in double exponential time. The sequence $(b^n\nu)_{n\geqslant 0}$ has discrepancy $O(\frac{1}{N^{1/6}})$. The calculation does not appear in [11]. We give it in Section 4.1.

Turing. Alan Turing gave a computable construction to show that almost all real numbers with respect to Lebesgue measure are absolutely normal. His construction remained unpublished and appeared first in his collected works [128]. Becher, Figueira and Picchi [13] completed his manuscript and showed that Turing's algorithm computes the digits of an absolutely normal number α in double exponential time. The discrepancy of the sequence $(b^n\alpha)_{n\geqslant 0}$, for integer bases b, is $O(\frac{1}{N^{1/16}})$. This calculation does not appear in [13], we give it in Section 4.4.

Schmidt. In [117], Schmidt gave an algorithmic proof that there exist uncountably many real numbers normal to all bases in a given set R and not normal to all bases in a set S where R and S are such that elements of R are multiplicatively independent of elements of S and such that $R \cup S = \mathbb{N}_{\geqslant 2}$. In his construction he requires S to be non-empty. However, in a final remark he points out that it should be possible to modify his construction for S empty.

The main purpose of this paper is to carry out the details of Schmidt's remark explicitly to give an algorithmic construction of an absolutely normal number ξ. We show that to output the first N digits of ξ to an integer base b it takes exponentially in N many (expensive) mathematical operations. The discrepancy of $(b^n\xi)_{n\geqslant 0}$ is $O(\frac{\log\log N}{\log N})$. A small modification of the algorithm allows for discrepancy $O(\frac{1}{(\log N)^B})$ for any fixed real number $B > 0$, but the output (i.e. ξ) depends on B. For $B > 1$ this convergence is simultaneously faster than the speed of convergence to normality of most constructions of normal numbers (to a single base) by concatenations of blocks (see for example [59] and [116]).

Schmidt's main tool is cancellation in a certain trigonometric sum related to multiplicatively independent bases (Hilfssatz 5 in [117] and Lemma 2.1 here). Schmidt's lemma does not make explicit the magnitude of the involved constants. In Lemma 3.1 we present the detailed calculation and make these constants explicit. The elucidation of the constants in Schmidt's lemma can be of interest independent to the present work.

Becher, Heiber, Slaman [17] gave an algorithm that computes the digits of an absolutely normal number X to some designated base b in polynomial time. The algorithm depends on a parameter function f that controls the speed of convergence to normality. Becher, Heiber and Slaman optimize in f to achieve a polynomial time algorithm. The resulting discrepancy of $(b^nX)_{n\geqslant 0}$ was not analyzed but has been recently presented in [91].

Notation. For a real number x, we denote by $\lfloor x \rfloor$ the largest integer not exceeding x. The fractional part of x is denoted as $\{x\}$, hence $x = \lfloor x \rfloor + \{x\}$. Two functions f and g are $f = O(g)$ or equivalently $f \ll g$ if there is a x_0 and a positive constant C such that $f(x) \leqslant Cg(x)$ for all $x \geqslant x_0$. We mean $\lim_{x\to\infty} f(x)/g(x) = 1$ when we say $f \sim g$ and $g \neq 0$. We abbreviate $e(x) = \exp(2\pi i x)$. Two integers r, s are multiplicatively dependent, $r \sim s$, when they are rational powers of each other.

In our terminology, *mathematical operations* include addition, subtraction, multiplication, division, comparison, exponentiation and logarithm. *Elementary operations* take a fixed amount of time to be computed. When we include the evaluation of a complex number of the form $\exp(2\pi i x)$ as a mathematical operation we refer to it as being *expensive.*

2. Schmidt's Algorithm

In this section we present an algorithm to compute an absolutely normal number. We derived this algorithm from Schmidt's work [117]. Schmidt's construction employs Weyl's criterion for uniform distribution and as such uses exponential sums. The following estimate for trigonometric series is his main tool.

Lemma 2.1 (Hilfssatz 5 in [117])**.** *Let r and s be integers greater than 1 such that $r \not\sim s$. Let K, l be positive integers such that $l \geqslant s^K$. Then*

$$\sum_{n=0}^{N-1} \prod_{k=K+1}^{\infty} |\cos(\pi r^n l / s^k)| \leqslant 2N^{1-a_{20}} \tag{2.1}$$

for some positive constant a_{20} only dependent on r and s.

In Section 3 we give an explicit version of Lemma 2.1.

2.1. **The Algorithm.** We begin by stating Schmidt's algorithm. In Schmidt's notation we are specializing to the case $R = \mathbb{N}_{\geqslant 2}$ and $S = \varnothing$. We considered Schmidt's indications on how to modify the construction to produce absolutely normal numbers.

Setup. Let $\mathcal{R} = (r_i)_{i \geqslant 1} = \mathbb{N}_{\geqslant 2}$ (in non-decreasing order) and let $\mathcal{S} = (s_j)_{j \geqslant 1}$ be a sequence of integers s greater than 2 such that $s_m \leqslant ms_1$ and such that for each $r \in \mathcal{R}$ there is an index $m_0(r)$ such that $r \not\sim s_m$ for all $m \geqslant m_0(r)$. Let $\beta_{i,j} = a_{20}(r_i, s_j)$ from Lemma 2.1 and denote by $\beta_k = \min_{1 \leqslant i,j \leqslant k} \beta_{i,j}$. We can assume that $\beta_k < \frac{1}{2}$. Let $\gamma_k = \max(r_1, \ldots, r_k, s_1, \ldots, s_k)$.

Schmidt assumes that the sequences $\mathcal{R}$ and $\mathcal{S}$ are such that $\beta_k \geqslant \beta_1 / k^{1/4}$ and that $\gamma_k \leqslant \gamma_1 k$ holds. This can be achieved by repeating the values of the sequences $\mathcal{R}$ and $\mathcal{S}$ sufficiently many times. Set $\varphi(1) = 1$ and let $\varphi(k)$ be the largest integer φ such that the conditions

$$\varphi \leqslant \varphi(k-1) + 1, \quad \beta_\varphi \geqslant \frac{\beta_1}{k^{1/4}} \quad \text{and} \quad \gamma_\varphi \leqslant \gamma_1 k$$

hold. Then modify the sequences $\mathcal{R}$ and $\mathcal{S}$ according to $r'_i = r_{\varphi(i)}$, $s'_i = s_{\varphi(i)}$. Note that (up to suitable repetition) $\mathcal{S}$ can be chosen to be the set of positive integers bigger than 2 that are not perfect powers. In principle, using the explicit version of Hilfssatz 5, Lemma 3.1, one could write down $\mathcal{R}$ and $\mathcal{S}$ explicitly.

Following Schmidt, we introduce the following symbols where m is a positive integer. Let $\langle m \rangle = \lfloor e^{\sqrt{m}} + 2s_1 m^3 \rfloor$, denote $\langle m; x \rangle = \lfloor \langle m \rangle / \log x \rfloor$ for $x > 1$ and let $a_m = \langle m; s_m \rangle$, $b_m = \langle m+1; s_m \rangle$.

Algorithm. Step 0: Put $\xi_0 = 0$.

Step m: Compute a_m, b_m, s_m. We have from the previous step ξ_{m-1}. Let $\sigma_m(\xi_{m-1})$ be the set of all numbers

$$\eta_m(\xi_{m-1}) + c^{s_m}_{a_m+1} s_m^{-a_m-1} + \ldots + c^{s_m}_{b_m-2} s_m^{-b_m+2}$$

where the digits c are 0 or 1, and where $\eta_m(\xi_{m-1})$ is the smallest of the numbers $\eta = g s_m^{-a_m}$, g an integer, that satisfy $\xi_{m-1} \leqslant \eta$.

Let ξ_m be the smallest of the numbers in $\sigma_m(\xi_{m-1})$ that minimize

$$A'_m(x) = \sum_{\substack{t=-m \\ t\neq 0}}^{m} \sum_{\substack{i\leqslant m \\ m_0(r_i)\leqslant m}} \left| \sum_{j=\langle m;r_i\rangle+1}^{\langle m+1;r_i\rangle} e(r_i^j t x) \right|^2 \tag{2.2}$$

The following lemma establishes cancellation in the sums A'_m in order for Weyl's criterion to apply.

Lemma 2.2. *There exists a positive absolute constant δ'_1 such that*

$$A'_m(\xi) \leqslant \delta'_1 m^2(\langle m+1\rangle - \langle m\rangle)^{2-\beta_m} \tag{2.3}$$

Proof. Schmidt's proof of Hilfssatz 7 in [117] can directly be adopted. The inner sum in A'_m over j is essentially the same as in Schmidt's function A_m. The outer sums over r_i and t are evaluated trivially and contribute a constant factor times m^2. □

Remark 2.3. *Following the constants in Schmidt's argument shows that $\delta'_1 = 36$ is admissible.*

Schmidt shows that the sequence $(\xi_m)_{m\geqslant 1}$ has a limit ξ that is normal to all bases in the set $\mathcal{R}$, i.e. absolutely normal. We have the approximations

$$\xi_m \leqslant \xi < \xi_m + s_m^{-b_m+2}. \tag{2.4}$$

2.2. **Complexity.** We given an estimate for the number of (expensive) mathematical operations Schmidt's algorithm takes to compute the first N digits of the absolutely normal number ξ to some given base $r \geqslant 2$.

Note that from inequality (2.4), the representation of ξ_M in base s_M agrees on the first $b_M - 2$ digits with the base s_M representation of ξ. These $b_M - 2$ digits of ξ to base s_M determine the first $(b_M - 2)\frac{\log s_M}{\log r}$ digits of ξ to base r. Thus we want to find M such that

$$(b_M - 2)\frac{\log s_M}{\log r} \geqslant N. \tag{2.5}$$

We find that $b_M - 2 > \frac{e^{\sqrt{M}}}{\log s_M}$ for M large enough. Thus, for N large enough, any M that satisfies

$$e^{\sqrt{M}} > N^2$$

also satisfies inequality (2.5). Hence, to compute first N digits of ξ to base r, N large enough, it is enough to carry out $4(\log N)^2$ many steps of the algorithm.

Naively finding the minimum of A'_m in each step $m \leqslant M$ by calculating all values $A'_m(x)$ for x in the set $\sigma_m(\xi_{m-1})$ costs $O(e^{m^{1/2}})$ computations of a complex number of the form $e(r_i^j tx)$ for each of the $2^{b_m - a_m - 2} = O(2^{e^{m^{1/2}}})$ elements x in $\sigma_m(\xi_{m-1})$. Hence in each step m we need to perform $e^{m^{1/2}} \cdot 2^{e^{m^{1/2}}} = O(N2^N)$ mathematical operations. Carrying out $M = 4(\log N)^2$ many steps, these are in total

$$O(N2^N 4(\log N)^2) = O(e^N)$$

many (expensive) mathematical operations.

2.3. **Discrepancy.** We fix a base $r \geqslant 2$ and t shall denote a non-zero integer. For a large natural number N, using Schmidt's Hilfssatz 7, the Erdős-Turán inequality, and via approximating N by a suitable value $\langle M; r\rangle$ we can find an upper bound for the discrepancy $D_N(\{r^n\xi\})$.

Theorem 2.4. *The discrepancy of Schmidt's absolutely normal number ξ is*

$$D_N(\{r^n\xi\}) \ll \frac{\log\log N}{\log N} \tag{2.6}$$

where the implied constant and 'N large enough' depend on the base r.

Proof. For a given N large enough, let M such that $\langle M; r\rangle \leqslant N < \langle M+1; r\rangle$. Such an M satisfies a lower bound of the form $M \gg (\log N)^2$ if N is large enough.

We split the Weyl sum $\sum_{n=1}^N e(r^n t\xi)$ according to

$$\sum_{n=1}^{N} e(r^n\xi t) = \sum_{n=1}^{\langle M;r\rangle} e(r^n\xi t) + \sum_{n=\langle M;r\rangle+1}^{N} e(r^n\xi t). \tag{2.7}$$

An estimate for the first sum $\sum_{n=1}^{\langle M;r\rangle} e(r^n \xi t)$ in equation (2.7) can be obtained from equation (2.2) and yields

$$\begin{aligned}\sum_{n=1}^{\langle M;r\rangle} e(r^n t\xi) &= \sum_{m=m_0(r)}^{M-1} \sum_{n=\langle m;r\rangle+1}^{\langle m+1;r\rangle} e(r^n t\xi) + O(1)\\ &\ll \sum_{m=m_0(r)}^{M-1} m(\langle m+1\rangle - \langle m\rangle)^{1-\frac{\beta_m}{2}}\\ &\leqslant M \sum_{m=1}^{M-1} (\langle m+1\rangle - \langle m\rangle)^{1-\frac{\beta_M}{2}}\\ &< M^2 \left(\sum_{m=1}^{M-1} \langle m+1\rangle - \langle m\rangle\right)^{1-\frac{\beta_M}{2}}\end{aligned}$$

which is equal to $M^2\langle M\rangle^{1-\frac{b_M}{2}}$. Using the decay property $\beta_M \geqslant \beta_1 M^{-1/2}$, the first sum in equation (2.7) is thus

$$\ll M^2 e^{M^{1/2}-\frac{\beta_1}{2}M^{1/4}}. \tag{2.8}$$

For the error of approximation of N via $\langle M;r\rangle$ we calculate for fixed r, s_1, and M large enough,

$$\langle M+1;r\rangle - \langle M;r\rangle \ll e^{\sqrt{M}}\left(e^{\frac{1}{2\sqrt{M}}} - 1 + \frac{M^2}{e^{\sqrt{M}}}\right) \tag{2.9}$$

where the implied constant depends on s_1 and r. We used $\sqrt{M+1}-\sqrt{M} = 1/(\sqrt{M+1}+\sqrt{M}) \leqslant 1/2\sqrt{M}$. For M large enough we have $e^{1/2\sqrt{M}} \leqslant 1 + \frac{1}{\sqrt{M}}$, hence the right-hand side of estimate (2.9) is

$$\leqslant e^{\sqrt{M}}\left(\frac{1}{\sqrt{M}} + \frac{M^2}{e^{\sqrt{M}}}\right).$$

Thus,

$$\langle M+1;r\rangle - \langle M;r\rangle = e^{\sqrt{M}} \cdot O\left(\frac{1}{\sqrt{M}}\right) = \langle M;r\rangle \cdot O\left(\frac{1}{\sqrt{M}}\right). \tag{2.10}$$

By the choice of M, $\langle M;r\rangle \leqslant N$ and $M \gg (\log N)^2$. Thus equation (2.10) is

$$\ll \frac{N}{\log N},$$

hence the second term in equation (2.7) dominates the first.

The Erdős-Turán inequality applied to the sequence $\{r^n\xi\}_{n\geqslant 0}$ is

$$D_N(\{r^n\xi\}) \ll \frac{1}{H} + \sum_{t=1}^{H} \frac{1}{t}\left|\frac{1}{N}\sum_{n=1}^{N} e(r^n\xi t)\right| \tag{2.11}$$

where H is a natural number. Splitting the exponential sum as before and upon putting $H = \log N$, we thus obtain

$$D_N(\{r^n\xi\}) \ll \frac{\log\log N}{\log N}$$

where the implied constant depends on the base r. □

2.4. **Modifying Schmidt's Algorithm.** We show that it is possible to modify Schmidt's algorithm for a given real number $B > 0$ to output an absolutely normal number ξ, depending on B, with discrepancy $D_N(\{r^n\xi\}) = O_r(\frac{\log\log N}{(\log N)^B})$ to base r, where the implied constant depends on r, thus exponentially lowering the discrepancy associated to Schmidt's algorithm by exponent of B.

Proposition 2.5. *Fix $0 < c < 1$. Schmidt's algorithm still holds when the function $\langle m\rangle$ is replaced by the function*

$$\langle m\rangle = \lfloor e^{m^c}\rfloor.$$

Note that the functions $\langle m; r\rangle$, a_m and b_m and also the construction of the sets σ_m have to be modified accordingly. The algorithm works in exact the same way, but the output depends on c.

Proof. We need to show that the estimate (2.3) for A'_m is still valid with this choice of $\langle m\rangle$. In course of the proof of this estimate, Schmidt evaluates the inner sum over j in A'_m trivially on a range of size $O(m)$. This range constitutes only a minor part of the full sum over j since $m \leqslant \delta(\langle m+1\rangle - \langle m\rangle)^{1-\varepsilon}$ for some $\delta > 0$ and some $0 < \varepsilon < 1$. This can be seen from

$$\begin{aligned} e^{(m+1)^c} - e^{m^c} &= e^{m^c}\left(e^{(m+1)^c - m^c} - 1\right) \\ &\geqslant e^{m^c}\left((m+1)^c - m^c\right) \\ &\gg c m^{c\alpha} m^{c-1} \end{aligned}$$

since $e^{m^c} \gg m^{c\alpha}$ for any $\alpha > 0$. Choosing $\alpha = \frac{2}{c} - 1 + \eta$ for some $\eta > 0$ gives

$$\langle m+1\rangle - \langle m\rangle \gg c m^{c\alpha} m^{c-1} = c m^{1+\eta}$$

which establishes our claim. □

The discrepancy of $\xi = \xi_c$ can be estimated the same way as before. Note that any N large enough can now be approximated by the function $\langle M \rangle$ with error

$$O(\langle M+1 \rangle - \langle M \rangle) \ll e^{M^c} \frac{1}{M^{1-c}}$$

which with M of order $(\log N)^{1/c}$ is

$$\frac{N}{(\log N)^{\frac{1-c}{c}}}.$$

Hence the discrepancy of the sequence $\{r^n \xi\}_{n \geqslant 0}$ satisfies

$$D_N(\{r^n \xi\}) \ll \frac{\log \log N}{(\log N)^B} \tag{2.12}$$

with $0 < B = \frac{1-c}{c} < \infty$.

3. The Constants a_{20} in Schmidt's Hilfssatz 5

In this section we prove the following explicit variant of Schmidt's Hilfssatz 5 in [117].

Lemma 3.1 (Explicit variant of Lemma 2.1)**.** *Let r and s be integers greater than* 1 *such that $r \not\sim s$. Let K, l be positive integers such that $l \geqslant s^K$ and denote $m = \max(r, s)$. Then for*

$$N \geqslant N_0(r, s) = \exp(288 \cdot (12m(\log m)^4 + 8(\log m)^3 + (\log m)^2)) \tag{3.1}$$

we have

$$\sum_{n=0}^{N-1} \prod_{k=K+1}^{\infty} |\cos(\pi r^n l / s^k)| \leqslant 2N^{1-a_{20}} \tag{3.2}$$

for some positive constant a_{20} as specified in equation (3.25) *that satisfies*

$$a_{20} = \frac{1}{6} \frac{\pi^2}{2} \cdot 0.007 \cdot \frac{1}{s^4} \frac{1}{\log s} \left(\frac{1}{\log s} - \frac{1}{s} \right). \tag{3.3}$$

Remark 3.2. *The statement of Lemma 3.1 holds true* for all N *with*

$$a_{20} = \min \left(\frac{1}{N_0 \log N_0}, \frac{-\log \cos(\frac{\pi}{s^2})}{2 \log N_0} \right) \tag{3.4}$$

as specified in equation (3.27) *where $N_0 = N_0(r, s)$ as in equation* (3.1)*.*

This enables us in principle to give an explicit description of the sequences $(r_i)_{i \geqslant 1}$ and $(s_j)_{j \geqslant 1}$ *after* the repetition of the entries via the function φ as suggested by Schmidt. Lemma 3.1 might also be of independent interest as its non-explicit variant has been used by several authors, see e.g. [8] and [19]. We do not claim optimality of the bounds in Lemma 3.1.

Proof. The proof is basically a careful line-by-line checking of Schmidt's proof of Lemma 2.1. The reader might find it helpful having a copy both of [118] and [117] at hand.

We follow Schmidt's notation and his argument in [117].

Let h be the number of distinct prime divisors of rs and let

$$r = p_1^{d_1} \cdot \ldots \cdot p_h^{d_h},$$
$$s = p_1^{e_1} \cdot \ldots \cdot p_h^{e_h}$$

be the prime factorizations of r and s with d_i and e_i not both equal to zero. We assume the p_i to be ordered such that

$$\frac{d_1}{e_1} \geqslant \ldots \geqslant \frac{d_h}{e_h},$$

with the convention that $\frac{d}{0} = +\infty$. This implies that $d_k e_l - d_l e_k \geqslant 0$ for all $k \geqslant l$.

Let $b = \max_i(d_i) \cdot \max_i(e_i)$. Schmidt denotes by l_i numbers not divisible by p_i^{2b}.

For $1 \leqslant i \leqslant h$, let

$$u_i = (p_1^{d_1} \ldots p_i^{d_i})^{e_i} (p_1^{e_i} \ldots p_i^{e_i})^{-d_i}$$
$$v_i = (p_{i+1}^{e_{i+1}} \ldots p_h^{e_h})^{d_i} (p_{i+1}^{d_{i+1}} \ldots p_h^{d_h})^{-e_i},$$

where empty products (for $i = h$) are 1. These numbers are integers, and $t_i = \frac{u_i}{v_i}$ is not equal to 1 since $r \not\sim s$. We have $t_i = \frac{r^{e_i}}{s^{d_i}}$, hence, when writing t_i in lowest terms, the prime p_i has been cancelled.

Let $f_i = p_i - 1$ if p_i is odd, and $f_i = 2$ otherwise. There are well-defined integers g_i such that

$$t_i^{f_i} \equiv 1 + q_i p_i^{g_i - 1} \pmod{p_i^{g_i}}$$

with $p_i \nmid q_i$ (especially $q_i \neq 0$). We have $g_i > 1$ by the small Fermat theorem and for $p_i = 2$ we even have $g_i > 2$ since squares are congruent 1 modulo 4. To give an upper bound for g_i, note that $p_i^{g_i}$ can be at most equal to $t_i^{f_i}$. Hence $g_i \leqslant \lfloor f_i \frac{\log t_i}{\log p_i} \rfloor + 1$. Since naively $\log p_i \geqslant \log 2$, $\log t_i = e_i \log r - d_i \log s \leqslant e_i \log r \leqslant \frac{\log r \log s}{\log 2}$ and $p_i \leqslant \max(r, s)$, a trivial upper bound on g_i, valid for all i, is

$$g_i \leqslant 12 \max(r, s) \log r \log s.$$

Let $a_1 = \max(g_1, \ldots, g_h)$. Then

$$2 \leqslant a_1 \leqslant 12 \max(r, s) \log r \log s. \tag{3.5}$$

Assume $k \geqslant a_1$, $e_i > 0$. The constant a_2 is such that at most $a_2(s/2)^k$ of the numbers $l_i t_i^n$ fall in the same residue class modulo s^k if n runs through a set of representatives modulo s^k (Hilfssatz 1 in [117]). At most $p_i^{2b} p_i^{g_i}$ of the numbers $t_i^n l_i$ fall in the same residue class modulo p_i^k if n runs through a set of representatives modulo p_i^k. If $p_i | s$, then there are at most $(s/2)^k$ elements in a set of representatives modulo s^k that are congruent to each other. Hence $a_2 = \max_{i,e_i>0} p_i^{2b+g_i}$. Naive upper and lower bounds on a_2 are thus

$$8 \leqslant a_2 \leqslant \max(r,s)^{8\log(\max(r,s))+12\max(r,s)\log r\log s}. \tag{3.6}$$

The constant a_4 (named α_3 in [118]) is chosen such that

$$(s^2-2)^{a_4} < 2^{1/4+2a_4} a_4^{a_4} (1-2a_4)^{1/2-a_4}. \tag{3.7}$$

The right-hand side of inequality (3.7) as a function of a_4 (denote it by $f(a_4)$) can be numerically analyzed. It is a strictly decreasing continuous function on the interval $(0, 1/16]$ with values $f(0^+) = \sqrt[4]{2} \approx 1.19 > f(1/16) \approx 1.028 > 1$. Hence any a_4 in $(0, 1/16)$ that satisfies

$$(s^2-2)^{a_4} \leqslant f(1/16) \tag{3.8}$$

also satisfies inequality (3.7). Note that $a_4 < 1/16$ is no proper restriction as $a_4(2) \approx 0.055 < 1/16$ and since a_4 is decreasing in s. Now, inequality (3.8) is easy to solve and gives

$$a_4(s) \geqslant \frac{c}{\log(s^2-2)}$$

for $c = \log(f(1/16)) \approx 0.028$. This constitutes a non-trivial (i.e. positive) lower bound on the values of a_4 that are admissible. To simplify matters we continue with this value for a_4, i.e. we put

$$a_4 = \frac{0.028}{\log(s^2-2)}. \tag{3.9}$$

The constant a_3 also comes from the earlier Schmidt paper [118] and was called α_4 there. Schmidt counts the number blocks of digits in base s with few ‘nice’ digit pairs. These are successive digits not both equal to zero or $s-1$. He derives the proof of Lemma 3 in [118] that the number of combinations of k base s digits with less than $\alpha_3 k (= a_4 k)$ nice digit pairs, counting only non-overlapping pairs of digits, does not exceed

$$k \binom{\frac{k}{2}}{\lfloor a_4 k \rfloor} (s^2-2)^{\lfloor a_4 k\rfloor} 2^{k/2-\lfloor a_4 k\rfloor}. \tag{3.10}$$

With the approximation

$$\sqrt{2\pi} n^{n+1/2} e^{-n} \leqslant n! \leqslant e n^{n+1/2} e^{-n}$$

we find that the quantity (3.10) is

$$\leqslant k\frac{e}{2\pi}\frac{\left(\frac{k}{2}\right)^{k/2+1/2}}{(a_4k)^{a_4k+1/2}\left(\frac{k}{2}-a_4k\right)^{k/2-a_4k+1/2}}(s^2-2)^{a_4k}2^{k/2-a_4k}2^{-1}$$

$$= \frac{e}{2\pi}\frac{1}{\sqrt{a_4}\sqrt{1-2a_4}}\frac{1}{2}\cdot\frac{1}{(2a_4)^{a_4k}(1-2a_4)^{(1/2-a_4)k}}. \tag{3.11}$$

In [118], Schmidt denotes the constant factor by α_5,

$$\alpha_5 = \frac{e}{4\pi\sqrt{a_4(1-2a_4)}}.$$

Using $a_4 \leqslant 0.055$ and $a_4 \geqslant \frac{c}{\log(s^2-2)}$ with $c \approx 0.028$ we obtain the upper bound

$$\alpha_5 \leqslant 1.87\sqrt{\log s} \approx 2\sqrt{\log s}. \tag{3.12}$$

Finally, a_3 is such that if $k \geqslant a_3$, and respecting the choice of a_4, then

$$\alpha_5 k\frac{(s^2-2)^{a_4k}2^{(1/2-a_4)k}}{(2a_4)^{a_4k}(1-2a_4)^{(1/2-a_4)k}} < 2^{3/4\cdot k}$$

holds. The left-hand side is equal to

$$\alpha_5 k\left(\frac{(s^2-2)^{a_4}}{f(a_4)}2^{3/4}\right)^k = \alpha_5 k\left(\frac{f(1/16)}{f(a_4)}2^{3/4}\right)^k \leqslant \alpha_5 k 2^{0.74k}$$

by the choice of a_4 and since $f(a_4) \geqslant f(0.055) > f(1/16)$. Using $\log(x) \leqslant x^{1/2}$ for all $x \geqslant 0$,

$$\alpha_5 k 2^{0.74k} < 2^{3/4\cdot k}$$

is satisfied for all k larger than

$$a_3 = 120\sqrt{\log(s)}. \tag{3.13}$$

Let $N \geqslant \max(s^{a_1}, s^{a_3+1})$ (hence certainly $N \geqslant s^2$ since $a_1 \geqslant 2$) and let k be such that $s^k \leqslant N < s^{k+1}$. The constants a_7 and a_5 in Hilfssatz 2 in [117] are such that

$$a_2(s/2)^k s 2^{3k/4} < a_7 N^{1-a_5}.$$

With $k > \frac{\log N}{\log s} - 1$ the left-hand side is

$$< a_2 s N^{1-\frac{\log 2}{4}\left(\frac{1}{\log s}-\frac{1}{\log N}\right)}$$

which is

$$\leqslant a_2 s N^{1-\frac{\log 2}{8\log s}} \tag{3.14}$$

due to $N \geqslant s^2$. Hence $a_7 = a_2 s$. We want quantity (3.14) to be $< N^{1-\frac{\log 2}{16\log s}}$, hence

$$a_5 = \frac{\log 2}{16\log s} > 0. \tag{3.15}$$

This happens, if

$$\frac{\log(a_2 s)}{\log N} < \frac{\log 2}{16 \log s}$$

which is satisfied when $N \geqslant N_0^{\text{HS2}}$, where

$$\log N_0^{\text{HS2}} = 288m(\log m)^4 + 192(\log m)^3 + 24(\log m)^2 \tag{3.16}$$

where we denoted $m = \max(r, s)$. Note that in particular N is much larger than e^s.

The constant a_6 is such that $a_4 k > a_6 \log N$. With $a_4 \geqslant \frac{0.028}{\log(s^2-2)} > \frac{0.014}{\log s}$ and $k > \frac{\log N}{\log s} - 1$ and due to $N \geqslant e^s$, we have

$$a_4 k > \log N \frac{0.014}{\log s}\left(\frac{1}{\log s} - \frac{1}{s}\right).$$

This is a positive value for all s. Hence

$$a_6 = \frac{0.014}{\log s}\left(\frac{1}{\log s} - \frac{1}{s}\right) > 0 \tag{3.17}$$

is an admissible choice for a_6.

Recall that h was defined as the number of distinct prime divisors in rs so that $r = p_1^{d_1} \cdot \ldots \cdot p_h^{d_h}$, $s = p_1^{e_1} \cdot \ldots \cdot p_h^{e_h}$ are the prime factorizations of r and s with d_i and e_i not both equal to zero. Recall that $b = \max_i(d_i) \cdot \max_i(e_i)$.

In Hilfssatz 3 in [117], Schmidt divides the set numbers lr^n in at most hb subsets each of which contains a certain number of consecutive lr^n. If the number of elements in such a subset is $\leqslant N^{1/2}$, he counts trivially. If the number of elements in such a subset is larger than $N^{1/2}$, he uses Hilfssatz 2 with this N. Hence the N in Hilfssatz 3 needs to be large enough such that $N^{1/2}$ is large enough for Hilfssatz 2. Thus, for

$$N \geqslant N_0^{\text{HS3}} = (N_0^{\text{HS2}})^2 = \exp(2 \cdot (288m(\log m)^4 + 192(\log m)^3 + 24(\log m)^2)) \tag{3.18}$$

there are at most hbN^{1-a_5} numbers of the lr^n having less than $a_6 \log \sqrt{N}$ nice digit pairs. Hence

$$a_9 = \frac{a_6}{2} = \frac{0.007}{\log s}\left(\frac{1}{\log s} - \frac{1}{s}\right). \tag{3.19}$$

We have the trivial bound is $h \leqslant \log_2(rs) \leqslant \frac{2\log m}{\log 2}$ with $m = \max(r, s)$. Another trivial bound is $b = \max_i(d_i) \cdot \max_i(e_i) \leqslant (\log_2(m))^2$. Thus with $N \geqslant e^{288m}$, we have

$$hbN^{1-a_5} \leqslant 7(\log m)^3 N^{1-a_5} \leqslant N^{1-a_8}$$

with

$$a_8 = a_5 - \frac{\log 7 + 3\log\log m}{288m} = \frac{\log 2}{16\log s} - \frac{\log 7 + 3\log\log m}{288m}. \tag{3.20}$$

Recall from Schmidt's paper that $z_K(x)$ denotes the number of nice digit pairs $c_{i+1}c_i$ of x with $i \geqslant K$ where the c are the digits of x in base s.

In Hilfssatz 4, Schmidt begins with the restriction $n \geqslant N^{2/3} \log s / \log r$ which reduces a_{14} to a value less than $1/3$. The remaining numbers lr^n are divided in at most $2N^{2/3}$ many intervals of length $\lfloor N^{1/3} \rfloor$ which are analyzed separately. The restriction $n \geqslant N^{2/3} \log s / \log r$ implies $lr^n \geqslant s^{K + \lfloor N^{1/3} \rfloor^2}$.

Denote by n_0 a number $N^{2/3} \log s / \log r \leqslant n_0 < N$. Schmidt wants to apply Hilfssatz 3 to intervals $N^{2/3} \log s / \log r \leqslant n_0 \leqslant n < n_0 + \lfloor N^{1/3} \rfloor$ of length $\lfloor N^{1/3} \rfloor$. However, he makes one further preliminary reduction in showing that one can assume that $z_K(l)$ is less than $\frac{a_9}{2} \log N$.

Denote by n_1 the least $n \geqslant N^{2/3} \log s / \log r$ such that $z_K(lr^n) < \frac{a_9}{2} \log N$. Replace lr^n for $n \geqslant n_1$ by $l^* r^{n-n_1}$ where $l^* = lr^{n_1}$. All lr^n with $N^{2/3} \log s / \log r \leqslant n < n_1$ are by the choice of n_1 such that $z_K(lr^n) \geqslant \frac{a_9}{2} \log N$. As Schmidt's version is not explicit, he can assume N to be large enough, and apply Hilfssatz 3 to the interval $n_1 \leqslant n < N$ (or $0 \leqslant n < N - n_1$ for numbers $l^* r^n$).

To make things explicit, we distinguish three cases for the size of n_1. We write $M = \lfloor N^{1/3} \rfloor$ for the number of lr^n under consideration. We want to find explicit lower bounds on M such that we can apply Hilfssatz 3.

Case 0: n_1 does not exist at all. Then the number of lr^n with z_K less than $a_9 \log M$ is trivially less than M^{1-a} for any $0 < a < 1$.

Case 1: n_1 is large such that the number of lr^n with $z_K(lr^n) < a_9 \log M$ can be trivially estimated by $M - n_1 \leqslant M^{1-a_8}$. This is the case when $n_1 \geqslant M - M^{1-a_8}$.

Case 2: $n_1 < M - M^{1-a_8}$. We need the interval $M - n_1$ to be large enough to be able to apply Hilfssatz 3 to obtain cancellation, i.e. $M - n_1 \geqslant N_0^{\mathrm{HS3}}$ which holds if $M \geqslant M_0 = (N_0^{\mathrm{HS3}})^{\frac{1}{1-a_8}}$. Thus by Hilfssatz 3 the number of lr^n, $n_0 \leqslant n < n_0 + M$, with $z_K(lr^n) < a_9 \log N$ is at most $(M - n_1)^{1-a_8} \leqslant M^{1-a_8}$.

Schmidt uses a reduction to count only z_K instead of all nice digit pairs. This reduction looses at one point 2 digit pairs, i.e. after an application of Hilfssatz 3 one finds numbers with at most $a_9 \log M - 2$ nice digit pairs. This is $\leqslant \frac{a_9}{2} \log M$ for

$$\log M > \frac{4}{a_9}. \tag{3.21}$$

Also, Schmidt's reduction works if

$$M \frac{\log r}{\log s} < \left\lfloor \frac{M^2 - 1}{\frac{a_9}{2} \log M} \right\rfloor - 1. \tag{3.22}$$

Note that inequalities (3.21) and (3.22) do not pose further restrictions on M.

Finally, from $M \geqslant (N_0^{\mathrm{HS3}})^{\frac{1}{1-a_8}}$, $M = \lfloor N^{1/3} \rfloor$, and since we may assume that $a_8 < \frac{1}{2}$, the requirement

$$N \geqslant N_0^{\mathrm{HS4}} = (N_0^{\mathrm{HS3}})^6 = \exp(288 \cdot (12m(\log m)^4 + 8(\log m)^3 + (\log m)^2)) \tag{3.23}$$

for the original N follows. We established that in each subsequence of length $\lfloor N^{1/3} \rfloor$ there are at most $\lfloor N^{1/3} \rfloor^{1-a_8}$ elements lr^n with $z_K(lr^n) < \frac{a_9}{2} \log \lfloor N^{1/3} \rfloor$.

In total, since there are at most $2N^{2/3}$ many intervals for n of length $\lfloor N^{1/3} \rfloor$, we obtain (for $\log N \geqslant \frac{6 \log 3}{a_8}$) that there are at most

$$N^{2/3} \frac{\log s}{\log r} + 2N^{2/3} \cdot \lfloor N^{1/3} \rfloor^{1-a_8} \leqslant 3N^{1-a_8/3} \leqslant N^{1-a_8/6}$$

elements lr^n, $0 \leqslant n < N$, with $z_K(lr^n) < \frac{a_9}{2} \log \lfloor N \rfloor^{1/3} \leqslant \frac{a_9}{6} \log N$. Thus

$$a_{14} = \frac{a_8}{6}, \quad a_{15} = \frac{a_9}{6}. \tag{3.24}$$

From Hilfssatz 5 follows that $a_{20} = \min(a_{14}, a_{22})$ where $a_{22} = -a_{15} \log a_{21}$ with $a_{21} = \cos(\pi/s^2)$. We have $-\log a_{21} = -\log\cos(\frac{\pi}{s^2}) \geqslant \frac{\pi^2}{2} \frac{1}{s^4}$. Plugging in the values of a_{14} and a_{15} shows that $\min(a_{14}, a_{22}) = a_{22}$. Hence

$$a_{20} = \frac{1}{6} \frac{\pi^2}{2} \cdot 0.007 \cdot \frac{1}{s^4} \frac{1}{\log s} \left(\frac{1}{\log s} - \frac{1}{s} \right) \tag{3.25}$$

where the constant factor is approximately 0.0057.

To find a_{20} such that Lemma 3.1 holds *for all* N, we need to replace a_{14} and a_{15} by sufficiently small constants such that Hilfssatz 4 holds for all N. This can be achieved by redefining

$$a_{14} = \min(a_{14}, 1 - \frac{\log(N_0 - 1)}{\log N_0}), \quad \text{and} \quad a_{15} = \min(a_{15}, \frac{1}{2 \log N_0})$$

where we denoted $N_0 = N_0^{\mathrm{HS4}}$. We have $a_{14}^{\mathrm{old}} \approx 0.007 \frac{1}{\log s}$ and $1 - \frac{\log(N_0-1)}{\log N_0} \leqslant \frac{2}{N_0 \log N_0}$ which decays worse than exponentially in m. Furthermore, $a_{15}^{\mathrm{old}} \approx 0.001 \frac{1}{\log s}$ and $\frac{1}{2 \log N_0}$ is worse than linear with in m a large constant. Note also $1 - \frac{\log(N_0-1)}{\log N_0} \geqslant \frac{1}{N_0 \log N_0}$. Hence Hilfssatz 4 holds true for all N with constants

$$a_{14} = \frac{1}{N_0 \log N_0}, \quad \text{and} \quad a_{15} = \frac{1}{2 \log N_0} \tag{3.26}$$

with $N_0 = N_0^{\mathrm{HS4}}$ as in equation (3.23).

The constant a_{20} then modifies according to

$$a_{20} = \min(a_{14}, a_{22}) = \min \left(\frac{1}{N_0 \log N_0}, \frac{-\log\cos(\frac{\pi}{s^2})}{2 \log N_0} \right). \tag{3.27}$$

For large m, a_{20} equals a_{14} but since $a_{22} \geqslant \frac{\pi^2}{4}\frac{1}{s^4 \log N_0}$, for small m we have $a_{20} = a_{22}$. Explicitly, with $a_{14} \leqslant \frac{1}{e^m 1728m}$ we have

$$a_{20} = \frac{1}{N_0 \log N_0} \tag{3.28}$$

for $m \geqslant 7$ were we denoted $m = \max(r, s)$ and $N_0 = N_0^{\mathrm{HS4}}$ as given in equation (3.23). □

4. Algorithms by Sierpinski and Turing

4.1. **Sierpinski's Algorithm.** In this section we estimate the runtime and discrepancy of the effective version of Sierpinsk's algorithm [123] by Becher and Figueira [11]. This algorithm outputs the digits to some specified base b of an absolutely normal number ν, depending on b, in double exponential time such that the sequence $(b^n\nu)_{n\geqslant 0}$ has discrepancy $O(\frac{1}{N^{1/6}})$.

Let $0 < \varepsilon \leqslant \frac{1}{2}$ be a rational (or computable real) number that remains fixed throughout the algorithm. We also choose in advance a base $b \geqslant 2$. The algorithm computes the digits to base b of an absolutely normal number ν. The output (i.e. ν) depends on the choice of ε and b.

Notation. Let m, q, p be integers such that $m \geqslant 1$, $q \geqslant 2$ and $0 \leqslant p \leqslant q-1$ and put $n_{m,q} = \lfloor \frac{24m^6q^2}{\varepsilon} \rfloor + 2$.

Let $\Delta_{q,m,n,p}$ be the interval $(\frac{0.b_1 \ldots b_{n-1}(b_n - 1)}{q^n}, \frac{0.b_1 \ldots b_{n-1}(b_n+2)}{q^n})$ where the string $b_1 \ldots b_n$ is such that the digit p appears too often, i.e. $|\frac{N_p(b_1 \ldots b_n)}{n} - \frac{1}{q}| \geqslant \frac{1}{m}$ where $N_p(b_1 \ldots b_n)$ denotes the number of occurrences of the digit p amongst the b_i.

Let

$$\Delta = \bigcup_{q=2}^{\infty} \bigcup_{m=1}^{\infty} \bigcup_{n=n_{m,q}}^{\infty} \bigcup_{p=0}^{q-1} \Delta_{q,m,n,p},$$

and denote a truncated version of Δ by

$$\Delta_k = \bigcup_{q=2}^{k+1} \bigcup_{m=1}^{k} \bigcup_{n=n_{m,q}}^{k \cdot n_{m,q}} \bigcup_{p=0}^{q-1} \Delta_{q,m,n,p}.$$

The complement of Δ in $[0, 1)$ is

$$E = [0, 1) \setminus \Delta.$$

Sierpinski's algorithm computes the digits to base b of a number $\nu \in E$. This number is absolutely normal as shown by Sierpinski and in Theorem 7 in [11].

The truncated sets Δ_k approximate Δ in the sense that if a number is not in Δ_k for large enough k, then it is also not in Δ. Becher and Figueira's algorithm computes the digits of ν such that the n-th digit ensures that ν is not in some Δ_{p_n}, where $p_n \to \infty$.

The Algorithm. First digit: Split the unit interval in subintervals $c_d^1 = [\frac{d}{b}, \frac{d+1}{b})$ for $0 \leqslant d < b$. Put $p_1 = 5 \cdot (b-1)$. Compute the Lebesgue measure of $\Delta_{p_1} \cap c_d^1$ for all d. The first digit b_1 of ν is chosen such that it is (the smallest among) the d such that the Lebesgue measure of $\Delta_{p_1} \cap c_{b_1}^1$ is minimal among the $\Delta_{p_1} \cap c_d^1$.

n-th digit: Split the interval $[0.b_1 \dots b_{n-1}, 0.b_1 \dots (b_{n-1}+1))$ in subintervals

$$c_d^n = [0.b_1 \dots b_{n-1}d, 0.b_1 \dots b_{n-1}(d+1))$$

for all $0 \leqslant d < b$. Put $p_n = 5 \cdot (b-1) \cdot 2^{2n-2}$. The n-th digit b_n of ν is the (smallest of the) d that minimize the Lebesgue measure of the $\Delta_{p_n} \cap c_d^n$.

4.2. **Runtime.** For fixed q, m, n and p, writing down all strings $b_1 \dots b_n$ of length n of digits $0 \leqslant b_i < b$ that satisfy the conditions of $\Delta_{q,m,n,p}$ takes exponential time in n. Naively estimating gives the complexity of computing Δ_k as being exponential in k. So, since p_n grows exponentially in n, the computation of Δ_{p_n} takes doubly exponentially many elementary operations.

4.3. **Discrepancy.** We give an estimate for the discrepancy of $(q^n\nu)_{n \geqslant 1}$, valid for any $\nu \in E$ and any base $q \geqslant 2$, not taking into account that the algorithm might in fact construct an element with better distributional properties.

The family of intervals $\bigcup_{p=0}^{q-1} \Delta_{b,m,n,p}$ contains all real numbers with expansion to base b not simply normal regarding the first n digits. The union

$$\Delta_{q,m} = \bigcup_{n=n_{m,q}}^{\infty} \bigcup_{p=0}^{q-1} \Delta_{q,m,n,p}$$

contains all real numbers whose base-q expansion is not simply normal regarding any large enough number of digits. Hence any ν not in $\Delta_{q,m}$ satisfies

$$\left| \frac{\sharp\{n \leqslant N \mid \{q^n\nu\} \in I\}}{N} - |I| \right| < \frac{1}{m}$$

for all $N \geqslant n_{m,q}$ and I of the form $I = [\frac{p}{q}, \frac{p+1}{q})$, $p = 0, \dots, q-1$.

Inverting the relation between N and m and using Sierpinski's choice for $n_{m,q} = \lfloor \frac{24m^6q^2}{\varepsilon} \rfloor + 2 \approx \frac{24m^6q^2}{\varepsilon}$, we find that

$$\sup_{p=0,\dots q-1} \left| \frac{\sharp\{n \leqslant N \mid \{q^n\nu\} \in [\frac{p}{q}, \frac{p+1}{q})\}}{N} - |I| \right| \leqslant \left(\frac{24}{\varepsilon}\right)^{1/6} \frac{q^{1/3}}{N^{1/6}} + O\left(\frac{1}{N^{1/3}}\right) \ll_\varepsilon q^{1/3} \frac{1}{N^{1/6}}$$

where the implied constant depends on ε but not on q.

Fix $I \subset [0,1)$, $\delta > 0$ and k such that $\frac{2}{q^k} < \delta$. Choose l, m such that $I \subset [\frac{l}{q^k}, \frac{m}{q^k})$ and $|I| < \frac{m-l}{q^k} + \frac{2}{q^k}$. Then

$$\begin{aligned}\frac{\sharp\{n \leqslant N \mid \{q^n\nu\} \in I\}}{N} &\leqslant \frac{\sharp\{n \leqslant N \mid \{q^n\nu\} \in [\frac{l}{q^k}, \frac{m}{q^k})\}}{N} \\ &\ll \frac{m-n}{q^k} + O\left((q^k)^{1/3}\frac{1}{N^{1/6}}\right) \\ &< |I| + \delta + O\left((q^k)^{1/3}\frac{1}{N^{1/6}}\right) \\ &= |I| + \delta + O_\delta\left(\frac{1}{N^{1/6}}\right).\end{aligned}$$

Since δ and I were arbitrary, this shows that

$$D_N(\{q^n\nu\}) \ll \frac{1}{N^{1/6}}$$

for any $\nu \in E$ and any base q.

4.4. **Turing's Algorithm.** Since Turing's algorithm has been very well studied in [13], we restrict ourselves to presenting their result in our terminology. Becher, Figueira and Picchi [13] show that Turing's algorithm computes the digits of an absolutely normal number α in double exponential time. With respect to the speed of convergence to normality Becher, Figueira and Picchi note (Remark 23 in [13]) that for each initial segment of α of length $N = k2^{2n+1}$ expressed to each base up to e^L all words of length up to $L = \sqrt{\log N}/4$ occur with the expected frequency plus or minus e^{-L^2}. Here, k is a positive integer parameter, and n is the step of the algorithm.

The discrepancy of $\{b^n\alpha\}$ for some base $b \geqslant 2$ can then be calculated as follows. Fix some arbitrary $\varepsilon > 0$ and an subinterval $I \subset [0,1)$. Let n be large enough, such that $\frac{2}{b^L} < \varepsilon$. Approximate I by a b^L-adic interval $[\frac{c}{b^L}, \frac{d}{b^L})$ such that $[\frac{c-1}{b^L}, \frac{d+1}{b^L}) \supset I \supset [\frac{c}{b^L}, \frac{d}{b^L})$. Then

$$\begin{aligned}\frac{\sharp\{0 \leqslant m < N \mid \{b^m\alpha\} \in I\}}{N} <& \frac{\sharp\{0 \leqslant m < N \mid \{b^m\alpha\} \in [\frac{c}{b^L}, \frac{d}{b^L})\}}{N} \\ \leqslant& \frac{d-c+2}{b^L} + O(e^{-L^2})) \\ \leqslant& |I| + \varepsilon + O\left(\frac{1}{N^{1/16}}\right).\end{aligned}$$

Since I and ε were arbitrary this means that $\{b^n\alpha\}$ is uniformly distributed modulo one with discrepancy bounded by $O(\frac{1}{N^{1/16}})$.

Acknowledgements. This research was supported by the Austrian Science Fund (FWF): I 1751-N26; W1230, Doctoral Program "Discrete Mathematics"; and SFB F 5510-N26. I would like to thank Manfred Madritsch and Robert Tichy for many discussions on the subject and for reading several versions of this manuscript. I am indebted to the anonymous referee for many valuable comments.

Squares with three nonzero digits

Michael Bennett, Adrian-Maria Scheerer[7]

Abstract. We determine all integers n such that n^2 has at most three base-q digits for $q \in \{2, 3, 4, 5, 8, 16\}$. More generally, we show that all solutions to equations of the shape

$$Y^2 = t^2 + M \cdot q^m + N \cdot q^n,$$

where q is an odd prime, $n > m > 0$ and $t^2, |M|, N < q$, either arise from "obvious" polynomial families or satisfy $m \leqslant 3$. Our arguments rely upon Padé approximants to the binomial function, considered q-adically.

1. Introduction

Let us suppose that $q > 1$ is an integer. A common way to measure the lacunarity of the base-q expansion of a positive integer n is through the study of functions we will denote by $N_q(n)$ and $S_q(n)$, the number of and sum of the nonzero digits in the base-q expansion of n, respectively. Our rough expectation is that, if we restrict n to lie in a subset $S \subset \mathbb{N}$, these quantities should behave in essentially the same way as for unrestricted integers, at least provided the subset is not too "thin". Actually quantifying such a statement can be remarkably difficult; particularly striking successes along these lines, for S the sets of primes and squares can be found in work of Mauduit and Rivat [95] and [96].

In this paper, we will restrict our attention to the case where S is the set of integer squares. Since (see [55])

$$\sum_{n<N} S_q(n) \sim \frac{1}{2} \sum_{n<N} S_q(n^2) \sim \frac{q-1}{2 \log q} N \log N,$$

it follows that the ratios

$$\frac{S_q(n^2)}{S_q(n)} \quad \text{and} \quad \frac{N_q(n^2)}{N_q(n)}$$

are infrequently "small". On the other hand, in the case $q = 2$ (where $S_q(n)$ and $N_q(n)$ coincide), Stolarsky [125] proved that, for infinitely many n,

$$\frac{N_2(n^2)}{N_2(n)} \leqslant \frac{4 (\log \log n)^2}{\log n},$$

[7] This article appeared in [25]

a result that was subsequently substantially sharpened and generalized by Hare, Laishram and Stoll [72]. Further developments are well described in [73] where, in particular, one finds that

$$\#\left\{n < N \ : \ N_2(n) = N_2(n^2)\right\} \gg N^{1/19}$$

and that the set

$$\left\{n \in \mathbb{N},\, n \text{ odd } \ : \ N_2(n) = N_2(n^2) = k\right\}$$

is finite for $k \leqslant 8$ and infinite for $k \in \{12, 13\}$ or $k \geqslant 16$.

In what follows, we will focus our attention on integers n with the property that $N_q(n^2) = k$, for small fixed positive integer k. Classifying those integers n in the set

$$B_k(q) = \left\{n \in \mathbb{N} \ : \ n \not\equiv 0 \mod q \ \text{ and } \ N_q(n) \geqslant N_q(n^2) = k\right\}$$

is, apparently, a rather hard problem, even for the case $k = 3$ (on some level, this is the smallest "nontrivial" situation as those n with $N_q(n^2) < 3$ are readily understood). There are infinitely many squares, coprime to q with precisely three nonzero digits base-q, as evidenced by the identity

$$\left(1 + q^b\right)^2 = 1 + 2 \cdot q^b + q^{2b}. \tag{1.1}$$

There are, however, other squares with three nonzero digits, arising more subtly. For example, if $n = 10837$, then, base $q = 8$, we have

$$10837 = 2 \cdot 8^4 + 5 \cdot 8^3 + 1 \cdot 8^2 + 2 \cdot 8 + 5$$

while

$$10837^2 = 7 \cdot 8^8 + 7 \cdot 8 + 1.$$

On the other hand, a result of Corvaja and Zannier [49] implies that all but finitely many squares with three base-q digits arise from polynomial identities like (1.1), and, further, that $B_3(q)$ is actually finite. The proof of this in [49], however, depends upon Schmidt's Subspace Theorem and is thus ineffective (in that it does not allow one to precisely determine $B_3(q)$ – it does, however, lead to an algorithmic determination of all relevant polynomial identities, if any). Analogous questions for $B_k(q)$ with $k \geqslant 4$ are, as far as we are aware, unsettled, except for the case of $B_4(2)$ (see [50]).

In this paper, we will explicitly determine $B_3(q)$ for certain fixed values of q. We prove the following theorem.

Theorem 1.1. *The only positive integers n for which n^2 has at most three nonzero digits base q for $q \in \{2, 3, 4, 5, 8, 16\}$ and $n \not\equiv 0 \mod q$ are as follows :*

$$q = 2 \ : \ n \in \{1, 5, 7, 23\} \ \textit{or}\ n = 2^b + 1,$$

$$q = 3 \ : \ n \in \{1, 5, 8, 13\} \ \textit{or}\ n = 3^b + 1,$$

$$q=4\ :\ n=t \textit{ or } 2t \textit{ for } t\in\{1,7,15,23,31,111\},\ \textit{ or } t=4^b+1 \textit{ or } 2\cdot 4^b+1,$$

$$q=5\ :\ n\in\{1,4,8,9,12,16,23,24,56,177\} \textit{ or } n=5^b+1, 2\cdot 5^b+1 \textit{ or } 5^b+2,$$

$$q=8\ :\ n\leqslant 63,\ n\in\{92,111,124,126,158,188,316,444,479,508,10837\}$$
$$\textit{or } n=r\cdot 8^b+s \textit{ for } r,s\in\{1,2,4\}$$

and

$$q=16\ :\ n=t, 2t \textit{ or } 4t \textit{ for } t\leqslant 100,\ t\in\{111,125,126,127\}$$
$$\textit{or } t=r\cdot 16^b+s \textit{ where either } r,s\in\{1,2,4,8\} \textit{ or the set}$$
$$\{r,s\} \textit{ is one of } \{1,3\},\{2,3\},\{3,8\},\{2,12\},\{4,12\} \textit{ or } \{8,12\}.$$

Here, b is a nonnegative integer.

This immediately implies

Corollary 1.2. *We have*

$$B_3(2)=\{7,23\},\ B_3(3)=\{13\},\ B_3(4)=\{23,30,31,46,62,111,222\},$$

$$B_3(5)=\{56,177\},\ B_3(8)=\{92,111,124,126,158,188,316,444,479,508,10837\}$$

and

$$B_3(16)=\{364,444,446,500,504,508,574,628,680,760,812,888,924,958,$$
$$1012,1016,1020,1022,1784,2296,3832,3966,4088,10837,15864,43348\}.$$

We note that the case $q=2$ of Theorem 1.1 was originally proved by Szalay [127] in 2002, through appeal to a result of Beukers [30]. This latter work was based upon Padé approximation to the binomial function (as are the results of the paper at hand, though our argument is quite distinct). In 2012, the first author [20] treated the case $q=3$ in Theorem 1.1. We should point out that there are computational errors in the last two displayed equations on page 4 of [20] that require repair; we will do this in the current paper.

Our main result which leads to Theorem 1.1 is actually rather more general – we state it for a prime base, though our arguments extend to more general q with the property that q has a prime-power divisor p^α with $p^\alpha > q^{3/4}$. We prove

Theorem 1.3. *If q is an odd prime, if we have a solution to the equation*

$$Y^2=t^2+Mq^m+Nq^n, \tag{1.2}$$

in integers Y,t,M,N,m and n satisfying

$$t,Y,N\geqslant 1,\ \ |M|,N,t^2\leqslant q-1 \ \ \textit{and} \ \ 1\leqslant m<n, \tag{1.3}$$

then either $n=2m$ and $Y=q^m\cdot Y_0\pm t$, for integers t and Y_0 with $\max\{Y_0^2,2tY_0\}<q$, or we have $m\leqslant 3$.

In the special case $t = 1, M = \pm 1, N = 1$, a sharper version of this result already appears as the main theorem of Luca [87]; the proof of this result relies upon primitive divisors in binary recurrence sequences and does not apparently generalize. It seems likely that the last upper bound in Theorem 1.3 can be replaced by $m \leqslant 2$; indeed our argument can be sharpened to prove this for "many" pairs (m, n), though not all. We know of a number of families of solutions to (1.2), with, for instance, $(m, n) = (2, 6)$, $q = r^2 + 1$ prime, $r \in \mathbb{Z}$:

$$\left(\frac{1}{2}r(r^6 + 5r^4 + 7r^2 + 5)\right)^2 = r^2 + (r^2 - 1)q^2 + \left(\frac{r^2 + 4}{4}\right)q^6 \tag{1.4}$$

and $(m, n) = (1, 5)$, for $q = 64r^2 + 1$, corresponding to the identity

$$\big(r(32768r^4 + 1280r^2 + 15)\big)^2 = 9r^2 - (40r^2 + 1)q + q^5.$$

Further families with $(m, n) = (1, 3), (2, 3)$ and $(1, 4)$ are readily observed (as are many more examples with $(m, n) = (1, 5)$). Beyond these, we also know a few (possibly) sporadic examples, with $(m, n) = (1, 6), (1, 7)$ and $(2, 7)$:

$$430683365^2 = 9^2 - 51 \cdot 311 + 205 \cdot 311^6,$$
$$6342918641^2 = 25^2 - 97 \cdot 673 + 433 \cdot 673^6,$$
$$49393781643^2 = 34^2 - 875 \cdot 1229 + 708 \cdot 1229^6,$$
$$559^2 = 1^2 - 4 \cdot 5 + 4 \cdot 5^7,$$
$$574588^2 = 3^2 + 13 \cdot 31 + 12 \cdot 31^7,$$
$$1815^2 = 2^2 + 7^2 + 4 \cdot 7^7$$

and

$$20958^2 = 2^2 - 11 \cdot 13^2 + 7 \cdot 13^7.$$

For a fixed odd prime q, Theorem 1.3 provides an effective way to completely solve equation (1.2) under the conditions of (1.3). Indeed, given an upper bound upon m, say m_0, solving (1.2) with (1.3) amounts to treating at most $O(q^{5/2}m_0)$ "Ramanujan-Nagell" equations of the shape

$$Y^2 + D = Nq^n \quad \text{where} \quad D = -(t^2 + Mq^m). \tag{1.5}$$

These can be handled efficiently via algorithms from Diophantine approximation; see Pethő and de Weger [105] or de Weger [131] for details. Alternatively, if $n \equiv n_0 \mod 3$, where $n_0 \in \{0, 1, 2\}$, we may rewrite (1.2) as

$$U^2 = V^3 + k, \tag{1.6}$$

where

$$U = Nq^{n_0}Y, \;\; V = q^{\frac{n+2n_0}{3}}N \quad \text{and} \quad k = N^2q^{2n_0}\left(t^2 + Mq^m\right). \tag{1.7}$$

We can therefore solve the equation (1.2) if we are able to find the "integer points" on at most $O(q^{5/2}m_0)$ "Mordell curves" of the shape (1.6), where we may subsequently check to see if any solutions encountered satisfy (1.7). The integer points on these curves are known for $|k| \leqslant 10^7$ (see [24]) and are listed at `http://www.math.ubc.ca/~bennett/BeGa-data.html`. For larger values of $|k|$, one can, in many cases, employ Magma or a similar computational package to solve equations of the shape (1.6). For our purposes, however, we are led to consider a number of values of k for which approaches to solving (1.6) reliant upon computation of a full Mordell-Weil basis (as Magma does) for the corresponding curve are extremely time-consuming. We instead choose to solve a number of equations of the form (1.5), via lower bounds for linear forms in p-adic logarithms and reduction techniques from Diophantine approximation, as in [105]. An alternative approach, at least for the equations we encounter, would be to appeal to strictly elementary properties of the corresponding binary recurrences, as in a paper of Bright [38] on the Ramanujan-Nagell equation.

It is probably worth mentioning that similar problems to those discussed in this paper, only for higher powers with few digits, are treated in a series of papers by the first author, together with Yann Bugeaud [21] and with Bugeaud and Maurice Mignotte [22], [23]. The results therein require rather different techniques than those employed here, focussing on lower bounds for linear forms in logarithm, p-adic and complex.

2. Three digits, without loss of generality

Suppose that $q > 1$ is an integer and that we have a square y^2 with (at most) three nonzero base-q digits. If q is either squarefree or a square, it follows that y is necessarily a multiple by some power of q (or $\sqrt{q}$ if q is a square) of an integer Y satisfying a Diophantine equation of the shape

$$Y^2 = C + M \cdot q^m + N \cdot q^n, \tag{2.1}$$

where C, M, N, m and n are nonnegative integers with

$$C, M, N \leqslant q - 1 \quad \text{and} \quad 1 \leqslant m < n. \tag{2.2}$$

If q is neither a square nor squarefree, we may similarly reduce to consideration of equation (2.1), only with weaker bounds for M and N.

The machinery we will employ to prove Theorems 1.1 and 1.3 requires that, additionally, the integer C in equation (2.1) is square. Whilst this is certainly without loss of generality if every quadratic residue modulo q in the range $1 \leqslant C < q$ is itself a square, it is easy to show that such a condition is satisfied only for $q \in \{2, 3, 4, 5, 8, 16\}$. If we have the somewhat weaker constraint upon q that every least positive quadratic residue C modulo q is either a square or has the property that it fails to be a quadratic residue modulo q^k for some exponent $k > 1$, then we may reduce to consideration of (2.1) with either C square, or m bounded. This weaker condition is satisfied for the following q :

$$q = 2, 3, 4, 5, 6, 8, 10, 12, 14, 15, 16, 18, 20, 21, 22, 24, 28, 30, 36, 40, 42, 44, 48, 54, 56, 60, 66, 70, 72, 78, 84, 88, 90, 102, 120, 126, 140, 150, 156, 168, 174, 180, 210, 240, 330, 390, 420, 462, 630, 660, 840, 2310.$$

Of these, the only ones with a prime power divisor p^α with $p^\alpha > q^{3/4}$ (another requirement for our techniques to enable the complete determination of squares with three base-q digits) are

$$q = 2, 3, 4, 5, 8, 16, 18, 22 \text{ and } 54.$$

The principal reason we restrict our attention to equation (2.1) with C square is to guarantee that the exponent n is relatively large compared to m, enabling us to employ machinery from Diophantine approximation (this is essentially the content of Section 3). This might not occur if C is nonsquare, as examples like

$$45454^2 = 13 + 22 \cdot 23^5 + 13 \cdot 23^6$$

and

$$9730060^2 = 46 + 96 \cdot 131^5 + 18 \cdot 131^6$$

illustrate.

3. Three digits : gaps between exponents

For the next few sections, we will restrict attention to the case where the base q is an odd prime. Let us now suppose that we have a solution to (1.2) with (1.3). In this section, we will show that necessarily the ratio n/m is not too small, except when $Y = q^m \cdot Y_0 \pm t$ for small Y_0. Specifically, we will prove the following result.

Lemma 3.1. *If there exists a solution to equation (1.2) with (1.3) and $m \geqslant 4$, then either $n = 2m$ and $Y = q^m \cdot Y_0 \pm t$, for integers t and Y_0 with $\max\{Y_0^2, 2tY_0\} < q$, or we have $n \geqslant 10m - 10$.*

Let us begin by considering the case where $M = 0$ (where we will relax the condition that $n \geqslant 2$). Since q is an odd prime, we may write

$$Y = q^n \cdot Y_0 + (-1)^\delta t,$$

for some positive integer Y_0 and $\delta \in \{0, 1\}$, whence

$$N = q^n \cdot Y_0^2 + (-1)^\delta 2t \cdot Y_0.$$

Since $1 \leqslant N, t^2 \leqslant q - 1$, if $n \geqslant 2$, it follows that

$$q - 1 \geqslant q^2 - 2\sqrt{q-1},$$

a contradiction since $q \geqslant 3$. We thus have $n = 1$, so that

$$N = q \cdot Y_0^2 + (-1)^\delta 2t \cdot Y_0,$$

whence $N < q$ implies that $Y_0 = \delta = 1$, corresponding to the identities

$$(q-t)^2 = t^2 + (q-2t)q.$$

It is worth observing that whilst there are no solutions to (2.1) with (2.2), q an odd prime and $M = 0$, provided C is square, this is not true without this last restriction, as the identity

$$32330691^2 = 182 + 157 \cdot 367^5$$

illustrates.

We may thus, without loss of generality, suppose that $M \neq 0$ in what follows and write

$$Y = q^m \cdot Y_0 + (-1)^\delta t,$$

for some positive integer Y_0 and $\delta \in \{0, 1\}$, so that

$$q^m Y_0^2 + 2(-1)^\delta t \cdot Y_0 = M + N q^{n-m}. \tag{3.1}$$

We thus have

$$q^m - 2q^{1/2} < q^{n-m+1} - q^{n-m} + q.$$

If $n \leqslant 2m-2$ (so that $m \geqslant 3$), it follows that $q^m - 2q^{1/2} < q^{m-1} - q^{m-2} + q$, an immediate contradiction. If $n = 2m-1$, then

$$q^{m-1} < q + 2q^{1/2},$$

and so $m = 2$, $n = 3$, whereby (3.1) becomes

$$q^2 Y_0^2 + 2(-1)^\delta t \cdot Y_0 = M + Nq \leqslant (q-1)q + q - 1 = q^2 - 1.$$

We thus have $Y_0 = 1$ and $\delta = 1$. Since $q \mid M - 2(-1)^\delta t = M + 2t$, it follows that either $M = -2t$ or $M = q - 2t$. In the first case, we have that $q \mid N$, a contradiction. The second corresponds to the identity

$$(q^2 - t)^2 = t^2 + (q-2t)q^2 + (q-1)q^3. \tag{3.2}$$

Otherwise, we may suppose that $n \geqslant 2m$. From the series expansion

$$(t^2 + x)^{1/2} = t + \frac{x}{2t} - \frac{x^2}{8t^3} + \frac{x^3}{16t^5} - \frac{5x^4}{128t^7} + \frac{7x^5}{256t^9} - \frac{21x^6}{1024t^{11}} + \frac{33x^7}{2048t^{13}} - \frac{429x^8}{32768t^{15}} + \cdots,$$

and (1.2), it follows that

$$Y \equiv (-1)^\delta \left(t + \frac{Mq^m}{2t} \right) \mod q^{2m},$$

so that

$$2tY \equiv (-1)^{\delta}\left(2t^2 + Mq^m\right) \mod q^{2m}.$$

If $2tY = (-1)^{\delta}(2t^2 + Mq^m)$, then

$$n = 2m, \quad \frac{M^2}{4t^2} = N \quad \text{and} \quad |Y_0| = \left|\frac{M}{2t}\right|,$$

corresponding to the identity

$$\left(q^m \cdot Y_0 + (-1)^{\delta} t\right)^2 = t^2 + ((-1)^{\delta} t 2Y_0) \cdot q^m + Y_0^2 \cdot q^{2m}, \tag{3.3}$$

where $\max\{t^2, Y_0^2, 2tY_0\} < q$.

If we are not in situation (3.3), we may write

$$2tY = \kappa q^{2m} + (-1)^{\delta}(Mq^m + 2t^2), \tag{3.4}$$

for some positive integer κ, so that

$$4t^2 \cdot N \cdot q^{n-2m} = \kappa^2 q^{2m} + 2\kappa(-1)^{\delta}\left(Mq^m + 2t^2\right) + M^2. \tag{3.5}$$

We rewrite this as

$$4t^2 \cdot N \cdot q^{n-2m} = \left(\kappa q^m + (-1)^{\delta} M\right)^2 + \kappa(-1)^{\delta} 4t^2. \tag{3.6}$$

If $n = 2m$, this becomes

$$4t^2 \cdot N = \left(\kappa q^m + (-1)^{\delta} M\right)^2 + \kappa(-1)^{\delta} 4t^2,$$

the left-hand-side of which is at most $4(q-1)^2$. Since the right-hand-side is at least

$$(\kappa q^m - q + 1)^2 - 4(q-1),$$

it follows that $m = 1$ and $\kappa \in \{1, 2\}$. If $\kappa = 1$, we have

$$q + (-1)^{\delta} M \equiv 0 \mod 2t,$$

say $q = 2tq_0 - (-1)^{\delta} M$, for q_0 a positive integer with $N = q_0^2 + (-1)^{\delta}$, with corresponding identity

$$\left(q_0 q + (-1)^{\delta} t\right)^2 = t^2 + (-1)^{\delta}(2tq_0 - q)q + (q_0^2 + (-1)^{\delta})q^2, \tag{3.7}$$

where $t, q_0 < \sqrt{q}$. If $\kappa = 2$, then M is necessarily even, say $M = 2M_0$, and

$$q + (-1)^{\delta} M_0 \equiv 0 \mod t,$$

say $q = tq_0 - (-1)^{\delta} M_0$. This corresponds to

$$\left(q_0 q + (-1)^{\delta} t\right)^2 = t^2 + (-1)^{\delta} 2(tq_0 - q)q + (q_0^2 + 2(-1)^{\delta})q^2, \tag{3.8}$$

where we require that $q/2 < tq_0 < 3q/2$, $t < \sqrt{q}$ and $q_0 < \sqrt{q - 2(-1)^{\delta}}$.

With these families excluded, we may thus assume that $n \geqslant 2m+1$ and that (3.6) is satisfied. For the remainder of this section, we will suppose that $m \geqslant 4$. Then, since the right-hand-side of (3.5) is

$$\kappa^2 q^{2m}\left(1+(-1)^\delta\left(\frac{2M}{\kappa}q^{-m}+\frac{4t^2}{\kappa}q^{-2m}\right)+\frac{M^2}{\kappa^2}q^{-2m}\right), \tag{3.9}$$

and we assume that $|M|<q$ and $t<\sqrt{q}$, we have

$$N\cdot q^{n-2m} > \frac{1-2q^{1-m}-4q^{1-2m}}{4}\,q^{2m-1}. \tag{3.10}$$

Since $N<q$, $m \geqslant 4$ and $q \geqslant 3$ this implies that

$$q^{n-2m+1} > \frac{2021}{8748}q^{2m-1}$$

and hence $n \geqslant 4m-3 \geqslant 3m+1$. We thus have

$$Y \equiv (-1)^\delta\left(t+\frac{Mq^m}{2t}-\frac{M^2q^{2m}}{8t^3}\right) \mod q^{3m},$$

whence

$$8t^3Y \equiv (-1)^\delta\left(8t^4+4t^2Mq^m-M^2q^{2m}\right) \mod q^{3m}.$$

If

$$8t^3Y = (-1)^\delta\left(8t^4+4t^2Mq^m-M^2q^{2m}\right),$$

then

$$64t^6\cdot N\cdot q^{n-3m} = M^4q^m-8t^2\cdot M^3,$$

an immediate contradiction, since $n \geqslant 3m+1$ and q is coprime to tM.

We may thus assume that

$$8t^3Y = \kappa_1 q^{3m}+(-1)^\delta\left(-M^2q^{2m}+4t^2Mq^m+8t^4\right),$$

for a positive integer κ_1, whereby

$$\begin{gathered} 64t^6Nq^{n-3m} = \kappa_1^2q^{3m}+M^4q^m-8t^2M^3 \\ +(-1)^\delta\left(-2\kappa_1M^2q^{2m}+8t^2\kappa_1Mq^m+16t^4\kappa_1\right) \end{gathered} \tag{3.11}$$

and so

$$64t^6Nq^{n-3m} > q^{3m}-2M^2q^{2m}-8t^2|M|q^m. \tag{3.12}$$

This implies that

$$64q^{n-3m+4} > q^{3m}\left(1-2q^{2-m}-8q^{2-2m}\right). \tag{3.13}$$

For $q \geqslant 7$, we therefore have

$$q^{n-3m+4} > \frac{1}{67}\,q^{3m},$$

so that $n \geqslant 6m - 4$ if $q \geqslant 67$. If $q = 3$, we obtain the inequality $n \geqslant 6m - 4$ directly from (3.12). For each $5 \leqslant q \leqslant 61$, (3.13) implies that $n \geqslant 6m - 6$. In every case, we may thus assume that $n \geqslant 6m - 6 > 4m$, so that

$$Y \equiv (-1)^{\delta} \left(t + \frac{Mq^m}{2t} - \frac{M^2q^{2m}}{8t^3} + \frac{M^3q^{3m}}{16t^5} \right) \mod q^{4m}$$

and hence

$$16t^5Y = \kappa_2 q^{4m} + (-1)^{\delta} \left(16t^6 + 8t^4Mq^m - 2t^2M^2q^{2m} + M^3q^{3m} \right)$$

for a nonnegative integer κ_2, whence

$$\begin{aligned} 256t^{10}Nq^{n-4m} = \kappa_2^2 q^{4m} + (-1)^{\delta} \, (32\kappa_2 t^6 + 16\kappa_2 t^4 Mq^m \\ -4\kappa_2 t^2 M^2 q^{2m} + 2\kappa_2 M^3 q^{3m}) + 20t^4M^4 - 4t^2M^5q^m + M^6q^{2m}. \end{aligned} \tag{3.14}$$

If $\kappa_2 = 0$,

$$256t^{10}Nq^{n-4m} = 20t^4M^4 - 4t^2M^5q^m + M^6q^{2m},$$

contradicting the fact that $q \nmid tM$. We therefore have that

$$256t^{10}Nq^{n-4m} > q^{4m} - 2|M|^3q^{3m} - 4t^2M^2q^{2m} \tag{3.15}$$

and so

$$q^{n-4m+6} > \frac{1}{263} q^{4m}, \tag{3.16}$$

whence $n \geqslant 8m - 8$ unless, possibly, $q \in \{3, 5\}$. If $q = 3$, since $t = 1$ and $|M|, N \leqslant 2$, inequality (3.15) implies a stronger inequality. If $q = 5$, $t \leqslant 2$, $|M|, N \leqslant 4$ and inequality (3.15) again yield $n \geqslant 8m - 8$ and hence we may conclude, in all cases that, provided $m \geqslant 4$, we have $n \geqslant 8m - 8 \geqslant 6m$.

From (3.14), we have

$$(-1)^{\delta} 8\kappa_2 t^2 + 5M^4 \equiv 0 \mod q^m. \tag{3.17}$$

If this is equality, we must have $\delta = 1$ and so (3.14) becomes

$$256t^{10}Nq^{n-5m} = \kappa_2^2 q^{3m} - 16\kappa_2 t^4 M + 4\kappa_2 t^2 M^2 q^m - 2\kappa_2 M^3 q^{2m} - 4t^2M^5 + M^6q^m.$$

It follows that

$$4\kappa_2 t^2 + M^4 \equiv 0 \mod q^m. \tag{3.18}$$

Combining (3.17) and (3.18), we thus have

$$7M^4 \equiv 0 \mod q^m,$$

contradicting the fact that $m \geqslant 4$, while $0 < |M| < q$.

We thus have

$$(-1)^{\delta} 8\kappa_2 t^2 + 5M^4 = \upsilon q^m \tag{3.19}$$

for some nonzero integer υ. If υ is negative, necessarily $\kappa_2 > \frac{q^m}{8t^2}$. If $\upsilon \geqslant 6$, we have that, again, $\kappa_2 > \frac{q^m}{8t^2}$. Let us therefore assume that $1 \leqslant \upsilon \leqslant 5$. Now (3.14) is

$$\begin{gathered}256t^{10}Nq^{n-5m} = \kappa_2^2 q^{3m} + 4t^4\upsilon + (-1)^\delta \left(16\kappa_2 t^4 M\right.\\ \left.-4\kappa_2 t^2 M^2 q^m + 2\kappa_2 M^3 q^{2m}\right) - 4t^2 M^5 + M^6 q^m\end{gathered}$$

and so, since $n \geqslant 6m$,

$$t^2\upsilon + (-1)^\delta 4\kappa_2 t^2 M - M^5 \equiv 0 \mod q^m.$$

From (3.17), we therefore have

$$5\upsilon + (-1)^\delta 28\kappa_2 M \equiv 0 \mod q^m. \tag{3.20}$$

Since $1 \leqslant \upsilon \leqslant 5$, the left hand side here is nonzero and so

$$28\kappa_2|M| \geqslant q^m - 25.$$

For $q^m \geqslant 375$, it follows immediately that

$$\kappa_2 > \frac{q^{m-1}}{30}, \tag{3.21}$$

whilst the inequality if trivial if $q = 3$ and $m = 4$. If $q = 3$ and $m = 5$, we check that for $|M| \in \{1, 2\}$ and $1 \leqslant \upsilon \leqslant 5$, the smallest positive solution to the congruence (3.20) has $\kappa_2 \geqslant 17$, whereby (3.21) is again satisfied.

Combining this with (3.14), we have that

$$256t^{10}Nq^{n-4m} > \frac{1}{900}q^{6m-2} - \frac{1}{15}|M|^3 q^{4m-1} - \frac{2}{15}t^2 M^2 q^{3m-1} - \frac{8}{15}t^4|M|q^{2m-1}, \tag{3.22}$$

whence

$$q^{n-4m+6} > \frac{1}{480^2}q^{6m-2}\left(1 - 60q^{4-2m} - 120q^{4-3m} - 480q^{4-4m}\right).$$

It follows that

$$n \geqslant 10m - 10 \tag{3.23}$$

if $q \geqslant 23$.

We note that, combining (3.19) and (3.20), we have

$$2\upsilon t^2 \equiv 7M^5 \mod q^{m-\delta_5}, \tag{3.24}$$

where $\delta_5 = 1$ if $q = 5$ and 0 otherwise. For $q = 3$, we have $t = 1$, $M = \pm 1, \pm 2$, and find that $\upsilon \equiv \pm 37 \mod 81$ if $|M| = 1$ and $\upsilon \equiv \pm 31 \mod 81$ if $|M| = 2$. In all cases, from (3.19), we have

$$\kappa_2 \geqslant \frac{1}{8}\left(31 \cdot 3^m - 80\right) > \frac{15}{4}3^m.$$

Together with (3.14), we find, after a little work, that, again, $n \geqslant 10m - 10$. If $q = 5$, congruence (3.24) implies that $|v| \geqslant 13$, so that (3.19) yields, crudely,

$$\kappa_2 \geqslant \frac{1}{32}\left(13 \cdot 5^m - 1280\right) > \frac{1}{3}5^m,$$

which again, with (3.14), implies (3.23). Arguing similarly for the remaining values of q with $7 \leqslant q \leqslant 19$, enables us to conclude that inequality (3.23) holds for all $q \geqslant 3$ and $m \geqslant 4$. This concludes the proof of Lemma 3.1.

4. Padé approximants to the binomial function

We now consider Padé approximants to $(1+x)^{1/2}$, defined, for n_1 and n_2 nonnegative integers, via

$$P_{n_1,n_2}(x) = \sum_{k=0}^{n_1} \binom{n_2+1/2}{k}\binom{n_1+n_2-k}{n_2} x^k \tag{4.1}$$

and

$$Q_{n_1,n_2}(x) = \sum_{k=0}^{n_2} \binom{n_1-1/2}{k}\binom{n_1+n_2-k}{n_1} x^k. \tag{4.2}$$

As in [4], we find that

$$P_{n_1,n_2}(x) - (1+x)^{1/2}\ Q_{n_1,n_2}(x) = x^{n_1+n_2+1}\, E_{n_1,n_2}(x), \tag{4.3}$$

where (see e.g. Beukers [30])

$$E_{n_1,n_2}(x) = \frac{(-1)^{n_2}\,\Gamma(n_2+3/2)}{\Gamma(-n_1+1/2)\Gamma(n_1+n_2+1)} F(n_1+1/2, n_1+1, n_1+n_2+2, -x), \tag{4.4}$$

for F the hypergeometric function given by

$$F(a,b,c,-x) = 1 - \frac{a\cdot b}{1\cdot c}x + \frac{a\cdot(a+1)\cdot b\cdot(b+1)}{1\cdot 2\cdot c\cdot(c+1)}x^2 - \cdots .$$

Appealing twice to (4.3) and (4.4) and eliminating $(1+x)^{1/2}$, the quantity

$$P_{n_1+1,n_2}(x)Q_{n_1,n_2+1}(x) - P_{n_1,n_2+1}(x)Q_{n_1+1,n_2}(x)$$

is a polynomial of degree n_1+n_2+2 with a zero at $x=0$ of order n_1+n_2+2 (and hence is a monomial). It follows that we may write

$$P_{n_1+1,n_2}(x)Q_{n_1,n_2+1}(x) - P_{n_1,n_2+1}(x)Q_{n_1+1,n_2}(x) = cx^{n_1+n_2+2}. \tag{4.5}$$

Here, we have

$$c = (-1)^{n_2+1}\frac{(2n_1-2n_2-1)\Gamma(n_2+3/2)}{2(n_1+1)!\,(n_2+1)!\,\Gamma(-n_1+1/2)} \neq 0.$$

We further observe that

$$\binom{n+\frac{1}{2}}{k}4^k \in \mathbb{Z},$$

so that, in particular, if $n_1 \geqslant n_2$, $4^{n_1}P_{n_1,n_2}(x)$ and $4^{n_1}Q_{n_1,n_2}(x)$ are polynomials with integer coefficients.

4.1. **Choosing n_1 and n_2.** For our purposes, optimal choices for n_1 and n_2 are as follows (we denote by $[x]$ the greatest integer not exceeding a real number x and set $x = [x]+\{x\}$).

Definition 1. *Define*

$$(n_1, n_2) = \left(\left[\frac{3n}{4m}\right] + \delta - \Delta_1, \left[\frac{n}{4m}\right] - \delta + \Delta_2\right)$$

where $\delta \in \{0, 1\}$,

$$\Delta_1 = \begin{cases} 1 & \textit{if } \left\{\frac{n}{4m}\right\} \in [0, 1/4] \cup [1/3, 1/2] \cup [2/3, 3/4] \\ 0 & \textit{if } \left\{\frac{n}{4m}\right\} \in (1/4, 1/3) \cup (1/2, 2/3) \cup (3/4, 1), \end{cases}$$

and

$$\Delta_2 = \begin{cases} 1 & \textit{if } \left\{\frac{n}{4m}\right\} > 0 \\ 0 & \textit{if } \left\{\frac{n}{4m}\right\} = 0. \end{cases}$$

Note that for these choices of n_1 and n_2, we may check that

$$(n_1 + n_2 + 1)m = n + \left(\Delta_2 - \Delta_1 + 1 - \left\{\frac{n}{4m}\right\} - \left\{\frac{3n}{4m}\right\}\right) m \geqslant n.$$

Further, we have

$$n_1(m + 1) = \frac{3n}{4} + \frac{3n}{4m} + \kappa_1(m, n, \delta)$$

and

$$n_2(m + 1) + n_1 - n_2 + \frac{n}{2} = \frac{3n}{4} + \frac{3n}{4m} + \kappa_2(m, n, \delta),$$

where

$$\kappa_1(m, n, \delta) = (m + 1) \left(\left[3\left\{\frac{n}{4m}\right\}\right] + \delta - \Delta_1 - 3\left\{\frac{n}{4m}\right\}\right)$$

and

$$\kappa_2(m, n, \delta) = -(m + 3)\left\{\frac{n}{4m}\right\} + \left[3\left\{\frac{n}{4m}\right\}\right] + (\Delta_2 - \delta)m + \delta - \Delta_1.$$

A short calculation ensures that, in every situation, we have

$$\max\{n_1(m + 1), n_2(m + 1) + n_1 - n_2 + n/2\} \leqslant \frac{3n}{4} + \frac{3n}{4m} + m - \frac{5}{4}, \tag{4.6}$$

where the right-hand-side is within $O(1/m)$ of the “truth” for $\delta = 0$, $\Delta_1 = \Delta_2 = 1$.

Note that the fact that $n \geqslant 10m - 10$ implies that we have $n_2 \geqslant 2$, unless

$$(m, n) \in \{(4, 30), (4, 31), (4, 32), (5, 40)\},$$

where we might possibly have $n_2 = 1$. In all cases, we also have

$$|n_1 - 3n_2| \leqslant 3. \tag{4.7}$$

4.2. **Bounds for $|P_{n_1,n_2}(x)|$ and $|Q_{n_1,n_2}(x)|$.** We will have need of the following result.

Lemma 4.1. *If n_1 and n_2 are as given in Definition 1, where $m \geqslant 4$ and $n \geqslant 10m - 10$ are integers, then we have*

$$|P_{n_1,n_2}(x)| \leqslant 2\,|x|^{n_1} \quad \text{and} \quad |Q_{n_1,n_2}(x)| \leqslant 2^{n_1+n_2-1}\left(1 + \frac{|x|}{2}\right)^{n_2},$$

for all real numbers x with $|x| \geqslant 16$.

Proof. Arguing as in the proof of Lemma 1 of Beukers [31], we have that

$$|Q_{n_1,n_2}(x)| \leqslant \sum_{k=0}^{n_2} \binom{n_1}{k}\binom{n_1+n_2-k}{n_1}|x|^k = \sum_{k=0}^{n_2}\binom{n_2}{k}\binom{n_1+n_2-k}{n_2}|x|^k.$$

Since $n_1 > n_2$ and $\binom{n_1+n_2-k}{n_2} \leqslant 2^{n_1+n_2-k-1}$, it follows that

$$|Q_{n_1,n_2}(x)| \leqslant 2^{n_1+n_2-1}\left(1 + \frac{|x|}{2}\right)^{n_2}.$$

Next, note that, since $n_1 > n_2$, $|P_{n_1,n_2}(x)|$ is bounded above by

$$\sum_{k=0}^{n_2+1}\binom{n_2+1}{k}\binom{n_1+n_2-k}{n_2}|x|^k + \sum_{k=n_2+2}^{n_1}\frac{(n_2+1)!(k-n_2-1)!}{k!}\binom{n_1+n_2-k}{n_2}|x|^k.$$

The first sum here is, arguing as previously, at most

$$2^{n_1+n_2-1}\left(1 + \frac{|x|}{2}\right)^{n_2+1}.$$

For the second, we split the summation into the ranges $n_2 + 2 \leqslant k \leqslant \left[\frac{n_1+n_2}{2}\right]$ and $\left[\frac{n_1+n_2}{2}\right] + 1 \leqslant k \leqslant n_1$. In the second of these, we have $n_1 + n_2 - k < k$ and so

$$\binom{n_1+n_2-k}{n_2} < \binom{k}{n_2},$$

whence

$$\sum_{k=\left[\frac{n_1+n_2}{2}\right]+1}^{n_1}\frac{(n_2+1)!(k-n_2-1)!}{k!}\binom{n_1+n_2-k}{n_2}|x|^k < \sum_{k=\left[\frac{n_1+n_2}{2}\right]+1}^{n_1}\frac{n_2+1}{k-n_2}\,|x|^k.$$

Appealing to Definition 1, we may show that $2n_2 \leqslant \left[\frac{n_1+n_2}{2}\right] + 2$ and hence $\frac{n_2+1}{k-n_2} \leqslant 1$, so that

$$\sum_{k=\left[\frac{n_1+n_2}{2}\right]+1}^{n_1}\frac{n_2+1}{k-n_2}\,|x|^k \leqslant \sum_{k=\left[\frac{n_1+n_2}{2}\right]+1}^{n_1}|x|^k < \frac{|x|}{|x|-1}\,|x|^{n_1},$$

provided $|x| > 1$. Since

$$\sum_{k=n_2+2}^{\left[\frac{n_1+n_2}{2}\right]} \frac{(n_2+1)!(k-n_2-1)!}{k!} \binom{n_1+n_2-k}{n_2} |x|^k < \sum_{k=n_2+2}^{\left[\frac{n_1+n_2}{2}\right]} \binom{n_1+n_2-k}{n_2} |x|^k$$

and

$$\sum_{k=n_2+2}^{\left[\frac{n_1+n_2}{2}\right]} \binom{n_1+n_2-k}{n_2} |x|^k \leqslant \sum_{k=n_2+2}^{\left[\frac{n_1+n_2}{2}\right]} 2^{n_1+n_2-k-1} |x|^k < \sum_{k=n_2+2}^{\left[\frac{n_1+n_2}{2}\right]} |2x|^k,$$

we may conclude that $|P_{n_1,n_2}(x)|$ is bounded above by

$$2^{n_1+n_2-1}\left(1+\frac{|x|}{2}\right)^{n_2+1} + \frac{|x|}{|x|-1}\,|x|^{n_1} + \frac{|2x|}{|2x|-1}\,|2x|^{\frac{n_1+n_2}{2}}.$$

Since $|x| \geqslant 16$ and, via (4.7), $n_1 \geqslant 3n_2 - 3$, checking values with $n_2 \leqslant 10$ separately, we may conclude that

$$|P_{n_1,n_2}(x)| < 2\,|x|^{n_1}.$$

This concludes our proof. □

5. Proof of Theorem 1.3

To prove Theorem 1.3, we will, through the explicit Padé approximants of the preceding section, construct an integer that is nonzero and, in archimedean absolute value "not too big", while, under the assumptions of the theorem, being divisible by a very large power of our prime q. With care, this will lead to the desired contradiction.

Setting $\eta = \sqrt{t^2 + Mq^m}$, since $(1+x)^{1/2}$, $P_{n_1,n_2}(x)$ and $Q_{n_1,n_2}(x)$ have q-adic integral coefficients, the same is also true of $E_{n_1,n_2}(x)$ and so, via equation (4.3),

$$\left| tP_{n_1,n_2}\left(\frac{Mq^m}{t^2}\right) - \eta\, Q_{n_1,n_2}\left(\frac{Mq^m}{t^2}\right)\right|_q \leqslant q^{-n}.$$

On the other hand, from the fact that $\eta^2 \equiv Y^2 \mod q^n$, we have

$$\eta \equiv (-1)^{\delta_1} Y \mod q^n,$$

for some $\delta_1 \in \{0,1\}$, and hence

$$\left| tP_{n_1,n_2}\left(\frac{Mq^m}{t^2}\right) - (-1)^{\delta_1} Y\, Q_{n_1,n_2}\left(\frac{Mq^m}{t^2}\right)\right|_q \leqslant q^{-n}.$$

Equation (4.5) implies that for at least one of our two pairs (n_1, n_2), we must have

$$tP_{n_1,n_2}\left(\frac{Mq^m}{t^2}\right) \neq (-1)^{\delta_1} Y\, Q_{n_1,n_2}\left(\frac{Mq^m}{t^2}\right)$$

and hence, for the corresponding pair (n_1, n_2), we have that

$$(2t)^{2n_1}\, P_{n_1,n_2}\left(\frac{Mq^m}{t^2}\right) - (-1)^{\delta_1} Y\, 2^{2n_1}\, t^{2n_1-1}\, Q_{n_1,n_2}\left(\frac{Mq^m}{t^2}\right)$$

is a nonzero integer, divisible by q^n, and so, in particular,

$$\left|(2t)^{2n_1}\, P_{n_1,n_2}\left(\frac{Mq^m}{t^2}\right) - (-1)^{\delta_1} Y\, 2^{2n_1}\, t^{2n_1-1}\, Q_{n_1,n_2}\left(\frac{Mq^m}{t^2}\right)\right| \geqslant q^n. \tag{5.1}$$

From Lemma 4.1 and the fact that $Y < q^{(n+1)/2}$, we thus have

$$q^n \leqslant 2^{2n_1+1}|M|^{n_1} q^{mn_1} + 2^{3n_1+n_2-1} q^{(n+1)/2} t^{2n_1-1}\left(1 + \frac{|M|q^m}{2t^2}\right)^{n_2}. \tag{5.2}$$

From the inequalities

$$|M|, t^2 < q \ \text{ and } \ \frac{|M|q^m}{2t^2} \geqslant \frac{81}{2},$$

it follows from (5.2) that

$$q^n \leqslant 2^{2n_1+1} \cdot q^{(m+1)n_1} + 2^{3n_1-1} q^{n/2+(m+1)n_2+n_1-n_2}\,(83/81)^{n_2}, \tag{5.3}$$

and hence, since $n \geqslant 10m - 10$ and $m \geqslant 4$, we may argue rather crudely to conclude that

$$q^n < 9^{n_1} \cdot q^{\max\{n_1(m+1), n_2(m+1)+n_1-n_2+n/2\}}. \tag{5.4}$$

Inequality (4.6) thus implies

$$q^n < 9^{\frac{3n}{4m}+1} \cdot q^{\frac{3n}{4}+\frac{3n}{4m}+m-\frac{5}{4}},$$

whence

$$q^{1-\frac{3}{m}-\frac{4m}{n}+\frac{5}{n}} < 9^{\frac{3}{m}+\frac{4}{n}}. \tag{5.5}$$

Since $m \geqslant 4$, if n is suitably large, this provides an upper bound upon q. In particular, if

$$n > \frac{4m^2 - 5m}{m-3}, \tag{5.6}$$

then

$$q < 3^{\frac{6n+8m}{mn-3n-4m^2+5m}}. \tag{5.7}$$

Since $m \geqslant 4$ and $n \geqslant 10m - 10$, (5.6) is satisfied unless we have $m = 4$ and $30 \leqslant n \leqslant 44$. Excluding these values for the moment, we thus have

$$q < 3^{\frac{68m-60}{6m^2-35m+30}}.$$

Since $q \geqslant 3$, it follows, therefore, that, in all cases, $m \leqslant 16$. If $q \geqslant 5$, we have the sharper inequality $m \leqslant 12$.

5.1. **Small values of m.** To treat the remaining values of m, we argue somewhat more carefully. For fixed q and m, equation (1.2) under the conditions in (1.3) can, in many cases, be shown to have no solutions via simple local arguments. In certain cases, however, when the tuple (t, M, N, m) matches up with an actual solution, we will not be able to find such local obstructions. For example, the identities

$$(q^m \cdot Y_0 \pm t)^2 = t^2 \pm 2tY_0q^m + Y_0^2q^{2m}$$

imply that we cannot hope, through simple congruential arguments, to eliminate the cases (here $n \equiv n_0 \mod 3$)

$$(t, M, N, n_0) = (t, \pm 2tY_0, Y_0^2, 2m \mod 3), \tag{5.8}$$

where $\max\{t^2, Y_0^2, 2tY_0\} < q$. For even values of m, we are also unable to summarily dismiss tuples like

$$(t, M, N, n_0) = (t, Y_0^2, 2tY_0, m/2 \mod 3). \tag{5.9}$$

Additionally, the "trivial" identity

$$t^2 = t^2 - M \cdot q^m + M \cdot q^m$$

leaves us with the necessity of treating tuples

$$(t, M, N, n_0) = (t, -N, N, m \mod 3) \tag{5.10}$$

via other arguments. By way of example, if $q = m = 5$, sieving by primes p with the property that the smallest positive t with $5^t \equiv 1 \mod p$ divides 300, we find that all tuples (t, M, N, n_0) are eliminated except for

$$\begin{gathered}(1,-2,1,1),(1,-1,1,2),(1,2,1,1),(1,-2,2,2),(1,1,2,1),(1,-3,3,2),\\(1,-4,4,1),(1,-4,4,2),(1,4,4,1),(2,-4,1,1),(2,-1,1,2),(2,4,1,1),\\(2,-2,2,2),(2,-3,3,2) \text{ and } (2,-4,4,2).\end{gathered}$$

These all correspond to (5.8) or (5.10), except for $(t, M, N, n_0) = (1, 1, 2, 1)$ which arises from the identity $56^2 = 1^2 + 2 \cdot 5 + 5^5$.

For the cases where we fail to obtain a local obstruction, we can instead consider equations (1.6), with the conditions (1.7). Our expectation is that, instead of needing to treat roughly $6(q-1)^{5/2}$ such equations (for a fixed pair (q, m)), after local sieving we will be left with on the order of $O(q)$ Mordell curves to handle.

By way of example, let us begin with the case where $q = 3$. Here, from (5.2),

$$3^n \leqslant 2^{3n_1+1}3^{mn_1} + 2^{3n_1+n_2-1}(82/81)^{n_2}3^{mn_2+(n+1)/2}.$$

Since $\max\{mn_1, mn_2 + (n+1)/2\} \leqslant \frac{3n}{4} + m + \frac{1}{4}$, and $n_2 \geqslant 2$ (provided $n > 40$), we thus have

$$3^n \leqslant 2^{3n_1+n_2}(82/81)^{n_2}3^{\frac{3n}{4}+m+\frac{1}{4}},$$

so that

$$3^{n/4-m-1/4} \leqslant 2^{3n_1+n_2}(82/81)^{n_2}.$$

We check that $n_2 \leqslant \frac{n}{4m} + 1$ and $3n_1 + n_2 \leqslant \frac{5n}{2m} + \frac{3}{2}$, whence either $n \leqslant 40$, or we have

$$3^{\frac{n}{4}-m-\frac{1}{4}} \leqslant 2^{\frac{5n}{2m}+\frac{3}{2}}(82/81)^{\frac{n}{4m}+1}.$$

In this latter case, if $m \geqslant 12$, the fact that $n \geqslant 10m-10$ leads to a contradiction, whilst, for $8 \leqslant m \leqslant 11$, we have that $n \leqslant 157$. A short calculation ensures that there are no solutions to equation (1.2) with (1.3), if $q = 3$, $8 \leqslant m \leqslant 11$ and $10m - 10 \leqslant n \leqslant 157$. For $q = 3$ and $4 \leqslant m \leqslant 7$, we are led to equation of the shape (1.6), where now $|k| \leqslant 324\,(1 + 2\cdot 3^m) \leqslant 1417500$. As noted previously, the integer points on the corresponding Mordell curves are known (see [24]) and listed at `http://www.math.ubc.ca/~bennett/BeGa-data.html`. We check that no solutions exist with U and V as in (1.7).

We may thus suppose that $q \geqslant 5$ and hence it remains to treat the values of m with $4 \leqslant m \leqslant 12$. If $m = 12$, appealing to (5.7), we have, from the fact that $n \geqslant 110$, necessarily $110 \leqslant n \leqslant 118$ and $q = 5$. A short calculation ensures that there are no corresponding solutions to equation (1.2) with (1.3). Similarly, if $m = 11$, we have that either $q = 5$ and $100 \leqslant n \leqslant 125$, or $q = 7$, $100 \leqslant n \leqslant 103$. If $m = 10$, $q = 5$ and $90 \leqslant n \leqslant 139$, or $q = 7$ and $90 \leqslant n \leqslant 109$, or $q = 11$ and $n = 90$. For $m = 9$ we have, in all cases, $n \leqslant 172$ and $q \leqslant 19$. For $m = 8$, $n \leqslant 287$ and $q \leqslant 47$. A modest computation confirms that we have no new solutions to the equation of interest and hence we may suppose that $4 \leqslant m \leqslant 7$ (and that $q \geqslant 5$).

For small values of q, each choice of m leads to at most $2q^{5/2}$ Ramanujan-Nagell equations (1.5) which we can solve as in [105]. In practice, the great majority of these are eliminated by local sieving. By way of example, if $q = 5$, after local sieving, we are left to treat precisely 32 pairs (D, N) in equation (1.5), corresponding to

$$\begin{aligned} D \in \{&-312498, -15624, -15623, -12498, -2498, -1249,\\ &-624, 1251, 2502, 6251, 12502, 31251, 312502\}, \quad \text{if} \quad N = 1, \end{aligned}$$

$$D \in \{-156248, -31248, 3126, 15626\}, \quad \text{if} \quad N = 2,$$

$$D \in \{-234374, -234373, -46874, -46873, -1873, 31252\}, \quad \text{if} \quad N = 3$$

and

$$D \in \{-312499, -62498, -2499, -2498, 627, 2501, 12501, 15627, 62501\} \quad \text{if} \quad N = 4.$$

For these values of (D, N), we find that equation (1.5) has precisely solutions as follows

D	N	n	D	N	n
-312499	4	7	2501	4	2
-312499	4	14	2501	4	8
-234374	3	7	3126	2	1
-46874	3	6	6251	1	10
-15624	1	6	12501	4	10
-2499	4	4	15626	2	3
-2499	4	8	31251	1	12
-1249	1	8	62501	4	3
-624	1	4	62501	4	12
1251	1	8			

In all cases, these solutions correspond to values of m that have either $m \geqslant n$ or $n = 2m$. More generally, implementing a "Ramanujan-Nagell" solver as in [105], in conjunction with local sieving, we completely solve equation (1.2) with (1.3), for $m \in \{4, 5, 6, 7\}$ and $5 \leqslant q \leqslant 31$. No new solutions accrue. If we appeal again to inequality (5.7), using that $q \geqslant 37$, we find that $60 \leqslant n \leqslant 81$ (if $m = 7$), $50 \leqslant n \leqslant 109$ (if $m = 6$) and $40 \leqslant n \leqslant 499$ (if $m = 5$). After a short computation, we are left to consider the cases with $m = 4$ and $q \geqslant 37$.

For the value $m = 4$, proceeding in this manner would entail an extremely large computation, without additional ingredients. By way of example, in case $m = 4$ and $n = 45$, inequality (5.7) implies an upper bound upon q that exceeds 10^{144} (and no upper bound whatsoever for $30 \leqslant n \leqslant 44$). To sharpen this and related inequalities, we will argue as follows. Notice that if we have

$$tP_{n_1,n_2}\left(\frac{Mq^m}{t^2}\right) = (-1)^{\delta_1} Y\, Q_{n_1,n_2}\left(\frac{Mq^m}{t^2}\right), \tag{5.11}$$

then

$$t^2 P^2_{n_1,n_2}\left(\frac{Mq^m}{t^2}\right) - (t^2 + Mq^m + Nq^n) Q^2_{n_1,n_2}\left(\frac{Mq^m}{t^2}\right) = 0.$$

From our construction, it follows that

$$\left| t^2 P^2_{n_1,n_2}\left(\frac{Mq^m}{t^2}\right) - (t^2 + Mq^m) Q^2_{n_1,n_2}\left(\frac{Mq^m}{t^2}\right) \right|_q \leqslant q^{-m(n_1+n_2+1)}.$$

and hence, if $(n_1 + n_2 + 1)m > n$ and (5.11), then

$$q^{(n_1+n_2+1)m-n} \text{ divides } Q^2_{n_1,n_2}(0) = \binom{n_1+n_2}{n_2}^2. \tag{5.12}$$

In particular, if $m = 4$ and $30 \leqslant n \leqslant 32$, then we have $(n_1, n_2) \in \{(5,2),(6,1)\}$ and hence, since $q \geqslant 37$, (5.12) fails to hold. We thus obtain inequality (5.1) for both pairs (n_1, n_2), rather than just for one of them, provided $n \in \{30, 31\}$ (if $n = 32$, we have $(n_1 + n_2 + 1)m = n$). Choosing $(n_1, n_2) = (5, 2)$, it follows from (5.4) that, if $n = 30$, we have $q^2 < 3^{10}$, so that $q \leqslant 241$, while $n = 31$ implies $q^{5/2} < 3^{10}$, i.e. $q \leqslant 79$. If $n = 32$, the worse case corresponds to $(n_1, n_2) = (6, 1)$, where we find, again from (5.4), that $q^2 < 3^{12}$ and so $q \leqslant 727$. Continuing in this fashion, observing that the greatest prime factor $\binom{n_1+n_2}{n_2}$ is bounded above by roughly $n/4$, and that $4(n_1 + n_2 + 1) = n$ precisely when $4 \mid n$, we have, via (5.4), an upper bound upon q of the shape $q < \min_{\delta\in\{0,1\}}\{3^{2n_1/(n-\mu)}\}$, if $4 \not| n$, and $q < \max_{\delta\in\{0,1\}}\{3^{2n_1/(n-\mu)}\}$, if $4 \mid n$, where

$$\mu = \max\{n_1(m + 1), n_2(m + 1) + n_1 - n_2 + n/2\}.$$

Here, we exclude the cases where $\mu \geqslant n$, corresponding to $(n_1, n_2) = (5, 3)$ if $n = 33$ or 34 and $(n_1, n_2) = (9, 2)$ if $n = 45$; in each of these, the other choice of (n_1, n_2) leads to a bound upon q. For $n \leqslant 1000$, we find that $q < 3^{10}$, in case $n = 36$, $q < 3^{28/3}$ (if $q = 41$), $q < 3^8$ (if $n = 52$ or $n = 57$) and otherwise $q < 3155$. A painful but straightforward computation finds that we have no additional solutions to equation (1.2) with (1.3) for $n \leqslant 1000$. Applying once again inequality (5.7), we may thus assume that $q \leqslant 1021$. After local sieving and solving corresponding equations of the shape (1.5), we verify that equation (1.2) has no unexpected solutions with (1.3), for $m = 4$ and $37 \leqslant q \leqslant 1021$. This completes the proof of Theorem 1.3.

Full details of our computations are available from the authors upon request.

6. Proof of Theorem 1.1

For $q \in \{3, 5\}$, we may apply Theorem 1.3 to conclude that either $n = 3^b + 1$ (in case $q = 3$) or that $n \in \{5^b + 1, 2 \cdot 5^b + 1, 5^b + 2\}$ (if $q = 5$), for some positive integer b, or that we have either

$$(6.1) \quad n^2 = 1 + M \cdot 3^m + N \cdot 3^n, \; n^2 = 1 + M \cdot 5^m + N \cdot 5^n \; \text{ or } \; n^2 = 4 + M \cdot 5^m + N \cdot 5^n,$$

with $m \in \{1, 2, 3\}$, $n > m$ and $1 \leqslant M, N \leqslant q - 1$. Checking the corresponding solutions to (1.6) (all available at `http://www.math.ubc.ca/~bennett/BeGa-data.html`), we find that the only solutions to (6.1) are with

$$n \in \{4, 5, 8, 9, 12, 13, 16, 23, 24, 56, 177\},$$

as claimed. Adding in the "trivial" solutions with $n \in \{1, 2\}$, completes the proof of Theorem 1.1 in case $q \in \{3, 5\}$.

Our argument for $q \in \{2, 4, 8, 16\}$ follows along very similar lines to the proof of Theorem 1.3, only with slight additional complications, arising from the fact that none of $(1 + x)^{1/2}$,

$P_{n_1,n_2}(x)$ or $Q_{n_1,n_2}(x)$ have 2-adic integral coefficients. On the other hand, $(1+4x)^{1/2}$, $P_{n_1,n_2}(4x)$ and $Q_{n_1,n_2}(4x)$ do have 2-adic integral coefficients and so we can proceed as in Section 5, taking $x = Mq^m/t^2$, where now $q = 2^\alpha$ for $\alpha \in \{1,2,3,4\}$. Under mild assumptions upon m ($m \geqslant 5$ is satisfactory), the arguments of Sections 3 and 5 go through with essentially no changes. We are left to treat a number of equations of the shape (1.5), to complete the proof of Theorem 1.1. We suppress the details.

7. Concluding remarks

In this paper, we have focussed our attention on equation (2.1) in case C is square and q is prime. Even in this very restricted situation, we have been able to use our results to completely determine $B_3(q)$ only for $q \in \{2,3,5\}$. We conclude with some speculations upon the structure of the sets $B_3(q)$. Let us write

$$B_k(q) = \bigcup_{j=k}^{\infty} B_{k,j}(q),$$

where

$$B_{k,j}(q) = \left\{ n \in \mathbb{N} \,:\, n \not\equiv 0 \mod q,\ N_q(n) = j \text{ and } N_q(n^2) = k \right\}.$$

If $q = r^2+1$ is prime for r an integer, since we have

$$\frac{1}{2} r (r^6 + 5r^4 + 7r^2 + 5) = r + r \cdot q^2 + \frac{r}{2} \cdot q^3,$$

identity (1.4) implies that $B_{3,3}(q)$ is nonempty for such q. Further, for odd prime q, we can find examples to verify that $B_{3,4}(q)$ is nonempty for (at least)

$$q = 7, 11, 17, 23, 31, 47, 101, 131, 151,$$

amongst the primes up to 200. We observe that

$$35864 \in B_{3,5}(11).$$

We know of no other value in $B_{3,j}(q)$ for $j \geqslant 5$ and q prime. Perhaps there are none.

8. Acknowledgments

The authors are grateful to the referees for pointing out a number of errors, typographical and otherwise.

Computable Absolutely Pisot Normal Numbers

Manfred G. Madritsch, Adrian-Maria Scheerer, Robert F. Tichy[8]

Abstract. We analyze the convergence order of an algorithm producing the digits of an absolutely normal number. Furthermore, we introduce a stronger concept of absolute normality by allowing Pisot numbers of arbitrary degree as bases.

1. Introduction

In this paper we are interested in simultaneous normality to several bases. In particular, we analyze the order of convergence to normality of an absolutely normal number generated by an algorithm of Becher, Heiber and Slaman (Section 2) and are concerned with normality to non-integer bases. We give an algorithmic construction of a real number that is normal to each base from a given sequence of Pisot numbers (Section 3 and Section 4).

1.1. **Normality to a single base.** A real number $x \in [0,1)$ is called *simply normal to base* b, $b \geqslant 2$ an integer, if in its b-ary expansion

$$x = \sum_{n \geqslant 1} a_n b^{-n},\ a_n \in \{0, \dots, b-1\}$$

every digit $d \in \{0, 1, \dots b-1\}$ appears with the expected frequency $\frac{1}{b}$. The number x is called *normal to base* b if each of x, bx, b^2x, $\dots$ is simply normal to every base b, b^2, b^3, $\dots$. This is equivalent (see e.g. [42, Chapter 4]) to the property that all digital blocks of arbitrary length k appear with the expected frequency, i.e. if for all $k \geqslant 1$ and all $d \in \{0, \dots, b-1\}^k$,

$$\lim_{N \to \infty} \frac{1}{N} |\{1 \leqslant n \leqslant N : (a_n, \dots, a_{n+k-1}) = d\}| = \frac{1}{b^k}. \tag{1.1}$$

Furthermore, Pillai [107] has shown that x is normal to base b if and only if it is simply normal to every base b, b^2, b^3, $\dots$.

Normal numbers were introduced by Borel [34] in 1909. He showed that almost all real numbers (with respect to Lebesgue measure) are simply normal to all bases $b \geqslant 2$, thus *absolutely normal* (see Section 1.3). It is a long standing open problem to show that important real numbers such as $\sqrt{2}$, $\ln 2, e, \pi, \dots$ are normal, for instance in decimal expansion. There has only been little progress in this direction in the last decades, see e.g. [5].

[8] This article appeared in [91]

However, specifically constructed examples of normal numbers are known. Champernowne in 1935 [47] has shown that the real number constructed by concatenating the expansions in base 10 of the positive integers, i.e.

$$0,1\,2\,3\,4\,5\,6\,7\,8\,9\,10\,11\ldots,$$

is normal to base 10. This construction has been extended in various directions (*cf.* Erdős and Davenport [53], Schiffer [116], Nakai and Shiokawa [98], Madritsch, Thuswaldner and Tichy [92], Scheerer [115]).

1.2. **Discrepancy of normal numbers.**

The *discrepancy* of a sequence $(x_n)_{n\geqslant 1}$ of real numbers is defined as

$$D_N(x_n) = \sup_J \left| \frac{1}{N} |\{1 \leqslant n \leqslant N : x_n \bmod 1 \in J\}| - \lambda(J) \right|,$$

where the supremum is extended over subintervals $J \subseteq [0,1)$ and where λ denotes the Lebesgue measure. A sequence is *uniformly distributed modulo* 1 if its discrepancy tends to zero as $N \to \infty$.

It is known [130] that x is normal to base b if and only if the sequence $(b^n x)_{n\geqslant 1}$ is uniformly distributed modulo 1. Hence x is normal to base b if and only if $D_N(b^n x) \to 0$ as $N \to \infty$. It is thus a natural quantitative measure for the normality of x to base b to consider the discrepancy of the sequence $(b^n x)_{n\geqslant 1}$.

Answering a question of Erdős, in 1975 Philipp [106] has shown a law of the iterated logarithm for discrepancies of lacunary sequences which implies $D_N(b^n x) = O(\sqrt{\log\log N/N})$ almost everywhere. Recently, Fukuyama [67] was able to determine

$$\limsup_{N\to\infty} \frac{D_N(b^n x)\sqrt{N}}{\sqrt{\log\log N}} = c(b) \quad \text{a.e.},$$

for some explicit positive constant $c(b)$. Schmidt [119] showed that there is an absolute constant $c > 0$ such that for any sequence $(x_n)_{n\geqslant 1}$ of real numbers $D_N(x_n) \geqslant c\frac{\log N}{N}$ holds for infinitely many N. Schiffer [116] showed that the discrepancies of constructions of normal numbers in the spirit of Champernowne satisfy upper bounds of order $O(\frac{1}{\log N})$. Levin [85] constructed for any integer $b \geqslant 2$ a real number α such that $D_N(b^n\alpha) = O(\frac{(\log N)^2}{N})$. It is an open question whether there exist an integer $b \geqslant 2$ and a real number x with optimal discrepancy bound $D_N(b^n x) = O(\frac{\log N}{N})$.

1.3. **Absolute normality and order of convergence.**

A number x is called *absolutely normal* if it is normal to any integer base $b \geqslant 2$. Since normality to base b is equivalent to simple normality to all bases b^n, $n \geqslant 1$, absolute normality is equivalent to simple normality to all bases $b \geqslant 2$.

Since most constructions of numbers normal to a single base b are concatenations of the b-ary expansions of $f(n)$, $n \geqslant 1$, where f is a positive-integer-valued increasing function, they essentially depend on the choice of the base b. Therefore they cannot be used for producing absolutely normal numbers.

All known examples of absolutely normal numbers have been established in the form of algorithms[9] that output the digits of this number to some base one after the other. The first such construction is due to Sierpinski [123] from 1917. This construction was made computable by Becher and Figueira [11] who gave a recursive formulation of Sierpinski's construction. Other algorithms for constructing absolutely normal numbers are due to Turing [128] (see also Becher, Figueira and Picchi [13]), Schmidt [117] (see also Scheerer [113]) and Levin [84] (see also Alvarez and Becher [2]).

There seems to be a trade-off between the complexity of the algorithms and the speed of convergence of the corresponding discrepancies. The discrepancies satisfy upper bounds of the order $O(N^{-1/6})$ (Sierpinski), $O(N^{-1/16})$ (Turing), $O((\log N)^{-1})$ (Schmidt) and $O(N^{-1/2}(\log N)^3)$ (Levin). All algorithms, except the one due to Schmidt, need double exponential many mathematical operations to output the first N digits of the produced absolutely normal number. Schmidt's algorithm requires exponentially many mathematical operations.

No construction of an absolutely normal number x is known such that the discrepancy $D_N(b^n x)$ for some $b \geqslant 2$ decays faster than what one would expect for almost all x.

In Section 2 we are interested in another construction of an absolutely normal number which is due to Becher, Heiber and Slaman [17]. They established an algorithm which computes the digits of an absolutely normal number in polynomial time. We show (Theorem 2.8) that the corresponding discrepancy is slightly worse than $O(\frac{1}{\log N})$, and that at a small loss of computational speed the discrepancy can in fact be $O(\frac{1}{\log N})$.

1.4. **Normality to non-integer bases.** Section 3 of the present article treats normality in a context where the underlying base is not necessarily integer. Let $\beta > 1$ be a real number. Expansions of real numbers to base β, so-called *β-expansions*, were introduced and studied by Rényi [112] and Parry [103] and later by many authors from an arithmetic and ergodic-theoretic point of view.

In the theory of β-expansions it is natural to consider *Pisot numbers β*, i.e. real algebraic integers $\beta > 1$, such that all its conjugates lie inside the (open) unit disc. A real number x is called *normal to base β*, or β-normal, if the sequence $(\beta^n x)_{n\geqslant 1}$ is uniformly distributed

[9] With the exception of Chaitin's constant, which is absolutely normal but not computable [46].

modulo 1 with respect to the unique entropy maximizing measure for the underlying transformation $x \mapsto \beta x \bmod 1$ (see Section 3.1). A real number is called *absolutely Pisot normal* if it is normal to all bases that are Pisot numbers. Since there are only countably many Pisot numbers, the Birkhoff ergodic theorem implies that almost all real numbers are in fact absolutely Pisot normal.

The main result of Section 3 is an algorithm that computes an absolutely Pisot normal number. More generally, for a sequence $(\beta_j)_{j\geqslant 1}$ of Pisot numbers, we construct a real number x that is normal to each of the bases β_j, $j \geqslant 1$ (Section 3.3 and Theorem 3.6). Bearing in mind that the set of computable real numbers is countable, we thus show that there is in fact a computable real number that is β_j-normal for each $j \geqslant 1$.

Our algorithm constructs in each step a sequence of finitely many nested intervals, corresponding to the first finitely many bases considered. This is also the essential idea of the construction of an absolutely normal number by Becher, Heiber and Slaman [17]. We need to establish lower and upper bounds for the length of β-adic subintervals in a given interval to control the number of specified digits when changing the base. However, the equivalence (absolute normality) $\Leftrightarrow$ (simple normality to all bases) does not hold for non-integer expansions. Instead, we argue with the concept of (ε, k)-*normality* as introduced by Besicovitch [29] and studied in the case of Pisot numbers by Bertrand-Mathis and Volkmann [27].

Our algorithm should be compared to the one due to Levin [84]. While his construction is not restricted to Pisot numbers, it uses exponential sums and is as such not realizable only with elementary operations. The algorithm we present in Section 3 is completely elementary.

In Section 4 we give explicit estimates of all constants that appear in our algorithm. We use a theorem on large deviations for a sum of dependent random variables to give an estimate for the measure of the set of non-(ε, k)-normal numbers of length n (Proposition 4.3). Our approach gives all implied constants explicitly, and as such makes a consequence of the ineffective Shannon-McMillan-Breimann theorem effective. The results of this section might be of independent interest.

1.5. **Notation.** For a real number x, we denote by $\lfloor x \rfloor$ the largest integer not exceeding x. The fractional part of x is denoted as $\{x\}$, hence $x = \lfloor x \rfloor + \{x\}$. We put $\lceil x \rceil = -\lfloor -x \rfloor$. Two functions f and g are $f = O(g)$ or equivalently $f \ll g$ if there is a x_0 and a positive constant C such that $f(x) \leqslant Cg(x)$ for all $x \geqslant x_0$. We mean $\lim_{x\to\infty} f(x)/g(x) = 1$ when we say $f \sim g$ and $g \neq 0$.

When we speak of *words*, we mean finite or infinite sequences of symbols (called letters) of a certain (specified) set, the alphabet. *Blocks* are finite words. The concatenation of two blocks $u = u_1 \dots u_k$ and $v_1 \dots v_l$ is the block $u_1 \dots u_k v_1 \dots v_l$ and is denoted by uv or $u * v$. If u_i for $i \leqslant m$ are blocks, $*_{i<m} u_i$ is their concatenation in increasing order of i. The *length* of the block $u = u_1 \dots u_k$ is denoted by $\|u\|$ and is in this case equal to k.

We denote by λ the Lebesgue measure.

For a finite set, $|\cdot|$ means its number of elements.

Mathematical operations include addition, subtraction, multiplication, division, comparison, exponentiation and logarithm. *Elementary operations* take a fixed amount of time. The cost of mathematical operations depends on the digits of the input or on the desired precision of the output. Addition or subtraction of two n-digit numbers takes $O(n)$ elementary operations, multiplication or division of two n-digit numbers takes $O(n^2)$ elementary operations, and to compute the first n digits of exp and log takes $O(n^{5/2})$ elementary operations. These estimates are crude but sufficient for our purposes.

The complexity of a computable function f is the time it takes to compute the first N values $f(i)$, $1 \leqslant i \leqslant N$. The algorithm we analyze outputs the digits of a real number X to some base. By the complexity of the algorithm we mean the time it takes to output the first N digits of X to some base.

2. Discrepancy

In this section, we analyze the speed of convergence to normality of the absolutely normal number produced by the algorithm by Becher, Heiber and Slaman in [17]. We follow the notation and terminology therein.

2.1. The Algorithm.

Notation. A *t-sequence* is a nested sequence of intervals $\mathbf{I} = (I_2, \dots, I_t)$, such that I_2 is dyadic and for each base $2 \leqslant b \leqslant t-1$, I_{b+1} is a $(b+1)$-adic subinterval of I_b such that $\lambda(I_{b+1}) \geqslant \lambda(I_b)/2(b+1)$.

Let $x_b(\mathbf{I})$ be the block in base b such that $0.x_b(\mathbf{I})$ is the representation of the left endpoint of I_b in base b. In each step i, the algorithm computes a sequence $\mathbf{I}_i = (I_{i,2}, \dots, I_{i,t_i})$ of nested intervals $I_{i,2} \supset \dots \supset I_{i,t_i}$. If $b \leqslant t_i$, let $x_b(\mathbf{I}_i) = x_{i,b}$ be the base b representation of the left endpoint of $I_{i,b}$ and let $u_{i+1,b} = u_b(\mathbf{I}_{i+1})$ be such that $x_{i+1,b} = x_{i,b} * u_{i+1,b}$.

If u is a block of digits to base b, the *simple discrepancy* of u in base b is defined as $D(u,b) = \max_{0 \leqslant d < b} |N_d(u)/\|u\| - 1/b|$ where $N_d(u)$ is the number of times the digit d appears in the block u.

Let $k(\varepsilon, \delta, t)$ be the function

$$k(\varepsilon, \delta, t) = \max(\lceil 6/\varepsilon \rceil, \lceil -\log(\delta/(2t)) 6/\varepsilon^2 \rceil) + 1.$$

From Lemma 4.1 and 4.2 of [17] we further have a function h that counts the number of mathematical operations needed to carry out one step of the algorithm. See also Lemma 2.5.

Input. A computable non-decreasing unbounded function $f : \mathbb{N} \to \mathbb{R}$ such that $f(1)$ is known and satisfies $f(1) > h(2,1)$.

First step. Set $t_1 = 2$, $\varepsilon_1 = \frac{1}{2}$, $k_1 = 1$ and $\mathbf{I}_1 = (I_{1,2})$ with $I_{1,2} = [0,1)$.

Step $i+1$ for $i \geqslant 1$. Given are from step i of the algorithm values $t_i = v$, $\varepsilon_i = \frac{1}{v}$ and a t_i-sequence $\mathbf{I}_i$.

We want to assign values to $t_{i+1}, \varepsilon_{i+1}$. If $i+1$ is a power of 2, then we carry out the following procedure.

- We spend i computational steps on computing the first m values of f, $1 \leqslant m \leqslant i$.
- We put $\delta = (8t_i 2^{t_i+v+1} t_i!(v+1)!)^{-1}$.
- We try to compute $k(\frac{1}{v+1}, \delta, v+1)$ and $h(v+1, \frac{1}{v+1})$ in i steps each. If we succeed in computing these values, and if additionally

$$h(v+1, \frac{1}{v+1}) < f(m) \tag{2.1}$$

  and for each $b \leqslant t_i$

$$\frac{\lceil \log_2(v+1) \rceil k(1/(v+1), \delta, v+1) + \lceil -\log_2(\delta) \rceil}{\|x_{i,b}\|} < \frac{1}{v+1}, \tag{2.2}$$

  then we define $t_{i+1} = v+1$ and $\varepsilon_{i+1} = \frac{1}{v+1}$. Otherwise, we let $t_{i+1} = t_i = v$, $\varepsilon_{i+1} = \varepsilon_i = \frac{1}{v}$.

If $i+1$ is no power of 2, then define $t_{i+1} = t_i = v$, $\varepsilon_{i+1} = \varepsilon_i = \frac{1}{v}$.

Furthermore, we compute $\delta_{i+1} = (8t_i 2^{t_i+t_{i+1}} t_i! t_{i+1}!)^{-1}$ and

$$k_{i+1} = \max(\lceil 6/\varepsilon_{i+1} \rceil, \lceil -\log(\delta_{i+1}/(2t_i))6/\varepsilon_{i+1}^2 \rceil) + 1.$$

Then we find a t_{i+1}-sequence $\mathbf{I}_{i+1}$ by means of the following steps.

- We let L be a dyadic subinterval of I_{i,t_i} such that $\lambda(L) \geqslant \lambda(I_{i,t_i})/4$.
- For each dyadic subinterval J_2 of L of measure $2^{-\lceil \log_2 t_i \rceil k_{i+1}} \lambda(L)$, we find $\mathbf{J} = (J_2, J_3, \ldots, J_{t_{i+1}})$, a t_{i+1}-sequence starting with J_2.
- Finally we choose $\mathbf{I}_{i+1}$ to be the leftmost of the t_{i+1} sequences $\mathbf{J}$ considered above such that for each $b \leqslant t_i$, $D(u_b(\mathbf{J}), b) \leqslant \varepsilon_{i+1}$.

Output. Let X be the unique real number in the intersection of the intervals of the sequences $\mathbf{I}_i$. In base b we have $X = \lim_{i \to \infty} 0.x_{i,b} = 0. *_{i \geqslant 1} u_{i,b}$. It is the content of Theorem 3.9 in [17] that X is absolutely normal.

2.2. **Speed of convergence to normality.** In this section we estimate the discrepancy $D_N(b^nX)$ for integer $b \geqslant 2$. Two factors play a role: How many digits in each step are computed, and how rapidly ε_i decays to zero. By virtue of the algorithm, at least one digit is added in each step, and ε_i can decay at most as fast as $O(\frac{1}{\log i})$. As can be expected from the algorithm, the discrepancy depends both on growth and complexity of f.

It was shown in [17] that to output the first N digits of X, the algorithm requires time $O(N^2 f(N))$.

We begin our analysis by first showing that in each step of the algorithm not too many digits are attached.

Lemma 2.1 (Lemma 3.3 in [17])**.** *For an interval I and a base b, there is a b-adic subinterval I_b such that $\lambda(I_b) \geqslant \lambda(I)/(2b)$.*

Lemma 2.2. *If i is large enough, then $1 \leqslant \|u_{i,b}\| \ll (\log i)^A$ for $A > 3$. Thus $i \ll \|x_{i,b}\| \ll i(\log i)^A$.*

Proof. We assume the base b to be fixed and i large enough such that $t_{i+1} \geqslant b$. In step $i+1$ we have the following sequence of nested subintervals:

$$I_{i,b} \supset \ldots \supset I_{i,t_i} \supset L \supset I_{i+1,2} \supset \ldots \supset I_{i+1,b}. \tag{2.3}$$

By Lemma 2.1, and the choice of $I_{i+1,2}$, we know the following lower bounds on the measures of the intervals in (2.3). We have $\lambda(I_{i,t_i}) \geqslant \lambda(I_{i,b})/(2^{t_i-b}t_i!/b!)$, $\lambda(L) \geqslant \lambda(I_{i,t_i})/4$, $\lambda(I_{i+1,2}) = 2^{-\lceil \log_2 t_i \rceil k_{i+1}} \lambda(L)$ and $\lambda(I_{i+1,b}) \geqslant \lambda(I_{i+1,2})/(2^b b!)$. Combining inequalities yields $\lambda(I_{i+1,b}) \geqslant \lambda(I_{i,b})/(2^{2+t_i} 2^{\lceil \log_2 t_i \rceil k_{i+1}} t_i!)$. Hence in stage $i+1$ we are adding at most $O(t_i + (\log t_i)k_{i+1} + \log t_i!)$ many digits in base b. The way the algorithm is designed only allows for $t_i = O(\log i)$. The growth of k_{i+1} can be analyzed and is $O(t_i^3 \log t_i)$. Hence in stage $i+1$ at most $O(t_i + (\log t_i)k_{i+1} + \log t_i!) = O((\log i)^A)$ digits are added to the b-ary expansion of X, where $A > 3$ to accommodate all double-log factors.

The lower bound on the number of digits added comes from the fact that by the choice of $I_{i+1,2}$, $I_{i+1,b}$ is strictly smaller than $I_{i,b}$, so at least one digit is added in each stage. □

Next, we investigate the conditions involving k and h that are responsible for how fast $t_i \to \infty$ and $\varepsilon_i \to 0$ with step i of the algorithm. We start by showing that condition (2.2) on k always holds, provided i is large enough. This involves estimating the growth as well as the complexity of k.

Recall that $k(\varepsilon, \delta, t) = \max(\lceil 6/\varepsilon \rceil, \lceil -\log(\delta/(2t))6/\varepsilon^2 \rceil) + 1$.

Lemma 2.3. *Let $v \geqslant 2$ be an integer and $\delta = (8v2^{2v+1}v!(v+1)!)^{-1}$. Then the growth of $k(\frac{1}{v+1}, \delta, v+1)$ is $O(v^3 \log v)$. Furthermore, $k(\frac{1}{v+1}, \delta, v+1)$ can be computed in $O(v^2(\log v)^2)$ elementary operations.*

Proof. We have for the growth

$$\begin{aligned} k(\frac{1}{v+1}, \delta, v+1) &= \max(\lceil 6(v+1)\rceil, \lceil \log(2(v+1)8v2^{2v+1}v!(v+1)!)6(v+1)^2\rceil) + 1 \\ &\leqslant 6(v+1)^2\left(\log(16v(v+1)) + (2v+1)\log 2 + \log v! + \log(v+1)!\right) + 2 \\ &= O(v^2(\log v + v + v\log v)) \\ &= O(v^3 \log v). \end{aligned}$$

Since in the expression for k we are rounding, the most relevant part is the computation of the significant digits of $\log(16v(v+1)2^{2v+1}v!(v+1)!)$. The argument of this expression is computable with $O(v^2(\log v)^2)$ elementary operations and has $O(v \log v)$ many digits. We only need to compute $O(\log v)$ many digits of the logarithm, which takes another $O((\log v)^{5/2})$ elementary operations. In total this are $O(v^2(\log v)^2)$ many elementary operations. □

Corollary 2.4. *For i to be large enough, condition (2.2) on k is always satisfied, i.e. for each $b \leqslant t_i$*

$$\frac{\lceil \log(v+1)\rceil k(1/(v+1), \delta, v+1) + \lceil -\log(\delta)\rceil}{\|x_{i,b}\|} < \frac{1}{v+1}$$

where v is such that $t_i = v = 1/\varepsilon_i$.

Proof. This is a consequence of $k(1/(v+1), \delta, v+1) = O(v^3 \log v)$, $\log(1/\delta) = O(v \log v)$, $\|x_{i,b}\| \gg i$ and $v = t_i = O(\log i)$ by the way the algorithm is designed. □

Now we investigate condition (2.1) on h involving f. The function h counts the number of mathematical operations needed to carry out one step of the algorithm. We want to know an upper bound for the growth of h.

Lemma 2.5. *With $t_i = \frac{1}{\varepsilon_i} = O(\log i)$ we have*

$$h(t_i, \varepsilon_i) = O(i^{\log^4 i}).$$

This upper bound for h can be computed with i elementary operations, provided i is large enough.

Proof. The function h decomposes as $h = h_*(h_1 g + h_2 + h_3 + h_4)h_0$ as can be seen from the proof of Lemma 4.2 in [17]. Here:

- g (from Lemma 4.1 in [17]), is the minimum number of digits sufficient to represent all the endpoints of the intervals that we are working with in one step (squared). We know from Lemma 2.2 that $g = O(i^2(\log i)^{2A})$ for $A > 3$.
- It takes $h_1 g$ many mathematical operations to find a t_{i+1}-sequence for each J_2. We have $h_1 = t_{i+1}$.
- h_2 is the number of mathematical operations needed to compute the base b representation $u_b(\mathbf{J})$ for each $2 \leqslant b \leqslant t_i$. We have $h_2 \leqslant \lceil \log_2 t_i \rceil k_{i+1}$.
- h_3 counts the number of mathematical operations needed to compute thresholds of the form $(1/b + \varepsilon_{i+1})\|u_b(\mathbf{J})\|$. We have $h_3 = t_i$.
- h_4 comes from counting occurrences of digits in $u_b(\mathbf{J})$ and comparing with the previously computed thresholds. We have $h_4 \ll t_i(\lceil \log_2 t_i \rceil k_{i+1})^2$.
- h_* is the maximum number of iterations it takes to find a suitable t_{i+1}-sequence. There are $2^{\lceil \log_2 t_i \rceil k_{i+1}}$ many different subintervals J_2 of L, hence $h_* = 2^{\lceil \log_2 t_i \rceil k_{i+1}}$. With $k_{i+1} = O(\log^4 i)$ we obtain $h_* = O(i^{\log^4 i})$.
- Finally, the function h_0 is the number of elementary operations needed to carry out each mathematical operation in one step of the algorithm. Since all values that appear in the calculations of one step of the algorithm are at most exponential in t_i which is at most of order $\log i$, and because the number of elementary operations involved depends only on the number of digits of the numbers involved, h_0 is at most of order poly$(\log i)$.

These bounds can be seen from Lemma 4.1 and Lemma 4.2 in [17]. Combining them gives $h = O(i^{\log^4 i})$.

Remark that, when t_i is bounded by a slower growing function in i such as $\log \log i$, then the significant term in h comes from g and is a power of i. Otherwise h_* is the significant term.

For the complexity of the upper bound for h, note that $i^{\log^4 i}$ can be computed in a power of $\log i$ many elementary operations, so certainly with i elementary operations when i is large enough. □

Lemma 2.5 has the following two immediate corollaries for the speed of convergence to normality of Becher, Heiber and Slaman's algorithm.

Proposition 2.6. *Becher, Heiber, Slaman's algorithm achieves discrepancy of $D_N(b^n X) = O(\frac{1}{\log N})$ for f computable in real-time with growth $f \gg i^{\log^4 i}$. In this case, the complexity is $O(i^{2+\log^4 i})$.*

Proposition 2.7. *If f is a polynomial in i of degree d, then the complexity of X is $O(N^{d+2})$ but the discrepancy of $(b^n X)_{n \geqslant 0}$ is $D_N(b^n X) = O_d(\frac{1}{(\log N)^{1/5}})$.*

Proof. These corollaries follow by observing that the complexity of f is such that f is for large enough i computed up to the actual value $f(i)$ (i.e. $m = i$) and that either the condition on h, (2.1), is satisfied, hence the discrepancy is optimal, or that condition (2.1) is only satisfied for $e^{(\log i)^{1/5}}$ of the values that it is checked for. □

In a similar manner, using Lemma 2.5, one can show quantitatively how growth and complexity of f influence the discrepancy (and the complexity) of Becher, Heiber, Slaman's algorithm. This can be done for example by measuring complexity and growth of f in the following (crude) way. We denote by $\log_{(k)}$ and $\exp_{(k)}$ the k times iterated logarithm or exponential where $\exp_{(k)} = \log_{(-k)}$, and $\exp_{(0)} = \log_{(0)} = id$. Let c be the integer such that in i elementary operations f can be computed up to a value $f(m)$ with $m \sim \log_{(c)} i$. Let g be the integer such that f grows as $f \sim \exp_{(g)} i$. We allow $g \in \mathbb{Z}$ but c is non-negative.

Theorem 2.8. *Assume f is such that the integers c and g above can be defined. Then Becher, Heiber, Slaman's algorithm computes an absolutely normal number X such that for any base $b \geqslant 2$,*

$$D_N(b^n X) = O\left(\frac{1}{(\log_{(1-g+c)} N)^{1/5}}\right) \tag{2.4}$$

if $1 - g + c > 0$, and

$$D_N(b^n X) = O\left(\frac{1}{\log N}\right) \tag{2.5}$$

otherwise.

Proof. We have $h \ll \max(\text{poly}(i), e^{t_i^5})$ and $t_i \ll \log i$ by the way the algorithm is defined. t_i only increases if i is a power of two and if $h \leqslant f(m)$. The latter condition is satisfied for all i large enough if $g - c \geqslant 1$, and for all i (that are powers of two) that satisfy $i \ll \exp((\exp_{g-c-1}(i))^{1/5})$. With $1/t_i = \varepsilon_i$ this gives in this case an upper bound for the discrepancy of order $1/(\log_{(1-g+c)} N)^{1/5}$. □

3. Absolutely Pisot Normal Numbers

In this section, we give an algorithmic construction of a real number that is normal to each base from a given sequence of Pisot numbers. For more information about β-expansions and β-normal numbers see for example the book [42]. We have partly followed the notation in [27].

3.1. **β-expansions of real numbers.** Let $\beta > 1$ be a real number. Then each real number $x \in [0,1)$ has a representation of the form

$$x = \sum_{i=1}^{\infty} \varepsilon_i \beta^{-i}, \tag{3.1}$$

with integer digits $0 \leqslant \varepsilon_i < \beta$. One way to obtain such a representation is the following. Let T_β be the *β-transformation* $T_\beta : [0,1) \to [0,1)$, $x \mapsto \beta x \pmod 1$. Then $\varepsilon_i = \lfloor \beta T_\beta^{i-1}(x) \rfloor$ for $i \geqslant 1$.

Rényi [112] showed that there is a unique probability measure μ_β on $[0,1)$ that is equivalent to the Lebesgue measure and such that μ_β is invariant and ergodic with respect to T_β and has maximum entropy. The measure μ_β satisfies $(1 - \frac{1}{\beta})\lambda \leqslant \mu_\beta \leqslant \frac{\beta}{\beta-1}\lambda$.

Let $c(d)$ be the *cylinder set* corresponding to the block d, i.e. the set of all real numbers in the unit interval whose first $\|d\|$ digits coincide with d. A *β-adic interval* is a cylinder set $c(d)$ for some d.

Let W^∞ be the set of right-infinite words $\omega = \omega_1\omega_2\ldots$ with digits $0 \leqslant \omega_i < \beta$ that appear as the β-expansions of real numbers in the unit interval. Let $\mathcal{L}_n$ be the set of all finite subwords of length n of words $\omega \in W^\infty$ and let $W = \bigcup_{n\geqslant 1} \mathcal{L}_n$. We call the words in W *admissible.*

We have $\beta^n \leqslant |\mathcal{L}_n| \leqslant \frac{\beta}{\beta-1}\beta^n$ for the number of elements of $\mathcal{L}_n$.

For an infinite word $\omega = \omega_1\omega_2 \ldots \in W^\infty$ and a block $d = d_1 d_2 \ldots d_k$ of digits $0 \leqslant d_i < \beta$ we denote by $N_d(\omega, n)$ the number of (possibly overlapping) occurrences of d within the first n letters of ω. If the word ω is finite, we write $N_d(\omega)$ for $N_d(\omega, \|\omega\|)$.

An infinite word $\omega \in W^\infty$ is called *μ_β-normal* if for all $d \in \mathcal{L}_k$,

$$\lim_{n\to\infty} \frac{1}{n} N_d(\omega, n) = \mu_\beta(c(d)).$$

A real number $x \in [0,1)$ is called *normal to base β* or *β-normal*, if the infinite word $\varepsilon_1\varepsilon_2\ldots$ defined by its β-expansion (3.1) is μ_β-normal.

For fixed $\varepsilon > 0$ and positive integers k, n, a word $\omega \in \mathcal{L}_n$ is called *(ε, k)-normal* if for all $d \in \mathcal{L}_k$

$$\mu_\beta(c(d))(1-\varepsilon)\|\omega\| < N_d(\omega) < \mu_\beta(c(d))(1+\varepsilon)\|\omega\|.$$

The set of all (ε, k)-normal numbers in $\mathcal{L}_n$ will be denoted by $E_n(\varepsilon, k)$ and its complement by $E_n^c(\varepsilon, k)$.

A *Pisot number* β is a real algebraic integer $\beta > 1$ such that all its conjugates have absolute value less than 1, and as usual we include all positive integers $b \geqslant 2$ in this definition. All Pisot numbers smaller than the golden mean were found by Dufresnoy and Pisot [60]. In particular, they showed that the smallest one is the positive root of $x^3 - x - 1$ (called the plastic number) which is approximately $1.32471 > \sqrt[3]{2}$.

3.2. **Preliminaries.**

Lemma 3.1 ([27, Lemma 3])**.** *Let $\beta > 1$ be Pisot. For every $\varepsilon > 0$ and positive integer k there exist $\eta = \eta(\varepsilon, k)$, $0 < \eta < 1$, $C = C(\varepsilon, k) > 0$ and $n_0 = n_0(\varepsilon, k)$ such that for the number of non-(ε, k)-normal words of length n*

$$|E_n^c(\varepsilon, k)| < C\, |\mathcal{L}_n|^{1-\eta}$$

holds for all $n \geqslant n_0$.

In Section 4.2 we give explicit estimates for n_0, C and η.

The following Lemma contains the underlying idea of our construction.

Lemma 3.2 ([27, Lemma 4])**.** *Let $a_1, a_2, \dots$ be a sequence of finite words $a_n \in W$ such that $a = a_1 a_2 \dots \in W^\infty$ and $\|a_n\| \to \infty$ as $n \to \infty$. Suppose that for any $\varepsilon > 0$ and any positive integer k there exists an integer $n_0(\varepsilon, k)$ such that all a_n with $n \geqslant n_0(\varepsilon, k)$ are (ε, k)-normal. If*

$$n = o\left(\|a_1 a_2 \dots a_n\|\right) \quad \textit{and} \quad \|a_{n+1}\| = o(\|a_1 a_2 \dots a_n\|), \tag{3.2}$$

then the infinite word $a = a_1 a_2 \dots$ is μ_β-normal.

Proof. Let $\varepsilon > 0$ and $d \in \mathcal{L}_k$. It suffices to show that, as $N \to \infty$,

$$\mu_\beta(c(d))(1-\varepsilon)N < N_d(a, N) < \mu_\beta(c(d))(1+\varepsilon)N.$$

We have $N_d(a, N) = N_d(a_1 a_2 \dots a_n, N)$, where n is such that $\|a_1 a_2 \dots a_{n-1}\| < N \leqslant \|a_1 \dots a_n\|$. Then, for N large enough,

$$\begin{aligned} N_d(a_1 \dots a_n, N) &\leqslant N_d(a_1 \dots a_{n_0(\varepsilon,k)}) + n(k-1) + N_d(a_{n_0+1}) + \dots + N_d(a_n) \\ &\leqslant \text{const}(\varepsilon, k) + n(k-1) + \sum_{i=n_0+1}^{n} \mu_\beta(c(d))(1+\varepsilon)\|a_i\|. \end{aligned}$$

Dividing by N gives the desired result, assuming conditions (3.2). The calculation for the lower bound for $N_d(a, N)$ is similar. □

Lemma 3.3. *Let $\beta > 1$ be Pisot. There exists $M \geqslant 0$ such that for all $n \geqslant 1$ and all $d \in L_n$ the Lebesgue measure of the cylinder set $c(d)$ satisfies*

$$\beta^{-(M+1)}\beta^{-n} \leqslant \lambda(c(d)) \leqslant \beta^{-n}. \tag{3.3}$$

Proof. This is Proposition 2.6 of [86]. □

Following the argument in [86], one can take M to be the size of the largest block of consecutive zeros in the modified β-expansion of 1 (see Section 4.1). We give an explicit upper bound on M in Proposition 4.1.

We wish to control the lengths when changing the base. The following is an analogue to Lemma 3.3 in [17]; see also Lemma 2.1.

Lemma 3.4. *Let β be Pisot and M as above. For any interval I there is a β-adic subinterval I_β of I such that $\lambda(I_\beta) \geqslant \lambda(I)/2\beta^{M+4}$.*

Proof. We can assume $\lambda(I) > 0$. Let m be the smallest integer such that $\beta^{-m} < \lambda(I)$. Thus $\lambda(I)/\beta \leqslant \beta^{-m} < \lambda(I)$. If there exists an interval of order m in I, then let I_β be this β-adic interval and we have $\lambda(I_\beta) \geqslant \lambda(I)/\beta$.

Otherwise there must be a word $a \in \mathcal{L}_m$ such that $\pi(a) \in I$ but neither $\pi(a^-)$ nor $\pi(a^+)$ is in I, where a^- and a^+ are the lexicographically previous or next elements of a of the same length and where $\pi(a)$ is the real number in the unit interval whose β-expansion starts with a. Then by Lemma 3.3 we have that $\lambda(I) < 2\beta^{-m}$. Since $\beta^{-m} < \lambda(I)$ and the smallest Pisot number is bigger than $2^{1/3}$, we get that $2\beta^{-m-3} < \lambda(I)$. Thus there must be a β-adic interval I_β of order $m+3$ in I and we have

$$\lambda(I_\beta) \geqslant \frac{1}{\beta^{M+1+m+3}} = \frac{1}{2\beta^{M+4}} \cdot \frac{2}{\beta^m} > \frac{\lambda(I)}{2\beta^{M+4}}.$$

□

3.3. **The Algorithm.**

Notation. Let $(\beta_j)_{j\geqslant 1}$ be a sequence of Pisot numbers. Let t be a positive integer. A *t-sequence* is a sequence of intervals $\mathbf{I} = (I_1, \ldots, I_t)$ such that for $1 \leqslant j \leqslant t$, I_j is β_j-adic, such that for $1 \leqslant j \leqslant t-1$, $I_{j+1} \subset I_j$, and such that $\lambda(I_{j+1}) \geqslant \lambda(I_j)/2\beta_{j+1}^{M_{\beta_{j+1}}+4}$. If we have two β-adic intervals $J \subset I$ then $u_\beta(J)$ means the block of digits that is added to the base β expansion of the numbers in I to obtain the β-expansion of numbers in J. The notation $u_j(\mathbf{J})$ for a t-sequence $\mathbf{J}$ shall mean $u_{\beta_j}(J_j)$. We denoted the dependence on β_j of all appearing constants M, n_0, C and of $\mathcal{L}_n$ explicitly with an β_j.

Input. Given are values $\varepsilon_1 = 1$, $k_1 = 1$, $t_1 = 1$ and a sequence $(\beta_j)_{j\geqslant 1}$ of Pisot numbers β_j.

First step. Let $\mathbf{I}_1$ be a t_1-sequence such that $\mathbf{I}_1 = (I_{1,t_1})$, with $I_{1,t_1} = [0,1)$. Repeat the bases β_j according to conditions

$$\max_{1\leqslant j\leqslant t_i} \beta_j \leqslant \beta_1 i, \tag{3.4}$$

$$\max_{1\leqslant j\leqslant t_i} M_{\beta_j} \leqslant (M_{\beta_1}+1)(1+\log i), \tag{3.5}$$

$$\sum_{1\leqslant j\leqslant t_i} (M_{\beta_j}+4)\log\beta_j \leqslant (M_{\beta_1}+4)\log\beta_1(1+\log i). \tag{3.6}$$

Step $i+1$ for $i \geqslant 1$. From step i, we have a t_i-sequence $\mathbf{I}_i$ of nested intervals $I_{i,1} \supset \ldots \supset I_{i,t_i}$ where each $I_{i,j}$ is β_j-adic.

Let

$$t_{i+1} = \lceil \log(i+1) \rceil, \quad \varepsilon_{i+1} = \frac{1}{t_{i+1}}, \quad k_{i+1} = t_{i+1},$$

$$\delta_{i+1} = \frac{1}{2}\frac{1}{2\beta_1^{M_{\beta_1}+4}}\frac{1}{t_i}\frac{1}{2^{t_i}\prod_{j\leqslant t_i}\beta_j^{M_{\beta_j}+4}}\frac{1}{2^{t_{i+1}}\prod_{j\leqslant t_{i+1}}\beta_j^{M_{\beta_j}+4}}.$$

Choose n_{i+1} to be the least integer such that

$$n_{i+1} \geqslant \max_{j\leqslant t_{i+1}} \left(n_{\beta_j}(\varepsilon_{i+1}, k_{i+1})\right), \tag{3.7}$$

and such that for all $1 \leqslant j \leqslant t_{i+1}$

$$\lambda(E_n^c(\varepsilon_{i+1}, k_{i+1})) < \delta_{i+1}. \tag{3.8}$$

Furthermore, let

$$v_i = \left\lceil \max_{j=1,\ldots,t_i} \frac{\log\beta_j}{\log\beta_1} \right\rceil.$$

Then we perform the following steps.

- Take L to be a β_1-adic interval of I_{i,t_i} of length $\lambda(L) \geqslant \lambda(I_{i,t_i})2^{-1}\beta_1^{-(M_{\beta_1}+4)}$.
- For each β_1-adic sub-interval J_1 of L with $u_1(J_1) = v_i n_{i+1}$ find a t_{i+1}-sequence $\mathbf{J} = (J_1, \ldots, J_{t_{i+1}})$.
- Choose the "leftmost" of the t_{i+1}-sequences $\mathbf{J}$ such that $u_j(\mathbf{J})$ is $(\varepsilon_{i+1}, k_{i+1})$-normal for $1 \leqslant j \leqslant t_i$.

Output. The unique real number X in the intersection of all $I_{i,j}$.

We need to show that the algorithm is well-defined and that the produced number is in fact β_j-normal for all $j \geqslant 1$.

Proposition 3.5. *This algorithm is well-defined.*

Proof. We have to show that in each step $i+1$ there exists at least one t_{i+1}-sequence $\mathbf{J}$. Let $\mathcal{S}$ be the union of the intervals $J_{t_{i+1}}$ over the $|\mathcal{L}^{\beta_1}_{v_i n_{i+1}}|$ many t_{i+1}-sequences $\mathbf{J}$. By definition of the interval L we have that $\lambda(L) \geqslant \lambda(I_{i,t_i})2^{-1}\beta_1^{-(M_{\beta_1}+4)}$. Furthermore for each sequence we have that $\lambda(J_{t_{i+1}}) \geqslant 2^{-t_{i+1}} \prod_{j=1}^{t_{i+1}} \beta_j^{-(M_{\beta_j}+4)} \lambda(J_1)$. Since the sub-intervals $J_1 \subset L$ form a partition of L we have that $\lambda(\mathcal{S}) \geqslant 2^{-t_{i+1}} \prod_{j=1}^{t_{i+1}} \beta_j^{-(M_{\beta_j}+4)} \lambda(L)$. Combining these inequalities yields

$$\lambda(\mathcal{S}) \geqslant 2^{-t_i - t_{i+1} - 1} \prod_{j=1}^{t_i} \beta_j^{-(M_{\beta_j}+4)} \prod_{j=1}^{t_{i+1}} \beta_j^{-(M_{\beta_j}+4)} \lambda(I_{i,1}).$$

Now we calculate the measure of the set $\mathcal{N}$ of non-suitable intervals and show that it is less than $\lambda(\mathcal{S})$. For the length of the added word we have $\|u_1(\mathbf{J})\| \geqslant v_i n_{i+1}$ and for each $2 \leqslant j \leqslant t_{i+1}$ we have $\|u_j(\mathbf{J})\| \geqslant n_{i+1}$. By the choice of n_{i+1}, the subsets of $I_{i,j}$, where $u_j(\mathbf{J})$ is not $(\varepsilon_{i+1}, k_{i+1})$-normal, have Lebesgue measure less that $\delta_{i+1}\lambda(I_{i,j})$, and hence less than $\delta_{i+1}\lambda(I_{i,1})$. Since we consider t_i many bases, we obtain $\lambda(\mathcal{N}) < t_i \delta_{i+1} \lambda(I_{i,1})$.

Combining the estimates of $\mathcal{N}$ and $\mathcal{S}$ we obtain $\lambda(\mathcal{N}) < \lambda(\mathcal{S})$. Since $\mathcal{N} \subset \mathcal{S}$ there must be a t_{i+1}-sequence $\mathbf{J}$ such that $u_j(\mathbf{J})$ is $(\varepsilon_{i+1}, k_{i+1})$-normal for each $1 \leqslant j \leqslant t_i$. □

Theorem 3.6. *Let $(\beta_j)_{j \geqslant 1}$ be a sequence of Pisot numbers. Then the real number X generated by this algorithm is β_j-normal for each $j \geqslant 1$.*

Proof. We need to verify the growth and normality assumptions of Lemma 3.2 on the words that correspond to the digits added in each considered base in each step of the algorithm.

To find bounds for the number of added digits in step $i+1$ in base β_j, for $j \leqslant t_i$, consider the chain of intervals

$$I_{i,j} \supset \ldots \supset I_{i,t_i} \supset L \supset J_1 \supset \ldots \supset J_j$$

which is considered in step $i+1$. We find a lower bound on the Lebesgue measure of J_j in the form of

$$\lambda(J_j) \geqslant \frac{1}{2^{t_i}} \frac{1}{\beta_1^{M_1+1}} \frac{1}{\beta_1^{v_i n_{i+1}}} \prod_{l=1}^{t_i} \frac{1}{\beta_l^{M_{\beta_l}+4}} \cdot \lambda(I_{i,j}).$$

Thus, Lemma 3.3 implies for the number $\|u_j^{(i+1)}(\mathbf{J})\|$ of digits added in base β_j, $j \leqslant t_i$, in step $i+1$ of the algorithm, that

$$\frac{\log\left(\frac{1}{F_{i+1}} \frac{1}{\beta_j^{M_{\beta_j}+1}}\right)}{\log \beta_j} \leqslant \|u_j^{(i+1)}(\mathbf{J})\| \leqslant \frac{\log \frac{1}{F_{i+1}}}{\log \beta_j}$$

where $F_{i+1} = 2^{-t_i}\beta_1^{-(M_1+1)}\beta_1^{-v_i n_{i+1}} \prod_{l=1}^{t_i} \beta_l^{-M_{\beta_l}-4}$.

Hence $\|u_j^{(i+1)}(\mathbf{J})\| \sim \log 1/F_{i+1}$ with implied constants only depending on β_j. We thus need to show that

$$\log 1/F_{i+1} = t_i \log 2 + (v_i n_{i+1} + M_1 + 1)\log\beta_1 + \sum_{l=1}^{t_i}(M_l+4)\log\beta_l$$

satisfies assumptions (3.2) of Lemma 3.2.

We now look at the growth of n_{i+1}. In light of Proposition 4.3, condition (3.7) requires

$$n_{i+1} \geqslant M_{\beta_j} + k_{i+1} \tag{3.9}$$

for all $1 \leqslant j \leqslant t_{i+1}$. We have $\varepsilon_{i+1} = 1/t_{i+1} \to 0$ and $k_{i+1} = t_{i+1} \to \infty$ as $t_{i+1} \to \infty$. Thus also n_{i+1} tends to infinity at least logarithmically in i.

Since $\lambda \leqslant \frac{\beta}{\beta-1}\mu_\beta$, $\beta^k \leqslant |\mathcal{L}_k| \leqslant \frac{\beta}{\beta-1}\beta^k$, and because of Proposition 4.3, condition (3.8) on n_{i+1} is satisfied, if for all $j \leqslant t_i$,

$$4\left(\frac{\beta_j}{\beta_j-1}\right)^2 \beta_j^k \beta_j^{n_{i+1}\eta(\varepsilon_{i+1},k_{i+1})} < \delta_{i+1}.$$

With η from equation (4.3), this translates into the requirement that for every $j \leqslant t_i$,

$$n_{i+1} \geqslant \frac{(M_{\beta_j}+1)\log\beta_j + \log\frac{\beta_j}{\beta_j-1}}{\varepsilon_{i+1}\min(\frac{\varepsilon_{i+1}\beta_j^{k_{i+1}}}{16}, \frac{3}{4})}\left(\log\left(4\left(\frac{\beta_j}{\beta_j-1}\right)^2\beta_j^{k_{i+1}}\right) + \log\frac{1}{\delta_{i+1}}\right), \tag{3.10}$$

where

$$\begin{aligned}\log\frac{1}{\delta_{i+1}} =& 2\log 2 + \log t_i + (t_i + t_{i+1})\log 2 + (M_{\beta_1}+4)\log\beta_1 \\ &+ 2\sum_{1\leqslant j\leqslant t_i}(M_{\beta_j}+4)\log\beta_j + \sum_{t_i<j\leqslant t_{i+1}}(M_{\beta_j}+4)\log\beta_j\end{aligned}$$

(where the last sum is empty if $t_i = t_{i+1}$).

Properties (3.4) and (3.6) on the sequence $(\beta_j)_{j\geqslant 1}$ imply

(3.11)

$$\max_{1\leqslant j\leqslant t_i}\left((M_{\beta_j}+1)\log\beta_j + \log\frac{\beta_j}{\beta_j-1}\right) \leqslant \left((M_{\beta_1}+4)\log\beta_1 + \log\frac{\beta_1}{\sqrt[3]{2}-1} + 1\right)(1+\log i).$$

Conditions (3.4) - (3.6) can be achieved by suitably repeating the bases β_j. All conditions are satisfied in step 1, and the process of repeating the bases is possible computably.

Properties (3.4) - (3.6) and (3.11), together with $t_{i+1} = k_{i+1} = 1/\varepsilon_{i+1} \sim \log i$, imply that for i large enough

$$n_{i+1} \geqslant O\left(\frac{\log i}{1/\log i}\left(\log i + (\log i)^2 + \log\log i + \log i + \log i\right)\right) = O\left((\log i)^4\right)$$

where the implied constant only depends on β_1. Hence n_{i+1} grows at least as $O(\log i)$ and at most as $O((\log i)^4)$, where the implied constants depend only on β_1. Thus $\log 1/F_{i+1}$ and hence also $\|u_j^{(i+1)}(\mathbf{J})\|$ growths at least as $O(\log i)$ and at most as $O((\log i)^4)$, where again the implied constants only depend on β_1. Thus $\|u_j^{(i+1)}(\mathbf{J})\|$ satisfies conditions (3.2) of Proposition 3.2. Hence the number X produced by this algorithm is β_j-normal for every $j \geqslant 1$. □

Remark. The choices of how t_i, ε_i and k_i change with the step i of the algorithm and the conditions on the sequence of bases $(\beta_j)_{j\geqslant 1}$ are rather arbitrary. There is a lot of freedom to optimize for other quantities, such as done in Becher, Heiber, Slaman [17] where computational speed is optimized. This is not taken into account here.

Remark. Following these lines, an extension of Becher, Heiber, Slaman's algorithm to a countable set of real bases that are β-numbers is possible, provided these bases are bounded away from 1 and such there is a uniform bound on the length of the periodic part in their orbit of 1.

A β-number is a real number β such that the orbit of 1 under T_β is finite. Pisot numbers are β-numbers. It is not known under which conditions Salem numbers are or are not β-numbers (a *Salem number* is a real algebraic integer $\beta > 1$ such that all its conjugates have absolute values at most equal to one, with equality in at least one case). Salem numbers of degree 4 are β-numbers, but there is computational and heuristic evidence that higher degree Salem numbers exist that are no β-numbers, see for example [36].

Note that β-numbers satisfy the specification property - one can always use a block of zeros to make the concatenation of two admissible blocks admissible. This is because admissible words can be characterized as precisely the subwords of the lexicographic largest word in the β-shift. Since the orbit of 1 is finite, this word will be eventually periodic and hence the lengths of subwords consisting of only zeros is bounded. Thus Lemma 3 in [27] on the number of (ε, k)-normal admissible words is valid and can be used as an existence criterion for a t_i sequence $\mathbf{J}$ in each step of the algorithm.

Note also that β-numbers also satisfy Proposition 2.6 of [86] needed to control the decay of the length of subintervals. However, we are looking for a lower bound for the measure of cylinder intervals of the form (3.3) that is uniform for all bases β under consideration. This can achieved by requiring that there is a uniform bound on the length of the period of the orbit of 1 under T_β for each β under consideration.

When adapting the proof of Lemma 3.4 to β-numbers, we moreover need to require that the set of β-numbers under consideration is bounded away from 1, as above with the plastic number.

4. Explicit Estimates for β-expansions

In this section we make explicit the constants in Lemma 3.1 using large deviation estimates for certain dependent random variables. This requires us to provide an upper bound for the length of the largest block of zeros appearing in the modified β-expansion of 1 for a Pisot number β.

4.1. **Number of zeros in the expansion of 1.** Let β be a Pisot number and denote by $d_\beta(1) = 0.\varepsilon_1\varepsilon_2\dots$ the β-expansion of 1, i.e. $\varepsilon_1 = \lfloor \beta \rfloor$ and $\varepsilon_i = \lfloor \beta T_\beta^{i-1}(1) \rfloor$ for $i \geqslant 1$. Let $d_\beta^*(1)$ be the modified β-expansion of 1, i.e. $d_\beta^*(1) = d_\beta(1)$ if the sequence $\varepsilon_1\varepsilon_2\dots$ does not end with infinitely many zeros, and $d_\beta^*(1) = 0.(\varepsilon_1\varepsilon_2\dots\varepsilon_{n-1}(\varepsilon_n - 1))^\omega$ when $d_\beta(1)$ ends in infinitely many zeros and ε_n is the last non-zero digit. It is known that $d_\beta^*(1)$ is purely periodic or eventually periodic if β is Pisot. We reprove this fact here and give an explicit upper bound for the preperiod length v and period length p and take $v + p$ as a trivial upper bound for the size of the largest block of zeros in $d_\beta^*(1)$. Note that $d_\beta^*(1)$ is (eventually) periodic if the orbit of 1 under T_β is finite, and that the number of distinct elements in this orbit is precisely $v + p$.

Proposition 4.1. *Let β be a Pisot number of degree d with r real conjugates $\beta = \beta_1, \beta_2, \dots, \beta_r$ and $2s$ complex conjugates $\beta_{r+1}, \dots, \beta_d$. Then the orbit of 1 under the map T_β, i.e. the set*

$$\{T_\beta^k(1) \mid k \geqslant 0\},$$

is finite and its number of elements is bounded by

$$M = d! \det(B)^{-1} 2^{r+s-1} \pi^s C^{r+2s-1} + d \tag{4.1}$$

where

$$B = \begin{pmatrix} 1 & \beta & \dots & \beta^{d-1} \\ 1 & \beta_2 & \dots & \beta_2^{d-1} \\ \vdots & \vdots & & \vdots \\ 1 & \beta_d & \dots & \beta_d^{d-1} \end{pmatrix} \tag{4.2}$$

and where

$$C = 1 + \frac{\lfloor \beta \rfloor}{1 - \eta}$$

with $\eta = \max_{2 \leqslant j \leqslant d} |\beta_j| < 1$.

Proof. For $k \geqslant 0$, $T_\beta^k(1)$ is an element of $\mathbb{Z}[\beta]$, hence there is a unique representation $T_\beta^k(1) = p_0^{(k)} + p_1^{(k)}\beta + \dots + p_{d-1}^{(k)}\beta^{d-1}$ with $p_i^{(k)} \in \mathbb{Z}$. Denote by σ_j, $1 \leqslant j \leqslant d$, the j-th conjugation, ordered such that the first r are real, and $\sigma_{r+i} = \bar{\sigma}_{r+s+i}$ for $1 \leqslant i \leqslant s$. We have

$$T_\beta^k(1) = \beta^k \left(1 - \sum_{l=1}^{k} \varepsilon_l \beta^{-l}\right)$$

hence for $2 \leqslant j \leqslant d$

$$|\sigma_j(T_\beta^k(1))| \leqslant 1 + \frac{\lfloor \beta \rfloor}{1-\eta}$$

where $\eta = \max_{2 \leqslant j \leqslant d} |\beta_j| < 1$.

Note that

$$B \begin{pmatrix} p_0^{(k)} \\ p_1^{(k)} \\ \vdots \\ p_{d-1}^{(k)} \end{pmatrix} = \begin{pmatrix} T_\beta^k(1) \\ \sigma_2(T_\beta^k(1)) \\ \vdots \\ \sigma_d(T_\beta^k(1)) \end{pmatrix}$$

where B is as in (4.2) and has determinant $\det B = \prod_{1 \leqslant i < j \leqslant d}(\beta_j - \beta_i) \neq 0$. Now, since the vector of $T_\beta^k(1)$ and its conjugates can be canonically embedded in a compact convex set in $\mathbb{R}^{r+2s}$ of volume $2^{r+s-1}\pi^s C^{r+2s-1}$, we can count the $\mathbb{Z}^d$-lattice points in a compact convex set in $\mathbb{R}^d$ of volume $\det(B)^{-1} 2^{r+s-1}\pi^s C^{r+2s-1}$. By loosing a factor of 2, we can make this set additionally centrally symmetric if we allow $T_\beta^k(1)$ (formally) to take on values in the interval $[-1, 1]$. Then we can use a result by Blichfeldt [33] and bound the number of $\mathbb{Z}^d$-lattice points in $B^{-1}Y$ by

$$|B^{-1}Y \cap \mathbb{Z}^d| \leqslant d! \det(B)^{-1} 2^{r+s-1}\pi^s C^{r+2s-1} + d$$

with $C = 1 + \frac{\lfloor \beta \rfloor}{1-\eta}$ and hence obtain an upper bound for the number of distinct points in the orbit of 1 under T_β which is also a trivial upper bound for the maximum number of consecutive zeros in the modified β-expansion of 1 as explained above. □

4.2. **Number of not (ε, k)-normal numbers.** Let β be a Pisot number and let $\mathcal{L}_n$ be the set of all admissible words of length n. Fix $\varepsilon > 0$ and a positive integer k. We wish to find explicit estimates for the number of non-(ε, k)-normal words of length n for fixed $\varepsilon > 0$ and k such as given in Lemma 3.1 (Lemma 3 in [27]). The method in [27] uses methods of ergodic theory and the authors are not aware of a method to make the implied constants explicit. Therefore we use a probabilistic approach by viewing the digits to base β as random variables and using a variant of Hoeffding's inequality for dependent random variables to bound the tail distribution of their sum. This approach automatically gives all involved constants explicitly. We use the following Lemma due to Siegel (Theorem 5 in [122]).

Lemma 4.2. *Let $X = X_1 + X_2 + \ldots + X_l$ be the sum of l possibly dependent random variables. Suppose that X_i, for $i = 1, 2, \ldots, l$, is the sum of n_i mutually independent random variables having values in the interval $[0, 1]$. Let $\mathbb{E}[X_i] = n_i p_i$. Then for $a \geqslant 0$*

$$\mathbb{P}(X - \mathbb{E}[X] \geqslant a) < \exp\left(-\frac{a^2}{8(\sum_i \sqrt{p_i(1-p_i)n_i})^2}\right) + \exp\left(-\frac{3a}{4\sum_i (1-p_i)^2}\right).$$

Proposition 4.3. *Let β be a Pisot number. The μ_β-measure of the set of not (ε, k)-normal words of length n satisfies*

$$\mu_\beta(E_n^c(\varepsilon, k)) \leqslant 4|\mathcal{L}_k||\mathcal{L}_n|^{-\eta}$$

for $n \geqslant M + k$ with $\eta > 0$ as in equation (4.3) and M as in equation (4.1).

Proof. Let $d \in \mathcal{L}_k$ and for $n \geqslant M + k$, let $X_1, \ldots, X_{M+1} : \mathcal{L}_n \to \mathbb{R}$ be random variables where $X_i(\omega)$ denotes the number of occurrences of the word d in $\omega = \omega_1 \ldots \omega_n$ at positions

$$\omega_{i+j(M+1)}\omega_{i+j(M+1)+1} \cdots \omega_{i+j(M+1)+k-1}$$

for $0 \leqslant j \leqslant \lfloor \frac{n-k}{M+1} \rfloor$. The X_i are dependent, but each is a sum of $n_i = \lfloor \frac{n-k}{M+1} \rfloor + 1$ independent identically distributed random variables $Y_j^{(i)}$ that take value one if and only if the word d appears in ω starting at digit $\omega_{i+j(M+1)}$ and zero otherwise. We have $\mathbb{E}[X] = n\mu_\beta(c(d))$ and $\mathbb{E}[X_i] = n_i\mu_\beta(c(d))$. Denote by $\bar{E}_n(\varepsilon, k)$ the set of words of length n for which there is a subword d of length k that appears more often than $n(\mu_\beta(c(d)) + \varepsilon)$ times and let $\bar{E}_n(\varepsilon, d)$ be the set of words of length n for which the subword d appears more often than $n(\mu_\beta(c(d)) + \varepsilon)$ times. We apply Lemma 4.2 with $l = M + 1$, n_i as above, $p_i = \mu_\beta(c(d))$ and $a = n\varepsilon$ and obtain

$$\begin{aligned}\mu_\beta(X > n(\mu_\beta(c(d)) + \varepsilon)) &= \mu_\beta(\bar{E}_n(\varepsilon, d)) \\ &< \exp\left(-\frac{(n\varepsilon)^2}{8\mu_\beta(c(d))(1-\mu_\beta(c(d)))(M+1)^2(\lfloor \frac{n-k}{M+1} \rfloor + 1)}\right) \\ &\quad + \exp\left(-\frac{3n\varepsilon}{4(M+1)(1-\mu_\beta(c(d)))^2}\right).\end{aligned}$$

Using $c\beta^{-k} \leqslant \mu_\beta(c(d)) \leqslant \beta^{-k}$ and $n \geqslant M + 1$, this is

$$< \exp\left(-\frac{\varepsilon^2 n}{16(M+1)\beta^{-k}}\right) + \exp\left(-\frac{3\varepsilon n}{4(M+1)}\right) < 2\exp\left(-\frac{\varepsilon n}{M+1}\min(\frac{\varepsilon}{16\beta^{-k}}, \frac{3}{4})\right).$$

Finally, since $\mu_\beta(\bar{E}_n(\varepsilon, k)) \leqslant \sum_{d \in \mathcal{L}_k} \mu_\beta(\bar{E}_n(\varepsilon, d))$ and using that $\beta^n \leqslant |\mathcal{L}_n| \leqslant \frac{\beta}{\beta-1}\beta^n$ we obtain

$$\begin{aligned}\mu_\beta(\bar{E}_n(\varepsilon, k)) &\leqslant |\mathcal{L}_k| 2\exp\left(-\frac{\varepsilon n}{M+1}\min(\frac{\varepsilon}{16\beta^{-k}}, \frac{3}{4})\right) \\ &\leqslant 2|\mathcal{L}_k||\mathcal{L}_n|^{-\eta}\end{aligned}$$

with

$$\eta = \frac{\varepsilon \min(\frac{\varepsilon}{16\beta^{-k}}, \frac{3}{4})}{\log(\frac{\beta}{\beta-1}) + (M+1)\log\beta} > 0. \tag{4.3}$$

Using the same argument with $Y = n - X$ gives a symmetrical upper bound for the number of words ω of length n in which the word d appears less than $n\mu_\beta(c(d)) - \varepsilon n$ times. Thus we obtain an upper bound for the number of not (ε, k)-normal words of length n of the form

$$4|\mathcal{L}_k||\mathcal{L}_n|^{-\eta}$$

for $n \geqslant M + k$ with η as in (4.3). □

Corollary 4.4. *The number of not (ε, k)-normal words of length n satisfies*

$$|E_n^c(\varepsilon, k)| \leqslant C|\mathcal{L}_n|^{1-\eta}$$

for $n \geqslant M + k$ with $\eta > 0$ as in equation (4.3)*, M as in equation* (4.1)*, and where $C = 4|\mathcal{L}_k|\beta^{M+1}\frac{\beta}{\beta-1}$.*

Proof. Since the Parry measure μ_β satisfies

$$\left(1 - \frac{1}{\beta}\right)\lambda \leqslant \mu_\beta \leqslant \frac{\beta}{\beta-1}\lambda$$

with respect to the Lebesgue measure λ, and due to the bounds on the Lebesgue measure of β-adic cylinder intervals from Lemma 3.3, the bound from Proposition 4.3 on the μ_β measure of the set of non-(ε, k)-normal words of length n implies for the number of such words

$$|E_n^c(\varepsilon, k)| \leqslant C|\mathcal{L}_n|^{1-\eta}, \tag{4.4}$$

where $C = C(\beta, k) = 4|\mathcal{L}_k|\beta^M\frac{\beta}{\beta-1}$ and $\eta = \eta(\beta, \varepsilon, k)$ as given in equation (4.3) and where we used that $\beta^n \leqslant |\mathcal{L}_n| \leqslant \frac{\beta}{\beta-1}\beta^n$. □

Acknowledgements. For the realization of the present paper the first author received support from the Conseil Régional de Lorraine. Parts of this research work were done when the first author was visiting the Department of Mathematics of Graz University of Technology. The author thanks the institution for their hospitality. The second author was supported by the Austrian Science Fund (FWF): I 1751-N26; W1230, Doctoral Program “Discrete Mathematics”; and SFB F 5510-N26. He would like to thank Karma Dajani and Bing Li for some interesting discussions on β-expansions. All authors thank the Erwin-Schrödinger-Institute (ESI) for its hospitality during the workshop *Normal Numbers: Arithmetic, Computational and Probabilistic Aspects*, November 14–18, 2016.

On the continued fraction expansion of absolutely normal numbers

Adrian-Maria Scheerer[10]

Abstract. We construct an absolutely normal number whose continued fraction expansion is normal in the sense that it contains all finite patterns of partial quotients with the expected asymptotic frequency. The construction is based on ideas of Sierpinski and a large deviation theorem for sums of mixing random variables.

1. Introduction

Consider a real number x in the unit interval $[0,1)$. Let $b \geqslant 2$ be a positive integer and consider the maps $T_b : [0,1) \to [0,1), x \mapsto bx \bmod 1$ and the Gauss map $T_G : [0,1) \to [0,1)$ defined by $T_G(x) = \frac{1}{x} \bmod 1$ if $x > 0$ and $T_G(0) = 0$. Then x is called *normal to base* b, if for all real numbers $0 \leqslant a < b < 1$

$$\frac{1}{n}\sum_{i=0}^{n-1} \chi_{[a,b)}(T_b^i(x)) \to b - a \tag{1.1}$$

holds, as n tends to infinity. Here, χ_A is the characteristic function of the set A. x is called *continued fraction normal*, if for all $0 \leqslant a < b < 1$

$$\frac{1}{n}\sum_{i=0}^{n-1} \chi_{[a,b)}(T_G^i(x)) \to \mu_G([a,b)), \tag{1.2}$$

where μ_G is the Gauss-Kuzmin measure on $[0,1)$, given by

$$\mu_G(A) = \frac{1}{\log 2}\int_A \frac{1}{1+x}dx$$

for any Borel set A.

The maps T_b are invariant and ergodic with respect to the Lebesgue measure and the Gauss map T_G is invariant and ergodic with respect to μ_G. An application of the point-wise ergodic theorem thus shows that with respect to Lebesgue measure almost all real numbers in the unit-interval are simultaneously normal to all integer bases $b \geqslant 2$ (such numbers are called *absolutely normal*) and continued fraction normal. The aim of this note is to exhibit an example of such a number by means of describing its binary expansion one digit after the other using a recursive construction.

[10] This article appeared in [114]

Our construction is based on ideas of Sierpinski and Becher and Figueira and can be described as follows. We consider a suitable large subset Ω of $[0,1)$ as our ambient set. This set contains all real numbers whose partial quotients grow at a controlled rate (see Section 3). We wish to exclude from this set from the set of all non-normal numbers and do so by collecting these numbers in a set E. This set will in fact have positive but arbitrarily small measure. Part of the proof is showing that this set is 'small'. The corresponding calculations are carried out in Sections 2 and 4. The main new ingredient is the use of a large deviations theorem for sums of mixing random variables to control deviations in (1.2). In Section 6 we compute the binary expansion of a number ν in $\Omega \setminus E$. This is done starting with the interval $[0,1)$ and then considering recursively both halves of the preceding interval and deciding which half is 'best', i.e. contains more of $\Omega \setminus E$. To make this construction computable, we actually work with finitary versions of Ω and E, at the cost of a small but controllable error. Finally, in Theorem 6.1 we show that ν is computable and indeed simultaneously normal to every integer base $b \geqslant 2$, as well as continued fraction normal.

It is in fact enough to consider in definitions (1.1) and (1.2) so-called cylinder sets. These are intervals, all of whose elements share the same beginning in their base b expansion or continued fraction expansion. This way we recover the more familiar definition of normality via the expected behaviour of the asymptotic frequencies of all finite digit patterns.

Normal numbers originated in work of Borel from 1909, and much has since been written about them. The reader is best advised to have a look at Bugeaud. The problem of constructing an absolutely normal number that is also continued fraction normal is also mentioned there. Although there exist many constructions of normal numbers (to a single base), no easy construction of a number normal to two multiplicatively independent bases is known. However, recently constructions of absolutely normal numbers via recursively formulated algorithms have received much interest. If 'easy' is interpreted from a computational viewpoint, the problem has been solved by Becher, Heiber, Slaman, who gave a polynomial time algorithm for computing the digits (to some base) of an absolutely normal number.

existence/almost all properties of normality in cantor sets both for integer bases and cf-defined cantor sets. recently simmons, weiss. However these constructions do not seem to be constructive.

2. Large Deviation Estimates

2.1. **Non-normal numbers for integer bases.** Let $b \geqslant 2$ be an integer. A word $\omega = \omega_1 \ldots \omega_n$ of n digits $0 \leqslant \omega_i \leqslant b-1$, $1 \leqslant i \leqslant n$, is called $(\varepsilon, 1)$-*normal of length* n, if for each digit $0 \leqslant d \leqslant b-1$,

$$n\frac{1}{b}(1-\varepsilon) < N(d,\omega) < n\frac{1}{b}(1+\varepsilon),$$

where $N(\omega, d)$ is the number of i, $1 \leqslant i \leqslant n$, such that $\omega_i = d$. Let $E_b(\varepsilon, n)$ be the set of all real numbers $x \in [0,1)$ such that the first n digits of the b-ary expansion of x form an $(\varepsilon,1)$-normal word of length n. Denote the complement of $E_b(\varepsilon,n)$ in $[0,1)$ by $E_b^c(\varepsilon,n)$.

Fix a digit d, $0 \leqslant d \leqslant b-1$ and consider the random variables $X_i : [0,1) \to \mathbb{R}$, for $1 \leqslant i \leqslant n$, defined by $X_i(x) = 1$ if the i-th digit in the b-ary expansion of x equals d, and $X_i(x) = 0$ otherwise. The X_i are independent and have expectation $\frac{1}{b}$. Let $S_n = X_1 + \ldots + X_n$. Then Hoeffding's inequality for the sum of n i.i.d. random variables bounded by 0 and 1 yields

$$\mathbb{P}\left(\left|\frac{S_n}{n} - \mathbb{E}\left(\frac{S_n}{n}\right)\right| \geqslant t\right) \leqslant 2\exp(-2nt^2).$$

In our case, the probability measure is the Lebesgue measure λ on the unit interval. With $t = \frac{\varepsilon}{b}$,

$$\lambda\left(\left\{x \in [0,1) : \left|\frac{1}{n}\sharp\{1 \leqslant i \leqslant n : X_i(x) = d\} - \frac{1}{b}\right| \geqslant \frac{\varepsilon}{b}\right\}\right) \leqslant 2\exp\left(-\frac{2\varepsilon^2}{b^2}n\right).$$

Hence, for the number of non-$(\varepsilon,1)$-normal numbers of length n,

$$\lambda\left(E_b^c(\varepsilon,n)\right) \leqslant 2b\exp\left(-\frac{2\varepsilon^2}{b^2}n\right).$$

If we define $(\varepsilon,1)$-normality as $n(\frac{1}{b}-\varepsilon) < N(d,\omega) < n(\frac{1}{b}+\varepsilon)$, then

$$\lambda(E_b^c(\varepsilon,n)) \leqslant 2b\exp(-2\varepsilon^2 n).$$

2.2. **Non-normal numbers for continued fractions.** Let A be a Borel subset of $[0,1)$ and denote the Gauss measure of A by $\mu_G(A) = \frac{1}{\log 2}\int_A \frac{1}{1+x}dx$. Let $\varepsilon > 0$ and let k, D, n be positive integers. A word $\omega = \omega_1 \ldots \omega_n$ of length n of digits $\omega_i \in \{1, \ldots D\}$ will be called (ε,k,D,n)-*CF-normal*, if for all words $d = d_1 \ldots d_k$ of length k of digits $d_j \in \{1, \ldots, D\}$,

$$(n-k+1)\mu_G(\Delta_d)(1-\varepsilon) < N(d,\omega) < (n-k+1)\mu_G(\Delta_d)(1+\varepsilon) \tag{2.1}$$

holds, where $N(d,\omega)$ is the number of i, $1 \leqslant i \leqslant n-k+1$, such that $\omega_i \ldots \omega_{i+k-1} = d_1 \ldots d_k$ and where Δ_d is the set of all real numbers in $[0,1)$ whose continued fraction expansion coincides on the first k digits with d.

The set of real numbers $x \in [0,1)$ whose first n partial quotients form a word that is (ε,k,D,n)-CF-normal will be denoted by $E_{\mathrm{CF}}(\varepsilon,k,D,n)$. We denote its complement in $[0,1)$ by $E_{\mathrm{CF}}^c(\varepsilon,k,D,n)$.

We also require a notation for the set of $x \in [0,1)$, where the number of occurrences of only one specific d of length k of digits in $\{1,\dots,D\}$ satisfies (2.1). This set will be denoted by $E_{\mathrm{CF}}(\varepsilon, \mathbf{d}, D, n)$.

Similarly, we introduce the sets $E_{\mathrm{CF}}(\varepsilon, k, n)$ and $E_{\mathrm{CF}}(\varepsilon, d, n)$.

Fix a word d of length k composed from positive integers. For $i \geqslant 1$ we have the random variables $a_i : [0,1) \to \mathbb{R}$ and derived random variables $X_i : [0,1) \to \mathbb{R}$. The a_i are defined by $a_i(x) = a_i$ when the continued fraction expansion of x is $x = [0; a_1, a_2, \dots, a_i, \dots]$. The X_i are defined to be $1 - \mu_i$ if the string d appears in the continued fraction expansion of x starting at a_i, and $-\mu_i$ if not. The numbers μ_i are chosen such that $E[X_i] = 0$.

A sequence $(X_i)_{i\geqslant 1}$ of random variables $X_i : [0,1) \to \mathbb{R}$ is called *strongly mixing*, if

$$\alpha(n) := \sup_{l\geqslant 1} \alpha(M_l, G_{l+n}) \to 0 \tag{2.2}$$

as $n \to \infty$. Here $M_l = \sigma(X_i, i \leqslant l)$ and $G_{l+n} = \sigma(X_i, i \geqslant l+n)$ are the σ-algebras generated by X_i, for $i \leqslant l$, and by X_i, for $i \geqslant l+n$. The *α-mixing coefficients* $\alpha(M_l, G_{l+n})$ are defined by

$$\alpha(M_l, G_{l+n}) = \sup_{A\in M_l, B\in G_{l+n}} |\mathbb{P}(A\cap B) - \mathbb{P}(A)\mathbb{P}(B)|.$$

We know the following mixing property of $(a_i)_{i\geqslant 1}$ with respect to the Gauss map μ_G on $[0,1)$.

Theorem 2.1 (Philipp (1988))**.** *The a_i are exponentially strongly mixing. In fact we have for some $0 \leqslant \rho < 0.8$*

$$|\mu_G(A\cap B) - \mu_G(A)\mu_G(B)| \leqslant \rho^n \mu_G(A)\mu_G(B) \tag{2.3}$$

for all $A \in \sigma(a_i, i \leqslant l)$ and $B \in \sigma(a_i, i \geqslant n+l)$.

The constant ρ has been subject to later improvements. We worked here with $\rho = 0.8$.

From Theorem 2.1 we can derive exponential strong mixing for the random variables X_i with respect to the Gauss measure μ_G. We look at $|\mu_G(A\cap B) - \mu_G(A)\mu_G(B)|$ where $A \in \sigma(X_1,\dots,X_l)$ and $B \in \sigma(X_{l+n}, X_{l+n+1}, \dots)$. Since $\sigma(X_i) = X_i^{-1}\mathcal{B}(\mathbb{R})$ is generated by $\{\varnothing, [0,1), T_G^{-i}(d) = a_i^{-1}(d_1) \cap a_{i+1}^{-1}(d_2) \cap \dots \cap a_{i+k-1}^{-1}(d_k), [0,1) \smallsetminus T_G^{-i}(d)\}$ where T_G is the Gauss map on $[0,1)$, we have that $\sigma(X_i) \subset \sigma(a_i, \dots, a_{i+k-1})$ and hence $\sigma(X_1,\dots,X_l) \subset \sigma(a_1,\dots,a_{l+k-1})$. Consequently $\sigma(X_l, X_{l+1}, \dots) \subset \sigma(a_l, a_{l+1}, \dots)$. Thus any mixing coefficient $\alpha(n-k+1)$ for the a_i is a valid mixing coefficient $\alpha(n)$ for the X_i, for $n \geqslant k$. For smaller values of n, note that in general $\alpha(n) \leqslant \frac{1}{4}$. Hence the X_i are strongly mixing with α-mixing coefficient $\alpha(n) \leqslant \exp(-2nc)$ for all $n \geqslant 1$ with

$$c = -\frac{\log 0.8}{2k}. \tag{2.4}$$

We have thus shown that there is an explicit $c > 0$ such that $(X_i)_{i\geqslant 1}$ is a sequence of strongly mixing centred real-valued bounded random variables with α-mixing coefficient $\alpha(n)$ satisfying $\alpha(n) \leqslant \exp(-2cn)$. As such the X_i satisfy the assumptions of the following large deviation theorem.

Theorem 2.2 (Corollary 12 of Bernstein inequality..). *Let $(X_i)_{i\geqslant 1}$ be a sequence of centered real-valued random variables bounded by a uniform constant M and with $\alpha(n)$ satisfying $\alpha(n) \leqslant \exp(-2nc)$ for some $c > 0$. Then for all $n \geqslant 2 \cdot \max(c, 2)$ and $x \geqslant 0$*

$$\mathbb{P}(|S_n| \geqslant x) \leqslant \exp\left(-\frac{x^2}{n(\log n)4CM^2 + 4Mx(\min(c,1))^{-1}}\right), \tag{2.5}$$

where $C = 6.2K + (\frac{1}{c} + \frac{8}{c^2}) + \frac{2}{c\log 2}$, with $K = 1 + 8\sum_{i\geqslant 1}\alpha(i)$.

Here S_n denotes again the sum $X_1 + X_2 + \ldots + X_n$.

The following theorem is thus a corollary of Theorem 2.2.

Theorem 2.3. *Fix a string d of positive integers of length k. We have for $N \geqslant 2(k+1)$*

$$\mu_G(E^c_{CF}(\varepsilon, d, N)) \leqslant \exp\left(-\frac{(\varepsilon\mu_G(\Delta_d))^2}{16(C + (\varepsilon\mu_G(\Delta_d))/c)}\frac{N}{\log N}\right). \tag{2.6}$$

Proof. We set $x = \varepsilon\mu_G(\Delta_d)n$, $\mathbb{P} = \mu_G$, $n = N-k+1$ and $M = 1$. Hence $|S_n| \geqslant x$ is the same as $|\sum_{i=1}^{N-k+1} X_i - (N-k+1)\mu_G(\Delta_d)| \geqslant \varepsilon\mu_G(\Delta_d)(N-k+1)$ which is equivalent to the defining condition of non-(ε, d, N)-CF-normality from (2.1). We have $0.09 < -\log 0.8 < 0.1$, so for any k, $\max(c, 1) = 1$ and Theorem 2.2 can be applied provided $N - k + 1 \geqslant 4$ holds. To estimate the exponent we used $N - k + 1 \geqslant \frac{1}{2}N$, valid for $N \geqslant 2(k-1)$. The requirement $N \geqslant 2(k+2)$ meets both conditions on N. □

We put

$$\tilde{\eta}_{\mathrm{CF}}(\varepsilon, d, k) = \frac{(\varepsilon\mu_G(\Delta_d))^2}{16(C + (\varepsilon\mu_G(\Delta_d))/c)}$$

and wish to simplify this expression by bounding it from below. This can be achieved by straight-forward calculations, noting that $c \leqslant 1/20 < 1$ for any k, and that $N\mu_G(\Delta_d)(1 + \varepsilon) \leqslant N$, so that $\mu_G\varepsilon \leqslant 1 - \mu_G \leqslant 1$.

We obtain

$$\tilde{\eta}_{\mathrm{CF}}(\varepsilon, d, k) > \eta_{\mathrm{CF}}(\varepsilon, d, k) = \left(\frac{\varepsilon\mu_G(\Delta_d)}{900k}\right)^2. \tag{2.7}$$

From here on, we will work with η_{CF} defined by this equation as the constant from Theorem 2.3.

Remark. The bound obtained in Theorem 2.3 bounds a set of certain real numbers with a priori no restrictions on their partial quotients. Since $E^c_{\mathrm{CF}}(\varepsilon, d, D, N) \subset E^c_{\mathrm{CF}}(\varepsilon, d, N)$ the bound (2.6) is also valid for this smaller set. Note that $E^c_{\mathrm{CF}}(\varepsilon, d, D, N)$ is a union of finitely many intervals with rational endpoints and thus can be computed, as well as its Lebesgue measure.

The bound from (2.6) is valid for the Lebesgue measure of $E^c_{\mathrm{CF}}(\varepsilon, d, N)$ with an additional factor of $\frac{1}{\log 2}$.

3. Restricting partial quotients

Fix $f\colon \mathbb{N} \to \mathbb{N}$ and denote

$$\Omega_N = \{x \in [0,1) \mid a_i(x) \leqslant f(i), 1 \leqslant i \leqslant N\}$$
$$\Omega = \bigcap_{N \geqslant 1} \Omega_N = \{x \in [0,1) \mid a_i(x) \leqslant f(i), i \geqslant 1\}.$$

By appropriately choosing f, Ω has measure arbitrarily close to 1.

Proposition 3.1. *Let $f(i) = A2^i - 2$ with a positive integer A. Then*

$$\lambda(\Omega) \geqslant 1 - \frac{2}{A}, \qquad \text{and} \qquad \lambda(\Omega_N \setminus \Omega) \leqslant \frac{1}{A}\frac{1}{2^{N+1}}.$$

Proof. Since $\log(2)\mu_G \leqslant \lambda \leqslant 2\log(2)\mu_G$ and the invariance of μ_G under the Gauss map we have

$$\begin{aligned}\lambda(\Omega) &= \lambda\{x \in [0,1) \mid a_i(x) \leqslant f(i), i \geqslant 1\} = 1 - \lambda\left(\bigcup_{i \geqslant 1}\{x \in [0,1) : a_i \geqslant f(i)+1\}\right) \\ &\geqslant 1 - 2\log(2)\sum_{i=1}^{\infty} \mu_G\{a_i \geqslant f(i)+1\} = 1 - 2\log(2)\sum_{i=1}^{\infty}\mu_G\{a_1 \geqslant f(i)+1\} \\ &\geqslant 1 - 2\sum_{i=1}^{\infty}\lambda\{a_1 \geqslant f(i)+1\} = 1 - 2\sum_{i=1}^{\infty}\frac{1}{f(i)+2}.\end{aligned}$$

Choosing $f(i) = A2^i - 2$ with a positive real numbers A gives

$$\lambda(\Omega) \geqslant 1 - \frac{2}{A}.$$

For the second assertion,

$$\Omega_N \setminus \Omega = \bigcap_{1 \leqslant i \leqslant N}\{x \in [0,1) : a_i(x) \leqslant f(i)\} \cap \bigcap_{i \geqslant N+1}\{x \in [0,1) : a_i(x) \geqslant f(i)+1\}.$$

Thus

$$\begin{aligned}\lambda(\Omega_N \smallsetminus \Omega) &\leqslant \lambda(\{x \in [0,1) : a_{N+1}(x) \geqslant f(N+1)+1\}) \\ &= \frac{1}{A2^{N+1}},\end{aligned}$$

since the measure of the intersection of a number of sets can be trivially bounded above by the measure of one of the intersecting sets. □

Let $\omega = \frac{2}{A}$ and $\omega_N = \frac{1}{A}\frac{1}{2^{N+1}}$ so that $\lambda(\Omega) \geqslant 1-\omega$ and $\lambda(\Omega_N \smallsetminus \Omega) \leqslant \omega_N$.

Note that Ω_N in $[0,1)$ is a union of cylinder intervals with rational endpoints and is thus computable, as well as its Lebesgue measure $\lambda(\Omega_N)$.

4. A set containing all non-normal numbers

Let $\beta > 0$ be a parameter such that $1-\omega-\beta > 0$. β will be used to control the measure of a set E which contains all non-normal numbers.

Let

$$E = \bigcup_{b\geqslant 2}\bigcup_{m\geqslant 1}\bigcup_{N\geqslant N_b(m)} \tilde{E}_b^c(1/m,N) \cup \bigcup_{d}\bigcup_{m\geqslant 1}\bigcup_{N\geqslant N_{CF}(m,d,k)+1} \tilde{E}_{CF}^c(1/m,d,N)$$

Here, the tilde shall indicate that we take each interval of which the E_b and E_{CF} consist to be three times the length.

We further introduce a finite version of E. For a positive integer k, let

$$E_k = \bigcup_{b=2}^{k}\bigcup_{m=1}^{k}\bigcup_{N=N_b(m)}^{kN_b} E_b^c(1/m,N) \cup \bigcup_{m=1}^{k}\bigcup_{d,|d|\leqslant k, d_i\leqslant k}\bigcup_{N=N_{CF}(m,d,k)+1}^{kN_{CF}} E_{CF}^c(1/m,d,f(N),N)$$

Trivial upper bounds for the Lebesgue measure of E and E_k are

$$\lambda(E) \leqslant \sum_{b\geqslant 2}\sum_{m\geqslant 1}\sum_{N\geqslant N_b(m)} \lambda(E_b^c(1/m,N)) + \sum_{d}\sum_{m\geqslant 1}\sum_{N\geqslant N_{CF}(m,d,k)+1} \lambda(E_{CF}^c(1/m,d,f(N),N))$$

and

$$\lambda(E_k) \leqslant \sum_{b=2}^{k}\sum_{m=1}^{k}\sum_{N=N_b(m)}^{kN_b} \lambda(E_b^c(1/m,N)) + \sum_{\substack{d,|d|\leqslant k,\\ d_i\leqslant k, 1\leqslant i\leqslant k}}\sum_{m=1}^{k}\sum_{N=N_{CF}(m,d,k)+1}^{kN_{CF}} \lambda(E_{CF}^c(1/m,d,f(N),N))$$

The starting lengths N_b and N_{CF} are chosen such that $\lambda(E) \leqslant \beta$. In the integer case, they are allowed to depend on the base and $\varepsilon = 1/m$ and in the continued fraction case on $\varepsilon = 1/m$ and on the word d. The function f ensures computability of the set E_k and its measure.

Let $r_k = \lambda(E \smallsetminus E_k)$.

Proposition 4.1. *We have $\lambda(E) \leqslant \beta$ and $r_k \leqslant \frac{1}{k}$.*

Proof. We show that for $N_b(m) = \frac{1}{2}C_1 b^4 m^3$ with $C_1 = \sqrt[3]{\frac{48}{\beta}}$

$$\sum_{b\geqslant 2}\sum_{m\geqslant 1}\sum_{N\geqslant N_b(m)} \lambda(E_b^c(1/m, N)) \leqslant \frac{\beta}{6}, \tag{4.1}$$

and that for $N_{\mathrm{CF}}(m,d,k) = C_2 900^8 \mu_G(\Delta_d)^{-8} k^8 m^6 d_k^2 \cdot \ldots \cdot d_1^2$ with $C_2 = \frac{384}{\beta}$

$$\sum_{d}\sum_{m\geqslant 1}\sum_{N\geqslant N_{\mathrm{CF}}(m,d,k)+1} \lambda(E_{CF}^c(1/m, d, f(N), N)) \leqslant \frac{\beta}{6}. \tag{4.2}$$

We treat sum (4.1) first. We have

$$\sum_{b\geqslant 2}\sum_{m\geqslant 1}\sum_{N\geqslant N_b(m)} 2be^{-\frac{2}{m^2b^2}N} = 2\sum_{b\geqslant 2} b \sum_{m\geqslant 1} e^{-\frac{2}{m^2b^2}N_b(m)} \frac{1}{1-e^{-2/(m^2b^2)}}.$$

Note that $(1-e^{-2/(m^2b^2)})^{-1} \leqslant 2m^2b^2$ for all $m \geqslant 1$, $b \geqslant 2$ and that $\int_0^\infty x^2 e^{-cx}dx = \frac{2}{c^3}$ for $c > 0$. Hence this is

$$\leqslant 4\sum_{b\geqslant 2} b^3 \sum_{m\geqslant 1} m^2 e^{-C_1 b^2 m} \leqslant 4\sum_{b\geqslant 2} b^3 \frac{2}{C_1^3 b^6} = \frac{8}{C_1^3}\sum_{b\geqslant 2}\frac{1}{b^3} < \frac{8}{C_1^3}.$$

This is $\leqslant \frac{\beta}{6}$ for $C_1^3 \geqslant \frac{48}{\beta}$.

For continued fractions we use

$$\lambda(E_{CF}^c(1/m, d, f(N), N)) \leqslant \lambda(E_{CF}^c(1/m, d, N)) \leqslant e^{-\eta_{\mathrm{CF}}(\varepsilon,d,k)N^{1/2}}$$

instead of the better term $e^{-\eta_{\mathrm{CF}}(\varepsilon,d,k)\frac{N}{\log N}}$ which is more difficult to work with. We also use

$$\eta_{\mathrm{CF}}(\varepsilon, d, k) = \left(\frac{\varepsilon\mu_G(\Delta_d)}{900k}\right)^2$$

from equation (2.7).

We have $\frac{N}{\log N} \geqslant N^{1/2}$ for all $N \geqslant 1$ and that $e^{-\eta N^{1/2}}$ is strictly decaying for $N \geqslant 0$. Also note that

$$\int_{x_0}^\infty e^{-\eta x^{1/2}}dx = \frac{2}{\eta^2}\frac{\eta x_0^{1/2}+1}{e^{\eta x_0^{1/2}}}.$$

We have

$$(4.2) \leqslant \sum_{d}\sum_{m\geqslant 1}\sum_{N\geqslant N_{\mathrm{CF}}+1} e^{-\eta(m,d,k)N^{1/2}} \leqslant \sum_{d}\sum_{m\geqslant 1} \frac{4}{\eta(m,d,k)} e^{-\frac{1}{2}\eta(m,d,k)\sqrt{N_{\mathrm{CF}}(m,d,k)}},$$

where we used that $\eta N^{1/2}+1 \leqslant 2\eta N^{1/2}$ for $N \geqslant \frac{1}{\eta^2}$. Put $N_{\mathrm{CF}}(m,d,k) = N_{\mathrm{CF}}(d,k)m^6$ and set $\eta(m,d,k) = \eta(d,k)m^{-2}$ with $\eta(d,k) = (\mu_G(\Delta_d)/(900k))^2$ independent of m. Use again $\int_0^\infty x^2 e^{-cx}dx = \frac{2}{c^3}$. Then

$$\begin{aligned}\sum_d \sum_{m\geqslant 1} \frac{4m^2}{\eta(d,k)} e^{-\frac{1}{2}\eta(d,k)\sqrt{N_{\mathrm{CF}}(d,k)}m} &\leqslant \sum_d \frac{64}{\eta(d,k)^4 N_{\mathrm{CF}}(d,k)^{3/2}} \\ &\leqslant 64 \sum_{k\geqslant 1}\sum_{d_k\geqslant 1}\cdots\sum_{d_1\geqslant 1} \frac{1}{\eta(d,k)^4 N_{\mathrm{CF}}(d,k)},\end{aligned}$$

where we split up the sum over all d into $\sum_{k\geqslant 1}\sum_{d,|d|=k} = \sum_{k\geqslant 1}\sum_{d_k\geqslant 1}\cdots\sum_{d_1\geqslant 1}$. Put $N_{\mathrm{CF}}(d) = C_2\frac{900^8}{\mu_G(\Delta_d)^8}k^8 d_k^2\cdot\ldots\cdot d_1^2$ for some positive constant C_2 only dependent on β. Then the previous term is

$$\leqslant \frac{64}{C_2}\sum_{k\geqslant 1}\sum_{d_k\geqslant 1}\cdots\sum_{d_1\geqslant 1}\frac{1}{k^2 d_k^2\cdot\ldots\cdot d_1^2}. \tag{4.3}$$

Since $\sum_{n\geqslant 1} n^{-2} < 1$, this is just

$$\leqslant \frac{64}{C_2},$$

which is $\leqslant \frac{\beta}{6}$ for $C_2 \geqslant \frac{384}{\beta}$.

We continue showing that $r_k \leqslant \frac{1}{k}$. Since $r_k = \lambda(E \smallsetminus E_k)$, r_k can be bounded above by the sum an upper bound (4.4) of the integer part and an upper bound for the continued fraction part (4.5),

$$r_k \leqslant (4.4) + (4.5).$$

We tread the integer-base part first.

$$\left(\sum_{b=2}^{k}\sum_{m=1}^{k}\sum_{N=kN_b}^{\infty} + \sum_{b=2}^{k}\sum_{m=k+1}^{\infty}\sum_{N=N_b}^{\infty} + \sum_{b=k+1}^{\infty}\sum_{m=1}^{\infty}\sum_{N=N_b}^{\infty}\right) 2be^{-\frac{2}{m^2}N}. \tag{4.4}$$

Recall $N_b(m) = \frac{1}{2}C_1 b^4 m^3$ with $C_1 = \sqrt[3]{\frac{48}{\beta}}$. We have for the first sum in (4.4),

$$\sum_{b=2}^{k}\sum_{m=1}^{k}\sum_{N=kN_b+1}^{\infty} 2be^{-\frac{2}{m^2b^2}N} \leqslant 4\sum_{b=2}^{k} b\sum_{m=1}^{k} m^2 e^{-\frac{2}{m^2b^2}kN_b} \leqslant \frac{8}{C_1^3}\sum_{b=2}^{k} b^3\frac{1}{b^6k^3}$$

For the second sum in (4.4),

$$\begin{aligned}\sum_{b=2}^{k}\sum_{m=k+1}^{\infty}\sum_{N=N_b}^{\infty} 2be^{-\frac{2}{m^2}N} \leqslant 4\sum_{b=2}^{k} b^3 \sum_{m=k+1}^{\infty} m^2 e^{-\frac{2}{m^2b^2}kN_b} &\leqslant 4\sum_{b=2}^{k}\left(\frac{kb}{C_1}+\frac{2}{C_1^2kb}+\frac{2}{C_1^3k^3b^3}\right)e^{-C_1b^2k^2} \\ &\leqslant 20k\sum_{b=2}^{k} e^{-C_1b^2k^2} \leqslant 40ke^{-C_1k^2},\end{aligned}$$

where we used that $\int_{x_0}^{\infty} x^2 e^{-cx} dx = (x_0^2/c + 2x_0/c^2 + 2/c^3)e^{-cx_0}$.

For the third sum in (4.4),

$$\sum_{b=k+1}^{\infty} \sum_{m=1}^{\infty} \sum_{N=N_b}^{\infty} 2be^{-\frac{2}{m^2b^2}N} \leqslant 4 \sum_{b=k+1}^{\infty} b^3 \sum_{m=1}^{\infty} m^2 e^{-\frac{2}{m^2b^2}N_b} \leqslant 4 \sum_{b=k+1}^{\infty} b^3 \frac{2}{C_1^3 b^6} < \frac{8}{C_1^3 k^2}.$$

Thus

$$(4.4) \leqslant \frac{8}{C_1^3 k^3} + 40ke^{-C_1 k^2} + \frac{8}{C_1^3 k^2}.$$

The continued fraction part of r_k can be bounded above by

$$\left(\sum_{\substack{d,|d|\leqslant k,\\ d_i\leqslant k, 1\leqslant i\leqslant k}} \sum_{m=1}^{k} \sum_{N=kN_{\mathrm{CF}}+1}^{\infty} + \sum_{\substack{d,|d|\leqslant k,\\ d_i\leqslant k, 1\leqslant i\leqslant k}} \sum_{m=k+1}^{\infty} \sum_{N=N_{\mathrm{CF}}+1}^{\infty} + \sum_{\substack{d,|d|\leqslant k, \exists 1\leqslant i\leqslant k: d_i\geqslant k+1,\\ \text{or } d,|d|\geqslant k+1}} \sum_{m=1}^{\infty} \sum_{N=N_{\mathrm{CF}}+1}^{\infty} \right) e^{-\frac{1}{2}\eta(d,m)\sqrt{N_{\mathrm{CF}}(d,k,m)}} \tag{4.5}$$

The first sum in (4.5) decays linearly in k with constant C_2 replaced by kC_2.

The second sum of (4.5) requires some care. As before, we have

$$\sum_{|d|\leqslant k, d_i\leqslant k} \sum_{m=k+1}^{\infty} \sum_{N=N_{\mathrm{CF}}+1}^{\infty} e^{-\frac{1}{2}\eta(d,m)\sqrt{N_{\mathrm{CF}}(d,k,m)}} \leqslant \sum_{\text{all } d} \sum_{m\geqslant k+1} \frac{4m^2}{\eta(d)} e^{-\frac{1}{2}\eta(d)\sqrt{N_{\mathrm{CF}}(d)}m}$$

Note that $x^2 e^{-cx}$ is strictly decaying for $x \geqslant \frac{2}{c}$. Thus $\sum_{m\geqslant k+1} \leqslant \sum_{m\geqslant \max(k+1,2/c)}$, where $c = \frac{1}{2}\eta(d)\sqrt{N_{\mathrm{CF}}(d)}$.

We have $\int_k^{\infty} x^2 e^{-cx} dx \leqslant \int_k^{\infty} e^{-\frac{1}{2}cx} dx = \frac{2}{c} e^{-\frac{1}{2}ck}$ for $c \geqslant 2$. In our case $c = \frac{1}{2}\eta(d)\sqrt{N_{\mathrm{CF}}(d)}$ $= \frac{1}{2}\mu_G(\Delta_d)^{-1} 900 l^2 d_l \cdot \ldots \cdot d_1 \sqrt{C_2}$. Here l is the length of d, and C_2 is larger than 1. Thus c is at least 800, so large. We thus have $x^2 \leqslant e^{-\frac{1}{2}cx}$ for all $x \geqslant 1$.

Thus the last term is

$$\leqslant 4 \sum_d \frac{4}{\eta(d)^2 \sqrt{N_{\mathrm{CF}}(d)}} e^{-\frac{1}{4}\eta(d)\sqrt{N_{\mathrm{CF}}(d)}k}$$

$$\begin{aligned}
\leqslant 16 \cdot 1600 \sum_{l \geqslant 1} F_l^2 \sum_{a_l \geqslant 1} \cdots \sum_{a_1 \geqslant 1} e^{l^2 a_l \cdot \ldots \cdot a_1 k} &\leqslant 16 \cdot 1600 \sum_{l \geqslant 1} 2^l 2^l e^{-l^2 k} \\
&\leqslant 25600 \sum_{l \geqslant 1} e^{2l - l^2 k} \\
&\leqslant 25600 (e^{2-k} + e^{4-4k} + \sum_{l \geqslant 3} e^{-lk}) \\
&\leqslant 25600 (e^{2-k} + e^{4-4k} + 2e^{-3k}) \\
&\leqslant 2560000 e^{-k}
\end{aligned}$$

In the last sum of (4.5), the sum over the restricted range of words d splits up according to

$$\sum_{l \geqslant k+1} \sum_{|d|=l}$$

$$+ \sum_{1 \leqslant l \leqslant k} \left(\sum_{d_l \geqslant k+1} \sum_{d_i \geqslant 1, 1 \leqslant i \leqslant l-1} + \sum_{1 \leqslant d_l \leqslant k} \sum_{d_{l-1} \geqslant k+1} \sum_{d_i \geqslant 1, 1 \leqslant i \leqslant l-2} + \ldots + \sum_{1 \leqslant d_i \leqslant k, l \geqslant i \geqslant 2} \sum_{d_1 \geqslant k+1} \right)$$

The term that is summed over is $64/C_2 \cdot (l^2 d_l \cdot \ldots \cdot d_1)^{-2}$ by choice of N_{CF} (see (4.3)). Any sum over an unrestricted range of $d_i \geqslant 1$ gives a convergent term less than 1. The sums over the restricted range $d_i \geqslant k+1$ are bounded above by $\frac{1}{k}$. Finally, the restricted ranges $1 \leqslant d_i \leqslant k$ contribute at most $(\frac{\pi^2}{6} - 1 - \frac{1}{k+1})$ which is less than 0.7. Thus the last sum in (4.5) can be bounded above by

$$\leqslant \frac{64}{C_2} \left(\frac{1}{k} + \frac{1}{k} \sum_{1 \leqslant l \leqslant k} \frac{1}{l^2} \left(\sum_{i=0}^{l-1} 0.7^i \right) \right)$$

This expression converges and is

$$\leqslant \frac{214}{C_2 k}.$$

□

5. Set-theoretic Lemmas

In the following, let c be an interval and $M < N$, $k < l$ positive integers and Ω, Ω_N, E, E_k, r_k, ω_N and ω as before.

Proposition 5.1. *We have*

$$\lambda(E \smallsetminus E_k) \leqslant r_k \tag{5.1}$$

$$\lambda(E_l \smallsetminus E_k) \leqslant r_k \tag{5.2}$$

$$\lambda((\Omega \smallsetminus E) \cap c) \geqslant \lambda((\Omega \smallsetminus E_k) \cap c) - r_k \tag{5.3}$$

$$\lambda((\Omega_N \smallsetminus E) \cap c) \geqslant \lambda((\Omega_N \smallsetminus E_k) \cap c) - r_k \tag{5.4}$$

$$\lambda((\Omega \smallsetminus E_l) \cap c) \geqslant \lambda((\Omega \smallsetminus E_k) \cap c) - r_k \tag{5.5}$$

$$\lambda((\Omega_N \smallsetminus E_l) \cap c) \geqslant \lambda((\Omega_N \smallsetminus E_k) \cap c) - r_k \tag{5.6}$$

Proof. $\lambda(E \smallsetminus E_k) \leqslant r_k$ is immediate from the definition of E_k and r_k.

$\lambda(E_l \smallsetminus E_k) \leqslant r_k$ is also immediate since $E_l \smallsetminus E_k \subset E \smallsetminus E_k$.

We have

$$(\Omega \smallsetminus E) \cap c = ((\Omega \smallsetminus E_k) \cap c) \smallsetminus ((E \smallsetminus E_k) \cap c).$$

Hence

$$\begin{aligned}\lambda((\Omega \smallsetminus E) \cap c) &\geqslant \lambda((\Omega \smallsetminus E_k) \cap c) - \lambda(E \smallsetminus E_k \cap c)\\ &\geqslant \lambda((\Omega \smallsetminus E_k) \cap c) - \lambda(E \smallsetminus E_k)\\ &\geqslant \lambda((\Omega \smallsetminus E_k) \cap c) - r_k.\end{aligned}$$

The same argument works with Ω replaced by Ω_N and E replaced by E_k which gives the remaining inequalities. □

Lemma 5.2. *We have*

$$\lambda((\Omega \smallsetminus E_k) \cap c) \geqslant \lambda((\Omega_N \smallsetminus E_k) \cap c) - \omega_N$$
$$\lambda((\Omega_N \smallsetminus E_k) \cap c) \geqslant \lambda((\Omega_M \smallsetminus E_k) \cap c) - \omega_M$$

Proof.

$$\begin{aligned}(\Omega_N \smallsetminus E_k) \cap c &= ((\Omega \sqcup (\Omega_N \smallsetminus \Omega)) \smallsetminus E_k) \cap c\\ &= (\Omega \smallsetminus E_k \sqcup (\Omega_N \smallsetminus \Omega) \smallsetminus E_k) \cap c\\ &= (\Omega \smallsetminus E_k) \cap c \sqcup (\Omega_N \smallsetminus \Omega) \smallsetminus E_k \cap c.\end{aligned}$$

Consequently,

$$\begin{aligned}\lambda((\Omega \smallsetminus E_k) \cap c) &= \lambda((\Omega_N \smallsetminus E_k) \cap c) - \lambda((\Omega_N \smallsetminus \Omega) \smallsetminus E_k \cap c)\\ &\geqslant \lambda((\Omega_N \smallsetminus E_k) \cap c) - \lambda(\Omega_N \smallsetminus \Omega)\\ &\geqslant \lambda((\Omega_N \smallsetminus E_k) \cap c) - \omega_N.\end{aligned}$$

The second inequality follows using the same argument applied to $\Omega_M = \Omega_N \sqcup \Omega_M \setminus \Omega_N$. □

6. Algorithm

6.1. **First (binary) digit.** We choose N_1 and k_1 to be such that

$$\frac{1}{2}(1-\omega-\beta) - 2\omega_{N_1} - r_{k_1} \geqslant \frac{1}{4}(1-\omega-\beta) > 0$$

This can be achieved for example with N_1 and r_1 such that $\omega_{N_1} \leqslant \frac{1}{8}(1-\omega-\beta)$ and let r_1 be such that $r_{k_1} \leqslant \frac{1}{8}(1-\omega-\beta)$. Such values for N_1 and r_1 are computable.

We have

$$\begin{aligned} \lambda((\Omega_{N_1} \setminus E_{k_1}) \cap [0,1/2)) \ + \ \lambda((\Omega_{N_1} \setminus E_{k_1}) \cap [1/2,1)) &= \lambda(\Omega_{N_1} \setminus E_{k_1}) \\ &\geqslant \lambda(\Omega_{N_1}) - \lambda(E_{k_1}) \\ &\geqslant 1-\omega-\beta \end{aligned}$$

which is > 0 if we assume that $\omega + \beta < 1$. The last lower bound is independent of N_1 and k_1, because $\lambda(\Omega_N) \geqslant \lambda(\Omega) \geqslant 1-\omega$ for any N and $\lambda(E_k) \leqslant \lambda(E) < \beta$ for any k.

Hence there is an interval $c_1 \in \{[0,1/2),[1/2,1)\}$ such that

$$\lambda((\Omega_{N_1} \setminus E_{k_1}) \cap c_1) \geqslant \frac{1}{2}(1-\omega-\beta) > 0.$$

Since the Lebesgue measure of $(\Omega_{N_1} \setminus E_{k_1}) \cap c_1$ can be computed, the interval c_1 can be computably obtained.

We have

$$\begin{aligned} \lambda((\Omega \setminus E) \cap c_1) &\geqslant \lambda((\Omega \setminus E_{k_1}) \cap c_1) - r_{k_1} \\ &\geqslant \lambda((\Omega_{N_1} \setminus E_{k_1}) \cap c_1) - \omega_{N_1} - r_{k_1} \\ &\geqslant \frac{1}{2}(1-\omega-\beta) - \omega_{N_1} - r_{k_1}. \end{aligned}$$

Hence $\lambda((\Omega \setminus E) \cap c_1) > 0$, so there are numbers in $\Omega \cap c_1$ outside E, i.e. whose first binary digit is given by c_1.

6.2. **Second digit.** Let N_2 and k_2 be such that $\varepsilon_{N_2} \leqslant \frac{1}{32}(1-\omega-\beta)$ and $r_{k_2} \leqslant \frac{1}{32}(1-\omega-\beta)$.

We have

$$\begin{aligned}\lambda((\Omega_{N_2} \smallsetminus E_{k_2}) \cap c_2^1) + \lambda((\Omega_{N_2} \smallsetminus E_{k_2}) \cap c_2^2) &= \lambda((\Omega_{N_2} \smallsetminus E_{k_2}) \cap c_1) \\ &\geqslant \lambda((\Omega_{N_2} \smallsetminus E_{k_1}) \cap c_1) - r_{k_1} \\ &\geqslant \lambda((\Omega_{N_1} \smallsetminus E_{k_1}) \cap c_1) - \omega_{N_1} - r_{k_1} \\ &\geqslant \frac{1}{4}(1 - \omega - \beta) \\ &> 0\end{aligned}$$

by the choice of N_1 and k_1 from step 1. Hence one half c_2 of c_1 satisfies

$$\lambda((\Omega_{N_2} \smallsetminus E_{k_2}) \cap c_2) \geqslant \frac{1}{8}(1 - \omega - \beta) > 0.$$

Which half of c_1 to choose can be computed.

Finally, we have

$$\begin{aligned}\lambda((\Omega \smallsetminus E) \cap c_2) &\geqslant \lambda((\Omega \smallsetminus E_{k_2}) \cap c_2) - r_{k_2} \\ &\geqslant \lambda((\Omega_{N_2} \smallsetminus E_{k_2}) \cap c_2) - \omega_{N_2} - r_{k_2} \\ &\geqslant \frac{1}{8}(1 - \omega - \beta) - \omega_{N_2} - r_{k_2} \\ &\geqslant \frac{1}{16}(1 - \omega - \beta) \\ &> 0.\end{aligned}$$

Hence there are numbers in $\Omega \cap c_2$ outside E, i.e. whose binary expansion starts with digits given by c_1, c_2.

This algorithm produces the binary digits of a real number ν.

Theorem 6.1. *The number ν is computable. It is furthermore absolutely normal and continued fraction normal.*

Proof. All values N_i, k_i, ω_{N_i}, r_{k_i} and all appearing measures can be computed, hence ν is computable.

Suppose ν was not absolutely normal and continued fraction normal. Then ν is an element of E, i.e. ν is contained in an interval $I \in E$ of positive measure. Since ν by construction lies in all c_i, for some i it holds that $c_i \subset I$, hence $c_i \subset E$. This implies that $(\Omega \smallsetminus E) \cap c_i = \varnothing$, a contradiction since we choose c_i to be such that $\lambda((\Omega \smallsetminus E) \cap c_i) > 0$. □

Acknowledgements. The author was supported by the Austrian Science Fund (FWF): I 1751-N26; W1230, Doctoral Program "Discrete Mathematics"; and SFB F 5510-N26. He would like to thank the Erwin-Schrödinger-Institute for its hospitality.

On absolutely normal numbers and their discrepancy estimate

Verónica Becher, Adrian-Maria Scheerer, Theodore Slaman[11]

Abstract. We construct the base 2 expansion of an absolutely normal real number x so that for every integer b greater than or equal to 2 the discrepancy modulo 1 of the sequence $(b^0 x, b^1 x, b^2 x, \ldots)$ is essentially the same as that realized by almost all real numbers.

For a real number x, we write $\{x\} = x - \lfloor x \rfloor$ to denote the fractional part of x. For a sequence $(x_j)_{j \geqslant 1}$ of real numbers in the unit interval, the discrepancy of the N first elements is

$$D_N((x_j)_{j\geqslant 1}) = \sup_{0\leqslant u<v\leqslant 1} \left| \frac{\#\{j : 1 \leqslant j \leqslant N \text{ and } u \leqslant x_j < v\}}{N} - (v-u) \right|.$$

In this note we prove the following.

Theorem 0.1. *There is an algorithm that computes a real number x such that for each integer b greater than or equal to 2,*

$$\limsup_{N\to\infty} \frac{D_N(\{b^j x\}_{j\geqslant 0})\sqrt{N}}{\sqrt{\log\log N}} < 3C_b,$$

where

$$C_b = 166 + 664/(\sqrt{b}-1) \text{ is Philipp's constant.}$$

The algorithm computes the first n digits of the expansion of x in base 2 after performing triple-exponential in n mathematical operations.

It is well known that for almost all real numbers x and for all integers b greater than or equal to 2, the sequence $\{b^j x\}_{j\geqslant 0}$ is uniformly distributed in the unit interval, which means that its discrepancy tends to 0 as N goes to infinity. In [69], Gál and Gál proved that there is a constant C such that for almost all real numbers x,

$$\limsup_{N\to\infty} \frac{D_N(\{2^j x\}_{j\geqslant 0})\sqrt{N}}{\sqrt{\log\log N}} < C.$$

Philipp [106] bounded the existential constant C and extended this result for lacunary sequences. He proved that given a sequence of positive integers $(n_j)_{j\geqslant 1}$ such that $n_{j+1}/n_j \geqslant$

[11] This article appeared in [18]

θ for some real number $\theta > 1$, then for almost all real numbers x the sequence $\{n_j x\}_{j\geqslant 1}$ satisfies

$$\limsup_{N\to\infty} \frac{D_N(\{n_j x\}_{j\geqslant 1})\sqrt{N}}{\sqrt{\log\log N}} < 166 + 664/(\sqrt{\theta} - 1).$$

Finally, Fukuyama [67] explicitly determined, for any real $\theta > 1$, the constant C'_θ (see [67, Corollary]) such that for almost all real numbers x,

$$\limsup_{N\to\infty} \frac{D_N(\{\theta^j x\}_{j\geqslant 0})\sqrt{N}}{\sqrt{\log\log N}} = C'_\theta.$$

For instance, in case θ is an integer greater than or equal to 2,

$$C'_\theta = \begin{cases} \sqrt{84}/9, & \text{if } \theta = 2 \\ \sqrt{2(\theta+1)/(\theta-1)}/2, & \text{if } \theta \text{ is odd} \\ \sqrt{2(\theta+1)\theta(\theta-2)/(\theta-1)^3}/2, & \text{if } \theta \geqslant 4 \text{ is even.} \end{cases}$$

The proof of Theorem 0.1 is based on the explicit construction of a set of full Lebesgue measure given by Philipp in [106], which, in turn, follows from that in [69]. Unfortunately we do not know an explicit construction of a set with full Lebesgue measure achieving the constants proved by Fukuyama [67]. If one could give such an explicit construction one could obtain a version of Theorem 0.1 with the constant $3C_b$ replaced by C'_b.

The algorithm stated in Theorem 0.1 achieves a lower discrepancy bound than that in Levin's work [84]. Given a countable set L of positive real numbers greater than 1, Levin constructs a real number x such that for every θ in L there is a constant C''_θ such that

$$D_N(\{\theta^j x\}_{j\geqslant 0}) < C''_\theta \frac{(\log N)^3}{\sqrt{N}}.$$

The recent analysis in [113] reports no constructions with smaller discrepancy.

For $L = \{2, 3, \ldots\}$, Levin's construction produces a computable sequence of real numbers that converge to an absolutely normal number [2]. To compute the n-th term it requires double-exponential in n many operations including trigonometric operations. In contrast, the algorithm presented in Theorem 0.1 is based just on discrete mathematics and yields the expansion of the computed number by outputting one digit after the other. Unfortunately, to compute the first n digits it performs triple-exponential in n many operations. Thus, the question raised in [17] remains open :

> Is there an absolutely normal number computable in polynomial time having a nearly optimal discrepancy of normality ?

Finally we comment that it is possible to prove a version of Theorem 0.1 replacing the set of integer bases by any countable set of computable real numbers greater than 1. The proof would remain essentially the same except that one needs a suitable version of Lemma 1.2.

1. Primary definitions and results

We use some tools from [69] and [106]. For non-negative integers M and N, for a sequence of real numbers $(x_j)_{j\geqslant 1}$ and for real numbers α_1, α_2 such that $0 \leqslant \alpha_1 < \alpha_2 \leqslant 1$, we define

$$F(M, N, \alpha_1, \alpha_2, (x_j)_{j\geqslant 1}) = \big|\#\{j : M \leqslant j < M+N : \alpha_1 \leqslant x_j < \alpha_2\} - (\alpha_2 - \alpha_1)N\big|.$$

We write μ to denote Lebesgue measure.

Lemma 1.1 ([13, Lemma 8], adapted from Hardy and Wright [71, Theorem 148])**.** *Let b be an integer greater than or equal to 2. Let m and N be positive integers and let ε be a real such that $6/\lfloor N/m \rfloor \leqslant \varepsilon \leqslant 1/b^m$. Then, for any non-negative integer M and for any integer a such that $0 \leqslant a < b^m$,*

$$\mu\{x \in (0,1) : |F(M, N, ab^{-m}, (a+1)b^{-m}, \{b^j x\}_{j\geqslant 0})| > \varepsilon N\}$$

is less than $2b^{2m-2}m\ e^{-\varepsilon^2 N b^m/(6m)}$.

The next lemma is similar to Lemma 1.1 but it considers dyadic intervals instead of b-adic intervals.

Lemma 1.2. *Let b be an integer greater than or equal to 2, let k and N be positive integers and let ε be a real such that $\sqrt{6k/N} \leqslant \varepsilon \leqslant 1/2^k$. Then, for any pair of integers M and a such that $M \geqslant 0$ and $0 \leqslant a < 2^k$,*

$$\mu\left\{x \in (0,1) : F(M, N, a2^{-k}, (a+1)2^{-k}, \{b^j x\}_{j\geqslant 0}) \geqslant \varepsilon N\right\}$$

is less than $9 \cdot 2^{2(k+2)}(k+2)e^{-\varepsilon^2 N b^{k+2}/(6(k+2))}$.

Proof. For $b = 2$ let $m = k$and apply Lemma 1.1.

For $b \geqslant 3$, let $I = (a/2^k, (a+1)/2^k)$ and consider the partition of I in J, K and L as follows. Let

$$m = \lceil k/\log_2 b \rceil + 1, d = \lceil ab^{2-\{k/\log_2 b\}} \rceil, p = (a+1)b^{2-\{k/\log_2 b\}} - \lceil ab^{2-\{k/\log_2 b\}} \rceil$$

and define

$$K = (a/2^k, d/b^m], J = (d/b^m, (d+p)/b^m), L = [(d+p)/b^m, (a+1)/2^k).$$

Notice that

$$\mu K + \mu J + \mu L = \mu I = 2^{-k},$$

with

$$(b-1)/b^m \leqslant \mu J \leqslant b^2/b^m, 0 \leqslant \mu K \leqslant 1/b^m, \text{ and } 0 \leqslant \mu L \leqslant 1/b^m.$$

Thus,

$$\begin{aligned}F(M,N,a2^{-k},(a+1)2^{-k},\{b^jx\}_{j\geqslant 0}) =&|\#\{j: M+1\leqslant j\leqslant N : \{b^jx\}\in I\} - N\mu I|\\ \leqslant&|\#\{j: M+1\leqslant j\leqslant N : \{b^jx\}\in J\} - N\mu J|\\ &+|\#\{j: M+1\leqslant j\leqslant N : \{b^jx\}\in K\} - N\mu K|\\ &+|\#\{j: M+1\leqslant j\leqslant N : \{b^jx\}\in L\} - N\mu L|.\end{aligned}$$

Let $z_1, z_2, \ldots$ be the expansion of μK in base b, that is $\sum_{j\geqslant 1} z_j b^{-j} = \mu K$. Let $y_1, y_2, \ldots$ be the expansion of μL in base b, that is $\sum_{j\geqslant 1} y_j b^{-j} = \mu L$. Then, by Lemma 1.1,

$$\begin{aligned}&\mu\{x\in(0,1): F(M,N,a2^{-k},(a+1)2^{-k},\{b^jx\}_{j\geqslant 0}) > \varepsilon N\}\\ &\quad\leqslant p\ \mu\{x\in(0,1): F(M,N,db^{-m},(d+1)b^{-m},\{b^jx\}_{j\geqslant 0}) > \varepsilon N\}\\ &\qquad+\sum_{h\geqslant m+1}\mu\{x\in(0,1): F(M,N,y_hb^{-h},(y_h+1)b^{-h},\{b^jx\}_{j\geqslant 0}) > \varepsilon N\}\\ &\qquad+\sum_{h\geqslant m+1}\mu\{x\in(0,1): F(M,N,z_hb^{-h},(z_h+1)b^{-h}\{b^jx\}_{j\geqslant 0}) > \varepsilon N\}\\ &\quad\leqslant p\ \mu\{x\in(0,1): F(M,N,db^{-m},(d+1)b^{-m},\{b^jx\}_{j\geqslant 0}) > \varepsilon N\}\\ &\qquad+2\sum_{h\geqslant m+1}\max_{0\leqslant c<b^h}\mu\{x\in(0,1): F(M,N,cb^{-h},(c+1)b^{-h},\{b^jx\}_{j\geqslant 0}) > \varepsilon N\}\\ &\quad\leqslant p\ b^{2m-2}me^{-\varepsilon^2Nb^m/(6m)}\ +\ 2\sum_{h\geqslant m+1}2b^{2h-2}he^{-\varepsilon^2Nb^h/(6h)}\\ &\quad\leqslant b^2\ b^{2m-2}me^{-\varepsilon^2Nb^m/(6m)}\ +\ 4b^{2(m+1)-2}(m+1)e^{-\varepsilon^2Nb^{m+1}/(6(m+1))}\sum_{h\geqslant 0}e^{-h}\\ &\quad\leqslant b^{2m}me^{-\varepsilon^2Nb^m/(6(k+2))}+\ 8b^{2m}me^{-\varepsilon^2Nb^m/(6m)}\\ &\quad\leqslant 9\cdot 2^{2(k+2)}(k+2)e^{-\varepsilon^2Nb^{k+2}/(6(k+2))}.\end{aligned}$$

□

Remark 1.3. *In [106], Philipp proves a proposition more general than Lemma 1.2. His result yields the same order of magnitude but does not make explicit the underlying constant while Lemma 1.2 does.*

Clearly, for arbitrary reals α_1, α_2 such that $0\leqslant\alpha_1<\alpha_2\leqslant 1$, for any sequence $(x_j)_{j\geqslant 1}$ and for any non-negative integers M, N and k,

$$|F(0,N,\alpha_1,\alpha_2,(x_j)_{j\geqslant 1})| \leqslant N/2^{k-1} + \sum_{m=1}^{k}\max_{0\leqslant a<2^m}|F(0,N,a2^{-m},(a+1)2^{-m},(x_j)_{j\geqslant 1})|.$$

Lemma 1.4 ([106, Lemma 4], adapted from [69, Lemma 3.10])**.** *Let b be an integer greater than or equal to 2, let N be a positive integer and let n be such that $2^n \leqslant N < 2^{n+1}$. Then, there are integers $m_1, \ldots, m_n$ with $0 \leqslant m_\ell \leqslant 2^{n-\ell} - 1$ for $\ell = 1, \ldots, n$, such that for any positive integer h and any a, with $0 \leqslant a < 2^h$,*

$$F(0, N, a2^{-h}, (a+1)2^{-h}, \{b^j x\}_{j\geqslant 0}) \leqslant N^{1/3} + F(0, 2^n, a2^{-h}, (a+1)2^{-h}, \{b^j x\}_{j\geqslant 0}) + \sum_{\ell=n/2}^{n} F(2^n + m_\ell 2^\ell, 2^{\ell-1}, a2^{-h}, (a+1)2^{-h}, \{b^j x\}_{j\geqslant 0}).$$

Let η and δ be positive reals. For each integer b greater than or equal to 2 and for each positive integer N let

$$\begin{aligned} \tilde{C}_b &= 1/2 + 2/(\sqrt{b} - 1), \\ \varphi(N) &= 2(1 + 2\delta)\tilde{C}_b (N \log\log N)^{1/2}, \\ T(N) &= \lfloor \log N / \log 4 \rfloor + 1. \end{aligned}$$

For integers b, n, a, h, ℓ and m such that

$$b \geqslant 2,\ n \geqslant 1,\ 0 \leqslant a < 2^T,\ 1 \leqslant h \leqslant T(2^n),\ n/2 \leqslant \ell \leqslant n, \text{ and } 1 \leqslant m \leqslant 2^{n/2},$$

define the following sets

$$\begin{aligned} G(b,n,a,h) =& \{x \in (0,1) : F(0, 2^n, \alpha_1, \alpha_2, \{b^j x\}_{j\geqslant 0}) \geqslant 2^{-h/8}\varphi(2^n)\}, \\ & \text{where } \alpha_1 = a2^{-(h+1)},\ \alpha_2 = (a+1)2^{-(h+1)}, \text{ if } 1 \leqslant h < T(2^n); \\ & \text{and } \alpha_1 = a2^{-T(2^n)},\ \alpha_2 = (a+1)2^{-T(2^n)}, \text{ if } h = T(2^n). \\ H(b,n,a,h,\ell,m) =& \{x \in (0,1) : F(2^n + m2^\ell, 2^{\ell-1}, \beta_1, \beta_2, \{b^j x\}_{j\geqslant 0}) \geqslant 2^{-h/8} 2^{(\ell-n-3)/6}\varphi(2^n)\}, \\ & \text{where } \beta_1 = a2^{-(h+1)},\ \beta_2 = (a+1)2^{-(h+1)}, \text{ if } 1 \leqslant h < T(2^{\ell-1}); \\ & \text{and } \beta_1 = a2^{-T(2^{\ell-1})},\ \beta_2 = (a+1)2^{-T(2^{\ell-1})}, \text{ if } h = T(2^{\ell-1}). \\ G_{b,n} =& \bigcup_{h=1}^{T} \bigcup_{a=0}^{2^h-1} G(b,n,a,h), \\ H_{b,n} =& \bigcup_{h=1}^{T} \bigcup_{a=0}^{2^h-1} \bigcup_{\ell=n/2}^{n} \bigcup_{m=1}^{2^{n-\ell}} H(b,n,a,h,\ell,m). \end{aligned}$$

Lemma 1.5. *Let η and δ be positive real numbers. For each $n > e^{6/(\delta \log 2)}$ and for every $b \geqslant 2$,*

$$\mu(G_{b,n}) = n^{-1-4\delta}, \quad \mu(H_{b,n}) = 2n^{-1-3\delta},$$

and there is $n_0 = n_0(\eta, \delta)$ *such that*

$$\mu\left(\bigcup_{n\geqslant n_0}(G_{b,n}\cup H_{b,n})\right) < \eta$$

and such that for every real x *outside* $\bigcup_{n\geqslant n_0}(G_{b,n}\cup H_{b,n})$*,*

$$\limsup_{N\to\infty}\frac{D_N(\{b^n x\}_{n\geqslant 0})\sqrt{N}}{\sqrt{\log\log N}} < (1+4\delta)C_b,$$

where C_b *is Philipp's constant,* $C_b = 166 + 664/(\sqrt{b}-1)$*.*

Proof. To bound $\mu G_{b,n}$ we apply twice Lemma 1.2, first with $N = 2^n$, $k = (h+1)$ and $\varepsilon = 2^{-T/8}\varphi(2^n)2^{-n}$, and then with $N = 2^n$, $k = T$ and $\varepsilon = 2^{-T/8}\varphi(2^n)2^{-n}$. We write $\exp(x)$ to denote e^x. Assuming $n \geqslant 10$,

$$\begin{aligned}
\mu G_{b,n} &\leqslant \mu\left(\bigcup_{a=0}^{2^T-1} G(b,n,a,T)\right) + \sum_{h=1}^{T-1}\mu\left(\bigcup_{a=0}^{2^h-1} G(b,n,a,h)\right)\\
&\leqslant \sum_{h=1}^{T-1} 2^h 9\cdot 2^{2(h+1)}(h+3)\exp\left(-2^{-h/4}\varphi^2(2^n)2^{-n}b^{h+1}\frac{b^2}{6(h+3)}\right)\\
&\quad + 2^T 9\cdot 2^{2(T+2)}(T+2)\exp\left(-2^{-T/4}\varphi^2(2^n)2^{-n}b^{T}\frac{b^2}{6(T+2)}\right)\\
&\leqslant 9\cdot 2^{3T+5}(T+2)\exp\left(-2^{-T/4}\log\log(2^n)4(1+2\delta)^2 b^{T+2}\frac{1}{6(T+2)}\tilde{C}_b^2\right)\\
&\leqslant n^{-(1+4\delta)}.
\end{aligned}$$

To bound $\mu H_{b,n}$ we apply twice Lemma 1.2 first letting $N = 2^{\ell-1}$, $k = (h+1)$ and $\varepsilon = 2^{-h/8}\varphi(2^n)2^{-n}$, and then letting $N = 2^{\ell-1}$, $k = T$ and $\varepsilon = 2^{-T/8}\varphi(2^n)2^{-n}$. Assuming $\log\log(2^n) \geqslant 8/\delta^2$,

$$\begin{aligned}
\mu H_{b,n} = {} & \mu\left(\bigcup_{h=1}^{T}\bigcup_{a=0}^{2^h-1}\bigcup_{\ell=n/2}^{n}\bigcup_{m=1}^{2^{n-\ell}} H(b,n,a,h,\ell,m)\right)\\
\leqslant {} & \sum_{\ell=n/2}^{n} 2^{n-\ell}\sum_{h=1}^{T-1} 9\ 2^{3h+6}(h+3)\exp\left(-2^{-h/4}b^{h+3}2^{2(n-\ell)/3}\log\log(2^n)(1+\delta)^2\frac{4}{6(h+3)}\tilde{C}_b^2\right)\\
& + \sum_{\ell=n/2}^{n} 2^{n-\ell}9\ 2^{3T+4}(T+2)\exp\left(-2^{-T/4}b^{T+2}2^{2(n-\ell)/3}\log\log(2^n)(1+\delta)^2\frac{4}{6(T+2)}\tilde{C}_b^2\right)
\end{aligned}$$

$$\begin{aligned}
&\leqslant \sum_{\ell=n/2}^{n} 2^{n-\ell} \exp\left(-2^{-1/4} 2^{2(n-\ell)/3} \log\log(2^n)(1+4\delta)\frac{b^4}{24}\right) \sum_{h=1}^{T-1} 2^{-h} \\
&\quad + \sum_{\ell=n/2}^{n} 2^{n-\ell} 9\ 2^{3T+4}(T+2) \exp\left(-2^{-T/4} b^{T+2} 2^{2(n-\ell)/3} \log\log(2^n)(1+\delta)^2 \frac{1}{6(T+2)}\right) \\
&\leqslant \exp\left(-2^{-1/4} \log\log(2^n)(1+3\delta)\frac{b^4}{24}\right) \sum_{\ell=n/2}^{n} 2^{n/2-\ell-1} \\
&\quad + \exp\left(-2^{-T/4} b^{T+2} \log\log(2^n)(1+3\delta)\frac{1}{6(T+2)}\right) \sum_{\ell=n/2}^{n} 2^{n/2-\ell-1} \\
&\leqslant 2\ n^{-(1+3\delta)}.
\end{aligned}$$

Thus, there is n_0 such that for every integer b greater than or equal to 2,

$$\mu\left(\bigcup_{n\geqslant n_0} (G_{b,n} \cup H_{b,n})\right) < \sum_{n\geqslant n_0} \left(n^{-1-4\delta} + 2n^{-1-3\delta}\right) < \eta.$$

It follows from Philipp's proof of [106, Theorem 1] that for every real x outside $\bigcup_{n\geqslant n_0}(G_{b,n} \cup H_{b,n})$,

$$\limsup_{N\to\infty} \frac{D_N(\{b^j x\}_{j\geqslant 0})\sqrt{N}}{\sqrt{\log\log N}} < (1+4\delta)C_b,$$

where $C_b = 166 + 664/(\sqrt{b}-1)$. □

2. Proof of Theorem 0.1

We give an algorithm to compute a real outside the set $\bigcup_{b\geqslant 1}\bigcup_{n\geqslant n_0}(G_{b,n} \cup H_{b,n})$. The technique is similar to that used in the computable reformulation of Sierpinski's construction given in [11].

The next definition introduces finite approximations to this set. Recall that by Lemma 1.5, for every integer $b \geqslant 2$, provided $\delta \geqslant 1/2$ and $n_0 = n_0(\eta, \delta) \geqslant e^{6/(\delta^2 \log 2)}$,

$$\mu\left(\bigcup_{n\geqslant n_0} (G_{b,n} \cup H_{b,n})\right) \leqslant \sum_{n\geqslant n_0} n^{-(1+4\delta)} + 2n^{-(1+3\delta)} \leqslant \sum_{n\geqslant n_0} n^{-2} < \eta.$$

Definition 2.1. *Fix $\delta = 1/2$ and fix $\eta \leqslant 1/8$. Let*

$$\Delta = \bigcup_{b=2}^{\infty} \bigcup_{m=z_b}^{\infty} (G_{b,m} \cup H_{b,m}),$$

$$s = \sum_{b=2}^{\infty} \sum_{k=z_b}^{\infty} \frac{1}{k^2},$$

where, for each base b, z_b is the least integer greater than $e^{6/(\delta \log 2)} = e^{12/\log 2}$ such that

$$\sum_{k=z_b}^{\infty} \frac{1}{k^2} < \frac{\eta}{2^b}.$$

Observe that by the first condition on z_b, $\mu(\Delta) < s < \eta$. Furthermore define for each n,

$$\begin{aligned} b_n &= \max(2, \lfloor \log_2 n \rfloor), \\ \Delta_n &= \bigcup_{b=2}^{b_n} \bigcup_{m=z_b}^{n} (G_{b,m} \cup H_{b,m}), \\ s_n &= \sum_{b=2}^{b_n} \sum_{k=z_b}^{n} \frac{1}{k^2}, \\ r_n &= s - s_n = \sum_{b=2}^{b_n} \sum_{k=\max(n+1, z_b)}^{\infty} \frac{1}{k^2} + \sum_{b=b_n+1}^{\infty} \sum_{k=z_b}^{\infty} \frac{1}{k^2}, \\ p_n &= 2^{2n+2}. \end{aligned}$$

The following propositions follow immediately from these definitions.

Proposition 2.2. *For every n, $\mu(\Delta - \Delta_n) \leqslant r_n$.*

Proposition 2.3. *For every n and q such that $n \leqslant q$, $\mu(\Delta_q - \Delta_n) \leqslant r_n - r_q$.*

Proposition 2.4. *For any interval I and any n, $\mu(\Delta \cap I) \leqslant \mu(\Delta_n \cap I) + r_n$.*

The proof of Theorem 0.1 follows from the next lemma.

Lemma 2.5. *There is a computable sequence of nested dyadic intervals $I_0, I_1, I_2, \ldots$ such that for each n, $\mu I_n = 2^{-n}$ and $\mu(\Delta \cap I_n) < 2^{-n}$.*

Proof. Proposition 2.4 establishes, for any interval I and any m,

$$\mu(\Delta \cap I) < \mu(\Delta_m \cap I) + r_m.$$

Then, to prove the lemma it suffices to give a computable sequence of nested dyadic intervals $I_0, I_1, I_2, \ldots$ such that for each n, $\mu I_n = 2^{-n}$ and $\mu(\Delta_{p_n} \cap I_n) + r_{p_n} < 2^{-n}$. We establish

$$p_n = 2^{2n+2}.$$

This value of p_n is large enough so that the error r_{p_n} is sufficiently small to guarantee that even if all the intervals in $\Delta - \Delta_{p_n}$ fall in the half of I_n that will be chosen as I_{n+1}, I_{n+1} will not be completely covered by Δ. We define the $I_0, I_1, \ldots$ inductively.

Base case, $n = 0$. Let $I_0 = [0, 1)$. We need to check that $\mu\left(\Delta_{p_0} \cap I_0\right) + r_{p_0} < 2^0$. Since $p_0 = 2^{2\cdot 0+2} = 4$, $b_{p_0} = 2$ and $z_b = 2^2/\eta \geqslant 2^5$,

$$\Delta_{p_0} = \bigcup_{b=2}^{b_{p_0}} \bigcup_{n=z_b}^{p_0} (G_{b,n} \cup H_{b,n}) = \varnothing.$$

Since $I_0 = (0, 1)$ and $\Delta_{p_0} = \varnothing$, $\Delta_{p_0} \cap I_0 = \varnothing$. Then,

$$r_{p_0} = s = \sum_{b=2}^{\infty} \sum_{k=z_b}^{\infty} \frac{1}{k^2}.$$

We conclude $\mu\left(\Delta_{p_0} \cap I_0\right) + r_{p_0} = 0 + s < \eta < 1$.

Inductive case, $n > 0$. Assume that for each $m = 0, 1, \ldots, n-1$,

$$\mu\big(\Delta_{p_m} \cap I_m\big) + r_{p_m} < \frac{1}{2^m}\Big(\eta + \sum_{j=1}^{m} 2^{j-1} \cdot r_{p_j}\Big),$$

where $p_m = 2^{2m+2}$. Note that for $m = 0$, $\sum_{j=1}^{m}$ is the empty sum. We split the interval I_{n-1} in two halves of measure 2^{-n}, given with binary representations of their endpoints as

$$I_n^0 = [0.d_1 \ldots d_{n-1}\ ,\ 0.d_1 \ldots d_{n-1}1] \text{ and } I_n^1 = [0.d_1 \ldots d_{n-1}1\ ,\ 0.d_1 \ldots d_{n-1}111111\ldots].$$

Since $I_n^0 \cup I_n^1$ is equal to interval I_{n-1}, we have

$$\mu\left(\Delta_{p_n} \cap I_n^0\right) + \mu\left(\Delta_{p_n} \cap I_n^1\right) = \mu\left(\Delta_{p_n} \cap I_{n-1}\right).$$

Since $p_n \geqslant p_{n-1}$, we obtain

$$\mu\left(\Delta_{p_n} \cap I_n^0\right) + \mu\left(\Delta_{p_n} \cap I_n^1\right) \leqslant \mu\left(\Delta_{p_{n-1}} \cap I_{n-1}\right) + r_{p_{n-1}} - r_{p_n}.$$

Adding $r_{p_n} + r_{p_n}$ to both sides of this inequality we obtain

$$\left(\mu\left(\Delta_{p_n} \cap I_n^0\right) + r_{p_n}\right) + \left(\mu\left(\Delta_{p_n} \cap I_n^1\right) + r_{p_n}\right) \leqslant \mu\left(\Delta_{p_{n-1}} \cap I_{n-1}\right) + r_{p_{n-1}} + r_{p_n}.$$

Then, by the inductive condition for $m = n-1$,

$$\left(\mu\left(\Delta_{p_n} \cap I_n^0\right) + r_{p_n}\right) + \left(\mu\left(\Delta_{p_n} \cap I_n^1\right) + r_{p_n}\right) < \frac{1}{2^{n-1}}\Big(\eta + \sum_{j=1}^{n} 2^{j-1} \cdot r_{p_j}\Big).$$

Hence, it is impossible that the terms

$$\mu\left(\Delta_{p_n} \cap I_n^0\right) + r_{p_n} \text{ and } \mu\left(\Delta_{p_n} \cap I_n^1\right) + r_{p_n}$$

be both greater than or equal to

$$\frac{1}{2^n}\Big(\eta + \sum_{j=1}^{n} 2^{j-1} \cdot r_{p_j}\Big).$$

Let $d \in \{0,1\}$ be smallest such that

$$\mu\left(\Delta_{p_n} \cap I_n^d\right) + r_{p_n} < \frac{1}{2^n}\Big(\eta + \sum_{j=1}^{n} 2^{j-1} \cdot r_{p_j}\Big)$$

and define

$$I_n = I_n^d.$$

To verify that I_n satisfies the inductive condition it suffices to verify that

$$\eta + \sum_{j=1}^{n} 2^{j-1} \cdot r_{p_j} < 1.$$

Developing the definition of r_{p_j} we obtain

$$\begin{aligned}
\sum_{j=1}^{n} 2^{j-1} \cdot r_{p_j} &= \sum_{j=1}^{n} 2^{j-1} \left(\sum_{b=2}^{b_{p_j}} \sum_{k=\max(z_b, p_j+1)}^{\infty} \frac{1}{k^2} + \sum_{b=b_{p_j}+1}^{\infty} \sum_{k=z_b}^{\infty} \frac{1}{k^2} \right) \\
&= \left(\sum_{j=1}^{n} 2^{j-1} \sum_{b=2}^{b_{p_j}} \sum_{k=\max(z_b, p_j+1)}^{\infty} \frac{1}{k^2} \right) + \left(\sum_{j=1}^{n} 2^{j-1} \sum_{b=b_{p_j}+1}^{\infty} \sum_{k=z_b}^{\infty} \frac{1}{k^2} \right) \\
&< \left(\sum_{j=1}^{n} 2^{j-1} b_{p_j} \sum_{k=p_j+1}^{\infty} \frac{1}{k^2} \right) + \left(\sum_{j=1}^{n} 2^{j-1} \sum_{b=b_{p_j}+1}^{\infty} \frac{\eta}{2^b} \right) \\
&< \left(\sum_{j=1}^{n} 2^{j-1} \frac{b_{p_j}}{p_j+1} \right) + \left(\sum_{j=1}^{n} 2^{j-1} \frac{\eta}{2^{b_{p_j}}} \right) \\
&< \left(\sum_{j=1}^{n} 2^{j-1} \frac{2j+2}{2^{2j+2}+1} \right) + \left(\sum_{j=1}^{n} 2^{j-1} \frac{\eta}{2^{2j+2}} \right) \\
&< \frac{3}{4} + \frac{\eta}{4} \\
&< \frac{7}{8}.
\end{aligned}$$

Then, using that $\eta < 1/8$ we obtain the desired result,

$$\mu\left(\Delta_{p_n} \cap I_n\right) + r_{p_n} < \frac{1}{2^n}\Big(\eta + \sum_{j=1}^{n} 2^{j-1} \cdot r_{p_j}\Big) < \frac{1}{2^n}\Big(\eta + \frac{7}{8}\Big) < \frac{1}{2^n}.$$

□

2.1. **Algorithm.** Computation of the binary expansion $d_1 d_2 \dots$ of a number x such that for every integer base b, $\limsup_{N\to\infty} D_N(\{b^j x\}_{j\geqslant 0})(N/\log\log N)^{1/2} < 3\ C_b$, where $C_b = 166 + 664/(\sqrt{b}-1)$.

$$F(M,N,\alpha_1,\alpha_2,(x_j)_{j\geqslant 1}) = \big|\#\{j : M \leqslant j < M+N : \alpha_1 \leqslant x_j < \alpha_2\} - (\alpha_2-\alpha_1)N\big|,$$

$$\varphi(N) = \Big(2 + 8/(\sqrt{b}-1)\Big)\sqrt{N\log\log N},$$

$$T(N) = \lfloor \log N/\log 4\rfloor + 1,$$

$$G(b,n,a,h) = \{x \in (0,1) : F(0,2^n,\alpha_1,\alpha_2,\{b^j x\}_{j\geqslant 0}) \geqslant 2^{-h/8}\varphi(2^n)\},$$

where $\alpha_1 = a2^{-(h+1)},\ \alpha_2 = (a+1)2^{-(h+1)},$ if $1 \leqslant h < T(2^n)$;

and $\alpha_1 = a2^{-T(2^n)},\ \alpha_2 = (a+1)2^{-T(2^n)},$ if $h = T(2^n)$.

$$H(b,n,a,h,\ell,m) = \{x \in (0,1) : F(2^n + m2^\ell, 2^{\ell-1},\beta_1,\beta_2,\{b^j x\}_{j\geqslant 0}) \geqslant 2^{-h/8}2^{(\ell-n-3)/6}\varphi(2^n)\},$$

where $\beta_1 = a2^{-(h+1)},\ \beta_2 = (a+1)2^{-(h+1)},$ if $1 \leqslant h < T(2^{\ell-1})$;

and $\beta_1 = a2^{-T(2^{\ell-1})},\ \beta_2 = (a+1)2^{-T(2^{\ell-1})},$ if $h = T(2^{\ell-1})$.

$$G_{b,n} = \bigcup_{h=1}^{T(2^n)} \bigcup_{a=0}^{2^h-1} G(b,n,a,h),$$

$$H_{b,n} = \bigcup_{h=1}^{T(2^{\ell-1})} \bigcup_{a=0}^{2^h-1} \bigcup_{\ell=n/2}^{n} \bigcup_{m=1}^{2^{n-\ell}} H(b,n,a,h,\ell,m).$$

```
For each base $b$ fix $z_b \geqslant 12/\log 2$ such that $\sum_{k=z_b}^{\infty} 1/k^2 < 1/(8\cdot 2^b)$
$I_0 = [0,1)$
n=1
repeat
        $I_n^0$ is the left half of $I_{n-1}$ and $I_n^1$ is the right half of $I_{n-1}$
         $p_n = 2^{2n+2}$
         $b_{p_n} = 2n+2$
         $\Delta_{p_n} = \bigcup_{b=2}^{b_{p_n}} \bigcup_{k=z_b}^{p_n} (G_{b,k} \cup H_{b,k})$
         $r_{p_n} = \sum_{b=2}^{b_{p_n}} \sum_{k=\max(z_b,p_n+1)}^{\infty} k^{-2} + \sum_{b=b_{p_n}+1}^{\infty} \sum_{k=z_b}^{\infty} k^{-2}$
        if $\mu(\Delta_{p_n} \cap I_n^0) + r_{p_n} < 2^{-n}$ then
              $d_n = 0$
              $I_n = I_n^0$
        else
```

```
            $d_n = 1$
            $I_n = I_n^1$
        n=n+1
forever
```

Let's see that the number $x = 0.d_1d_2d_3$ obtained by the next Algorithm 2.1 is external to

$$\Delta = \bigcup_{b=2}^{\infty} \bigcup_{n=n_{z_b}}^{\infty} (G_{b,n} \cup H_{b,n})$$

Suppose not. Then, there must be an open interval J in Δ such that $x \in J$. Consider the intervals $I_1^{d_1}, I_2^{d_2}, I_3^{d_3}, \ldots$ By our construction, x belongs each of them. Let j be the smallest index such that $I_j^{d_j} \subset J$, which exists because the measure of $I_n^{d_n}$ goes to 0 as n increases. Then $I_j^{d_j}$ is fully covered by Δ. This contradicts that in our construction at each step n we choose an interval $I_n^{b_n}$ not fully covered by Δ, because as ensured by the proof of Lemma 2.5,

$$\mu(\Delta \cap I_n^{d_n}) < 2^{-n}.$$

We conclude that x belongs to no interval of Δ. Recall that we fixed $\delta = 1/2$; thus, by Lemma 1.5, for for each integer b greater than or equal to 2,

$$\limsup_{N\to\infty} \frac{D_N(\{b^n x\}_{n\geqslant 0})\sqrt{N}}{\sqrt{\log\log N}} < 3C_b,$$

where C_b is Philipp's constant.

Finally, we count the number of mathematical operations that the algorithm performs at step n to compute the digit d_n in the binary expansion of x. To determine d_n, the algorithm tests for $d_n \in \{0, 1\}$ whether

$$\mu(\Delta_{p_n} \cap I_n^{d_n}) + r_{p_n} < 2^n.$$

The naive way to obtain this is by constructing the set $\Delta_{p_n} = \bigcup_{b=2}^{b_{p_n}} \bigcup_{k=z_b}^{p_n} G_{b,k} \cup H_{b,k}$, for $b = 2, 3, \ldots, b_{p_n}$. The more demanding is $G_{b_{p_n}, p_n}$ which requires the examination of all the strings of digits in $\{0, \ldots, b_{p_n} - 1\}$ of length 2^{p_n}. Since $b_{p_n} = 2n + 2$ and $p_n = 2^{2n+2}$, the number of strings to be examined is

$$\sum_{b=2}^{b_{p_n}} b^{2^{p_n}} < 2b_{p_n}^{2^{p_n}} = (2n+2)^{2^{2^{(2n+2)}}}.$$

Thus, with this naive way, the algorithm at step n performs in the order of

$$(2n+2)^{2^{2^{2n+2}}}$$

many mathematical operations.

An incremental construction of the sets $G_{b,n}$ and $H_{b,n}$ can lower the number of needed mathematical operations, but would not help to lower the triple-exponential order of computational complexity.

Acknowledgements. We thank Robert Tichy for early discussions on this work. Becher is supported by the University of Buenos Aires and CONICET. Becher is a member of the Laboratoire International Associé INFINIS, CONICET/Universidad de Buenos Aires-CNRS/Université Paris Diderot. Scheerer is supported by the Austrian Science Fund (FWF): I 1751-N26; W1230, Doctoral Program "Discrete Mathematics"; and SFB F 5510-N26. Slaman is partially supported by the National Science Foundation grant DMS-1600441. The present paper was completed while Becher visited the Erwin Schrödinger International Institute for Mathematics and Physics, Austria.

References

[1] R. Adler, M. Keane, and M. Smorodinsky, *A construction of a normal number for the continued fraction transformation*, Journal of Number Theory **13** (1981), no. 1, 95 - 105, DOI http://dx.doi.org/10.1016/0022-314X(81)90031-7.

[2] N. Alvarez and V. Becher, *M. Levin's construction of absolutely normal numbers with very low discrepancy*, arXiv:1510.02004.

[3] E. Artin, *Ein mechanisches system mit quasiergodischen bahnen*, Abh. Math. Sem. Univ. Hamburg **3** (1924), no. 1, 170–175, DOI 10.1007/BF02954622 (German). MR3069425

[4] M. Bauer and M. A. Bennett, *Applications of the hypergeometric method to the generalized Ramanujan-Nagell equation*, Ramanujan J. **6** (2002), no. 2, 209–270, DOI 10.1023/A:1015779301077. MR1908198

[5] D. H. Bailey and J. Borwein, *Pi Day is upon us again and we still do not know if pi is normal*, Amer. Math. Monthly **121** (2014), no. 3, 191–206, DOI 10.4169/amer.math.monthly.121.03.191.

[6] D. H. Bailey and R. E. Crandall, *On the random character of fundamental constant expansions*, Experiment. Math. **10** (2001), no. 2, 175–190. MR1837669

[7] V. Becher, *Turing's normal numbers: towards randomness*, How the world computes, Lecture Notes in Comput. Sci. vol. 7318, Springer, Heidelberg, 2012, pp. 35–45, DOI 10.1007/978-3-642-30870-35. MR2983667

[8] V. Becher, Y. Bugeaud, and T. A. Slaman, *On simply normal numbers to different bases*, Math. Ann. **364** (2016), no. 1-2, 125–150, DOI 10.1007/s00208-015-1209-9. MR3451383

[9] V. Becher, O. Carton, and P. A. Heiber, *Normality and automata*, J. Comput. System Sci. **81** (2015), no. 8, 1592–1613, DOI 10.1016/j.jcss.2015.04.007. MR3389924

[10] V. Becher, S. Daicz, and G. Chaitin, *A highly random number*, Combinatorics, computability and logic (Constanţa, 2001), Springer Ser. Discrete Math. Theor. Comput. Sci. Springer, London, 2001, pp. 55–68. MR1934821

[11] V. Becher and S. Figueira, *An example of a computable absolutely normal number*, Theoretical Computer Science **270** (2002), 126–138.

[12] V. Becher, S. Figueira, S. Grigorieff, and J. S. Miller, *Randomness and halting probabilities*, J. Symbolic Logic **71** (2006), no. 4, 1411–1430, DOI 10.2178/jsl/1164060463. MR2275867

[13] V. Becher, S. Figueira, and R. Picchi, *Turing's unpublished algorithm for normal numbers*, Theoret. Comput. Sci. **377** (2007), no. 1-3, 126–138, DOI 10.1016/j.tcs.2007.02.022.

[14] V. Becher and S. Grigorieff, *Random reals and possibly infinite computations. I. Randomness in $\varnothing'$*, J. Symbolic Logic **70** (2005), no. 3, 891–913, DOI 10.2178/jsl/1122038919. MR2155271

[15] V. Becher and P. A. Heiber, *Normal numbers and finite automata*, Theoret. Comput. Sci. **477** (2013), 109–116, DOI 10.1016/j.tcs.2013.01.019. MR3027887

[16] V. Becher, P. A. Heiber, and T. A. Slaman, *Normal numbers and the Borel hierarchy*, Fund. Math. **226** (2014), no. 1, 63–78, DOI 10.4064/fm226-1-4. MR3208295

[17] V. Becher, P. A. Heiber, and T. A. Slaman, *A polynomial-time algorithm for computing absolutely normal numbers*, Inform. and Comput. **232** (2013), 1–9. MR3132518

[18] V. Becher, A.-M. Scheerer, and T. A. Slaman, *On absolutely normal numbers and their discrepancy estimate*, available at `arxiv.org/abs/1702.04072`.

[19] V. Becher and T. A. Slaman, *On the normality of numbers to different bases*, J. Lond. Math. Soc. (2) **90** (2014), no. 2, 472–494, DOI 10.1112/jlms/jdu035. MR3263961

[20] M. A. Bennett, *Perfect powers with few ternary digits*, Integers **12** (2012), no. 6, 1159–1166, DOI 10.1515/integers-2012-0033. MR3011554

[21] M. A. Bennett and Y. Bugeaud, *Perfect powers with three digits*, Mathematika **60** (2014), no. 1, 66–84, DOI 10.1112/S0025579313000107. MR3164519

[22] M. A. Bennett, Y. Bugeaud, and M. Mignotte, *Perfect powers with few binary digits and related Diophantine problems, II*, Math. Proc. Cambridge Philos. Soc. **153** (2012), no. 3, 525–540, DOI 10.1017/S0305004112000345. MR2990629

[23] ———, *Perfect powers with few binary digits and related Diophantine problems*, Ann. Sc. Norm. Super. Pisa Cl. Sci. (5) **12** (2013), no. 4, 941–953. MR3184574

[24] M. A. Bennett and A. Ghadermarzi, *Mordell's equation: a classical approach*, LMS J. Comput. Math. **18** (2015), no. 1, 633–646, DOI 10.1112/S1461157015000182. MR3406453

[25] M. Bennett and A.-M. Scheerer, *Squares with three non-zero digits*, to appear in Number Theory - Diophantine problems, uniform distribution and applications, Festschrift in honour of Robert F. Tichy's 60th birthday (C. Elsholtz, P. Grabner, Eds.), Springer-Verlag, Berlin (2016), available at `arxiv.org/abs/1610.09830`.

[26] Y. Benoist and J.-F. Quint, *Mesures stationnaires et fermés invariants des espaces homogènes*, Ann. of Math. (2) **174** (2011), no. 2, 1111–1162, DOI 10.4007/annals.2011.174.2.8 (French, with English and French summaries). MR2831114

[27] A. Bertrand-Mathis and B. Volkmann, *On (ε, k)-normal words in connecting dynamical systems*, Monatsh. Math. **107** (1989), no. 4, 267–279, DOI 10.1007/BF01517354.

[28] A. Bertrand-Mathis, *Points génériques de Champernowne sur certains systèmes codes; application aux θ-shifts*, Ergodic Theory Dynam. Systems **8** (1988), no. 1, 35–51, DOI 10.1017/S0143385700004302 (French, with English summary). MR939059

[29] A. S. Besicovitch, *The asymptotic distribution of the numerals in the decimal representation of the squares of the natural numbers*, Math. Z. **39** (1935), no. 1, 146–156, DOI 10.1007/BF01201350. MR1545494

[30] F. Beukers, *On the generalized Ramanujan-Nagell equation. I*, Acta Arith. **38** (1980/81), no. 4, 389–410. MR621008

[31] ———, *On the generalized Ramanujan-Nagell equation. II*, Acta Arith. **39** (1981), no. 2, 113–123. MR639621

[32] P. Billingsley, *Ergodic theory and information* (1965), xiii+195.

[33] H. F. Blichfeldt, *Notes on Geometry of Numbers*, Bull. Amer. Math. Soc. **27** (1921), no. 4, 150–153.

[34] É. Borel, *Les probabilités dénombrables et leurs applications arithmétiques*, Rendiconti del Circolo Matematico di Palermo **27** (1909), no. 1, 247-271, DOI 10.1007/BF03019651 (French).

[35] C. Bourke, J. M. Hitchcock, and N. V. Vinodchandran, *Entropy rates and finite-state dimension*, Theoret. Comput. Sci. **349** (2005), no. 3, 392–406, DOI 10.1016/j.tcs.2005.09.040. MR2183164

[36] D. W. Boyd, *On the beta expansion for Salem numbers of degree* 6, Math. Comp. **65** (1996), no. 214, 861–875, $S29$–$S31$, DOI 10.1090/S0025-5718-96-00700-4.

[37] L. Breiman, *The strong law of large numbers for a class of Markov chains*, Ann. Math. Statist. **31** (1960), 801–803, DOI 10.1214/aoms/1177705810. MR0117786

[38] C. Bright, *Solving Ramanujan's Square Equation Computationally* (2007), 1–4. `https://cs.uwaterloo.ca/~cbright/nsra/ramanujans-square-equation.pdf`.

[39] G. Brown, W. Moran, and C. E. M. Pearce, *A decomposition theorem for numbers in which the summands have prescribed normality properties*, J. Number Theory **24** (1986), no. 3, 259–271, DOI 10.1016/0022-314X(86)90034-X. MR866972

[40] ———, *Riesz products and normal numbers*, J. London Math. Soc. (2) **32** (1985), no. 1, 12–18, DOI 10.1112/jlms/s2-32.1.12. MR813380

[41] ———, *Riesz products, Hausdorff dimension and normal numbers*, Math. Proc. Cambridge Philos. Soc. **101** (1987), no. 3, 529–540, DOI 10.1017/S0305004100066895. MR878900

[42] Y. Bugeaud, *Distribution modulo one and Diophantine approximation*, Cambridge Tracts in Mathematics, vol. 193, Cambridge University Press, Cambridge, 2012. MR2953186

[43] Cristian S. Calude and Peter H. Hertling and Bakhadyr Khoussainov and Yongge Wang, *Recursively enumerable reals and Chaitin Ω numbers*, Theoretical Computer Science **255** (2001), no. 1–2, 125 - 149.

[44] J. W. S. Cassels, *On a problem of Steinhaus about normal numbers*, Colloq. Math. **7** (1959), 95–101. MR0113863

[45] G. J. Chaitin, *Algorithmic information theory*, Cambridge Tracts in Theoretical Computer Science, vol. 1, Cambridge University Press, Cambridge, 1987. With a foreword by J. T. Schwartz. MR917482

[46] ———, *A theory of program size formally identical to information theory*, J. Assoc. Comput. Mach. **22** (1975), 329–340. MR0411829

[47] D. G. Champernowne, *The Construction of Decimals Normal in the Scale of Ten*, J. London Math. Soc. **S1-8**, no. 4, 254, DOI 10.1112/jlms/s1-8.4.254.

[48] A. H. Copeland and P. Erdös, *Note on normal numbers*, Bull. Amer. Math. Soc. **52** (1946), 857–860. MR0017743

[49] P. Corvaja and U. Zannier, *On the Diophantine equation $f(a^m, y) = b^n$*, Acta Arith. **94** (2000), no. 1, 25–40. MR1762454

[50] ———, *Finiteness of odd perfect powers with four nonzero binary digits*, Ann. Inst. Fourier (Grenoble) **63** (2013), no. 2, 715–731 (English, with English and French summaries). MR3112846

[51] J. J. Dai, J. I. Lathrop, J. H. Lutz, and E. Mayordomo, *Finite-state dimension*, Theoret. Comput. Sci. **310** (2004), no. 1-3, 1–33, DOI 10.1016/S0304-3975(03)00244-5. MR2019613

[52] K. Dajani and C. Kraaikamp, *Ergodic theory of numbers* **29** (2002), x+190.

[53] H. Davenport and P. Erdös, *Note on normal decimals*, Canadian J. Math. **4** (1952), 58–63.

[54] H. Davenport, P. Erdős, and W. J. LeVeque, *On Weyl's criterion for uniform distribution*, Michigan Math. J. **10** (1963), 311–314. MR0153656

[55] H. Delange, *Sur la fonction sommatoire de la fonction"somme des chiffres"*, Enseignement Math. (2) **21** (1975), no. 1, 31–47 (French). MR0379414

[56] M. Denker, C. Grillenberger, and K. Sigmund, *Ergodic theory on compact spaces* (1976), iv+360.

[57] R. Downey, *Randomness, computation and mathematics*, How the world computes, Lecture Notes in Comput. Sci. vol. 7318, Springer, Heidelberg, 2012, pp. 162–181, DOI 10.1007/978-3-642-30870-317. MR2983679

[58] R. G. Downey and D. R. Hirschfeldt, *Algorithmic randomness and complexity*, Theory and Applications of Computability, Springer, New York, 2010. MR2732288

[59] M. Drmota and R. F. Tichy, *Sequences, discrepancies and applications*, Lecture Notes in Mathematics, vol. 1651, Springer-Verlag, Berlin, 1997. MR1470456

[60] J. Dufresnoy and Ch. Pisot, *Etude de certaines fonctions méromorphes bornées sur le cercle unité. Application à un ensemble fermé d'entiers algébriques*, Ann. Sci. Ecole Norm. Sup. (3) **72** (1955), 69–92. MR0072902 (17,349d)

[61] M. Einsiedler, L. Fishman, and U. Shapira, *Diophantine approximations on fractals*, Geom. Funct. Anal. **21** (2011), no. 1, 14–35, DOI 10.1007/s00039-011-0111-1. MR2773102

[62] M. Einsiedler and T. Ward, *Ergodic theory with a view towards number theory*, Graduate Texts in Mathematics, vol. 259, Springer-Verlag London, Ltd., London, 2011. MR2723325

[63] Martin Epszteyn, *Cómputo eficiente de números absolutamente normales.* https://www-2.dc.uba.ar/profesores/becher/tl/epszteyn.pdf.

[64] S. Figueira and A. Nies, *Feasible analysis, randomness, and base invariance*, Theory Comput. Syst. **56** (2015), no. 3, 439–464, DOI 10.1007/s00224-013-9507-7. MR3334255

[65] C. Frougny and B. Solomyak, *Finite beta-expansions*, Ergodic Theory Dynam. Systems **12** (1992), no. 4, 713–723, DOI 10.1017/S0143385700007057.

[66] C. Frougny and W. Steiner, *Minimal weight expansions in Pisot bases*, J. Math. Cryptol. **2** (2008), no. 4, 365–392, DOI 10.1515/JMC.2008.017.

[67] K. Fukuyama, *Metric discrepancy results for alternating geometric progressions*, Monatsh. Math. **171** (2013), no. 1, 33–63, DOI 10.1007/s00605-012-0419-4.

[68] H. Furstenberg, *Ergodic fractal measures and dimension conservation*, Ergodic Theory Dynam. Systems **28** (2008), no. 2, 405–422, DOI 10.1017/S0143385708000084. MR2408385

[69] S. Gaal and L. Gál, *The discrepancy of the sequence* $\{(2^n x)\}$, Nederl. Akad. Wetensch. Proc. Ser. A 67 = Indag. Math. **26** (1964), 129–143. MR0163089

[70] P. J. Grabner and H. Prodinger, *Additive irreducibles in α-expansions*, Publ. Math. Debrecen **80** (2012), no. 3-4, 405–415, DOI 10.5486/PMD.2012.5086.

[71] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, 6th ed. Oxford University Press, Oxford, 2008. Revised by D. R. Heath-Brown and J. H. Silverman; With a foreword by Andrew Wiles. MR2445243

[72] K. G. Hare, S. Laishram, and T. Stoll, *Stolarsky's conjecture and the sum of digits of polynomial values*, Proc. Amer. Math. Soc. **139** (2011), no. 1, 39–49, DOI 10.1090/S0002-9939-2010-10591-9. MR2729069

[73] ———, *The sum of digits of n and n^2*, Int. J. Number Theory **7** (2011), no. 7, 1737–1752, DOI 10.1142/S1793042111004319. MR2854212

[74] D. Hensley, *The Hausdorff dimensions of some continued fraction Cantor sets*, J. Number Theory **33** (1989), no. 2, 182–198, DOI 10.1016/0022-314X(89)90005-X. MR1034198

[75] F. Hofbauer, *β-shifts have unique maximal measure*, Monatsh. Math. **85** (1978), no. 3, 189–198.

[76] M. Hochman and P. Shmerkin, *Equidistribution from fractal measures*, Invent. Math. **202** (2015), no. 1, 427–479, DOI 10.1007/s00222-014-0573-5. MR3402802

[77] B. Host, *Nombres normaux, entropie, translations*, Israel J. Math. **91** (1995), no. 1-3, 419–428, DOI 10.1007/BF02761660 (French, with English summary). MR1348326

[78] S. Ito and I. Shiokawa, *A construction of β-normal sequences*, J. Math. Soc. Japan **27** (1975), 20–23. MR0357361

[79] T. Jordan and T. Sahlsten, *Fourier transforms of Gibbs measures for the Gauss map*, Math. Ann. **364** (2016), no. 3-4, 983–1023, DOI 10.1007/s00208-015-1241-9. MR3466857

[80] R. Kaufman, *Continued fractions and Fourier transforms*, Mathematika **27** (1980), no. 2, 262–267 (1981), DOI 10.1112/S0025579300010147. MR610711

[81] H. Ki and T. Linton, *Normal numbers and subsets of* $\mathbf{N}$ *with given densities*, Fund. Math. **144** (1994), no. 2, 163–179. MR1273694

[82] L. Kuipers and H. Niederreiter, *Uniform distribution of sequences*, Wiley-Interscience [John Wiley & Sons], New York-London-Sydney, 1974. Pure and Applied Mathematics. MR0419394

[83] H. Lebesgue, *Sur certaines démonstrations d'existence*, Bull. Soc. Math. France **45** (1917), 132–144 (French). MR1504765

[84] M. B. Levin, *Absolutely normal numbers*, Vestnik Moskov. Univ. Ser. I Mat. Mekh. **1** (1979), 31–37, 87.

[85] ______, *On the discrepancy estimate of normal numbers*, Acta Arith. **88** (1999), no. 2, 99–111.

[86] B. Li and J. Wu, *Beta-expansion and continued fraction expansion*, J. Math. Anal. Appl. **339** (2008), no. 2, 1322–1331. MR2377089 (2008m:11148)

[87] F. Luca, *The Diophantine equation* $x^2 = p^a \pm p^b + 1$, Acta Arith. **112** (2004), no. 1, 87–101, DOI 10.4064/aa112-1-6. MR2040594

[88] Jack Lutz and Elvira Mayordomo, *Computing Absolutely Normal Numbers in Nearly Linear Time.* https://arxiv.org/abs/1611.05911.

[89] M. G. Madritsch, *Construction of normal numbers via pseudo-polynomial prime sequences*, Acta Arith. **166** (2014), no. 1, 81–100.

[90] M. G. Madritsch and B. Mance, *Construction of* μ*-normal sequences*, Monatshefte für Mathematik **179** (2016), no. 2, 259–280, DOI 10.1007/s00605-015-0837-1.

[91] M. Madritsch, A.-M. Scheerer, and R. Tichy, *Computable absolutely Pisot normal numbers*, submitted (2016), available at `arxiv.org/abs/1610.06388`.

[92] M. G. Madritsch, J. M. Thuswaldner, and R. F. Tichy, *Normality of numbers generated by the values of entire functions*, J. Number Theory **128** (2008), no. 5, 1127–1145, DOI 10.1016/j.jnt.2007.04.005.

[93] M. G. Madritsch and R. F. Tichy, *Construction of normal numbers via generalized prime power sequences*, J. Integer Seq. **16** (2013), no. 2, Article 13.2.12, 17.

[94] P. Martin-Löf, *The definition of random sequences*, Information and Control **9** (1966), 602–619. MR0223179

[95] C. Mauduit and J. Rivat, *La somme des chiffres des carrés*, Acta Math. **203** (2009), no. 1, 107–148, DOI 10.1007/s11511-009-0040-0 (French). MR2545827

[96] ______, *Sur un problème de Gelfond: la somme des chiffres des nombres premiers*, Ann. of Math. (2) **171** (2010), no. 3, 1591–1646, DOI 10.4007/annals.2010.171.1591 (French, with English and French summaries). MR2680394

[97] Elvira Mayordomo, *Construction of an absolutely normal real number in polynomial time.*

[98] Y. Nakai and I. Shiokawa, *A class of normal numbers*, Japan. J. Math. (N.S.) **16** (1990), no. 1, 17–29.

[99] ______, *Discrepancy estimates for a class of normal numbers*, Acta Arith. **62** (1992), no. 3, 271–284.

[100] ______, *Normality of numbers generated by the values of polynomials at primes*, Acta Arith. **81** (1997), no. 4, 345–356.

[101] J. S. B. Nielsen and J. G. Simonsen, *An experimental investigation of the normality of irrational algebraic numbers*, Math. Comp. **82** (2013), no. 283, 1837–1858, DOI 10.1090/S0025-5718-2013-02675-0. MR3042587

[102] A. Nies, *Computability and randomness*, Oxford Logic Guides, vol. 51, Oxford University Press, Oxford, 2009. MR2548883

[103] W. Parry, *On the β-expansions of real numbers*, Acta Math. Acad. Sci. Hungar. **11** (1960), 401–416.

[104] C. E. M. Pearce and M. S. Keane, *On normal numbers*, J. Austral. Math. Soc. Ser. A **32** (1982), no. 1, 79–87. MR643432

[105] A. Pethö and B. M. M. de Weger, *Products of prime powers in binary recurrence sequences. I. The hyperbolic case, with an application to the generalized Ramanujan-Nagell equation*, Math. Comp. **47** (1986), no. 176, 713–727, DOI 10.2307/2008185. MR856715

[106] W. Philipp, *Limit theorems for lacunary series and uniform distribution* mod 1, Acta Arith. **26** (1974/75), no. 3, 241–251.

[107] S. S. Pillai, *On normal numbers*, Proceedings of the Indian Academy of Sciences - Section A **12** (1940), no. 2, 179, DOI 10.1007/BF03173913.

[108] A. D. Pollington, *The Hausdorff dimension of a set of normal numbers*, Pacific J. Math. **95** (1981), no. 1, 193–204. MR631669

[109] A. G. Postnikov and I. I. Pyateckiĭ, *A Markov-sequence of symbols and a normal continued fraction*, Izv. Akad. Nauk SSSR. Ser. Mat. **21** (1957), 729–746 (Russian). MR0101857

[110] M. Queffélec, *Old and new results on normality*, Dynamics & Stochastics, 225–236, IMS Lecture Notes–Monograph Series, vol. 48, 2006.

[111] M. Queffélec and O. Ramaré, *Analyse de Fourier des fractions continues à quotients restreints*, Enseign. Math. (2) **49** (2003), no. 3-4, 335–356 (French, with English summary). MR2028020

[112] A. Rényi, *Representations for real numbers and their ergodic properties*, Acta Math. Acad. Sci. Hungar **8** (1957), 477–493.

[113] A.-M. Scheerer, *Computable absolutely normal numbers and discrepancies*, to appear in Mathematics of Computation (2015), available at `arxiv.org/abs/1511.03582`.

[114] ———, *On the continued fraction expansion of normal numbers* (2016), available at `arxiv.org/abs/1701.07979`.

[115] ———, *Normality in Pisot numeration systems*, to appear in Ergodic Theory and Dynamical Systems (2015), available at `arxiv.org/abs/1503.08047`.

[116] J. Schiffer, *Discrepancy of normal numbers*, Acta Arith. **47** (1986), no. 2, 175–186.

[117] W. M. Schmidt, *Über die Normalität von Zahlen zu verschiedenen Basen*, Acta Arith. **7** (1961/1962), 299–309 (German). MR0140482

[118] ———, *On normal numbers*, Pacific J. Math. **10** (1960), 661–672. MR0117212

[119] ———, *Irregularities of distribution. VII*, Acta Arith. **21** (1972), 45–50.

[120] C.-P. Schnorr and H. Stimm, *Endliche Automaten und Zufallsfolgen*, Acta Informat. **1** (1971/72), no. 4, 345–359. MR0437236

[121] C. Series, *The modular surface and continued fractions*, J. London Math. Soc. (2) **31** (1985), no. 1, 69–80, DOI 10.1112/jlms/s2-31.1.69. MR810563

[122] A. Siegel, *Toward a usable theory of Chernoff Bounds for heterogeneous and partially dependent random variables* (1992).

[123] W. Sierpinski, *Démonstration élémentaire du théorème de M. Borel sur les nombres absolument normaux et détermination effective d'un tel nombre*, Bulletin de la Société Mathématique de France **45** (1917), 127–132.

[124] David Simmons and Barak Weiss, *Random walks on homogeneous spaces and diophantine approximation on fractals*. arXiv:1611.05899.

[125] K. B. Stolarsky, *The binary digits of a power*, Proc. Amer. Math. Soc. **71** (1978), no. 1, 1–5, DOI 10.2307/2042203. MR495823

[126] M. Strauss, *Normal numbers and sources for BPP*, Theoret. Comput. Sci. **178** (1997), no. 1-2, 155–169, DOI 10.1016/S0304-3975(96)00099-0. MR1453848

[127] L. Szalay, *The equations* $2^n \pm 2^m \pm 2^l = z^2$, Indag. Math. (N.S.) **13** (2002), no. 1, 131–142, DOI 10.1016/S0019-3577(02)90011-X. MR2014980

[128] A. Turing, *A Note on Normal Numbers*, Collected Works of A. M. Turing, Pure Mathematics, edited by J. L. Britton, 1992, pp. 117–119.

[129] J. Vandehey, *New normality constructions for continued fraction expansions*, Journal of Number Theory **166** (2016), 424 - 451, DOI http://dx.doi.org/10.1016/j.jnt.2016.01.030.

[130] D. D. Wall, *Normal Numbers* (1950). Thesis (Ph.D.)–University of California, Berkeley.

[131] B. M. M. de Weger, *Algorithms for Diophantine equations*, CWI Tract, vol. 65, Stichting Mathematisch Centrum, Centrum voor Wiskunde en Informatica, Amsterdam, 1989. MR1026936

(A.-M. Scheerer) Institute of Analysis and Number Theory, Graz University of Technology, A-8010 Graz, Austria

E-mail address: scheerer@math.tugraz.at