MATHEMATICS OF COMPUTATION
Volume 00, Number 0, Pages 000–000
S 0025-5718(XX)0000-0

AN EXPERIMENTAL INVESTIGATION OF THE NORMALITY OF IRRATIONAL ALGEBRAIC NUMBERS

JOHAN SEJR BRINCH NIELSEN AND JAKOB GRUE SIMONSEN

Abstract. We investigate the distribution of digits of large prefixes of the expansion of irrational algebraic numbers to different bases.

We compute $2 \cdot 3^{18}$ bits of the binary expansions (corresponding to $2.33 \cdot 10^8$ decimals) of the 39 least Pisot-Vijayaraghavan numbers, the 47 least known Salem numbers, the least 20 square roots of positive integers that are not perfect squares, and 15 randomly generated algebraic irrationals. We employ these to compute the generalized serial statistics (roughly, the variant of the χ^2-statistic apt for distribution of sequences of characters) of the distributions of digit blocks for each number to bases 2,3,5,7 and 10, as well as the maximum relative frequency deviation from perfect equidistribution. We use the two statistics to perform tests at significance level $\alpha = 0.05$, respectively maximum deviation threshold $\alpha = 0.05$.

Our results suggest that if Borel's conjecture—that all irrational algebraic numbers are normal—is true, then it may have an empirical base: The distribution of digits in algebraic numbers appears close to equidistribution for large prefixes of their expansion. Of the 121 algebraic numbers studied, all numbers passed the maximum relative frequency deviation test in all considered bases for digit block sizes 1,2,3, and 4; furthermore, 92 numbers passed all tests up to block size 4 in all bases considered.

1. Borel's conjecture and normal numbers

Let $b \geq 2$ be a positive integer and let α be a real number in the interval $(0, 1)$. Then α is said to be *normal* to base b if the sequence of fractional parts of the numbers $b^n \cdot \alpha$ is uniformly distributed modulo 1. An equivalent, and perhaps more intuitive, definition of normality is: Write the expansion of $\alpha \mod 1$ to base b as $\alpha_1\alpha_2\cdots$; then α is normal to base b if each of the b^m possible blocks of m digits from the set $\{0, \ldots, b-1\}$ occurs in $\alpha_1\alpha_2\cdots$ with limiting frequency b^{-m}. Put colloquially, a number is normal to base b if, for each m and each possible block $x \in \{0, \ldots, b-1\}^m$, the probability of obtaining x when picking a place at random in the expansion of α is exactly b^{-m}.

The perennial example of a class of normal numbers is the family of Champernowne constants [23], obtained by concatenating the b-ary expansion of integers $1, 2, 3, 4, \ldots$ together. The Champernowne constant for base $b = 2$ is thus:

$$0.1101110010111011110001001 1010\cdots$$

2010 *Mathematics Subject Classification.* 11-04, 11Y60, 65-04 65-05.

This paper is accompanied by the document "An Experimental Investigation of the Normality of Irrational Algebraic Numbers: Results and Tables"containing results for a large number of algebraic numbers and bases; the document can be retrieved as part of the publically available file `http://www.diku.dk/~simonsen/submissions/polysource.zip`.

So far, all numbers known to be normal to some base have been explicitly constructed to be so [34], see for example [43, 40, 24, 25, 46, 8, 10, 41, 11, 42] for constructions of such numbers.

A celebrated conjecture by Borel [19, 20] states that *any irrational algebraic number is normal to every base*. Despite recent advances [5, 6, 9, 2, 36, 3, 4], a proof of the conjecture currently seems out of reach.

If Borel's conjecture is proved, it could conceivably be devoid of practical significance: Even if the distribution of the set of digits in successively larger prefixes of the expansions of a number converges towards equidistribution, the convergence could be so slow that for all prefixes that can realistically be computed, the distribution is skewed and far from equidistribution (experimental investigations on the digit distribution of π suggest that if π is normal, then the prefixes of its expansion to certain bases *do* converge rapidly [7, 45]).

A number of experimental investigations of the distributions of digits for prefixes of the expansions of square roots have previously been performed [31, 32, 15, 14, 35, 39]. In addition, for specific algebraic numbers, very large prefixes have been computed, and for specific *transcendental* numbers such as e and π, large prefixes of their expansions have been subjected to statistical analysis [44, 47, 26, 7, 45].

The purpose of the present paper is to perform an empirical investigation of the distribution of sequences of digits of certain classes of algebraic numbers. We treat two well-known classes of algebraic numbers: The Pisot-Vijayaraghavan Numbers and the Salem Numbers. Furthermore, we consider algebraic numbers occurring as the largest real roots of a certain class of polynomials with coefficients chosen at random, and finally we consider the first 20 square roots of positive integers that are not perfect squares.

2. Preliminaries on equidistribution and algebraic numbers

Throughout this paper, s is a finite sequence of symbols from $\{0, \ldots, b-1\}$ where b is an integer with $b \geq 2$. The length of s is denoted $|s|$; we use the capital letter N to denote $|s|$ for short.

Given s, we shall investigate the distribution of *blocks* of length n where $n = 1, 2, 3, \ldots$. For example, if $b = 10$, and $s = 52667193$, then $N = 8$, and s has the eight 1-blocks $5, 2, 6, 6, 7, 1, 9, 3$, the seven 2-blocks $52, 26, 66, 67, 71, 19, 93$, and so on.

We index the positions of s in the usual fashion $1, 2, \ldots, N$ and write the symbol at index i as s_i. Thus, the symbol, s_1, at index 1 in s above is "5".

Definition 2.1. If s has length N, $1 \leq m \leq N$, and $1 \leq i \leq N - m$, we define the *block of length m at index i* to be $s_i \cdots s_{i+m}$.

If x is a block in s, we denote by N_x the number of times x occurs in s.

Observe that there are $N - m + 1$ blocks of length m in s.

2.1. Equidistribution.

We briefly recapitulate basic facts concerning equidistribution and normality.

Definition 2.2. We say that an element s of $\{0, \ldots, b-1\}^N$ is (m, ϵ)-equidistributed if for each element $x \in \{0, \ldots, b-1\}^m$, $|N_x/N - b^{-m}| < \epsilon$. An infinite sequence $s \in \{0, \ldots, b-1\}^{\mathbb{N}}$ is said to be ∞-equidistributed [37] if, for each m and ϵ, there is a natural number $N_{m,\epsilon}$ such that for all $N > N_{m,\epsilon}$, the prefix of s of length N is (m, ϵ)-equidistributed. A number is *b-normal* if its b-ary expansion is equidistributed; a number is *normal* if it is b-normal for all integers $b \geq 2$.

Let the real number with b-ary expansion s be s_r; it is easy to see that a sequence $s \in \{0, \ldots, b-1\}^{\mathbb{N}}$ is ∞-equidistributed iff the sequence of real numbers $(b^n s_r)$ is

equidistributed modulo 1 in the sense of Weyl [38], that is, if for all $0 \leq a < b \leq 1$, we have

$$\lim_{n\to\infty} \frac{|\{bs_r \bmod 1, b^2 s_r \bmod 1, \ldots, b^n s_r \bmod 1\} \cap [a,b]|}{n} = \frac{1}{b-a}$$

Clearly, if $s \in \{0,\ldots,b-1\}^{\mathbb{N}}$ is ∞-equidistributed, we may prefix any finite sequence of elements from $\{0,\ldots,b-1\}$ to s and obtain another ∞-equidistributed sequence; the only thing that has changed is that, for each m, the constant $N_{m,\epsilon}$ at which $|N_x/N - b^{-k}| < \epsilon$ may have changed.

Our point of interest in this paper is how *small* $N_{m,\epsilon}$ is for concrete algebraic numbers as a function of b, m and ϵ. Observe that experimental results are formally meaningless in this regard: It is unknown whether the algebraic numbers we consider are b-normal to any base, and even if $N_{m,\epsilon}$ is "small" for the prefixes of the expansions we consider, larger prefixes might conceivably require larger values of $N_{m,\epsilon}$ (indeed, would likely have to, if the numbers are not normal). However, the empirical results for small values of k *do* look striking, see Section 5.

Throughout this paper, we shall consider an ϵ of $0.05 \cdot b^{-k}$. That is, we tolerate a deviation of 5 percent from the "probability" required by an equidistribution. Our choice of the exact value of 0.05 carries no significance, beyond being a small number.

2.2. **Classes of algebraic numbers.** We briefly describe the classes of polynomials considered in this paper.

Definition 2.3. A *Pisot-Vijayaraghavan number* (also called a *Pisot number*) is a real number > 1 that is a root of an irreducible monic polynomial such that all conjugate roots have magnitude < 1.

A *Salem number* is a real number > 1 that is a root of an irreducible monic polynomial such that all conjugate roots have magnitude ≤ 1 and at least one conjugate root has magnitude exactly 1.

The standard reference on both Pisot-Vijayaraghavan and Salem numbers is [12]; various fundamental properties of the two classes of numbers are proved in [22, 27]. Investigations into different subclasses of the Salem numbers can be found in [21, 13], and a survey of some recent appearances of Salem numbers in geometry and arithmetic can be found in [30].

The least Pisot number is the socalled *Plastic constant*—the unique real root of the polynomial $x^3 - x - 1$, approximately 1.32472. A better known example is the Golden number—the largest-magnitude root of the polynomial $x^2 - x - 1$, approximately 1.61803.

The least known Salem number is *Lehmer's constant*—the largest real root of Lehmer's polynomial $x^{10} + x^9 - x^7 - x^6 - x^5 - x^4 - x^3 + x + 1$, approximately 1.17628. Unlike Pisot numbers—where the least number in the class is known—it is not even known whether the class of Salem numbers is bounded properly away from 1 [30].

To compare the distribution of digits in Pisot and Salem numbers with other algebraic numbers, we define the following class of polynomials:

Definition 2.4. A *simply positive polynomial* is a polynomial on the form

$$x^n + c_{n-1}x^{n-1} + c_{n-2}x^{n-2} + \cdots + c_1 x - 1$$

where $c_1, \ldots, c_{n-1}$ are positive integers.

Note that a simply positive polynomial $P(x)$ is monic.

Proposition 2.5. *Let $P(x)$ be a simply positive polynomial of degree ≥ 2. Then $P(x)$ has at least one irrational root in the open interval $(0,1)$, any Pisot or Salem number can be a root of $P(x)$, nor can any of their conjugate elements.*

Proof. Observe that any positive real root of $P(x)$ must occur in the region $|x| \leq 1/c_1 \leq 1$. As $P(0) = -1$ and $P(1) \geq 0$, $P(x)$ must have at least one positive real root by the Intermediate Value Theorem. As any rational number p/q has minimal polynomial $qx - p$, and as the minimal polynomial will divide any polynomial in which p/q is a root, the only possible *rational* roots of $P(x)$ are 1 and -1; if $P(x)$ has degree at least 2, we have $P(1) > 0$, leaving -1 as the only possible rational root.

Hence, simply positive polynomials of degree ≥ 2 have at least one irrational root in the interval $(0,1)$.

By the above observations, the largest positive real root for a simply positive polynomial $P(x)$ of degree ≥ 2 must also be in the interval $(0,1)$. Hence, the minimal polynomial of a Pisot or Salem number cannot divide $P(x)$, as $P(x)$ would then have a real root strictly greater than 1. Thus, neither Pisot numbers, nor Salem numbers, nor any conjugate elements of Pisot or Salem numbers can be roots of simply positive polynomials of degree ≥ 2. □

Proposition 2.6. *Let $P(x)$ be a simply positive polynomial of degree ≥ 2. Then the irrational root of $P(x)$ in the interval $(0,1)$ is not the square root of any integer.*

Proof. If an irrational square root were a root of $P(x)$, then a polynomial of the form $x^2 - q$ would divide $P(x)$ with $q > 1$ an integer. But then $P(x) = x^n + \cdots - 1 = (x^2 - q)Q(x)$ for some polynomial $Q(x)$. Write $Q(x) = q_m x^m + \cdots + q_0$. Then $q_0 q = -1$. But then $q, q_0 \in \{-1, 1\}$, a contradiction. □

By Propositions 2.5 and 2.6, the class of simply positive polynomials is distinct from the classes Pisot and Salem numbers, and from the class of square roots.

The final class considered in this paper is the set of positive irrational square roots of positive integers, that is, the positive real roots of $x^2 = l$ where $l \neq r^2$ for any natural number r. These are well-known and we do not describe them further.

2.3. **Circularized sequences.** To make our notation simpler, we take inspiration from Good and Gover [31] and make use of "circularized" versions of sequences of digits.

Definition 2.7. Let $b \geq 2$ and let s be a finite sequence of symbols from the alphabet $\{0, \ldots, b-1\}$. The *circularized* version of s is the "sequence" obtained by concatenating the end of s to its beginning.

If s has length N and $1 \leq m \leq N$, and $1 \leq i \leq N$, we define the *block of length m at index i* to be $s_i \cdots s_{i+m}$ when $i + m \leq N$, and otherwise:

$$s_i \cdots s_{N-1} s_N s_1 \cdots s_{m-(N-i+1)}$$

(that is, the block wraps around the end of s). Recall that N_x denotes the number of times x occurs in s.

Thus, in the example above, the block of length 4 at index 7 in the circularized version of s is 9352. Note that, for any $m \geq 1$, there are exactly N blocks of length m in s.

Remark 2.8. Let s' be the circularized version of s, and let N_x and N'_x be the number of times that block x (of length $m \leq N$) occurs in s and s', respectively. Then $N_x \leq N'_x \leq N_x + m - 1$, and the frequencies with which x occurs in s and s' are $N_x/(N - m + 1)$ and N'_x/N, respectively. The difference between these two frequencies satisfies:

$$\left|\frac{N'_x}{N} - \frac{N_x}{N-m+1}\right| = \left|\frac{N(N'_x - N_x) - (m-1)N'_x}{N(N-m+1)}\right|$$
$$\leq \frac{|N'_x - N_x|}{N-m+1} + \frac{(m-1)N'_x}{N(N-m+1)}$$
$$\leq \frac{2(m-1)}{N-m+1}$$

Thus, for fixed block size m, the difference in frequency is negligible for large values of N.

If the blocks of s are "close" to being equidistributed, we expect, for large N, the frequency of every $x \in \{0, \ldots, b-1\}^m$ to be approximately b^{-m}.

Unless explicitly stated, we shall perform all analyses on sequences that have been circularized.

3. Statistical tests

We compute two statistics for every block size of every number: Maximum relative block frequency deviation, and the generalized serial statistic. The maximum relative frequency deviation is the maximal deviation of the frequency of occurrence of a given m-block of digits from the value b^{-m} predicted by equidistribution. The generalized serial statistic is a variation of the χ^2-statistic for multinomial distributions.

We will use each statistic to test whether the deviation differs from pure equidistribution; hence non-parametric tests are needed. Of the many such tests, each associated with a distance metric on an appropriate set of distributions, we considered the Anderson-Darling, Kolmogorov-Smirnov, and Siegel-Tukey tests, finding all of them prohibitely resource-consuming to compute for the very large data sets we have (each block in s corresponds to a datum, resulting in data sets approximately the same size as the number of digits that we compute; see Section 4 below).

Hence, we employ only the two statistics mentioned in the previous section; each of these can be computed fairly efficiently.

Maximum relative block frequency deviation.

Definition 3.1. The *absolute deviation* of $x \in \{0, \ldots, b-1\}^m$ is $|N'_x/N - b^{-m}|$. The *relative deviation* of x is $|(N'_x/N - b^{-m})/b^{-m}| = |b^m N'_x/N - 1|$.

Definition 3.2. Let y_m be the element of $\{0, \ldots, b-1\}^m$ with maximal relative deviation from the expected frequency:

$$y_m = \mathrm{maxarg}_x \left|\frac{b^m N'_x}{N} - 1\right|$$

We then define the *maximum relative block frequency deviation*, denoted $\Delta_{s,m,b}$ by:

$$\Delta_{s,m,b} = \left|\frac{b^m N_{y_m}}{N} - 1\right|$$

Proposition 3.3. *For $b \geq 2$, $m \geq 2$ and any s:*

$$\Delta_{s,m-1,b} \leq \Delta_{s,m,b}$$

Proof. Straightforward calculations. □

The maximum relative deviation for $1 \leq k < m$ is thus bounded by the maximum relative deviation for m. Consequently, in the presentation of the statistical results below, we only report the relative deviations for the maximum block sizes we have considered.

Generalized serial test. The *generalized serial statistic* is often used for sequences of characters [31], and is defined as:

$$\psi^2_{s,m,b} = \frac{b^m}{N} \sum_{x \in \{0,\ldots,b-1\}^m} (N_x - Nb^{-m})^2$$

where the sequence s is circularized.

On account of the similarity of the above formula to the χ^2-statistics, it is tempting to assume that $\psi^2_{s,m,b}$ has an asymptotically tabular χ^2-distribution. This is, however, not the case [31]. To circumvent this problem, and to interpret the generalized serial test, one can make a small change by passing to the following statistics [16, 31]:

$$\nabla^2\psi^2_{s,m,b} = \psi^2_{m,b} - 2\psi^2_{m-1,b} + \psi^2_{s,m-2,b} \quad (n = 1, 2, 3, \ldots)$$

where $\psi^2_0 = \psi^2_{-1} = 0$. The statistics $\nabla^2\psi^2_{s,m,b}$ all have asymptotic tabular χ^2-distributions with degrees of freedom $\mathrm{df}\left(\nabla^2\psi^2_{s,m,b}\right)$ given by

$$\mathrm{df}\left(\nabla^2\psi^2_{s,m,b}\right) = b^m - 2b^{m-1} + b^{m-2}$$

for $m \geq 2$, and $\mathrm{df}\left(\nabla^2\psi^2_{s,1,b}\right) = b - 1$.

Hence, one may interpret the $\nabla^2\psi^2_{s,m,b}$-statistics exactly as one would the χ^2-statistic.

Non-parametric tests using the statistics. As we do not compare the hypothesis of equidistribution to an a priori set of alternative candidate distributions, we cannot use simple distance measures to find the best fitting candidate distribution. Instead, we (admittedly arbitrarily) fix a "rejection level" of 0.05 for both of the statistics we use (for the generalized serial test, this corresponds exactly to a significance level of $\alpha = 0.05$), explained in the below text.

Definition 3.4. $s \in \{0, \ldots, b-1\}^*$ is said to *pass* the maximum relative deviation test for base b and block size m if $\Delta_{s,m,b} < 0.05$.

That is, s passes the test if the circularized version of s is $(m, 0.05)$-equidistributed.

Definition 3.5. $s \in \{0, \ldots, b-1\}^*$ is said to *pass* the generalized serial test for base b and block size m if it passes an upper one-sided goodness-of-fit test at significance level $\alpha = 0.05$ using $\nabla^2\psi^2_{s,m,b}$.

Thus, s passes the test if the value of $\nabla^2\psi^2_{s,m,b}$ is *above* the threshold value at which the cumulative probability density of the corresponding $\chi^2_{s,m,b}$ distribution is 0.95

The reader accustomed to χ^2-tests for significance should note that for goodness-of-fit, larger values of α are more stringent than lower values (we reject the null hypothesis more often with $\alpha = 0.05$ than with $\alpha = .01$).

3.1. **Least prefix size.** For each of the statistics, it is to be expected that the digit distribution in the "short" prefixes of the b-ary expansion of a number will have larger deviation from the values expected from an equidistribution than "long" prefixes. The following definition is an attempt to quantify this effect.

Definition 3.6. Let $s, t \in \{0, \ldots, b-1\}^*$; write $t \preceq s$ if t is a prefix of s.

Let $P \subseteq \{0, \ldots, b-1\}^*$ be a predicate on the set of finite sequences. We say that $s \in \{0, \ldots, b-1\}^*$ has *least prefix size k for P* if k is the least natural number with $k \leq |s|$ such that every prefix of s of size $\geq k$ satisfies P; in that case, we write $\mathrm{lps}_P(s) = k$.

If no k satisfying the above exists, we write $\mathrm{lps}_P(s) = \infty$.

Thus, $\mathrm{lps}_P(s)$ is the least prefix size such that all *larger* prefixes of s satisfy P. Also observe that it is possible for many prefixes of s to satisfy P even though $\mathrm{lps}_P(s) = \infty$.

We consider two predicates P corresponding to the two statistics we consider, namely the predicates that are true iff the (i) relative block frequency deviation is at most 0.05, respectively iff (ii) the $\nabla\psi^2$-goodness-of-fit test holds at $\alpha = 0.05$. These correspond to the following least prefix sizes:

- $\mathrm{lps}_\Delta(s)$: The least prefix size where the maximal relative frequency deviation is at most 0.05.
- $\mathrm{lps}_{\nabla^2\psi^2}(s)$: The least prefix size where the upper one-sided $\nabla\psi^2$-goodness-of-fit statistic holds at significance level $\alpha = 0.05$.

4. Computing prefixes of expansions of algebraic numbers: Practical considerations

Unlike root-finding methods from traditional numerical analysis (see e.g. [28]), we need algorithms for arbitrary precision arithmetic. We implemented three classic root-finding methods: Newton's Method, Laguerre's Method, the Power Method, and a variation of the Laguerre's method due to Gupta and Mittal [33]. The efficiency of the methods were compared to each other and to the root-finder MPSolve [18], itself able to compute digits of integer polynomials substantially faster than the current standard crop of arbitrary-precision root finders, in particular Mathematica's `NSolve`, Maple's `fsolve`, and PARI's rootpol [17]. We did not compare the speed of the methods to alternatives known to have performance superior to MPSolve in special cases such as high-degree or dense polynomials (for example Eigensolve [29]), as most polynomials we consider have low degree.

The output of all implemented methods were compared to MPSolve for correctness; performance comparison was performed by tabulating total CPU time for computing the binary expansion of the largest-magnitude root of the polynomial, for prefixes of sizes 2^{15} through 2^{26} bits with prefix size doubled in each increment. On the polynomials tested in this paper, it was found that an optimized version of Laguerre's method clearly outperformed the rest in terms of total CPU time used, and was hence subsequently used to compute all roots to high precision.

The computation of each root was performed by using MPSolve to compute 2^{12} stable bits of the root and subsequently seeding an implementation of Laguerre's method with the first 2^{11} bits as a start guess to compute the remaining bits. The last 2^{11} bits of the MPSolve solution was used for verification of the output from Laguerre's method. A slight optimization compared to the classic version of Laguerre's method (see for example [1]) was employed: The precision of the floating point number containing the root was extended by a factor of 3 in each iteration of the algorithm, hence extending the precision in line with the expected rate of convergence. The implementation was performed exclusively in the programming language Python using the GNU Multiple Precision Arithmetic Library (GMPlib).

For rapid computation of the roots, we elected to compute root sizes indexable by the software packages used (at most $2^{31} - 1$ bits per root).

All source code has been made available under the GNU public license at `http://www.diku.dk/~simonsen/submissions/polysource.zip`, or can be obtained by contacting either author.

Hardware and timing. The experiments were performed on two machines for computation and a separate database server. The machines used were a 2.66 GHZ Intel Core2 Quad Q9450 with 8 GB memory (four cores) and a 3.0 GHZ Intel Core2 Duo E8400 with 2 GB memory (two cores); all machines ran on the Linux operating system (Ubuntu Server 9.04).

The typical computation of expanding the representation of a root to $2 \cdot 3^{18}$ stable bits was completed in just below 20 minutes per root, thus allowing for computation of approximately 18 roots/hour on a total of 6 cores.

Attempts to compute the expansion to a higher precision ($> 2 \cdot 3^{18}$) yielded overflow errors due to the GMPlib Python wrapper's hardcoded 32-bit integer representation of bit-sizes. Note that this limitation occurs solely in the Python wrapper GMPy—GMPlib specifies the corresponding type as an 64-bit unsigned long, hence using a different wrapper would very likely overcome this problem.

Figure 1 shows the time used to compute 2^x bits of the expansion of several Pisot and Salem numbers. The graphs strongly suggest that computation of n bits takes $O(n)$ time for $n > 2^{20}$.

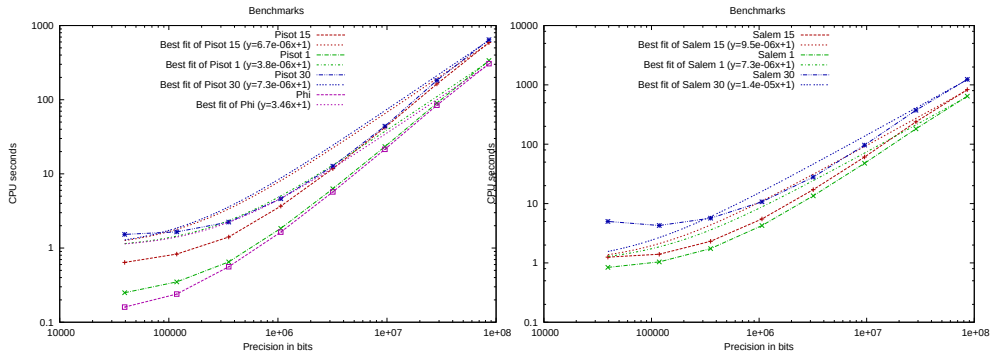

FIGURE 1. Benchmarks for Pisot numbers (left) and Salem numbers (right). Note the asymptotically affine relationship between precision and time used to compute the roots to the desired precision. Scientific e notation is used for exponentiation ($xey = x \cdot 10^y$).

Practical limitations. Due to resource constraints, computation to one precise digit of the least prefix size $\mathrm{lps}_P(s)$ for the two statistics is not realistically possible for all $|s|$ prefixes. Instead, we introduce a "scaling number" D that defines a smaller number of prefixes to use in the computation of $\mathrm{lps}_P(s)$, and thereby its precision: We only compute $\mathrm{lps}_P(s)$ for the prefixes of digits with largest index $(i+1) \cdot \lfloor |s|/D \rfloor$ for $0 \leq i \leq D$. Thus, $|s|$ is divided into D "chunks", each of size $\lfloor |s|/D \rfloor$, and we thus only consider $D < |s|$ distinct prefixes instead of $|s|$. For illustration, Table 1 lists examples of prefixes in base 2 and base 10.

TABLE 1. Example of prefixes with $D = 4$.

Prefix Nr.	Base 2	Base 10
1	01010011	32
2	0101001100100000	3247
3	010100110010000010110111	324717
4	01010011001000001011011101001110	32471795

Prefixes of a 32 bit long root with 4 divisions. In base 10, each of the roots has 9 decimals, however only $9 - (9 \mod D) = 8$ decimals are used.

We found $D = 2^{20} = 1,048,576$ to be the highest number of divisions feasible with the hardware at hand. With this D, the deviation of the $\mathrm{lps}_P(s)$ given in the

tables from its true value is at most $\lfloor |s|/D \rfloor = \lfloor (2 \cdot 3^{18})/2^{20} \rfloor = 738$ bits, or less than $\lfloor \lfloor (2 \cdot 3^{18}) \cdot \log_{10}(2) \rfloor / 2^{20} \rfloor = 222$ decimals.

5. Experimental results

For each of the statistical tests, we use a fixed report format. An arrow $\uparrow$ indicates that a value exceeds the maximum of its expected range. Space restrictions prevent us from showing the results for all numbers individually in the main paper; all tables may be found in the online supplementary document "An Experimental Investigation of the Normality of Irrational Algebraic Numbers: Results and Tables".

For illustration, consider Table 2 for the Plastic constant in base 10 (scientific e notation is used for exponentials, $xey = x \cdot 10^y$):

Table 2. Statistics for Pisot 1: $x^3 - x - 1$

Base	10				
Block size n	1	2	3	4	5
df	9	81	810	8100	81000
$\nabla^2\chi^2_{s,n,b}$	$6.022e0$	$8.295e1$	$8.594e2$	$8.149e3$	$8.117e4$
$\mathrm{lps}_{\nabla^2\chi^2}(s)$	$8.017e4$	$2.622e6$	$1.068e8$	$9.110e3$	$2.077e8$
$\Delta_{s,n,b}$	$1.000e0$	$0.999e0$	$0.993e0$	$0.975e0$	$\uparrow 1.098e0 \uparrow$
$\mathrm{lps}_{\Delta_{s,n,b}}(s)$	$3.097e4$	$2.861e5$	$6.064e6$	$6.549e7$	∞

Note in the above table that lps() is much *smaller* than the number of decimals in the largest prefix computed; that is, the prefixes stabilize *very quickly* to be within the 0.05 tolerance of the statistics considered. Furthermore, observe that block size 5 exceeds the 0.05 tolerance for the relative frequency deviation: There is a block of 5 decimals (e.g. 98144) that occurs either strictly more often than $1.05 \cdot 10^{-5} \cdot |s|$ times, or strictly less than $0.95 \cdot 10^{-5} \cdot |s|$ times.

To ascertain whether the sequences of digits stabilize quicker for low- or high-degree polynomials, we plotted $\mathrm{lps}_\Delta(s)$ against the degrees of the polynomials for each class of numbers (taking averages in case several polynomials were of identical degree). Using plain eyeballing, no clear tendencies were observed, and very high variations in $\mathrm{lps}_\Delta(s)$ were observed for polynomials of identical degree; we did not perform statistical tests to find possible correlations between the degrees and $\mathrm{lps}(s)$. For illustration, the plots for Pisot numbers to bases 7 and 10 and block size 1 are shown in Figure 2.

5.1. Summary of results.

Table 3 shows the number of polynomials failing at least one statistical test (bases are vertical, block sizes horizontal).

The following summarizes the results for the maximum relative frequency deviation test:

Table 3. Number of polynomials failing at least one test. Total number of tested polynomials: 121.

Base / block size	1	2	3	4	5
2	2	3	4	7	6
3	8	7	3	8	8
5	8	8	3	10	4
7	13	2	8	12	6
10	7	7	5	7	121

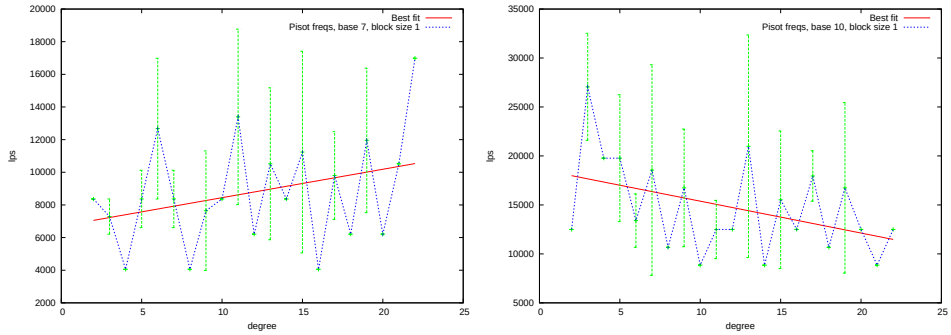

FIGURE 2. Average $\mathrm{lps}_\Delta(s)$ vs. degree for block length 1 of digit sequences of Pisot numbers. Also shown: Standard deviation and least-mean-squares linear fit. Note the high standard deviation and apparent lack of correlation between $\mathrm{lps}_\Delta(s)$ and degree.

- All tested numbers *pass* the relative frequency deviation test in bases 2,3,5 and 7 for block sizes 1 through 5.
- All tested numbers *pass* the relative frequency deviation test in base 10 for block sizes 1 through 4.
- All tested numbers *fail* the relative frequency deviation test in base 10 for block size 5.

The failures in Table 3 for small block sizes are thus due almost exclusively to the generalized serial test. The specific numbers failing the generalized serial test in each base are listed in Table 5 in Appendix A.

Table 4 below shows the numbers that pass all tests for block sizes 1 through 4 in all of the bases 2,3,5,7 and 10.

TABLE 4. Numbers passing all tests for block sizes 1 through 4 in bases 2,3,5,7, and 10.

Pisot 2, Pisot 3, Pisot 4, Pisot 5, Pisot 6, Pisot 8, Pisot 9, Pisot 10, Pisot 11, Pisot 12, Pisot 13, Pisot 14, Pisot 15, Pisot 16, Pisot 17, Pisot 18, Pisot 19, Pisot 20, Pisot 21, Pisot 25, Pisot 28, Pisot 29, Pisot 30, Pisot 31, Pisot 32, Pisot 34, Pisot 36, Pisot 37, Pisot 38, SSP 1, SSP 3, SSP 4, SSP 5, SSP 6, SSP 9, SSP 11, SSP 14, Salem 1, Salem 2, Salem 3, Salem 4, Salem 5, Salem 6, Salem 7, Salem 8, Salem 9, Salem 10, Salem 11, Salem 12, Salem 13, Salem 14, Salem 15, Salem 17, Salem 18, Salem 19, Salem 20, Salem 21, Salem 22, Salem 23, Salem 24, Salem 25, Salem 26, Salem 27, Salem 28, Salem 29, Salem 30, Salem 33, Salem 34, Salem 35, Salem 36, Salem 38, Salem 41, Salem 42, Salem 43, Salem 44, Salem 45, Salem 46, Salem 47, $\sqrt{2}$, $\sqrt{3}$, $\sqrt{5}$, $\sqrt{7}$, $\sqrt{8}$, $\sqrt{11}$, $\sqrt{13}$, $\sqrt{15}$, $\sqrt{17}$, $\sqrt{19}$, $\sqrt{20}$, $\sqrt{21}$, $\sqrt{23}$, $\sqrt{24}$

In summary, the results seem to lend experimental credence to Borel's conjecture: 92 numbers pass all tests up to block size 4 in all considered bases, and all numbers pass the maximum relative frequency deviation test up to this block size.

6. Suggestions for future work

While we have used the fairly pedestrian block frequency deviation as well as the generalized serial test, it is conceivable that using different metrics for the distance between the experimental distribution and equidistribution could yield a (slightly) different picture for the prefix sizes considered in this paper, but we do not expect so.

Certain algebraic numbers, perspicuously the Golden Number, have been computed to much greater precision than in this paper (see `http://numberworld.org` for current records; at the time of writing, both the Golden Number and $\sqrt{2}$ have been computed to a precision of 10^{15} decimals). We believe the precision of our root-finding to be close to what is realistically possible on current off-the-shelf sequential hardware, if experiments are to be conducted on larger sets of numbers over a time frame of weeks. One would expect the precision to increase by several orders of magnitude on current parallel hardware or on a grid, but it is not a priori clear how difficult this would be with current algorithms or software packages. It is possible that current software packages such as GMP *may* scale to higher precision, and *may* be straightforwardly parallelizable, but we have not been able to ascertain this. Note that the root-finding algorithms employed in this paper need to perform arbitrary-precision divisions that we currently do not know how to split and delegate across processors, though it is likely that it can be done.

As possible future work, we suggest that efforts be made not only to find a proof of Borel's conjecture, but find a constructive such proof, preferably in the sense of computable analysis [48] where a computable modulus of convergence of the distribution of digits to equidistribution can be found. Such a proof would enable immediate computation of the amount of digits needed to obtain a digit distribution within any desired, small deviation from pure equidistribution.

Acknowledgements

The authors wish to thank Nils Andersen and the anonymous referees for comments that have improved the presentation of this paper.

References

[1] F. Acton. *Numerical Methods that Work*. Mathematical Association of America, 1990.

[2] B. Adamczewski and Y. Bugeaud. Sur la complexité des nombres algébriques. *Comptes Rendus Mathématique. Académie des Sciences. Paris*, 339(1):11–14, 2004.

[3] B. Adamczewski and Y. Bugeaud. On the complexity of algebraic numbers i: Expansions in integer bases. *Annals of Mathematics*, 165(2):547–565, 2007.

[4] B. Adamczewski and B. Rampersad. On patterns occurring in binary algebraic numbers. *Proceedings of the American Mathematical Society*, 136:3105–3109, 2008.

[5] J.-P. Allouche and L. Zamboni. Algebraic irrational binary numbers cannot be fixed points of non-trivial constant length or primitive morphisms. *Journal of Number Theory*, 69(1):119 – 124, 1998.

[6] D. Bailey, J. Borwein, R. Crandall, and C. Pomerance. On the binary expansions of algebraic numbers. *Journal de théorie des nombres de Bordeaux*, 16(3):487–518, 2004.

[7] D. Bailey and R. Crandall. On the random character of fundamental constant expansions. *Experimental Mathematics*, 10(2):175–190, 2001.

[8] D. Bailey and R. Crandall. Random generators and normal numbers. *Experimental Mathematics*, 11:527–546, 2002.

[9] D. Bailey and M. Misiurewicz. A strong hot spot theorem. *Proceedings of the American Mathematical Society*, 134:2495–2501, 2006.

[10] V. Becher and S. Figueira. An example of a computable absolutely normal number. *Theoretical Computer Science*, 270(1-2):947 – 958, 2002.

[11] V. Becher, S. Figueira, and R. Picchi. Turing's unpublished algorithm for normal numbers. *Theoretical Computer Science*, 377(1-3):126–138, 2007.

[12] M. Bertin, A. Decomps-Builloux, M. Grandet-Hugot, and J. Pathiaux-Delefosse. *Pisot and Salem Numbers*. Birkhäuser, 1992.

[13] M. J. Bertin and D. W. Boyd. A characterization of two related classes of Salem numbers. *Journal of Number Theory*, 50(2):309 – 317, 1995.

[14] W. A. Beyer, N. Metropolis, and J. R. Neergaard. The generalized serial test applied to expansions of some irrational square roots in various bases. *Mathematics of Computation*, 24(111):745–747, 1970.

[15] W. A. Beyer, N. Metropolis, and J. R. Neergaard. Statistical study of digits of some square roots of integers in various bases. *Mathematics of Computation*, 24(110):455–473, 1970.

[16] P. Billingsley. Asymptotic distributions of two goodness of fit criteria. *Annals of Mathematical Statistics*, 27:1123–1129, 1995.

[17] D. Bini and G. Fiorentino. MPSolve benchmarks. http://www.dm.unipi.it/cluster-pages/mpsolve/bench.htm. Retrieved 2009-11-11, 5.55PM GMT.

[18] D. Bini and G. Fiorentino. Design, analysis and implementation of a multiprecision polynomial rootfinder. *Numerical Algorithms*, 23:127–173, 2000.

[19] E. Borel. Les probabilités dénombrables et leurs applications arithmétiques. *Rendiconti del Circolo Matematico di Palermo*, 27:247–271, 1909.

[20] É. Borel. Sur les chiffres décimaux de $\sqrt{2}$ et divers problèmes de probabilités en chaîne. *Comptes Rendus Mathématique. Académie des Sciences. Paris*, 230:591–593, 1950.

[21] D. Boyd. Small Salem numbers. *Duke Mathematical Journal*, 44(2):315–328, 1977.

[22] D. Boyd. Pisot and Salem numbers in intervals of the real line. *Mathematics of Computation*, 32(144):1244–1260, 1978.

[23] D. G. Champernowne. The Construction of Decimals Normal in the Scale of Ten. *J. London Math. Soc.*, s1-8(4):254–260, 1933.

[24] A. Copeland and P. Erdös. Note on normal numbers. *Bulletin of the American Mathematical Society*, 52:857–860, 1946.

[25] H. Davenport and P. Erdös. Note on normal decimals. *Canadian Journal of Mathematics*, 4:58–63, 1952.

[26] Y. Dodge. A natural random number generator. *International Statistical Review / Revue Internationale de Statistique*, 64(3):329–344, 1996.

[27] A. Dubickas. Sumsets of Pisot and Salem numbers. *Expositiones Mathematicae*, 26(1):85 – 91, 2008.

[28] B. Flannery. *Numerical Recipes*. Cambridge University Press, 3rd edition, 2007.

[29] S. Fortune. An iterated eigenvalue algorithm for approximating roots of univariate polynomials. *Journal of Symbolic Computation*, 33(5):627–646, 2002.

[30] E. Ghate and E. Hironaka. The arithmetic and geometry of Salem numbers. *Bulletin of the American Mathematical Society*, 38(3):293–314, 2001.

[31] I. J. Good and T. N. Gover. The generalized serial test and the binary expansion of $\sqrt{2}$. *Journal of the Royal Statistical Society. Series A (General)*, 130(1):102–107, 1967.

[32] I. J. Good and T. N. Gover. Corrigendum: The generalized serial test and the binary expansion of $\sqrt{2}$. *Journal of the Royal Statistical Society. Series A (General)*, 131(3):434, 1968.
[33] A. Gupta and A. Mittal. Symbolic computation of the roots of any polynomial with integer coefficients. Unpublished; available at http://arxiv.org/abs/math.GM/0001144, 2000.
[34] G. Harman. One hundred years of normal numbers. In M. Bennett, editor, *Surveys in Number Theory: Papers from the Milennial Conference on Number Theory*, pages 59–74. A.K. Peters, Ltd., 2002.
[35] B. R. Johnson and D. J. Leeming. A study of the digits of π, e and certain other irrational numbers. *Sankhyā: The Indian Journal of Statistics, Series B*, 52(2):183–189, 1990.
[36] T. Kärki. Transcendence of numbers with an expansion in a subclass of complexity 2n. *Theoretical Informatics and Applications*, 40(3):459–471, jul 2006.
[37] D. Knuth. *Art of Computer Programming, Volume 2: Seminumerical Algorithms*. Addison-Wesley Professional, third edition, November 1997.
[38] L. Kuipers and H. Niederreiter. *Uniform Distribution of Sequences*. Wiley-Interscience Series of Texts, Monographs and Tracts in Pure and Applied Mathematics. Wiley-Interscience, 1974.
[39] D. Lai and M.-F. Danca. Fractal and statistical analysis on digits of irrational numbers. *Chaos, Solitons and Fractals*, 36(2):246 – 252, 2008.
[40] H. Lebesgue. Sur certaines démonstrations d'existence. *Bulletin de la Société Mathématique de France*, 45:132–144, 1917.
[41] E. Lehrer. The game of normal numbers. *Mathematics of Operations Research*, 29:259–265, 2004.
[42] M. G. Madritsch, J. M. Thuswaldner, and R. F. Tichy. Normality of numbers generated by the values of entire functions. *Journal of Number Theory*, 128(5):1127 – 1145, 2008.
[43] 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*, 45:125–132, 1917.
[44] R. G. Stoneham. A study of 60,000 digits of the transcendental "e". *The American Mathematical Monthly*, 72(5):483–500, 1965.
[45] S. Tu and E. Fischbach. A study on the randomness of the digits of Pi. *International Journal of Modern Physics C*, 16(2):281–294, 2005.
[46] E. Ugalde. An alternative construction of normal numbers. *Journal de théorie des nombres de Bordeaux*, 12(1):165–177, 2000.
[47] S. Wagon. Is Pi normal? *The Mathematical Intelligencer*, pages 65–67, 1985.
[48] K. Weihrauch. *Computable Analysis: An Introduction*. Springer-Verlag, 1998.

Appendix A. Failures in the generalized serial test

Table 5. Numbers failing the generalized serial test. Each number is listed for each block size for which it fails.

Base 2	
Block size	Polynomials
1	Pisot 14, Salem 18
2	Pisot 37, SSP 9, Salem 21
3	Salem 21, Salem 34, Salem 41, Salem 42
4	Pisot 21, Pisot 25, Pisot 33, Salem 42, Salem 45, $\sqrt{3}$, $\sqrt{12}$
5	Pisot 27, Pisot 35, Salem 32, Salem 40, $\sqrt{18}$, $\sqrt{22}$
Base 3	
Block size	Polynomials
1	Pisot 4, Salem 4, Salem 5, Salem 30, Salem 37, $\sqrt{6}$, $\sqrt{10}$, $\sqrt{23}$
2	Pisot 28, SSP 10, Salem 6, Salem 30, Salem 31, Salem 45, $\sqrt{21}$
3	Pisot 26, SSP 10, $\sqrt{7}$
4	Pisot 14, Pisot 38, Salem 8, Salem 12, Salem 26, Salem 35, Salem 47, $\sqrt{21}$
5	Pisot 22, Pisot 33, SSP 2, SSP 7, SSP 12, Salem 31, Salem 37, $\sqrt{10}$
Base 5	
Block size	Polynomials
1	Pisot 25, Pisot 29, Pisot 30, Salem 21, Salem 24, $\sqrt{7}$, $\sqrt{8}$, $\sqrt{21}$
2	Pisot 32, Salem 40, Salem 45, $\sqrt{2}$, $\sqrt{3}$, $\sqrt{8}$, $\sqrt{12}$, $\sqrt{14}$
3	Pisot 23, SSP 5, Salem 42
4	Pisot 12, Pisot 31, SSP 7, SSP 10, SSP 13, Salem 25, Salem 35, Salem 42, $\sqrt{13}$, $\sqrt{23}$
5	Pisot 1, Salem 39, $\sqrt{12}$, $\sqrt{14}$
Base 7	
Block size	Polynomials
1	Pisot 7, Pisot 9, Pisot 14, Pisot 29, Pisot 32, SSP 4, Salem 1, Salem 27, Salem 31, Salem 32, Salem 35, Salem 38, $\sqrt{18}$
2	Pisot 17, Pisot 28
3	Pisot 15, Pisot 23, SSP 6, Salem 7, Salem 14, Salem 21, Salem 37, $\sqrt{13}$
4	Pisot 16, Pisot 31, Pisot 38, SSP 1, Salem 6, Salem 33, Salem 38, Salem 41, $\sqrt{6}$, $\sqrt{14}$, $\sqrt{20}$, $\sqrt{24}$
5	Pisot 23, Pisot 24, Pisot 26, Pisot 39, SSP 8, Salem 16
Base 10	
Block size	Polynomials
1	Pisot 17, Pisot 26, SSP 7, Salem 35, Salem 38, $\sqrt{14}$, $\sqrt{22}$
2	Pisot 24, Pisot 32, SSP 6, Salem 2, Salem 4, Salem 5, Salem 13
3	Pisot 10, Salem 3, Salem 21, Salem 43, $\sqrt{13}$
4	Pisot 17, Pisot 21, Pisot 35, SSP 1, Salem 38, Salem 44, Salem 47
5	Pisot 7, SSP 10, SSP 13, SSP 15, $\sqrt{6}$

Appendix B. Tables of polynomials

Table 6. List of numbers (given by their minimal polynomial)

Name	Polynomial
Pisot 1	$x^3 - x - 1$
Pisot 2	$x^4 - x^3 - 1$
Pisot 3	$x^5 - x^4 - x^3 + x^2 - 1$
Pisot 4	$x^3 - x^2 - 1$
Pisot 5	$x^6 - x^5 - x^4 + x^2 - 1$
Pisot 6	$x^5 - x^3 - x^2 - x - 1$
Pisot 7	$x^7 - x^6 - x^5 + x^2 - 1$
Pisot 8	$x^6 - 2x^5 + x^4 - x^2 + x - 1$
Pisot 9	$x^5 - x^4 - x^2 - 1$
Pisot 10	$x^8 - x^7 - x^6 + x^2 - 1$
Pisot 11	$x^7 - x^5 - x^4 - x^3 - x^2 - x - 1$
Pisot 12	$x^9 - x^8 - x^7 + x^2 - 1$
Pisot 13	$x^7 - x^6 - x^4 - x^2 - 1$
Pisot 14	$x^{10} - x^9 - x^8 + x^2 - 1$
Pisot 15	$x^9 - x^7 - x^6 - x^5 - x^4 - x^3 - x^2 - x - 1$
Pisot 16	$x^{11} - x^{10} - x^9 + x^2 - 1$
Pisot 17	$x^9 - x^8 - x^6 - x^4 - x^2 - 1$
Pisot 18	$x^{12} - x^{11} - x^{10} + x^2 - 1$
Pisot 19	$x^{11} - x^9 - x^8 - x^7 - x^6 - x^5 - x^4 - x^3 - x^2 - x - 1$
Pisot 20	$x^{13} - x^{12} - x^{11} + x^2 - 1$
Pisot 21	$x^{11} - x^{10} - x^8 - x^6 - x^4 - x^2 - 1$
Pisot 22	$x^{14} - x^{13} - x^{12} + x^2 - 1$
Pisot 23	$x^{13} - x^{11} - x^{10} - x^9 - x^8 - x^7 - x^6 - x^5 - x^4 - x^3 - x^2 - x - 1$
Pisot 24	$x^{15} - x^{14} - x^{13} + x^2 - 1$
Pisot 25	$x^{13} - x^{12} - x^{10} - x^8 - x^6 - x^4 - x^2 - 1$
Pisot 26	$x^{16} - x^{15} - x^{14} + x^2 - 1$
Pisot 27	$x^{15} - x^{13} - x^{12} - x^{11} - x^{10} - x^9 - x^8 - x^7 - x^6 - x^5 - x^4 - x^3 - x^2 - x - 1$
Pisot 28	$x^{17} - x^{16} - x^{15} + x^2 - 1$
Pisot 29	$x^{15} - x^{14} - x^{12} - x^{10} - x^8 - x^6 - x^4 - x^2 - 1$
Pisot 30	$x^{18} - x^{17} - x^{16} + x^2 - 1$
Pisot 31	$x^{17} - x^{15} - x^{14} - x^{13} - x^{12} - x^{11} - x^{10} - x^9 - x^8 - x^7 - x^6 - x^5 - x^4 - x^3 - x^2 - x - 1$
Pisot 32	$x^{19} - x^{18} - x^{17} + x^2 - 1$
Pisot 33	$x^{17} - x^{16} - x^{14} - x^{12} - x^{10} - x^8 - x^6 - x^4 - x^2 - 1$
Pisot 34	$x^{20} - x^{19} - x^{18} + x^2 - 1$
Pisot 35	$x^{19} - x^{17} - x^{16} - x^{15} - x^{14} - x^{13} - x^{12} - x^{11} - x^{10} - x^9 - x^8 - x^7 - x^6 - x^5 - x^4 - x^3 - x^2 - x - 1$
Pisot 36	$x^{21} - x^{20} - x^{19} + x^2 - 1$
Pisot 37	$x^{19} - x^{18} - x^{16} - x^{14} - x^{12} - x^{10} - x^8 - x^6 - x^4 - x^2 - 1$
Pisot 38	$x^{22} - x^{21} - x^{20} + x^2 - 1$
Pisot 39	$x^2 - x - 1$
Salem 1	$x^{10} + x^9 - x^7 - x^6 - x^5 - x^4 - x^3 + x + 1$
Salem 2	$x^{18} - x^{17} + x^{16} - x^{15} - x^{12} + x^{11} - x^{10} + x^9 - x^8 + x^7 - x^6 - x^3 + x^2 - x + 1$
Salem 3	$x^{14} - x^{11} - x^{10} + x^7 - x^4 - x^3 + 1$
Salem 4	$x^{14} - x^{12} - x^7 - x^2 + 1$

Continued on next page

Table 6 – continued from previous page

Name	Polynomial
Salem 5	$x^{10} - x^6 - x^5 - x^4 + 1$
Salem 6	$x^{18} - x^{17} - x^{10} + x^9 - x^8 - x + 1$
Salem 7	$x^{10} - x^7 - x^5 - x^3 + 1$
Salem 8	$x^{20} - x^{19} - x^{15} + x^{14} - x^{11} + x^{10} - x^9 + x^6 - x^5 - x + 1$
Salem 9	$x^{22} - x^{20} - x^{19} + x^{15} + x^{14} - x^{12} - x^{11} - x^{10} + x^8 + x^7 - x^3 - x^2 + 1$
Salem 10	$x^{16} - x^{15} - x^8 - x + 1$
Salem 11	$x^{26} - x^{24} - x^{21} - x^{18} + x^{16} + x^{13} + x^{10} - x^8 - x^5 - x^2 + 1$
Salem 12	$x^{12} - x^{11} + x^{10} - x^9 - x^6 - x^3 + x^2 - x + 1$
Salem 13	$x^{18} - x^{12} - x^{11} - x^{10} - x^9 - x^8 - x^7 - x^6 + 1$
Salem 14	$x^{20} - x^{18} - x^{15} - x^5 - x^2 + 1$
Salem 15	$x^{14} - x^{12} - x^{11} + x^9 - x^7 + x^5 - x^3 - x^2 + 1$
Salem 16	$x^{18} - x^{17} - x^{14} + x^{13} - x^9 + x^5 - x^4 - x + 1$
Salem 17	$x^{24} - x^{23} - x^{20} + x^{19} - x^{17} + x^{16} - x^{15} + x^{13} - x^{12} + x^{11} - x^9 + x^8 - x^7 + x^5 - x^4 - x + 1$
Salem 18	$x^{22} - x^{21} - x^{19} + x^{18} - x^{14} + x^{13} - x^{12} + x^{11} - x^{10} + x^9 - x^8 + x^4 - x^3 - x + 1$
Salem 19	$x^{10} - x^8 - x^5 - x^2 + 1$
Salem 20	$x^{26} - x^{25} - x^{20} + x^{13} - x^6 - x + 1$
Salem 21	$x^{14} - x^{13} - x^8 + x^7 - x^6 - x + 1$
Salem 22	$x^{22} - x^{21} - x^{20} + x^{19} - x^{13} + x^{11} - x^9 + x^3 - x^2 - x + 1$
Salem 23	$x^8 - x^5 - x^4 - x^3 + 1$
Salem 24	$x^{26} - x^{20} - x^{19} - x^{18} - x^{17} - x^{16} - x^{15} - x^{14} - x^{13} - x^{12} - x^{11} - x^{10} - x^9 - x^8 - x^7 - x^6 + 1$
Salem 25	$x^{20} - 2x^{19} + 2x^{18} - 2x^{17} + 2x^{16} - 2x^{15} + x^{14} - x^{12} + x^{11} - x^{10} + x^9 - x^8 + x^6 - 2x^5 + 2x^4 - 2x3 + 2x^2 - 2x + 1$
Salem 26	$x^{18} - x^{14} - x^{12} - x^{11} - x^9 - x^7 - x^6 - x^4 + 1$
Salem 27	$x^{26} - 2x^{25} + x^{24} + x^{23} - 2x^{22} + x^{21} - x^{18} + x^{17} - x^{15} + x^{14} - x^{13} + x^{12} - x^{11} + x^9 - x^8 + x^5 - 2x4 + x^3 + x^2 - 2x + 1$
Salem 28	$x^{30} - x^{25} - x^{24} - x^{23} - x^{22} - x^{21} - x^{20} + x^{15} - x^{10} - x^9 - x^8 - x^7 - x^6 - x^5 + 1$
Salem 29	$x^{30} - 2x^{29} + 2x^{28} - 2x^{27} + x^{26} - x^{24} + 2x^{23} - 2x^{22} + x^{21} - x^{19} + x^{18} - x^{17} + x^{16} - x^{15} + x^{14} - x^{13} + x^{12} - x^{11} + x^9 - 2x^8 + 2x^7 - x^6 + x^4 - 2x^3 + 2x^2 - 2x + 1$
Salem 30	$x^{30} - x^{29} - x^{22} - x^{18} - x^{15} - x^{12} - x^8 - x + 1$
Salem 31	$x^{26} - x^{24} - x^{23} + x^{19} - x^{17} - x^{16} + x^{14} + x^{13} + x^{12} - x^{10} - x^9 + x^7 - x^3 - x^2 + 1$
Salem 32	$x^{44} - x^{43} - x^{37} - x^{33} + x^{25} + x^{22} + x^{19} - x^{11} - x^7 - x + 1$
Salem 33	$x^{30} - x^{28} - x^{25} - x^{24} + x^{20} + x^{17} - x^{15} + x^{13} + x^{10} - x^6 - x^5 - x^2 + 1$
Salem 34	$x^{34} - x^{33} - x^{30} + x^{29} - x^{28} + x^{26} - x^{25} + x^{24} - x^{22} + x^{21} - x^{20} + x^{18} - x^{17} + x^{16} - x^{14} + x^{13} - x^{12} + x^{10} - x^9 + x^8 - x^6 + x^5 - x^4 - x + 1$
Salem 35	$x^{18} - 2x^{17} + 2x^{16} - 2x^{15} + 2x^{14} - 2x^{13} + 2x^{12} - 3x^{11} + 3x^{10} - 3x^9 + 3x^8 - 3x^7 + 2x^6 - 2x^5 + 2x^4 - 2x^3 + 2x^2 - 2x + 1$
Salem 36	$x^{26} - x^{25} - x^{22} + x^{21} - x^{20} + x^{18} - x^{17} + x^{16} - x^{14} + x^{13} - x^{12} + x^{10} - x^9 + x^8 - x^6 + x^5 - x^4 - x + 1$
Salem 37	$x^{24} - x^{23} - x^{18} - x^6 - x + 1$
Salem 38	$x^{20} - x^{18} - x^{15} - x^{12} + x^{10} - x^8 - x^5 - x^2 + 1$
Salem 39	$x^{40} - x^{37} - x^{35} - x^{33} - x^{31} - x^{29} + x^{26} + x^{24} + x^{22} + x^{20} + x^{18} + x^{16} + x^{14} - x^{11} - x^9 - x^7 - x^5 - x^3 + 1$
Salem 40	$x^{46} - x^{42} - x^{41} - x^{40} - x^{39} + x^{25} + x^{24} + x^{23} + x^{22} + x^{21} - x^7 - x^6 - x^5 - x^4 + 1$
Salem 41	$x^{10} - x^8 - x^7 + x^5 - x^3 - x^2 + 1$

Continued on next page

Table 6 – continued from previous page

Name	Polynomial
Salem 42	$x^{18}-x^{17}-x^{14}+x^{13}-x^{12}+x^{10}-x^9+x^8-x^6+x^5-x^4-x+1$
Salem 43	$x^{34}-x^{33}-x^{31}+x^{29}+x^{27}-2x^{26}+x^{23}+x^{22}-x^{21}-x^{20}-x^{19}+x^{18}+x^{17}+x^{16}-x^{15}-x^{14}-x^{13}+x^{12}+x^{11}-2x^8+x^7+x^5-x^3-x+1$
Salem 44	$x^{22}-x^{21}-x^{17}+x^{11}-x^5-x+1$
Salem 45	$x^{28}-x^{24}-x^{23}-x^{22}-x^{21}-x^{20}+x^{16}+x^{15}+x^{14}+x^{13}+x^{12}-x^8-x^7-x^6-x^5-x^4+1$
Salem 46	$x^{36}+x^{35}-x^{33}-2x^{32}-2x^{31}-x^{30}+x^{28}+x^{27}-x^{25}-x^{24}+x^{22}+x^{21}-x^{19}-x^{18}-x^{17}+x^{15}+x^{14}-x^{12}-x^{11}+x^9+x^8-x^6-2x^5-2x^4-x^3+x+1$
Salem 47	$x^{26}-x^{25}-x^{24}+2x^{22}-2x^{20}-x^{19}+2x^{18}+2x^{17}-2x^{16}-2x^{15}+3x^{13}-2x^{11}-2x^{10}+2x^9+2x^8-x^7-2x^6+2x^4-x^2-x+1$
$\sqrt{2}$	x^2-2
$\sqrt{3}$	x^2-3
$\sqrt{5}$	x^2-5
$\sqrt{6}$	x^2-6
$\sqrt{7}$	x^2-7
$\sqrt{8}$	x^2-8
$\sqrt{10}$	x^2-10
$\sqrt{11}$	x^2-11
$\sqrt{12}$	x^2-12
$\sqrt{13}$	x^2-13
$\sqrt{14}$	x^2-14
$\sqrt{15}$	x^2-15
$\sqrt{17}$	x^2-17
$\sqrt{18}$	x^2-18
$\sqrt{19}$	x^2-19
$\sqrt{20}$	x^2-20
$\sqrt{21}$	x^2-21
$\sqrt{22}$	x^2-22
$\sqrt{23}$	x^2-23
$\sqrt{24}$	x^2-24
SPP 1	$x^{17}+3098990841x^{16}+1912923433x^{15}+9045431x^{14}+3273968024x^{13}+1858720404x^{12}+3589583788x^{11}+121751485x^{10}+403123856x^9+3387540998x^8+2798570508x^7+1930549423x^6+2127877496x^5+1095513124x^4+3280387010x^3+3639700185x^2+577090035x-1$
SPP 2	$x^{18}+4077622507x^{17}+4272717488x^{16}+3105313243x^{15}+1690206298x^{14}+1849712021x^{13}+680249248x^{12}+2496252246x^{11}+2606193601x^{10}+2602510375x^9+1323436008x^8+2876470171x^7+3160967034x^6+3588440357x^5+364522444x^4+242886275x^3+4070888059x^2+4106135931x-1$
SPP 3	$x^{19}+3728226205x^{18}+2726705765x^{17}+646892616x^{16}+2744776763x^{15}+2045921453x^{14}+3592574577x^{13}+2019766385x^{12}+4276262006x^{11}+1006443814x^{10}+1113917010x^9+3596902319x^8+56556094x^7+281444308x^6+2687448242x^5+2593816815x^4+1588945341x^3+2337446724x^2+1022050291x-1$

Continued on next page

Table 6 – continued from previous page

Name	Polynomial
SPP 4	$x^{20} + 3437897288x^{19} + 3464545448x^{18} + 3560184500x^{17} + 3983477504x^{16} + 920842846x^{15} + 456053769x^{14} + 741588507x^{13} + 1188342905x^{12} + 2305023083x^{11} + 953174257x^{10} + 3286348354x^{9} + 3437916671x^{8} + 3942586889x^{7} + 1724820274x^{6} + 285680161x^{5} + 665600835x^{4} + 1701057199x^{3} + 443094743x^{2} + 1013818826x - 1$
SPP 5	$x^{21} + 3935673403x^{20} + 1200367622x^{19} + 930847405x^{18} + 56325016x^{17} + 2465058632x^{16} + 2335435107x^{15} + 1059022252x^{14} + 2014636220x^{13} + 486215916x^{12} + 3869338149x^{11} + 2787324482x^{10} + 4051686248x^{9} + 1999834073x^{8} + 124576507x^{7} + 3961355697x^{6} + 3177840181x^{5} + 4047793146x^{4} + 3415330358x^{3} + 3185950859x^{2} + 2675342408x - 1$
SPP 6	$x^{22} + 3450427731x^{21} + 1140404245x^{20} + 3457981463x^{19} + 2377759030x^{18} + 828863730x^{17} + 2929389923x^{16} + 2312003313x^{15} + 1778144125x^{14} + 3134573788x^{13} + 3444200774x^{12} + 1171229360x^{11} + 3307725408x^{10} + 1602711594x^{9} + 3263018231x^{8} + 2019726655x^{7} + 2846784051x^{6} + 1940101x^{5} + 1123655713x^{4} + 2083207864x^{3} + 3530265730x^{2} + 3407369714x - 1$
SPP 7	$x^{23} + 200071090x^{22} + 4192983751x^{21} + 1703729666x^{20} + 2478638291x^{19} + 4070378914x^{18} + 2694805171x^{17} + 958804052x16 + 531725375x^{15} + 3551302834x^{14} + 1823296034x^{13} + 389609426x^{12} + 300026760x^{11} + 1862494029x^{10} + 161042627x^{9} + 2179419879x^{8} + 249103486x^{7} + 1570621939x^{6} + 2301595683x^{5} + 311111483x^{4} + 2795742273x^{3} + 647892269x^{2} + 1390851135x - 1$
SPP 8	$x^{24} + 1109633603x^{23} + 488470614x^{22} + 1628116535x^{21} + 3874336669x^{20} + 1750902959x^{19} + 1145757521x^{18} + 85862007x^{17} + 1005808153x^{16} + 384681424x^{15} + 3567061709x^{14} + 825625181x^{13} + 2125934482x^{12} + 1946188973x^{11} + 1971964496x^{10} + 2756803937x^{9} + 899355981x^{8} + 4291224400x^{7} + 1062750938x^{6} + 365867941x^{5} + 3027165633x^{4} + 542587079x^{3} + 4133025708x^{2} + 973694252x - 1$
SPP 9	$x^{25} + 3204454556x^{24} + 1647827961x^{23} + 3325204342x^{22} + 2535870914x^{21} + 3967818719x^{20} + 2174409020x^{19} + 476516005x^{18} + 1022254626x^{17} + 674984870x^{16} + 3114132045x^{15} + 1941415070x^{14} + 3021425278x^{13} + 1627876806x^{12} + 175645976x^{11} + 2648491766x^{10} + 2380573534x^{9} + 347096267x^{8} + 3858160403x^{7} + 2159432591x^{6} + 27638347x^{5} + 3721854805x^{4} + 595022246x^{3} + 1603362537x^{2} + 1988601460x - 1$
SPP 10	$x^{26} + 4219432775x^{25} + 3297838299x^{24} + 571136783x^{23} + 2842608299x^{22} + 2945752650x^{21} + 1962074854x^{20} + 2898951944x^{19} + 1218130971x^{18} + 1638985230x^{17} + 2590683947x^{16} + 3694363524x^{15} + 191368206x^{14} + 4280179691x^{13} + 4092317463x^{12} + 1073727551x^{11} + 1407773507x^{10} + 2236257872x^{9} + 688180705x^{8} + 2806643162x^{7} + 3537287273x^{6} + 3493188175x^{5} + 885185167x^{4} + 2482883232x^{3} + 1842064464x^{2} + 2454155457x - 1$

Continued on next page

Table 6 – continued from previous page

Name	Polynomial
SPP 11	$x^{27} + 1039137331x^{26} + 816938268x^{25} + 255770050x^{24} + 2269380258x^{23} + 64427675x^{22} + 676431988x^{21} + 2643821685x^{20} + 2808575895x^{19} + 4143603118x^{18} + 4218488620x^{17} + 179874676x^{16} + 2978295604x^{15} + 3477396796x^{14} + 389426994x^{13} + 1303098501x^{12} + 404257167x^{11} + 3405809734x^{10} + 2705325684x^{9} + 2198630863x^{8} + 793110138x^{7} + 2522798630x^{6} + 2181161659x^{5} + 1999951822x^{4} + 3969454233x^{3} + 2404204091x^{2} + 1942955388x - 1$
SPP 12	$x^{28} + 2185820167x^{27} + 3930039573x^{26} + 261068283x^{25} + 79904862x^{24} + 3618094914x^{23} + 1737805114x^{22} + 1447402230x^{21} + 2950408474x^{20} + 320445937x^{19} + 3516805670x^{18} + 252648563x^{17} + 3891124326x^{16} + 696932843x^{15} + 1890020940x^{14} + 624070752x^{13} + 2840352436x^{12} + 2397408000x^{11} + 2583238311x^{10} + 2966072859x^{9} + 3480418382x^{8} + 1177027797x^{7} + 1609558288x^{6} + 46645248x^{5} + 612463853x^{4} + 2862211179x^{3} + 2823822897x^{2} + 2038265545x - 1$
SPP 13	$x^{29} + 3650460263x^{28} + 1102552364x^{27} + 3409218556x^{26} + 4077313028x^{25} + 3198677550x^{24} + 3549212110x^{23} + 3461944808x^{22} + 3477805148x^{21} + 3742139417x^{20} + 630116035x^{19} + 1184710267x^{18} + 61986656x^{17} + 2613067328x^{16} + 3597707318x^{15} + 1853623396x^{14} + 1265541121x^{13} + 918725848x^{12} + 2281979483x^{11} + 559260675x^{10} + 3152607366x^{9} + 967067445x^{8} + 632047036x^{7} + 990241686x^{6} + 797679253x^{5} + 3647871036x^{4} + 2938109465x^{3} + 2943160669x^{2} + 1112433002x - 1$
SPP 14	$x^{30} + 4200476012x^{29} + 877984508x^{28} + 357375657x^{27} + 1447688417x^{26} + 528394131x^{25} + 2799022850x^{24} + 708447329x^{23} + 2851854217x^{22} + 2367955797x^{21} + 642971878x^{20} + 2712975888x^{19} + 3454361812x^{18} + 1118419500x^{17} + 1537738650x^{16} + 3871754474x^{15} + 958920668x^{14} + 508522281x^{13} + 3339408317x^{12} + 1703700333x^{11} + 2938758908x^{10} + 1301323439x^{9} + 2828021294x^{8} + 3152760962x^{7} + 1098547466x^{6} + 1164431032x^{5} + 4038782759x^{4} + 2800499153x^{3} + 3017581848x^{2} + 458825076x - 1$
SPP 15	$x^{31} + 3995253174x^{30} + 2446480842x^{29} + 1546035534x^{28} + 2425331898x^{27} + 339127567x^{26} + 1803350800x^{25} + 1956515707x^{24} + 993794739x^{23} + 2196317197x^{22} + 3972150167x^{21} + 959457930x^{20} + 3425734602x^{19} + 3756088939x^{18} + 3684382278x^{17} + 981871294x^{16} + 1130926123x^{15} + 1205089165x^{14} + 3041671499x^{13} + 1452032911x^{12} + 1029568868x^{11} + 4294178027x^{10} + 3682257494x^{9} + 2926378821x^{8} + 3777386233x^{7} + 72501858x^{6} + 4236295687x^{5} + 678659486x^{4} + 3161059937x^{3} + 50056529x^{2} + 4145683430x - 1$

Department of Computer Science, University of Copenhagen (DIKU), Njalsgade 126–128, DK-2300 Copenhagen S, Denmark
E-mail address: {zerrez,simonsen}@diku.dk