Numeration 2016

Prague, Czech Republic, May 23–27 2016

Department of Mathematics FNSPE
Czech Technical University in Prague

Numeration 2016

Prague, Czech Republic, May 23–27 2016

Department of Mathematics FNSPE
Czech Technical University in Prague

Print: Česká technika — nakladatelství ČVUT

Editor: Petr Ambrož
petr.ambroz@fjfi.cvut.cz

Katedra matematiky
Fakulta jaderná a fyzikálně inženýrská
České vysoké učení technické v Praze
Trojanova 13   120 00 Praha 2

List of Participants

Rafael Alcaraz Barrera	rafalba@ime.usp.br *IME, University of São Paulo*
Karam Aloui	alouikaram@yahoo.fr *Institut Elie Cartan de Nancy / Faculté des Sciences de Sfax*
Petr Ambrož	petr.ambroz@fjfi.cvut.cz *FNSPE, Czech Technical University in Prague*
Hamdi Ammar	hamdi.ammar.lfm@hotmail.fr *Sfax University*
Myriam Amri	mmyriamamri@gmail.com *Sfax University*
Hamdi Aouinti	aouinti.hamdi@gmail.com *Université de Tunis*
Simon Baker	simonbaker412@gmail.com *University of Reading*
Christoph Bandt	bandt@uni-greifswald.de *University of Greifswald*
Attila Bérczes	berczesa@science.unideb.hu *University of Debrecen*
Anne Bertrand-Mathis	anne.bertrand@math.univ-poitiers.fr *University of Poitiers*
Dávid Bóka	bdavid1001@gmail.com *Eötvös Loránd University*
Horst Brunotte	brunoth@web.de
Marta Brzicová	m.brzicova@gmail.com *FNSPE, Czech Technical University in Prague*
Péter Burcsi	bupe@inf.elte.hu *Eötvös Loránd University*
Francesco Dolce	francesco.dolce@u-pem.fr *Université Paris-Est*
Artūras Dubickas	arturas.dubickas@mif.vu.lt *Vilnius University*
Lubomira Dvořáková	lubomira.balkova@gmail.com *FNSPE, Czech Technical University in Prague*
Jordan Emme	jordan.emme@univ-amu.fr *Aix-Marseille University*
Sébastien Ferenczi	ssferenczi@gmail.com *IMPA – CNRS, Rio de Janeiro, Brasil*
Aviezri Fraenkel	aviezri.fraenkel@weizmann.ac.il *Weizmann Institute of Science*

Christiane Frougny	christiane.frougny@liafa.univ-paris-diderot.fr *LIAFA / IRIF, Paris*
Kevin Hare	kghare@uwaterloo.ca *University of Waterloo*
Pavel Heller	pavel.heller@email.cz *Université Paris-Est*
Yuke Huang	huangyuke07@tsinghua.org.cn *School of Mathematics and Systems Science, BUAA*
Peter Hudoba	hudi1989@gmail.com *Eötvös Loránd University, Budapest*
Amara Chandoul	amarachandoul@yahoo.fr *Sfax University*
Koji Chinen	chinen@math.kindai.ac.jp *Kindai University, Osaka, Japan*
Maria Rita Iaco	maria-rita.iaco@liafa.univ-paris-diderot.fr *Université Paris Diderot*
Jonas Jankauskas	jonas.jankauskas@gmail.com *Montanuniversität Leoben*
Kan Jiang	K.Jiang1@uu.nl *Utrecht University*
Shoichi Kamada	168d9303@st.kumamoto-u.ac.jp *Kumamoto University*
Rania Kammoun	raniakammoun32@gmail.com *Université de Sfax, Tunisie*
Kamil Keprt	P15042@student.osu.cz *University of Ostrava*
Karel Klouda	karel.klouda@fit.cvut.cz *FIT, CTU in Prague*
Ondřej Kolouch	ondrej.kolouch@osu.cz *University of Ostrava*
Attila Kovács	attila.kovacs@inf.elte.hu *Eötvös Loránd University*
Daniel Krenn	daniel.krenn@aau.at *AAU Klagenfurt, Austria*
Tamás Krutki	krtamas@inf.elte.hu *Eötvös Loránd University*
Petr Kůrka	kurka@cts.cuni.cz *Center for Theoretical Study, Prague*
DoYong Kwon	doyong@jnu.ac.kr *Chonnam National University*

Revekka Kyriakoglou	krevekka@hotmail.gr *Université Paris Est Marne la Vallée (LIGM)*
Niels Langeveld	n.d.s.langeveld.2@umail.leidenuniv.nl *University of Leiden*
Manfred Madritsch	manfred.madritsch@univ-lorraine.fr *Université de Lorraine*
Faiza Mahjoub	faiza.mahjoub@yahoo.fr *Sfax University*
Merkhi Malika	malikamerkhi@yahoo.fr *Sfax University*
Bill Mance	mancew@impan.pl *Polish Academy of Sciences*
Zuzana Masáková	zuzana.masakova@fjfi.cvut.cz *FNSPE, Czech Technical University in Prague*
David W. Matula	matula@lyle.smu.edu *Southern Methodist University*
Mohamed Mkaouar	mohamed.mkaouar@fss.rnu.tn *Sfax University*
Hbaib Mohamed	mmmhbaib@gmail.com *Sfax University*
Clemens Müllner	clemens.muellner@tuwien.ac.at *Technical University of Vienna*
Gábor Nagy	nagygabr@gmail.com *Department of Computer Algebra, ELTE IK*
Radhakrishnan Nair	nair@liv.ac.uk *The University of Liverpool*
Lukáš Novotný	lukas.novotny@osu.cz *University of Ostrava*
Marco Pedicini	marco.pedicini@uniroma3.it *Roma Tre University*
Edita Pelantová	edita.pelantova@fjfi.cvut.cz *FNSPE, Czech Technical University in Prague*
Attila Pethő	petho.attila@inf.unideb.hu *University of Debrecen*
Joel Rivat	joel.rivat@univ-amu.fr *Université d'Aix-Marseille*
Driss Sana	sana_driss@yahoo.fr *Sfax University*
Zhang Shuqin	zhangsq_ccnu@sina.com *University of Leoben*

Klaus Scheicher	klaus.scheicher@boku.ac.at *BOKU, Vienna*
Johannes Schleischitz	johannes.schleischitz@boku.ac.at *BOKU Vienna*
Nikita Sidorov	sidorov@manchester.ac.uk *The University of Manchester*
Bernd Sing	bernd.sing@cavehill.uwi.edu *The University of the West Indies*
Lukas Spiegelhofer	lukas.spiegelhofer@tuwien.ac.at *Universite de Lorraine, France*
Štěpán Starosta	stepan.starosta@fit.cvut.cz *FIT, CTU in Prague*
Wolfgang Steiner	steiner@liafa.univ-paris-diderot.fr *CNRS, University Paris 7*
Paul Surer	paul.surer@boku.ac.at *BOKU Vienna*
Milena Svobodová	milenasvobodova@volny.cz *FNSPE, Czech Technical University in Prague*
Jan Šustek	jan.sustek@osu.cz *University of Ostrava*
Szabolcs Tengely	tengely@science.unideb.hu *University of Debrecen*
Tomas Vavra	t.vavra@seznam.cz *FNSPE, Czech Technical University in Prague*
Jean-Louis Verger-Gaugry	Jean-Louis.Verger-Gaugry@univ-smb.fr *CNRS, University Savoie Mont Blanc*
Walid Wannes	wannes_walid@ymail.com *Sfax University*
Mario Weitzer	mario_weitzer_at@yahoo.de *TU Graz*

Invited talks

Contributed talks

Algebraic Aspects of Canonical Number Systems

Horst Brunotte

A classical problem in algebraic number theory is the investigation of the question whether an algebraic number field is monogenic. B. Kovács proved that the existence of a power integral basis in an algebraic number field is equivalent to the existence of a canonical number system for its maximal order; here a canonical number system is a pair consisting of an algebraic integer α called the basis and a finite set of rational integers which is uniquely determined by α [4].

Definition 1. The algebraic integer α is called a basis of a canonical number system (CNS) for the order $\mathcal{O}$ of $\mathbb{Q}(\alpha)$ if every nonzero element of $\mathcal{O}$ can be represented in the form

$$n_0 + n_1\alpha + \cdots + n_k\alpha^k$$

with $n_0, \ldots, n_k \in \{0, \ldots, \left|Norm_{\mathbb{Q}(\alpha)|\mathbb{Q}}(\alpha)\right| - 1\}$ and $n_k \neq 0$.

Canonical number systems may be viewed as natural generalizations of radix representations of ordinary integers to algebraic integers. Originating from observations of D. E. Knuth and W. Penney the development of the theory of CNS was initiated by I. Kátai, J. Szabó, B. Kovács, W. J. Gilbert and others. Meanwhile several generalizations of canonical number systems and connections to other topics like finite automata and fractal tilings are investigated.

An algorithm for finding all CNS bases of monogenic algebraic number fields was established by B. Kovács and A. Pethő. A slight modification of this algorithm was presented in [8] based on the concept of CNS polynomials as introduced by A. Pethő [12].

Definition 2. Let $P \in \mathbb{Z}[X]$ be a monic integer polynomial of positive degree with $P(0) \neq 0$. We call P a CNS polynomial if for every $A \in \mathbb{Z}[X]$ can be canonically represented by P, i.e., there exists a polynomial $B \in \{0, \ldots, |P(0)| - 1\}[X]$ such that $A \equiv B \pmod{P}$.

We observe that the algebraic integer α is a CNS basis for $\mathbb{Z}[\alpha]$ if and only if its minimal polynomial belongs to the set $\mathcal{C}$ of all CNS polynomials.

An important role in the theory of CNS polynomials is played by the set

$$\mathcal{K} := \{p_d X^d + p_{d-1}X^{d-1} + \cdots + p_0 \in \mathbb{Z}[X] \ : \ d \geq 1, \ 1 = p_d \leq p_{d-1} \leq \ldots \leq p_1 \leq p_0 \geq 2\}$$

introduced by B. Kovács. The CNS polynomials in $\mathcal{K}$ are well-known:

Theorem 1 (Kovács – Pethő [11], Akiyama et al. [3])**.** *Let $P \in \mathcal{K}$ have degree d. If either P is irreducible or*

$$gcd\left\{j \in \{1, \ldots, d+1\} \ : \ p_j < p_{j-1}\right\} = 1 \qquad (p_{d+1} := 0)$$

then P is a CNS polynomial.

The combination of this fact with a useful result of B. Kovács – A. Pethő [11] on certain constants associated to an algebraic integer allows a modification of the above mentioned algorithm for the computation of CNS bases.

Theorem 2 (B. – Huszti – Pethő [8]). *Let γ be an algebraic integer and $\mathcal{C}_\gamma$ be set of all CNS bases for $\mathbb{Z}[\gamma]$. Then there exist finite effectively computable disjoint subsets $\mathcal{F}_0(\gamma), \mathcal{F}_1(\gamma) \subset \mathcal{C}_\gamma$ with the properties:*

(i) For every $\alpha \in \mathcal{C}_\gamma$ there exists some $n \in \mathbb{N}_0$ with $\alpha + n \in \mathcal{F}_0(\gamma) \cup \mathcal{F}_1(\gamma)$.

(ii) $\mathcal{F}_1(\gamma)$ consists of fundamental CNS bases for $\mathbb{Z}[\gamma]$.

Here the algebraic integer β is called a fundamental CNS basis for $\mathcal{O}$ if it satisfies the following properties:

(1) $\beta - n$ is a CNS basis for $\mathcal{O}$ for all $n \in \mathbb{N}_0$.

(2) $\beta + 1$ is a not CNS basis for $\mathcal{O}$.

Now we turn our attention to CNS polynomials. Let us mention that these polynomials have been put into a more general framework and refer the reader to the detailed survey by P. Kirschenhofer and J. M. Thuswaldner [10].

The CNS property of a given polynomial can be decided algorithmically and it is known that CNS polynomials are expansive and do not have positive real roots. Some characterization results on these polynomials are known, however, the complete description of these polynomials has remained an open problem even for small degrees. Moreover, the set $\mathcal{C}$ seems to have poor algebraic properties: For instance, $\mathcal{C}$ is not closed under multiplication, and there exist CNS polynomials none of whose factors belongs to $\mathcal{C}$.

Let us first consider multiplication. Some years ago, A. Pethő put forward the following interesting question regarding the set $\mathcal{A}$ of monic integer expansive polynomials without real positive roots: Is every $f \in \mathcal{A}$ a factor of a CNS polynomial? The answer to this question seems still to be open, but it is affirmative for certain subsets of $\mathcal{A}$ [7].

Theorem 3. *Let $f_1, \dots, f_m \in \mathcal{A}$ and assume that for each $i = 1 \dots, m$ one of the following two statements holds:*

1. *f_i has at most one pair of complex conjugate roots,*
2. *f_i is a Hurwitz polynomial.*

Then the product $f_1 \cdots f_m$ is a factor of a CNS polynomial.

Now we look at addition of constants to CNS polynomials. K. Scheicher and J. M. Thuswaldner published the first example of a CNS polynomial P such that $P + 1$ is not a CNS polynomial. The following result taken from [5] solves a problem of A. Pethő: It shows that there exists an infinite sequence of CNS polynomials P with the following properties:

1. $P + 1$ is not a CNS polynomial.
2. For any given positive integer k there exists a member P of this sequence such that $P - k$ is a CNS polynomial.

Proposition 1. *Let $n \in \mathbb{N}_0$. Then*

$$P_n = X^3 + (15n+50)X^2 + (22n+73)X + 17n + 55$$

is a CNS polynomial, $P_n + 1$ is not a CNS polynomial and $P_{100n} - n$ is a CNS polynomial.

Since the set $\mathcal{C}$ is not closed under addition of integers the following conjecture is quite challenging.

Conjecture (Akiyama [2])**.** *If $P \in \mathcal{C}$ then there exists $N \in \mathbb{N}$ such that $P + n \in \mathcal{C}$ for all $n \geq N$.*

This conjecture is supported by many examples. Recall that the polynomial $\sum_{i=0}^{d} a_i X^i \in \mathbb{C}[X]$ has a dominant constant term if $|a_0| \geq \sum_{i=1}^{d} |a_i|$.

Proposition 2. *Let $P = \sum_{i=0}^{d} p_i X^i \in \mathcal{C}$ with $d = \deg(P)$. Then Akiyama's conjecture holds for P provided that one of the following conditions is satisfied:*

1. $p_2, \dots, p_{d-1} \geq 0$,
2. $p_k < 0$ *for exactly one* $k \in \{1, \dots, d-1\}$ *and* $\sum_{1 \leq ki \leq d} p_{ki} \geq 0$,
3. *P is a trinomial,*
4. $d \leq 3$,
5. *P has a dominant constant term and $d \leq 5$,*
6. $p_0 = 2$ *and* $d \leq 8$.

Finally, we resume the representation of algebraic integers from other points of view and recall the following definition which has been introduced by P. Burcsi and A. Kovács [9].

Definition 3. Let $P \in \mathbb{Z}[X]$ be a monic integer polynomial of positive degree with $|P(0)| > 1$. We call P a semi-CNS polynomial if the set of canonically representable elements of $\mathbb{Z}[X]$ is additively closed.

W. Steiner [14] pointed out that this notion is intimately connected with positive finiteness as introduced by S. Akiyama and that an easy adaption of [1] to reducible polynomials shows that [9, Theorem 3.4] in fact describes all semi-CNS polynomials with negative constant term; in particular, there are exactly $\binom{d+k-3}{k-2}$ semi-CNS polynomials of degree d and constant term $-k \quad (k \geq 2)$.

Theorem 4 (Akiyama – Steiner)**.** *Let $P \in \mathbb{Z}[X]$ be a monic integer polynomial with $P(0) < -1$. Then P is a semi-CNS polynomial if and only if $P(1) < 0$ and apart from the constant term all coefficients of P are nonnegative.*

Recently, J.C. Rosales, M.B. Branco and D. Torrão investigated sets of positive integers and their relations to the number of their decimal digits. More precisely, for $b = 10$ they introduced and thoroughly studied digital semigroups whose definition can be formulated as follows.

Definition 4. Let $b \in \mathbb{Z} \setminus \{-1, 0, 1\}$ and set $Z_b := \mathbb{N}$ if b is positive, and $Z_b := \mathbb{Z} \setminus \{0\}$ if b is negative. A b-digital semigroup D is a subsemigroup of $(Z_b, \cdot)$ such that $\Delta_b(\ell_b(d)) \subseteq D$ for all $d \in D$. Here we use the notation

$$\Delta_b(n) := \{z \in Z_b \ : \ \ell_b(z) = n\} \qquad\qquad (n \in \mathbb{N}),$$

where $\ell_b(z)$ is the length of the usual b-ary representation of $z \in Z_b$.

Obviously, Z_b is contained in the set of canonically representable elements of the linear semi-CNS polynomial $X - b$. It turns out that for positive base b results on b-digital semigroup coincide with the respective results presented by J.C. Rosales et. al.; however, for negative base b some minor modifications have to be taken [6]. As an example we characterize LD-semigroups (cf. [13, Theorem 4]) whose definition can be generalized as follows.

Definition 5. Let S be a submonoid of $(\mathbb{N}_0, +)$. We call S a b-LD-semigroup if there exists a b-digital semigroup D such that

$$S = \{\ell_b(d) \ : \ d \in D\} \cup \{0\} .$$

Theorem 5. *Let S be a submonoid of $(\mathbb{N}_0, +)$ and $b \in \mathbb{Z} \setminus \{-1, 0, 1\}$. Then the following statements are equivalent:*

1. *S is a b-LD-semigroup.*
2. *$S \neq \{0\}$ and $s + t + e \in S$ for all $s, t \in S \setminus \{0, 1\}$ and $e = -1$ if b is positive, and $e \in \{-3, -1, 1\}$ if b is negative.*

References

[1] S. Akiyama, *Positive finiteness of number systems*, in Number theory, vol. 15 of Dev. Math., Springer, New York, 2006, pp. 1–10.

[2] S. Akiyama. Private communication, 2012.

[3] S. Akiyama, T. Borbély, H. Brunotte, A. Pethő, and J. M. Thuswaldner, *Basic properties of shift radix systems*, Acta Math. Acad. Paedagog. Nyházi. (N.S.), 22 (2006), pp. 19–25 (electronic).

[4] S. Akiyama, H. Brunotte, and A. Pethő, *Cubic CNS polynomials, notes on a conjecture of W. J. Gilbert*, J. Math. Anal. Appl., 281 (2003), pp. 402–415.

[5] H. Brunotte, *Unusual CNS polynomials*, Math. Pannon., 24 (2013), pp. 125–137.

[6] ——, *Digital semigroups.* to appear in RAIRO - Theoretical Informatics and Applications, 2016.

[7] ——, *Some comments on factors of CNS polynomials.* To appear in Acta Math. Acad. Paed. Nyiregyhaziensis, 2016.

[8] H. Brunotte, A. Huszti, and A. Pethő, *Bases of canonical number systems in quartic algebraic number fields*, J. Théor. Nombres Bordeaux, 18 (2006), pp. 537–557.

[9] P. Burcsi and A. Kovács, *Exhaustive search methods for CNS polynomials*, Monatsh. Math., 155 (2008), pp. 421–430.

[10] P. Kirschenhofer and J. M. Thuswaldner, *Shift radix systems—a survey*, in Numeration and substitution 2012, RIMS Kôkyûroku Bessatsu, B46, Res. Inst. Math. Sci. (RIMS), Kyoto, 2014, pp. 1–59.

[11] B. Kovács and A. Pethő, *Number systems in integral domains, especially in orders of algebraic number fields*, Acta Sci. Math. (Szeged), 55 (1991), pp. 287–299.

[12] A. Pethő, *Connections between power integral bases and radix representations in algebraic number fields*, in Proceedings of the 2003 Nagoya Conference "Yokoi-Chowla Conjecture and Related Problems", S. Katayama, C. Levesque, and T. Nakahara, eds., Saga, 2004, Saga Univ., pp. 115–125.

[13] J. C. Rosales, M. B. Branco, and D. Torrão, *Sets of positive integers closed under product and the number of decimal digits*, J. Number Theory, 147 (2015), pp. 1–13.

[14] W. Steiner, *Zbl 1191.11004*. Zentralbl. Math. (2008).

Pisot Numbers and Their Conjugates

Artūras Dubickas

Department of Mathematics and Informatics, Vilnius University, Lithuania

A *Pisot number* $\alpha > 1$ is an algebraic integer whose conjugates over $\mathbb{Q}$, except for α itself, all lie in the unit disc $|z| < 1$. In 1944, Salem [7] proved that the set of Pisot numbers is closed, and Siegel [8] showed that the positive root $\theta = 1.32471\dots$ of $x^3 - x - 1 = 0$ is the smallest Pisot number. By a result of Smyth [9], the number θ number has the smallest possible Mahler measure (equal to θ itself) among all non-reciprocal algebraic numbers.

Another result of Smyth [10] implies that at most two conjugates of a Pisot number can have the same modulus. Later, Mignotte [6] generalized this by proving that there are no non-trivial multiplicative relations between the conjugates of a Pisot number.

Theorem 1 (Mignotte)**.** *The equality* $\alpha_1^{k_1}\alpha_2^{k_2}\dots\alpha_d^{k_d} = 1$ *with algebraic numbers* $\alpha_1, \dots, \alpha_d$ *that are conjugates of a Pisot number* α *of degree* d *over* $\mathbb{Q}$ *and* $k_1, k_2, \dots, k_d \in \mathbb{Z}$ *can only hold if* $k_1 = k_2 = \dots = k_d$.

The theorem implies, for instance, that no two non-real conjugates of a Pisot number can have the same argument. Indeed, if the arguments of α_1 and α_2 were equal, then we would have the non-trivial multiplicative relation $\alpha_1\overline{\alpha_2}\alpha_2^{-1}\overline{\alpha_1}^{-1} = 1$ with four conjugates of a Pisot number α (namely, with $\alpha_1, \alpha_2, \overline{\alpha_1}, \overline{\alpha_2}$; the exponents of other $\deg \alpha - 4$ conjugates in this equality are all equal to zero), which is impossible, by Theorem 1. This simple fact is, basically, everything we know about the geometry of the set of conjugates of a Pisot number.

In [5], the author and Smyth investigated some non-trivial geometric facts about the set of conjugates of a Salem number. (Recall that an algebraic integer $\alpha > 1$ is a *Salem number* if all of its conjugates except for α and α^{-1} are of modulus lie on the disc 1. See, e. g., [1] and [11] for more on Pisot and Salem numbers.) In particular, in [5] it was proved that no three conjugates of a Salem number lie on a line. In conclusion, we asked if two non-real conjugates of a Pisot number can have the same imaginary part and if four conjugates of a Pisot number can have the same real part. In both cases, the complex (non-real) numbers α_1, α_3 that are conjugates of a Pisot number α and their complex conjugates α_2, α_4 form a parallelogram (possibly degenerate) in the complex plane $\mathbb{C}$. Thus, a non-trivial additive relation

$$\alpha_1 + \alpha_2 = \alpha_3 + \alpha_4 \tag{1}$$

in distinct conjugates $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ of a Pisot number α holds. (Here, $\alpha_2 = \overline{\alpha_3}, \alpha_4 = \overline{\alpha_1}$ in case α_1, α_3 have the same imaginary part, and $\alpha_2 = \overline{\alpha_1}, \alpha_4 = \overline{\alpha_3}$ in case α_1, α_3, where $\alpha_1 \neq \overline{\alpha_3}$, have the same real part.)

In [5], the following example

$$\alpha := \alpha_1 = \frac{1 + \sqrt{3 + 2\sqrt{5}}}{2} = 1.86676\dots \tag{2}$$

with minimal polynomial $f(x) = x^4 - 2x^3 + x - 1$ whose conjugates satisfy (1) was found. Indeed, the number $\alpha = 1.86676\ldots$ defined in (2) is a Pisot number, with conjugates

$$\alpha_2 = \frac{1 - \sqrt{3 + 2\sqrt{5}}}{2}, \quad \alpha_{3,4} = \frac{1 \pm i\sqrt{-3 + 2\sqrt{5}}}{2}$$

satisfying $\alpha_2 = -0.86676\ldots$, $|\alpha_3| = |\alpha_4| = 0.78615\ldots$. Hence, two real conjugates α_1, α_2 and two complex conjugate numbers α_3 and $\alpha_4 = \overline{\alpha_3}$ satisfy $\alpha_1 + \alpha_2 = \alpha_3 + \alpha_4 = 1$, so that (1) is solvable in conjugates of a Pisot number.

Since the property (1) is quite unusual, it is quite tempting to conjecture that there are not many (possibly only finitely many) Pisot numbers α satisfying it.

The next theorem proved in [2] shows that this is indeed the case with the property (1). More precisely, the special Pisot number (2) is a unique Pisot number whose conjugates satisfy (1):

Theorem 2. *If α is a Pisot number of degree $d \geq 4$ whose four distinct conjugates over $\mathbb{Q}$ satisfy the relation*

$$\alpha_1 + \alpha_2 = \alpha_3 + \alpha_4$$

then

$$\alpha = \frac{1 + \sqrt{3 + 2\sqrt{5}}}{2}.$$

Moreover, there exists no Pisot number α whose four distinct conjugates satisfy the linear relation

$$\pm\alpha_1 = \alpha_2 + \alpha_3 + \alpha_4.$$

Since a real and a non-real conjugate of any algebraic number cannot have the same real part, Theorem 2 implies that, in particular,

Corollary 3. *No two non-real conjugates of a Pisot number can have the same imaginary part and at most two conjugates of a Pisot number can have the same real part.*

Note that Corollary 3 answers negatively both questions posed in [5]. In addition to Theorem 2, let us consider a three term linear equations in conjugates of a Pisot number. We showed in [2] that

Theorem 4. *If α is a Pisot number having three conjugates over $\mathbb{Q}$ satisfying the relation*

$$\alpha_1 + \alpha_2 + \alpha_3 = 0$$

then α is Siegel's number $\theta = 1.32471\ldots$ (the root of $x^3 - x - 1 = 0$). Furthermore, there does not exist a Pisot number α whose three conjugates satisfy the relation

$$\alpha_1 = \alpha_2 + \alpha_3.$$

How about equations

$$\alpha_1 = \alpha_2 + \alpha_3 \quad \text{and} \quad \alpha_1 + \alpha_2 + \alpha_3 = 0 \tag{3}$$

in conjugates of an algebraic number (which is not necessarily Pisot number)?

In [3], we showed that

Theorem 5. *Let d be an integer in the range $3 \leq d \leq 8$ and let α be an algebraic number of degree d over $\mathbb{Q}$. Then some three of its conjugates α_1, α_2, α_3 satisfy the relation*

$$\alpha_1 = \alpha_2 + \alpha_3$$

if and only if $d = 6$ and the minimal polynomial of α over $\mathbb{Q}$ is an irreducible polynomial of the form

$$p(x) = x^6 + 2ax^4 + a^2x^2 + b \in \mathbb{Q}[x].$$

The second equation in (3) has a trivial cubic solution, since three conjugates of each cubic algebraic number with trace zero satisfy the linaer relation $\alpha_1 + \alpha_2 + \alpha_3 = 0$. Note that there exist algebraic numbers of degree d whose three conjugates satisfy $\alpha_1 + \alpha_2 + \alpha_3 = 0$ with d not necessarily divisible by 3, for instance, of degree $d = 20$; see [4].

Restricting to the degrees in the range $4 \leq d \leq 8$ we have the following:

Theorem 6. *Let d be an integer in the range $4 \leq d \leq 8$ and let α be an algebraic number of degree d over $\mathbb{Q}$. Then some three of its conjugates α_1, α_2, α_3 satisfy the relation*

$$\alpha_1 + \alpha_2 + \alpha_3 = 0$$

if and only if $d = 6$ and the minimal polynomial of α over $\mathbb{Q}$ is an irreducible polynomial of the form

$$p(x) = x^6 + 2ax^4 + 2bx^3 + (a^2 - c^2t)x^2 + 2(ab - cet)x + b^2 - e^2t$$

for some rational numbers $a, b, c, e \in \mathbb{Q}$ and some square-free integer $t \in \mathbb{Z}$.

In order to verify whether a given polynomial

$$p(x) = x^6 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 \in \mathbb{Q}[x]$$

is of the form given in Theorem 6 or not we set $a := a_4/2$, $b := a_3/2$. Then, using $4c^2t = a_4^2 - 4a_2$, $4e^2t = a_3^2 - 4a_0$ and $4cet = a_3a_4 - 2a_1$, we can rewrite the condition of the theorem in the following equivalent form:

$$(a_4^2 - 4a_2)(a_3^2 - 4a_0) = (a_3a_4 - 2a_1)^2.$$

References

[1] M.J. Bertin, A. Decomps-Guilloux, M. Grandet-Hugo, M. Pathiaux-Delefosse and J.P. Schreiber, *Pisot and Salem numbers,* Birkhäuser, Basel, 1992.

[2] A. Dubickas, K. Hare and J. Jankauskas, *No two non-real conjugates of a Pisot number have the same imaginary part,* Math. Comp. (to appear).

[3] A. Dubickas and J. Jankauskas, *Simple linear relations with algebraic numbers of small degree,* J. Ramanujan Math. Soc. **30** (2) (2015), 219–235.

[4] A. Dubickas, C.J. Smyth, *Problem 11123,* Amer. Math. Monthly **111** (2004), 916.

[5] A. Dubickas and C.J. Smyth, *On the lines passing through two conjugates of a Salem number,* Math. Proc. Camb. Phil. Soc. **144** (2008), 29–37.

[6] M. Mignotte, *Sur les conjugués des nombres de Pisot,* C. R. Acad. Sci. Paris Sér. I. Math. **298** (1984), 21.

[7] R. Salem, *A remarkable class of algebraic numbers. Proof of a conjecture of Vijayaraghavan,* Duke Math. J. **11** (1944), 103–108.

[8] C.L. Siegel, *Algebraic numbers whose conjugates lie in the unit circle*, Duke Math. J. **11** (1944), 597–602.

[9] C. J. Smyth, *On the product of the conjugates outside the unit circle of an algebraic integer,* Bull. London Math. Soc. **3** (1971), 169–175.

[10] C.J. Smyth, *The conjugates of algebraic integers,* Amer. Math. Monthly **82** (1975), 86.

[11] C.J. Smyth, *Seventy years of Salem numbers,* Bull. London Math. Soc. **47** (2015), 379–395.

Freezing Arithmetic Algorithms into Foundational Number Representation Theorems

David W. Matula

SMU, Dallas, USA

An algorithm is often a winding path to a theorem: to arrive it is often needed to take the path less traveled. Today we embark on four examples inspired by a lifetime envisioning the design of the arithmetic engine of a computer. Novel new algorithms here have exposed arguably fundamental relations that could be "frozen" into theorems which indeed stand on their own right.

Our first milepost fully characterizes integer (digit set,radix) pairs that provide complete and unique representation of the integers. Recursive elementary residue arithmetic provides the path yielding this radix number system theorem. Our next theorem reveals an order preserving one-to-one correspondence between the rationals and the lexicographically ordered set of finite length bit strings. Here a bit serial binary radix division algorithm recursivly codes the bit strings. The strings provide an alternative data structure for arguably efficient rational arithmetic.

In another direction we contend with the arithmetic unit test question of characterizing and computing a large pseudo-random sample of floating point (dividend,divisor) pairs whose quotients are extremely close to "midpoints", so called "hard-to-round" cases. Employing rational and residue arithmetic fundamentals we obtain sequences of such pairs where sucessive terms are formed by elementary binary addition.

Our final development is a topological representation of the integers given by a one-to-one correspondence of the integers with rooted trees. The three pillars of this correspondence are provided by the fundamental theorem of arithmetic (unique prime factorization), the fundamental operation of arithmetic (counting), and the fundamental process of computation (recursion).

In summary we have seeked to demonstrate how analysis of the design of the computational heart of the computer has been the genesis for crafting radix, rational, and residue arithmetic fudamentals into recursive procedures that can be "frozen into theorems" adding new directions to the study of number systems.

Self-Affine Sets:
Topology, Uniqueness, Simultaneous Expansions

Nikita Sidorov

School of Mathematics, Thhe University of Manchester, United Kingdom

1 Self-affine family of IFS: positive real case

1.1 Introduction

Iterated function systems (IFS) are widely used to construct fractals. The general set-up is as follows: let $\{F_1, \dots, F_m\}$ be contracting maps on $\mathbb{R}^d$; then there exists a unique compact set (the *attractor*) A such that $A = \bigcup_{j=1}^m F_j(A)$.

Let $\beta_1, \beta_2 \in (1,2)$ and $T_i(x,y) = \left(\frac{x+i}{\beta_1}, \frac{y+i}{\beta_2}\right)$ for $i = \pm 1$. In other words,

$$T_{\pm 1}(x,y) = \begin{pmatrix} \beta_1^{-1} & 0 \\ 0 & \beta_2^{-1} \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \pm \begin{pmatrix} \beta_1^{-1} \\ \beta_2^{-1} \end{pmatrix}.$$

Let now $A := A_{\beta_1,\beta_2}$ be the *attractor* of the IFS $\{T_{-1}, T_1\}$, This means $A = T_1(A) \cup T_{-1}(A)$. It is well known that A is either connected or totally disconnected. Note that $(x,y) \in A_{\beta_1,\beta_2}$ if and only if there exists $(a_n)_1^\infty \in \{-1,1\}^{\mathbb{N}}$ such that

$$x = \sum_{n=1}^\infty a_n \beta_1^{-n}, \quad y = \sum_{n=1}^\infty a_n \beta_2^{-n}.$$

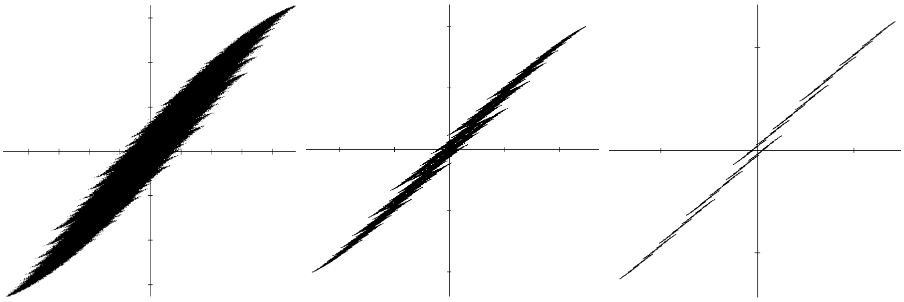

Figure 1: $A_{1.2,1.3}$, $A_{1.4,1.5}$ and $A_{1.7,1.8}$.

Figure 1 suggests that when β_1 and β_2 are "sufficiently small", A_{β_1,β_2} is connected and if, in addition, they "very small indeed", then A_{β_1,β_2} has a non-empty interior, whereas if β_1 or β_2 is "large enough", it is totally disconnected. Our goal os to make such statements (somewhat) quantifiable. We will also explain how to generalize some of these results to higher-dimensional self-affine systems.

This talk is based on my three recent papers [4, 5, 6] joint with **Kevin Hare** (University of Waterloo).

1.2 Non-empty interior

For the rest we will assume $\beta_1 \neq \beta_2$. Put

$$\mathcal{Z} = \{(\beta_1, \beta_2) : (0,0) \in A^o\},$$

where A^o is the interior of A.

Theorem 1. *[2] If* $1 < \beta_1, \beta_2 < 1.05$*, then* $(\beta_1, \beta_2) \in \mathcal{Z}$*.*

We have improved this result to show that

Theorem 2. *[4] If* $\beta_1 \neq \beta_2$ *are such that*

$$\left|\frac{\beta_2^8 - \beta_1^8}{\beta_2^7 - \beta_1^7}\right| + \left|\frac{\beta_2^7\beta_1^7(\beta_2 - \beta_1)}{\beta_2^7 - \beta_1^7}\right| \leq 2,$$

then $(\beta_1, \beta_2) \in \mathcal{Z}$*.*

Corollary 3. *If* $1 < \beta_1, \beta_2 < 1.202$ *then* $(\beta_1, \beta_2) \in \mathcal{Z}$*.*

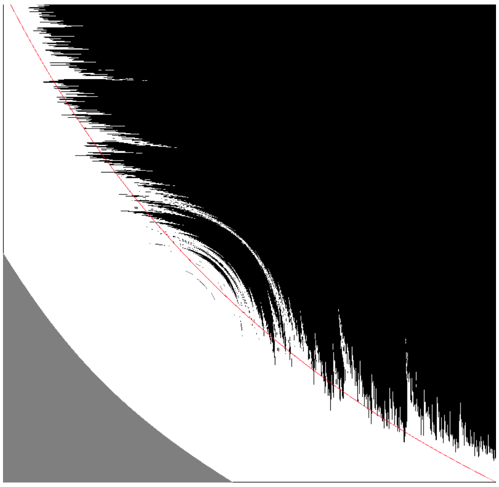

Figure 2: Empty interior (black) versus non-empty interior (grey)

The square in Figure 2 is $(\beta_1, \beta_2) \in (1,2) \times (1,2)$. Points known to be in $\mathcal{Z}$ (grey); points known to be not in $\mathcal{Z}$ (black); curve $\beta_1\beta_2 = 2$ (red). Note that if $\beta_1\beta_2 > 2$, then the attractor has zero Lebesgue measure and therefore, empty interior.

Theorem 2 corresponds to the grey region; our proof is essentially based on the same method as in [2] (which is in turn based on an idea from a paper [3] by Güntürk), except that we push it to the limit (or thereabouts).

1.3 Connectedness locus

Put

$$\mathcal{S} = \{(\beta_1, \beta_2) : A_{\beta_1,\beta_2} \text{ is totally disconnected}\}.$$

Theorem 4. *[4] The set $\mathcal{S}$ is disconnected.*

Remark 5. 1. It is worth mentioning that in the complex setting (see Section 2, Calegari, Koch and Walker [1] have shown that the analogue of $\mathcal{S}$ has infinitely many connected components. It is likely that their method works for our setting as well.

2. For our setting B. Solomyak [8] has shown that a large portion of the *connectedness locus* $\mathcal{N} = \mathcal{S}^c$ is connected and locally connected and conjectured that $\mathcal{N}$ is connected. (We know now that it is not simply connected.)

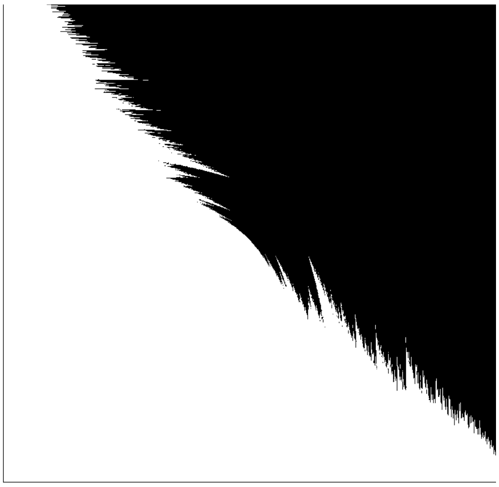

Figure 3: Points known to be in $\mathcal{S}$

1.4 The set of uniqueness

Let p stand for the letter $+1$ and m for -1. We define the map $s_\beta : \{p, m\}^{\mathbb{N}} \to \mathbb{R}$ as

$$s_\beta(w) = \sum_{n=1}^{\infty} \frac{w_n}{\beta^n}$$

and the map $\pi : \{p, m\}^{\mathbb{N}} \to \mathbb{R}$ as follows: $\pi(w) = (s_{\beta_1}(w), s_{\beta_2}(w))$. Thus, we have using this notation that

$$A_{\beta_1,\beta_2} = \left\{\pi(w) : w \in \{p, m\}^{\mathbb{N}}\right\}.$$

We say that $(x, y) = \pi(w)$ has a *unique address* if for any $w' \in \{p, m\}^{\mathbb{N}}$ with $w \neq w'$ we have $\pi(w') \neq (x, y)$.

We denote by U_{β_1,β_2} the set of all unique addresses and by $\mathcal{U}_{\beta_1,\beta_2}$ the projection $\pi(U_{\beta_1,\beta_2})$ and call it the *set of uniqueness.*

For example, if A_{β_1,β_2} is totally disconnected, then $U_{\beta_1,\beta_2} = \{p, m\}^{\mathbb{N}}$ and $\mathcal{U}_{\beta_1,\beta_2} = A_{\beta_1,\beta_2}$. On the other hand, if $(0, 0) \in A$ by $\pi(w) = (0, 0)$, then $\pi(\tilde{w}) = (0, 0)$ as well, where $\tilde{w}$ is the negation of w. In particular, $(0, 0)$ does not have a unique address.

Theorem 6. *The set of uniqueness $\mathcal{U}_{\beta_1,\beta_2}$ has positive Hausdorff dimension for any (β_1, β_2).*

In the self-similar setting (without rotations) the set of uniqueness has been studied in detail.

In particular, I proved in 2007 [7] that if the contraction ratios are sufficiently close to 1, then the set of uniqueness can contain only fixed points.

As we see, this is very different in the self-affine setting.

1.5 Simultaneous (signed) β-expansions

Put

$$\begin{aligned}\mathcal{D}_{\beta_1,\beta_2} &= \left\{x \in \mathbb{R} : \exists (a_n)_1^\infty \in \{\pm 1\}^{\mathbb{N}} \mid x = \sum_{n=1}^{\infty} a_n \beta_1^{-n} = \sum_{n=1}^{\infty} a_n \beta_2^{-n}\right\} \\ &= A_{\beta_1,\beta_2} \cap \{(x,y) : y = x\}.\end{aligned}$$

Theorem 7. *1. For any pair (β_1,β_2) the set $\mathcal{D}_{\beta_1,\beta_2}$ is non-empty;*

2. If $\min\{\beta_1,\beta_2\} < \frac{1+\sqrt{5}}{2}$, then the Hausdorff dimension of the set $\mathcal{D}_{\beta_1,\beta_2} > 0$ is positive;

3. If $\max\{\beta_1,\beta_2\} < 1.202$, then there exists a $\delta > 0.664$ such that $[-\delta,\delta] \subset \mathcal{D}_{\beta_1,\beta_2}$.

See Figure 4.

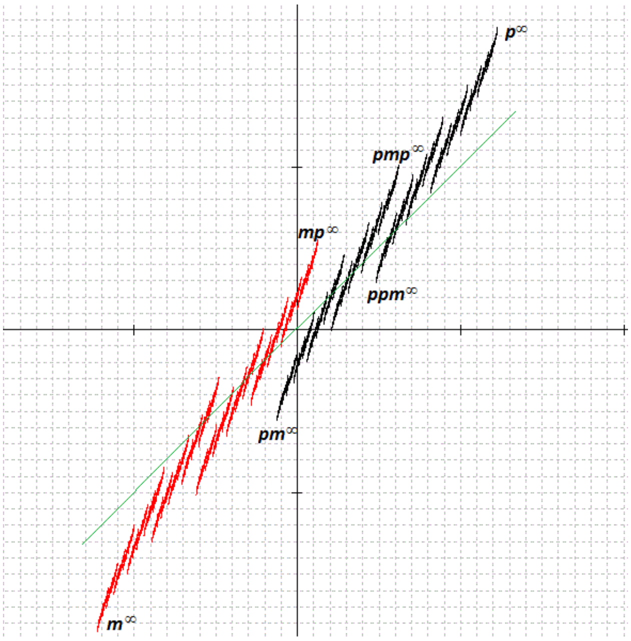

Figure 4: The attractor intersecting the diagonal for $\beta_1 = 1.923, \beta_2 = 1.754$.

2 Generalizations

2.1 Two-dimensional case

Consider two self-affine linear contraction maps $T_m, T_p : \mathbb{R}^2 \to \mathbb{R}^2$:

$$T_m(v) = Mv - u \quad \text{and} \quad T_p(v) = Mv + u, \tag{1}$$

where M is a 2×2 real matrix with both eigenvalues less than 1 in modulus and $u \neq 0$. Here "m" is for "minus" and "p" is for "plus". We are interested in the iterated function system (IFS) generated by T_m and T_p.

Theorem 8. *[5] If all eigenvalues of M are between $2^{-1/4} \approx 0.8409$ and 1 in absolute value, and the IFS is non-degenerate, then the attractor of the IFS has non-empty interior. More precisely,*

- *If $0.832 < \lambda < \mu < 1$ then $A_{\lambda,\mu}$, the attractor for the (positive) real case $M = \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}$, has non-empty interior (this is Corollary 3 with $\lambda = \beta_1^{-1}, \mu = \beta_2^{-1}$).*
- *If $2^{-1/2} \approx 0.707 < \lambda < \mu < 1$ then $A_{-\lambda,\mu}$, the attractor for the (mixed) real case $M = \begin{pmatrix} -\lambda & 0 \\ 0 & \mu \end{pmatrix}$, has non-empty interior.*
- *If $0.832 < \nu < 1$ then A_ν, the attractor for the Jordan block case $M = \begin{pmatrix} \nu & 1 \\ 1 & 0 \end{pmatrix}$, has non-empty interior.*
- *If $2^{-1/4} \approx 0.841 < |\kappa| < 1$ with $\kappa = a + bi \notin \mathbb{R}$ then A_κ, the attractor for the complex case $M = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$, has non-empty interior.*

Let $\mathcal{U}_M$ be the *set of uniqueness* for our IFS, i.e., the set of $x \in A_M$ each of which has a unique address. An analogous result holds:

Theorem 9. *For all non-degenerate IFS with real eigenvalues or complex eigenvalues with irrational arguments the set of points of uniqueness is uncountable, and with positive Hausdorff dimension.*

2.2 Multidimensional case.

Let $d \geq 3$ and M be a $d \times d$ real matrix whose eigenvalues are all less than 1 in modulus. Denote by A_M the attractor for the contracting IFS $\{Mv - u, Mv + u\}$, i.e., $A_M = \{\pi_M(a_0a_1\dots) \mid a_n \in \{\pm 1\}\}$, where

$$\pi_M(a_0a_1\dots) = \sum_{k=0}^{\infty} a_k M^k u.$$

If $A_M \ni x = \pi_M(a_0a_1\dots)$, then we call the sequence $a_0a_1\dots \in \{\pm 1\}^{\mathbb{N}}$ an *address* of x. We assume our IFS to be *non-degenerate*, i.e., A_M does not lie in any $(d-1)$-dimensional subspace of $\mathbb{R}^d$ (i.e., A_M *spans* $\mathbb{R}^d$). Let $u \in \mathbb{R}^d$ be a *cyclic vector* for M, i.e., $\operatorname{span}\{M^n u \mid n \geq 0\} = \mathbb{R}^d$.

Theorem 10. *[6] If*

$$|\det M| \geq 2^{-1/d},$$

then the attractor A_M has non-empty interior. In particular, this is the case when each eigenvalue of M is greater than $2^{-1/d^2}$ in modulus.

Remark 11. If $d = 2$ and M has real eigenvalues, then this result is weaker than Theorem 8.

Corollary 12. *For an IFS $\{Mv + u_j\}_{j=1}^m$ with $m \geq 2$ the same claim holds, provided the IFS is non-degenerate.*

As for the set of uniqueness, in most cases it has positive Hausdorff dimension as well. The precise claim can be found in [6, Theorem 2.5].

References

[1] D. Calegari, S. Koch and A. Walker, *Roots, Schottky Semigroups, and a proof of Bandt's Conjecture*, Ergodic Theory Dynam. Systems, to appear.

[2] K. Dajani, K. Jiang and T. Kempton, *Self-affine sets with positive Lebesgue measure*, Indag. Math. **25** (2014), 774–784.

[3] C. S. Güntürk, *Simultaneous and hybrid beta-encodings*, in Information Sciences and Systems, 2008. CISS 2008. 42nd Annual Conference on, pages 743–748, 2008.

[4] K. G. Hare and N. Sidorov, *On a family of self-affine sets: topology, uniqueness, simultaneous expansions*, Ergodic Theory Dynam. Systems, to appear.

[5] K. G. Hare and N. Sidorov, *Two-dimensional self-affine sets with interior points, and the set of uniqueness*, Nonlinearity **29** (2016), 1–26.

[6] K. G. Hare and N. Sidorov, *Multidimensional self-affine sets: non-empty interior and the set of uniqueness*, Studia Math. **229** (2015), 223–232.

[7] N. Sidorov, *Combinatorics of linear iterated function systems with overlaps*, Nonlinearity **20** (2007), 1299–1312.

[8] B. Solomyak, *Connectedness locus for pairs of affine maps and zeros of power series*, J. Fractal Geom. **2** (2015), 281–308.

Normality of Different Orders for the Cantor Series Expansions

Dylan Airey[(1)], Bill Mance[(2)]

[(1)] University of Texas, Austin, Texas, United States

[(2)] Polish Academy of Sciences, Warsaw, Poland

Let $\mathbb{N} = A \cup B$ be a partition of the natural numbers. We prove that if A is sufficiently close to being a subsemigroup, then there exists a basic sequence Q where the set of numbers that are Q-normal of all orders in A and not Q-normal of any orders in B is non empty. Furthermore, these sets will have full Hausdorff dimension under some additional conditions. This stands in sharp contrast to the fact that if a real number is normal of order k for the b-ary expansion, then it is also normal of all orders less than k.

Topological Transitivity and Entropy of Unique β-Expansions

Rafael Alcaraz Barrera[1], Simon Baker[2], Derong Kong[3]

[1] Institute of Mathematics and Statistics, University of São Paulo, Brazil

[2] Department of Mathematics and Statistics, University of Reading, U.K.

[3] School of Mathematical Science, Yangzhou University, China

After their introduction during the late 1950's by Rényi and Parry, expansions in non integer bases, colloquially known as β-expansions, have been actively studied. Possibly, the most interesting feature of these representations is the fact that they are not always unique. Also the univoque set $\mathcal{U}_\beta$, i.e. the set of points with a unique β-expansion, has been particularly well studied.

In this talk we present some results concerning the topological entropy of $\mathcal{U}_\beta$ and the topological dynamics of the following subshift: Let $\beta \in (M, M+1)$ with $M \in \mathbb{N}$, let $\alpha(\beta)$ be the quasi-greedy expansion of 1 in base β and let $\overline{x}$ is the reflection of a sequence x. Set $(\mathcal{V}'_\beta, \sigma)$ be the subshift given by

$$\mathcal{V}'_\beta = \left\{ x \in \Sigma_{M+1} : \overline{\alpha(\beta)} \preccurlyeq \sigma^j(x) \preccurlyeq \alpha(\beta) \text{ for every } j \geq 0 \right\}.$$

In particular, we characterise the set of β's in $(M, M+1)$ such that $(\mathcal{V}'_\beta, \sigma)$ is a transitive subshift using the symbolic properties of the quasi-greedy expansion of 1. We also study the function $H : [M, M+1] \to [0, \log(M+1)]$ given by $H(\beta) = h_{top}(\mathcal{U}_\beta)$. Using the notion of n-irreducible sequences, we characterise the intervals $[p, q] \subset (M, M+1]$ such that for every $\beta \in [p, q]$, $h_{top}(\mathcal{U}_\beta) = h_{top}(\mathcal{U}_p)$ and the set

$$\mathcal{E} = \{\beta \in [M, M+1] : H \text{ is not differentiable at } \beta\}.$$

Strongly q-Additive Functions and Largest Prime Factor of an Integer

Myriam Amri[*]

Sfax University, Tunisia

For every positive integer n, let $P(n)$ the largest prime factor of n, with the usual convention that $P(1) = 1$. The problem of the distribution of the largest prime factor in congruences classes has been previously considered by Ivič and Oon for a fixed modulus k. Using a similar approach to that of Ivič, Banks, Harman and Shparlinski obtained new bounds that are non-trivial for a wide range of values of the parameter k: in particular, if k is not too large relative to x, they derived the expected asymptotic formula:

$$\sharp\{n \le x,\ P(n) \equiv l \mod k\} \sim \frac{x}{\varphi(k)},$$

with an explicit error term that is independent of l. Moreover, by bounding of the exponential sum $\sum_{n\le x} e\big(\alpha P(n)\big)$ for a fixed irrational real number α, they deduced that the sequence $\{\alpha P(n),\ n \ge 1\}$ is uniformly distributed modulo 1, which is a reminiscent of the classical theorem of Vinogradov asserting that for a fixed irrational real number α, the sequence $\{\alpha p,\ p \text{ prime}\}$ is uniformly distributed modulo 1.

The main goal of our work is to provide asymptotic expansions for the cardinals of $\mathcal{A}(x) = \{n \le x, f\big(P(n)\big) \equiv a \mod b\}$ and $\mathcal{B}(x) = \{n \le x;\ P(n) \equiv k \mod l,\ f(P(n) + c) \equiv a \mod b\}$ where f is a strongly q-additive function, $b \ge 2$ and $a, c \in \mathbb{Z}$. (i.e. $f(sq^j + t) = f(a) + f(b)$, with $(s,t,j) \in \mathbb{N}^3, 0 \le t < q^j$). We also show that, for an irrational number α, the sequence $\{\alpha P(n), n \ge 1, f\big(P(n)\big) \equiv a \mod b\}$ is equidistributed modulo 1, for every $a \in \mathbb{Z}$.

To finish, we consider some sums involving $P(n)$ such as giving an asymptotic formula for the summatory fonctions of $P(n)$ where $n \in \mathcal{A}(x)$ and $\frac{1}{P^r(n)}$ with $n \in \{n \le x,\ f(P(n)) \equiv a \mod b,\ P(n) \equiv l \mod k\}$, for $r > 0$.

[*]Supported by Mohamed Mkaouar and Walid Wannes.

Unique Expansions and Intersections of Cantor Sets

Simon Baker

Department of Mathematics and Statistics, University of Reading

Given a Cantor set C, one can study the intersection of C with a translated copy of itself. It is natural to ask what are the properties of this intersection. In this talk I will discuss some recent work with Derong Kong where we successfully apply ideas from expansions in non-integer bases to this problem. Our results rely on a digit frequency argument and properties of a generalised Thue-Morse sequence.

Eventually Periodic Representations in Positional Number Systems*

Simon Baker(1), Zuzana Masáková(2), Edita Pelantová(2), Tomáš Vávra(2)

(1) Department of Mathematics and Statistics, University of Reading

(2) Department of Mathematics FNSPE, Czech Technical University in Prague

We study periodic expansions in positional number systems with a base $\beta \in \mathbb{C}$, $|\beta| > 1$, and with coefficients in a finite set of digits $\mathcal{A} \subset \mathbb{C}$. We are interested in determining those algebraic bases for which there exists $\mathcal{A} \subset \mathbb{Q}(\beta)$, such that all elements of $\mathbb{Q}(\beta)$ admit at least one eventually periodic representation with digits in $\mathcal{A}$. In this paper we prove a general result that guarantees the existence of such an $\mathcal{A}$. This result implies the existence of such an $\mathcal{A}$ when β is a rational number or an algebraic integer with no conjugates of modulus 1.

We also consider periodic representations of elements of $\mathbb{Q}(\beta)$ for which the maximal power of the representation is proportional to the absolute value of the represented number, up to some universal constant. We prove that if every element of $\mathbb{Q}(\beta)$ admits such a representation then β must be a Pisot number or a Salem number. This result generalises a well known result of Schmidt [5].

1 Positional representation of numbers

For $\beta \in \mathbb{C}, |\beta| > 1$ and a finite set $\mathcal{A} \subset \mathbb{C}$ we call the expression $x = \sum_{i=-L}^{+\infty} a_i\beta^{-i}$ a $(\beta, \mathcal{A})$-representation of x. Representations of the elements of $[0, 1)$ in the form $\sum_{i\geq 1} a_i\beta^{-i}$ for arbitrary real base $\beta > 1$ was introduced by Rényi in [4]. He considered the *greedy expansions*, a case when the sequence $(a_i)_{i\leq 1}$ is lexicographicaly biggest amongst all the $(\beta, \mathcal{A})$-representations with the alphabet $\mathcal{A} = \{a \in \mathbb{Z} \ : \ 0 \leq a < \beta\}$. Numbers whose coefficient sequence is eventually periodic are of special interest and they were studied by Schmidt [5] in 1980. Schmidt showed that if all the elements of $\mathbb{Q}(\beta) \cap [0, 1)$ have eventually periodic greedy expansion, then β is a Pisot or a Salem number.

Definition 1. A Pisot number is an algebraic integer $\beta > 1$ whose conjugates are < 1 in absolute value.

A Salem number is an algebraic integer $\beta > 1$ whose conjugates are ≤ 1 in absolute value, and at least one of them is equal to 1 in absolute value.

A complex Pisot number is an algebraic integer $\beta \in \mathbb{C} \setminus \mathbb{R}, |\beta| > 1$ whose conjugates except for the complex conjugate are < 1 in absolute value.

*This work was supported by the Czech Science Foundation, grant No. 13-03538S. We also acknowledge financial support of the Grant Agency of the Czech Technical University in Prague, grant No. SGS14/205/OHK4/3T/14.

As for the converse, it has been proved in the same paper that the greedy expansions of the elements of $\mathbb{Q}(\beta)\cap[0,1)$ are eventually periodic whenever β is a Pisot number. Moreover, it was conjectured that the Salem numbers share this property. This conjecture, however, remains unproved for any instance of a Salem base.

2 Periodic representations

A way to percieve Schmidt's result is that for β Pisot number there is an alphabet (for example take $\mathcal{A} = \{a \in \mathbb{Z} \ : \ 0 \le |a| < \beta\}$) such that every element of $\mathbb{Q}(\beta)$ has an eventually periodic $(\beta,\mathcal{A})$-representation. Our aim is to investigate which other bases have this property.

For a fixed $\mathcal{A} \subset \mathbb{C}$, let us define the set of numbers that admit a finite and an eventually periodic $(\beta,\mathcal{A})$-representation respectively.

$$\begin{aligned} Fin_{\mathcal{A}}(\beta) &= \Big\{ \sum_{k\in I} a_k\beta^{-k} : I \subset \mathbb{Z},\ I \text{ finite},\ a_k \in \mathcal{A} \Big\}\,, \\ Per_{\mathcal{A}}(\beta) &= \Big\{ \sum_{k\ge -L} a_k\beta^{-k} : L \in \mathbb{Z},\ a_k \in \mathcal{A},\ (a_i)_{i\ge -L} \text{ eventually periodic} \Big\}\,. \end{aligned}$$

Then the Schmidt's result can be reformulated as $\mathbb{Q}(\beta) = \mathrm{Per}_{\mathcal{A}}(\beta)$ for some $\mathcal{A}$. Note that if this equality holds, then necessarily $\mathcal{A} \subset \mathbb{Q}(\beta)$. In fact, it is not difficult to show that it suffices to consider $\mathcal{A} \subset \mathbb{Z}$.

When β has no conjugate on the unit circle, the number system allows parallel addition in some alphabet, see [3]. Roughly speaking, the digits of the sum of two numbers can be computed from the digit-wise sum only by processing a bounded neigborhood of their positions. This turns out to be a crucial instrument simplifying the study of the structure of $Fin_{\mathcal{A}}(\beta)$ and $Per_{\mathcal{A}}(\beta)$.

Proposition 2. *Let $\beta \in \mathbb{C}$, $|\beta| > 1$, and let $\mathcal{A}$ be a symmetric alphabet such that $(\beta,\mathcal{A})$ allows parallel addition. Then*

1. *$Fin_{\mathcal{A}}(\beta) \subset Per_{\mathcal{A}}(\beta)$;*
2. *$Fin_{\mathcal{A}}(\beta)$, $Per_{\mathcal{A}}(\beta)$ are closed under addition and subtraction;*
3. *$Fin_{\mathcal{A}}(\beta)$ is closed under multiplication;*
4. *$Fin_{\mathcal{A}}(\beta) \cdot Per_{\mathcal{A}}(\beta) \subset Per_{\mathcal{A}}(\beta)$;*
5. *$Fin_{\mathcal{A}}(\beta) = \mathbb{Z}[\beta,\beta^{-1}]$.*

Proposition 2 is an important ingredient to the following theorem presenting a sufficient condition for the existence of $\mathcal{A}$ such that $\mathbb{Q}(\beta) = \mathrm{Per}_{\mathcal{A}}(\beta)$.

Theorem 3. *Let $\beta \in \mathbb{C}$ be an algebraic number of degree d, $|\beta| > 1$, and let $a_dx^d - a_{d-1}x^{d-1} - \cdots - a_1x - a_0 \in \mathbb{Z}[x]$ be its minimal polynomial. Suppose that*

1. *$|\beta'| \ne 1$ for any conjugate β' of β;*

2. $1/a_d \in \mathbb{Z}[\beta, \beta^{-1}]$.

Then there exists a finite alphabet $\mathcal{A} \subset \mathbb{Z}$ *such that* $\mathbb{Q}(\beta) = Per_{\mathcal{A}}(\beta)$.

The assumption of Theorem 3 is satisfied for example by algebraic integers (without a conjugate on the unit circle) or by rational numbers. The complete classification can be derived from the following.

Theorem 4. *Let* β, $|\beta| > 1$, *be an algebraic number with minimal polynomial* $f(x) = \sum_{i=0}^{d} a_i x^i \in \mathbb{Z}[\beta]$, $\gcd(a_0, \ldots, a_d) = 1$, *and let* $n \in \mathbb{N}$, $n \geq 2$.

Then $1/n \in \mathbb{Z}[\beta, \beta^{-1}]$ *if and only if its prime factorization is* $n = \prod_{1 \leq k \leq m} p_k^{\alpha_k}$, $\alpha_k \geq 1$, *where each* p_k *divides* a_i *for all* $i \in \{0, \ldots, d\}$ *but one (possibly different for each* k*).*

Although these are the only bases known to posses the property $\mathbb{Q}(\beta) = \mathrm{Per}_{\mathcal{A}}(\beta)$ for some $\mathcal{A}$, computational experiments suggest that all algebraic bases without a conjugate on the unit circle have this property.

3 Weak greedy representations

Consider the base $\beta = \sqrt{5}$ and $\mathcal{A} = \{0, \pm 1, \pm 2\}$. Then every $x_1 + x_2\sqrt{5} \in \mathbb{Q}(\beta)$, $x_1, x_2 \in \mathbb{Q}$, has an eventually periodic $(\beta, \mathcal{A})$-representation. Indeed, x_1, x_2 have eventually periodic (greedy) representation in base $\gamma = 5$, say $x_1 = \sum_{k \geq -L_1} b_k 5^{-k}$, $x_2 = \sum_{k \geq -L_2} c_k 5^{-k}$. Together, we can write

$$x = \sum_{k \geq -L_1} b_k \beta^{-2k} + \sum_{k \geq -L_2} c_k \beta^{-2k+1}.$$

The resulting representation of x in base β is also eventually periodic. Moreover, one can choose a sequence $(x_1^{(n)}, x_2^{(n)})$ such that $x_1^{(n)} \to +\infty$, $x_2^{(n)} \to +\infty$ and $x^{(n)} = x_1^{(n)} + x_2^{(n)}\sqrt{5} \to 0$ as n tends to $+\infty$. If $(\beta, \mathcal{A})$-representations of $x^{(n)}$ are constructed as above, one can see that "great powers of the base are used in representations of small numbers". This leads us to the following definition.

Definition 5. Given $\beta \in \mathbb{C}$, $|\beta| > 1$, $\mathcal{A} \subset \mathbb{Q}(\beta)$, and $c > 0$, we say that a sequence $(a_k)_{k=-L}^{\infty}$ is a weak greedy $(\beta, \mathcal{A})$-representation for x with respect to c if $x = \sum_{k \geq -L} a_k \beta^{-k}$ and $|x| \geq c|\beta|^L$.

Of course, the definition is of interest only if the constant c is universal. Therefore we will further assume that c is common for all the elements of $\mathbb{Q}(\beta)$.

Our interest now is a description of bases that allow weak greedy eventually periodic $(\beta, \mathcal{A})$-representations. It has been already known that if β or $-\beta$ is a Pisot number, then $\mathbb{Q}(\beta)$ admits eventually periodic weak greedy representations. This fact is due to Schmidt for $\beta > 1$, and Frougny & Lai for $\beta < -1$, see [2]. It turns out that this is also true for complex Pisot bases.

Theorem 6. *For a base* β*, which is Pisot, complex Pisot, or the negative of a Pisot number, one can find an alphabet* $\mathcal{A} \subset \mathbb{Z}$ *and* $c > 0$ *so that every* $x \in \mathbb{Q}(\beta)$ *has eventually periodic weak greedy* $(\beta, \mathcal{A})$*-representation with respect to* c.

On the other hand, the weak greedy condition is rather a strong assumption.

Proposition 7. *Let $\beta \in \mathbb{C}$, $|\beta| > 1$, be such that there exists $\mathcal{A} \subset \mathbb{Q}(\beta)$ and $c > 0$ such that that every element of $\mathbb{Q}(\beta)$ has an eventually periodic weak greedy $(\beta, \mathcal{A})$-representation with respect to c. Then β is an algebraic integer such that for every conjugate β' of β it holds that $|\beta'| = |\beta|$ or $|\beta'| \leq 1$.*

The following theorem is an application of the result of Ferguson [1] to Proposition 7.

Theorem 8. *Given $\beta \in \mathbb{R}$, $|\beta| > 1$. Suppose there exists a finite alphabet $\mathcal{A} \subset \mathbb{Q}(\beta)$ and a constant $c > 0$ such that every $x \in \mathbb{Q}(\beta)$ has an eventually periodic weak greedy $(\beta, \mathcal{A})$-representation with respect to c. Then $|\beta|$ is a Pisot number or a Salem number.*

References

[1] Ronald Ferguson. Irreducible polynomials with many roots of equal modulus. *Acta Arith.*, 78(3):221–225, 1997.

[2] Christiane Frougny and Anna Chiara Lai. Negative bases and automata. *Discrete Math. Theor. Comput. Sci.*, 13(1):75–93, 2011.

[3] Christiane Frougny, Edita Pelantová, and Milena Svobodová. Parallel addition in non-standard numeration systems. *Theoret. Comput. Sci.*, 412(41):5714–5727, 2011.

[4] Alfred Rényi. Representations for real numbers and their ergodic properties. *Acta Math. Acad. Sci. Hungar*, 8:477–493, 1957.

[5] Klaus Schmidt. On periodic expansions of Pisot numbers and Salem numbers. *Bull. London Math. Soc.*, 12(4):269–278, 1980.

Kneading Sequences, Bernoulli Convolutions, and β-Expansion

Christoph Bandt

University of Greifswald, Germany

We present a two-dimensional density of all Bernoulli convolutions with $\beta \in (1,2)$. This density exists by a theorem of Solomyak. Computer visualizations show a remarkable structure which is connected with results by Allouche, Clarke and Sidorov, Komornik and de Vries, and others. The basic space is the set of all (t,y) where $\frac{1}{2} < t = 1/\beta < 1$ and $y \in [0,1]$.

A 01-sequence $b_1b_2...$ and the corresponding binary number $b = .b_1b_2...$ is called kneading sequence with respect to the map $g(y) = 2y \mod 1$ if no number $g^(k)(b) = .b_kb_{k+1}...$ with $k = 1,2,...$ is nearer to $\frac{1}{2}$ than b. The corresponding kneading functions $y(t) = \sum_{k=1}^{\infty} b_kt^k$ were introduced by Thurston and Milnor in the 1980s. In the two-dimensional Bernoulli density, they show up very clearly as parallel curves of low density. They transfer the 'Feigenbaum diagram' of one-dimensional dynamics to the Bernoulli scenario.

While Bernoulli convolutions can be interpreted as a multivalued β-representation, the intersections of the kneading functions with $y = 1 - t$ and $y = \frac{1}{2}$ define the greedy and symmetric β-representations, and topological entropy. The focus of the talk will be on intersections of pairs of these curves, with $b_1 = 0$ and $b_1 = 1$, in particular those pairs which express certain singularities of the Bernoulli measures. The landmark parameters $\beta = 1/t$ will be not only Pisot numbers, but Perron numbers, as indicated by a theorem of Thurston.

Rauzy's Tilings in the Light of Uniform Distribution; the Case $+\beta$ and the Case $-\beta$

Anne Bertrand-Mathis

LMA, CNRS UMR 7348, Université de Poitiers, France

Many of you know the β shift X_β who allows to write real numbers belonging to $[0,1]$ in basis β; Ito and Sadahiro recently explain how to write real numbers of $\left[\frac{-\beta}{\beta+1}, \frac{1}{\beta+1}\right]$ in basis $-\beta$. The methods are exactly the sames: iterating the transformation $x \to \beta x \mod 1$ (resp. $x \to -\beta x \mod 1$ we obtain an expansion $x = \sum_{n\geq 1} \frac{x_n}{\beta^n}$ (resp. $x = \sum_{n\geq 1} \frac{x_n}{(-\beta)^n}$). We call β shift and denote X_β^{right} (resp. $-\beta$ shift $X_{-\beta}^{right}$) the set of sequences $(x_n)_{n\in\mathbb{Z}}$ who are the expansion of a number x in basis β (resp. $-\beta$). The bilateral shifts X_β and $X_{-\beta}$ are their natural extensions (more precisly the two shifts $X_{\pm\beta}$ are the cloture of these sets). In all cases the sequences belonging to the shifts are caracterized by inequalities. Unfortunately the order relation used in the $-\beta$ shift is rather awful but don't worry, we can do without: we are interested in Pisot basis and then both dynamical systems $X_{\pm\beta}$ shall be sofic ones, so they have a very classical feature.

Let β be a Pisot number of degree d and g his minimal polynomial; β has $d-1$ conjugates $\alpha_2, \ldots, \alpha_d$ who verify $|\alpha_i| < 1$. So all the traces $\mathrm{Tr}\beta^n = \beta^n + \alpha_2^n + \cdots + \alpha_d^n$ of β^n are in $\mathbb{Z}$ and modulo one $\beta^n = -(+\alpha_2^n + \cdots + \alpha_d^n)$. The vectors $V_\beta = \frac{1}{g'(\beta)} \begin{pmatrix} \beta^{d-1} \\ \beta^{d-2} \\ \vdots \\ 1 \end{pmatrix}$ and his $d-1$ conjugates $V_{\alpha_i} = \frac{1}{g'(\alpha_i)} \begin{pmatrix} \alpha^{d-1} \\ \alpha^{d-2} \\ \vdots \\ 1 \end{pmatrix}$ for $i = 2, \ldots, d$ form a basis of $\mathbb{R}^d$; they are eigenvectors of the companion matrix of β. Define a map from X_β into $\mathbb{R}^d$:

$$F\left((x_n)_{n\in\mathbb{Z}}\right) = \left(\sum_{n>0} \frac{x_n}{\beta^n}\right) V_\beta - \left(\sum_{n\leq 0} x_n \alpha_2^{|n|}\right) V_{\alpha_2} - \cdots - \left(\sum_{n\leq 0} x_n \alpha_d^{|n|}\right) V_{\alpha_d}$$

F is a continuous map and X_β is compact: then the image is a compact set $\mathcal{M}_\beta$, it is the "Rauzy's Pavé". He has a nonempty interior because the sequence $\begin{pmatrix} x\beta^{n+d-1} \\ \vdots \\ x\beta^n \end{pmatrix}_{n\geq 0}$ is uniformly distributed modulo one for somes x.

Changing β in $-\beta$ we can do exactly the same thing to obtain $\mathcal{M}_{-\beta}$ (change β in $-\beta$ and α_i in $-\alpha_i$).

Let H_α the vector space spinned by $V_{\alpha_2}, \ldots, V_{\alpha_d}$; let F_α be the map from X_β into H_α:

$$F_\alpha\left((x_n)_{n\leq 0}\right) = -\left(\sum_{n\leq 0} x_n \alpha_2^{|n|}\right) V_{\alpha_2} - \cdots - \left(\sum_{n\leq 0} x_n \alpha_d^{|n|}\right) V_{\alpha_d}$$

The image $\mathcal{T}_\alpha = F_\alpha\left(X_\beta\right)$ is the Rauzy's fractale. $\mathcal{T}_\alpha$ is compact (F_α is continue) and has nonempty interior as $\mathcal{M}_{-\beta}$. Of course you can do exactly the same thing with $X_{-\beta}$, changing β in $-\beta$ and α_i in $-\alpha_i$.

The tile $\mathcal{T}_\alpha$ (or $\mathcal{T}_{-\alpha}$) is the countable union of similar small tiles. Suppose that β is unimodular ($|\beta\alpha_2 \cdots \alpha_d| = 1$); combining the efforts of both Lebesgue and Parry mesures we can prove that the small tiles are disjoints in measure and that $\mathcal{T}_\alpha$ has a frontier of null measure. The results concerning the case $-\beta$ are exactly the sames altough you have to work harder to obtain them: the $-\beta$ shift is not so simple as the β shift who remains the most efficace shift for a given entropy, with a very simple language.

The translates of $\mathcal{M}_\beta$(resp. $\mathcal{M}_{-\beta}$) give a multiple translation tiling of $\mathbb{R}^d$; a certain set of special smaller tiles form an autosimilar tiling of H_α (resp. $H_{-\alpha}$) of the same multiplicity.

There is also translation tiling of $H_{-\alpha}$ as in $+\beta$ case but we do not found a "Weyl-Shannon" method for him. It required to write relative numbers in basis $-\beta$ and is rather related to $-\beta$ substitution and Kronecker's theorem.

Remark: if $\beta < \frac{1+\sqrt{5}}{2}$ (they are 38 Pisot numbers between 1 and $\beta < \frac{1+\sqrt{5}}{2}$) the $-\beta$ shift is not transitive; they are words who can appears at the beginning of an expansion but not after; in this case we replace $X_{-\beta}$ by the set $X^\star_{-\beta}$ of sequences not beginning by these words; $X_{-\beta}/X^\star_{-\beta}$ has null measure and $X^\star_{-\beta}$ is still a sofic system; nothing is to change in proofs but $\mathcal{M}_{-\beta}$ is not connected.

Reconstruction of Matrix-Based Numeration Systems from Some Expansions

Dávid Bóka, Péter Burcsi

Eötvös Loránd University, Hungary

Consider a matrix-based numerations system (M, D), where M is a integer matrix of size $n \times n$ with non-zero determinant, D is a set of cardinality $|\det M|$ containing integer column vectors of size n, one of which is the origin. A finite expansion in base M with digits in D is a sum of the form $\overline{d_k d_{k-1} \dots d_1 d_0}_M := \sum_{j=0}^{k} M^j d_j$, where $d_j \in D$ and $d_k \neq 0$. We investigate the following problem: if we are promised that for an unknown pair (M, D), every vector in $\mathbb{Z}^n$ has a finite expansion, can we reconstruct M and D (at least up to some kind of "topological conjugacy") if we know the expansion of $d + d'$ for all pairs (d, d') from D. As an example, consider a ternary system with digits $(0, a, b)$, having expansions $a + a = \overline{bbb}_M$, $a + b = \overline{ba00}_M$ and $b + b = \overline{baa}_M$. Can we tell what dimension we are in, what the matrix M is, and what the digits are?

We address the problem by defining numeration systems abstractly from the expansion of pairwise digit sums and investigating properties of such systems. We show some reconstruction methods, present computational experiments for small digit sets and pose open questions.

On-line Mutliplication and Division in Number Systems with Complex Bases

Marta Brzicová[(1)], Christiane Frougny[(2)],
Edita Pelantová[(1)], Milena Svobodová[(1)]

[(1)] FNSPE, Czech Technical University in Prague, Czech Republic

[(2)] IRIF, UMR 8243 CNRS and Université Paris-Diderot, France

A positional numeration system is given by a base and by a set of digits. The base is a real or complex number β such that $|\beta| > 1$, and the digit set $\mathcal{A}$ is a finite set of real or complex digits including 0. We formulate a generalized version of the on-line algorithms for multiplication and division of Trivedi and Ercegovac and define the (OL) Property which guarantees that both algorithms are applicable in the system $(\beta, \mathcal{A})$. We show that for any base $\beta \in \mathbb{C}$ there exists an integer $a > 0$ such that, with $\mathcal{A} = \{-a, \ldots, -1, 0, 1 \ldots, a\} \subset \mathbb{Z}$, the numeration system $(\beta, \mathcal{A})$ has the (OL) Property. Provided that addition and subtraction are realizable in parallel in the system $(\beta, \mathcal{A})$, our on-line algorithms for multiplication and division have linear time complexity. As on a redundant alphabet zero may have a non-trivial representation, we discuss also the preprocessing of divisors as input of the on-line algorithm. Three examples connected to the Gaussian and Eisentein integers are presented in detail: base $\beta = i - 1$ with alphabet $\mathcal{A} = \{-2, -1, 0, 1, 2\}$, base $\beta = i - 1$ with alphabet $\mathcal{A} = \{0, \pm 1, \pm \imath\}$, and base $\beta = -\frac{3}{2} + \imath\frac{\sqrt{3}}{2} = -1 + \omega$, where $\omega = \exp\frac{2i\pi}{3}$, with alphabet $\mathcal{A} = \{0, \pm 1, \pm\omega, \pm\omega^2\}$.

Permutations and Negative Beta-Shifts

Émilie Charlier[(1)], Wolfgang Steiner[(2)]

[(1)] Institute of Mathematics, University of Liège

[(2)] IRIF, CNRS, Université Paris Diderot – Paris 7

The complexity of a dynamical system is usually measured by its entropy. For symbolic dynamical systems, the (topological) entropy is the logarithm of the exponential growth rate of the number of distinct patterns of length n. Bandt, Keller and Pompe [3] proved for piecewise monotonic maps that the entropy is also given by the number of permutations defined by consecutive elements in the trajectory of a point. Amigo, Elizalde and Kennel [1, 4] studied realizable permutations in full shifts in detail. Elizalde [5] extended this study to β-shifts (with $\beta > 1$), and he determined for each permutation the infimum of those bases β where successive elements of the β-shift are ordered according to the permutation. Archer and Elizalde [2] considered periodic patterns for full shifts with different orderings. We are interested in β-shifts with $\beta < -1$, which are ordered naturally by the alternating lexicographical order. Similarly to [5], we determine the set of $(-\beta)$-shifts allowing a given permutation. Our main results were obtained independently by Elizalde and Moore [6].

For an ordered space X, a map $f: X \to X$, a positive integer n, a point $x \in X$ such that $f^i(x) \neq f^j(x)$ for all $0 \le i < j < n$, and a permutation $\pi \in \mathcal{S}_n$, let

$$\mathrm{Pat}(x, f, n) = \pi \quad \text{if } \pi(i) < \pi(j) \text{ for all } 1 \le i, j \le n \text{ with } f^{i-1}(x) < f^{j-1}(x).$$

The set of allowed patterns of f is

$$\mathcal{A}(f) = \big\{\mathrm{Pat}(x, f, n) : x \in X, n > 0\big\}.$$

Here, we are interested in the $(-\beta)$-transformation for $\beta > 1$, which was defined by Ito and Sadahiro [7] as $x \mapsto \lfloor \frac{\beta}{\beta+1} - \beta x \rfloor - \beta x$ on the interval $[\frac{-\beta}{\beta+1}, \frac{1}{\beta+1})$. It is more convenient to consider the map

$$T_{-\beta}: (0,1] \to (0,1], \quad x \mapsto \lfloor \beta x \rfloor + 1 - \beta x,$$

which is easily seen to be topologically conjugate to Ito and Sadahiro's one, via $x \mapsto \frac{1}{\beta+1} - x$ (which reverses the order). Theorem 1 below gives a formula for

$$B(\pi) = \inf\big\{\beta > 1 : \pi \in \mathcal{A}(T_{-\beta})\big\}.$$

To $\pi \in \mathcal{S}_n$, associate the circular permutation

$$\hat{\pi} = \big(\pi(1)\pi(2)\cdots\pi(n)\big) \in \mathcal{S}_n,$$

i.e., $\hat{\pi}(\pi(j)) = \pi(j+1)$ for $1 \le j < n$, $\hat{\pi}(\pi(n)) = \pi(1)$, and the sequence of digits $z_{[1,n)}$ defined by

$$\begin{aligned} z_j = \#\{1 \le i < \pi(j) : \; & i \neq \pi(n) \neq i+1 \text{ and } \hat{\pi}(i) < \hat{\pi}(i+1), \\ & \text{or } i = \pi(n) - 1 \text{ and } \hat{\pi}(i) < \hat{\pi}(i+2)\}. \end{aligned}$$

Moreover, let

$$m = \pi^{-1}(n), \quad \ell = \pi^{-1}(\pi(n)-1) \text{ if } \pi(n) \neq 1, \quad r = \pi^{-1}(\pi(n)+1) \text{ if } \pi(n) \neq n.$$

We use the abbreviation $z_{[i,j)} = z_i z_{i+1} \cdots z_{j-1}$ for $i \le j$. When

$$z_{[\ell,n)} = z_{[r,n)} z_{[r,n)} \quad \text{or} \quad z_{[r,n)} = z_{[\ell,n)} z_{[\ell,n)}, \quad \text{if } \pi(n) \notin \{1,n\}, \tag{1}$$

we also use the following digits, for $0 \le i < |r-\ell|$, $1 \le j < n$,

$$z_j^{(i)} = z_j + \begin{cases} 1 & \text{if } \pi(j) \ge \pi(r+i) \text{ and } i \text{ is even, or } \pi(j) \ge \pi(\ell+i) \text{ and } i \text{ is odd,} \\ 0 & \text{otherwise.} \end{cases}$$

Now, we can define a sequence $a = a_1 a_2 \cdots$ associated to the permuation π by

$$a = \begin{cases} z_{[m,n)}\, \overline{z_{[\ell,n)}} & \text{if } n-m \text{ is even, } \pi(n) \neq 1, \text{ and (1) does not hold,} \\ \min_{0 \le i < |r-\ell|} z^{(i)}_{[m,n)}\, \overline{z^{(i)}_{[\ell,n)}} & \text{if } n-m \text{ is even, } \pi(n) \neq 1, \text{ and (1) holds,} \\ \overline{z_{[m,n)} 0} & \text{if } n-m \text{ is even and } \pi(n) = 1, \\ z_{[m,n)}\, \overline{z_{[r,n)}} & \text{if } n-m \text{ is odd and (1) does not hold,} \\ \min_{0 \le i < |r-\ell|} z^{(i)}_{[m,n)}\, \overline{z^{(i)}_{[r,n)}} & \text{if } n-m \text{ is odd and (1) holds.} \end{cases}$$

Here and in the following, $\overline{w}$ denotes the periodic sequence with period w, and sequences are ordered by the alternating lexicographical order, i.e., $v_1 v_2 \cdots < w_1 w_2 \cdots$ if $v_1 \cdots v_k = w_1 \cdots w_k$ and $(-1)^k v_{k+1} < (-1)^k w_{k+1}$, $k \ge 0$. (Ito and Sadahiro [7] used an "alternate order", which is the inverse of our order.)

Theorem 1. *Let $\pi \in \mathcal{S}_n$. Then $B(\pi)$ is the largest positive root of* $1 + \sum_{k=1}^{\infty} \frac{a_k+1}{(-x)^k} = 0$.

Note that $B(\pi)$ is the largest positive solution of the equation

$$(-x)^{p+q} + \sum_{k=1}^{p+q} (a_k+1)\,(-x)^{p+q-k} = (-x)^q + \sum_{k=1}^{q} (a_k+1)\,(-x)^{q-k}$$

when a is eventually periodic with preperiod of length q and period of length p.

Let φ be the substitution defined by $\varphi(0) = 1$, $\varphi(1) = 100$, with the unique fixed point $u = \varphi(u)$, i.e.,

$$u = 1001110010010011110011 \cdots .$$

Theorem 2. *Let $\pi \in \mathcal{S}_n$. We have $B(\pi) = 1$ if and only if $a = \overline{\varphi^k(0)}$ for some $k \ge 0$.*

If $B(\pi) > 1$, i.e., $a > u$, then $B(\pi)$ is a Perron number by [8, 9].

Instead of numbers $x \in (0,1]$, we can also consider their $(-\beta)$-expansions

$$x = -\sum_{k=1}^{\infty} \frac{d_{-\beta,k}(x)+1}{(-\beta)^k} \text{ with } d_{-\beta,k}(x) = \left\lfloor \beta\, T_{-\beta}^{k-1}(x) \right\rfloor.$$

Set $d_{-\beta}(x) = d_{-\beta,1}(x)d_{-\beta,2}(x)\cdots$. By [7], have $x < y$ if $d_{-\beta}(x) < d_{-\beta}(y)$ (w.r.t. the alternating lexicographical order), thus

$$\mathrm{Pat}(x, T_{-\beta}, n) = \mathrm{Pat}(d_{-\beta}(x), \Sigma, n),$$

where Σ denotes the shift map. For the proof of Theorem 1, infinite words w satisfying $\mathrm{Pat}(w, \Sigma, n) = \pi$ and lying in the $(-\beta)$-shift for all $\beta > B(\pi)$ are constructed. Note that, for an integer $N \geq 2$, the $(-N)$-shift is close to the full shift on N letters.

Theorem 3. *Let $\pi \in \mathcal{S}_n$. The minimal number of letters of an infinite word w satisfying $\mathrm{Pat}(w, \Sigma, n) = \pi$ (w.r.t. the alternating lexicographical order) is*

$$N(\pi) = 1 + \lfloor B(\pi) \rfloor = 1 + \mathrm{asc}(\hat{\pi}) + \begin{cases} 1 & \text{if (1) holds or } a = \overline{\mathrm{asc}(\hat{\pi})0}, \\ 0 & \text{otherwise,} \end{cases}$$

where $\mathrm{asc}(\hat{\pi})$ denotes the number of ascents in $\hat{\pi}$ with $\hat{\pi}(\pi(n)) = \pi(1)$ removed. We have $N(\pi) \leq n - 1$ for all $\pi \in \mathcal{S}_n$, $n \geq 3$, with equality for $n \geq 4$ if and only if

$$\pi \in \{12\cdots n,\ 12\cdots(n{-}2)n(n{-}1),\ n(n-1)\cdots 1,\ n(n-1)\cdots 312\}.$$

In Table 1, we give the values of $B(\pi)$ for all permutations of length up to 4, and we compare them with the values obtained by [5] for the (positive) beta-shift. We see that much more permutations satisfy $B(\pi) = 1$ for the negative beta-shift than for the positive one. Some other examples, together with corresponding infinite words are below.

$B(\pi)$	root of	π, negative beta-shift	π, positive beta-shift
1	$\beta - 1$	$12, 21$ $123, 132, 213, 231, 321$ $1324, 1342, 1432, 2134$ $2143, 2314, 2431, 3142$ $3214, 3241, 3421, 4213$	$12, 21$ $123, 231, 312$ $1234, 2341, 3412, 4123$
1.465	$\beta^3 - \beta^2 - 1$		$1342, 2413, 3124, 4231$
1.618	$\beta^2 - \beta - 1$	312 $1423, 3412, 4231$	$132, 213, 321$ $1243, 1324, 2431, 3142, 4312$
1.755	$\beta^3 - 2\beta^2 + \beta - 1$	$2341, 2413, 3124, 4123$	
1.802	$\beta^3 - 2\beta^2 - 2\beta + 1$		4213
1.839	$\beta^3 - \beta^2 - \beta - 1$	4132	$1432, 2143, 3214, 4321$
2	$\beta - 2$	$1234,\ 1243$	$2134, 3241$
2.247	$\beta^3 - 2\beta^2 - \beta + 1$	4321	4132
2.414	$\beta^2 - 2\beta - 1$		$2314, 3421$
2.618	$\beta^2 - 3\beta + 1$		1423
2.732	$\beta^2 - 2\beta - 2$	4312	

Table 1: $B(\pi)$ for the $(-\beta)$-shift and the β-shift, permutations of length up to 4.

1. Let $\pi = 3421$. Then $\hat{\pi} = 3142$, $z_{[1,4)} = 110$, $m = 2$, $\pi(n) = 1$, $r = 3$. We obtain that $a = \overline{z_{[2,4)}0} = \overline{100} = \overline{\varphi^2(0)}$, thus $B(\pi) = 1$. Indeed, $\mathrm{Pat}(0100\,\overline{10011}, \Sigma, n) = \pi$.

2. Let $\pi = 892364157$. Then $\hat{\pi} = 536174892$, $z_{[1,9)} = 33012102$, $m = 2$, $\ell = 5$, $r = 1$, thus $a = z_{[2,9)}\,\overline{z_{[1,9)}} = \overline{30121023}$, and $B(\pi)$ is the unique root $x > 1$ of
$$x^8 - 4x^7 + x^6 - 2x^5 + 3x^4 - 2x^3 + x^2 - 3x + 4 = 1.$$
We get $B(\pi) \approx 3.831$, and we have $\mathrm{Pat}(330121023\,\overline{301210220}, \Sigma, n) = \pi$.

3. Let $\pi = 453261$. Then $\hat{\pi} = 462531$, $z_{[1,6)} = 11001$, $m = 5$, $\pi(n) = 1$, $r = 4$, thus $a = z_5\,\overline{z_4 z_5} = \overline{10}$, and $B(\pi) = 2$. We have $\mathrm{Pat}(110010\,\overline{2}, \Sigma, n) = \pi$ and $N(\pi) = 3$.

4. Let $\pi = 7325416$. Then $\hat{\pi} = 6521473$, $z_{[1,7)} = 100100$, $m = r = 1$, $\ell = 4$. Hence (1) holds, $z^{(0)}_{[1,7)} = 200100$, $z^{(1)}_{[1,7)} = 200210$, $z^{(2)}_{[1,7)} = 211210$. Since $n - m$ is even, we have
$$a = \min_{i\in\{0,1,2\}} z^{(i)}_{[1,7)}\,\overline{z^{(i)}_{[4,7)}} = \min\{200\,\overline{100}, 200\,\overline{210}, 211\,\overline{210}\} = 211\,\overline{210}.$$
Therefore, $B(\pi) \approx 2.343$ is the largest positive root of
$$\begin{aligned} 0 &= (x^6 - 3x^5 + 2x^4 - 2x^3 + 3x^2 - 2x + 1) - (-x^3 + 3x^2 - 2x + 2) \\ &= x^6 - 3x^5 + 2x^4 - x^3 - 1. \end{aligned}$$
We have $\mathrm{Pat}(211210(210)^{2k+1}\overline{2}, \Sigma, n) = \pi$ for $k \geq 0$.

References

[1] José María Amigó, Sergi Elizalde, and Matthew B. Kennel. Forbidden patterns and shift systems. *J. Combin. Theory Ser. A*, 115(3):485–504, 2008.

[2] Kassie Archer and Sergi Elizalde. Cyclic permutations realized by signed shifts. *J. Comb.*, 5(1):1–30, 2014.

[3] Christoph Bandt, Gerhard Keller, and Bernd Pompe. Entropy of interval maps via permutations. *Nonlinearity*, 15(5):1595–1602, 2002.

[4] Sergi Elizalde. The number of permutations realized by a shift. *SIAM J. Discrete Math.*, 23(2):765–786, 2009.

[5] Sergi Elizalde. Permutations and β-shifts. *J. Combin. Theory Ser. A*, 118(8):2474–2497, 2011.

[6] Sergi Elizalde and Katherine Moore. Patterns of negative shifts and beta-shifts. arXiv:1512.04479, preprint.

[7] Shunji Ito and Taizo Sadahiro. Beta-expansions with negative bases. *Integers*, 9:A22, 239–259, 2009.

[8] Lingmin Liao and Wolfgang Steiner. Dynamical properties of the negative beta-transformation. *Ergodic Theory Dynam. Systems*, 32(5):1673–1690, 2012.

[9] Wolfgang Steiner. Digital expansions with negative real bases. *Acta Math. Hungar.*, 139(1-2):106–119, 2013.

Return Words and Palindromes in Specular Sets*

Francesco Dolce

Université Paris-Est, France

Abstract

In this contribution we introduce specular sets, a subclass of tree sets having particular symmetries. We give some cardinality results about different types of return words in these sets. We also give some results concerning palindromes, namely we prove that tree sets of characteristic one closed under reversal are rich and that an important class of specular sets verifies G-richness. This is a joint work with V. Berthé, C. De Felice, V. Delecroix, J. Leroy, D. Perrin, C. Reutenauer and G. Rindone.

1 Introduction

In [2] the authors started a series of papers ([5, 6, 7, 8, 9]) studing the links between uniformly recurrent languages, subgroups of free groups and bifix codes. In this paper, we continue this investigation in a situation which involves groups, named specular, which are free products of a free group and of a finite number of cyclic groups of order two (see also [4]). A specular set is a subset of such a group. It is a set of words stable by taking the inverse and defined in terms of restrictions on the extensions of its elements.

The paper is organized as follows. In Section 2, we recall some notions concerning words, extension graphs and bifix codes. We also consider tree sets of arbitrary characteristic (see [9]). In Section 3, we introduce specular groups and specular sets. In Section 4 we give a construction which allows to build specular sets from tree sets of characteristic 1 (Theorem 6). In Section 5, we introduce several notions of return words: complete, right, left and mixed return words. For each of them, we prove a cardinality theorem (Theorems 9, 11 and 13). Finally, in Section 6, we make a connection with the notion of G-rich words introduced in [14] and related to the palindromic complexity of [10].

This is a joint work with Valérie Berthé, Clelia De Felice, Vincent Delecroix, Julien Leroy, Dominique Perrin, Christophe Reutenauer and Giuseppina Rindone.

2 Preliminaries

Let A be a finite alphabet. We denote by A^* the free monoid on A. We denote by ε the empty word. The *reversal* of a word $w = a_1 a_2 \cdots a_n$ with $a_i \in A$ is the word

*This work was supported by grants from Région Île-de-France.

$\tilde{w} = a_n \cdots a_2 a_1$. A word w is said to be a *palindrome* if $w = \tilde{w}$. A set S of words is *closed under reversal* if $w \in S$ implies $\tilde{w} \in S$ for every $w \in S$.

A *factor* of a word x is a word v such that $x = uvw$ with u, w nonempty. If both u and w are nonempty, v is called an *internal factor*. A set of words on the alphabet A is said to be *factorial* if it contains the alphabet A and all the factors of its elements.

Given a set S and a word $w \in S$, we define $L(w) = \{a \in A \mid aw \in S\}, R(w) = \{a \in A \mid wa \in S\}, E(w) = \{(a,b) \in A \times A \mid awb \in S\}$. We denote also $\ell(w) = \mathrm{Card}(L(w)), r(w) = \mathrm{Card}(R(w))$ and $e(w) = \mathrm{Card}(E(w))$. A word w is *right-extendable* if $r(w) > 0$, *left-extendable* if $\ell(w) > 0$ and *biextendable* if $e(w) > 0$. A factorial set S is called *right-extendable* (resp. *left-extendable*, resp. *biextendable*) if every word in S is right-extendable (resp. left-extendable, resp. biextendable). A word w is called *right-special* if $r(w) \geq 2$. It is called *left-special* if $\ell(w) \geq 2$. It is called *bispecial* if it is both left-special and right-special. The *factor complexity* of a factorial set S of words on an alphabet A is the sequence $p_n = \mathrm{Card}(S \cap A^n)$.

Let S be a biextendable set of words. For $w \in S$, we consider the set $E(w)$ as an undirected graph on the set of vertices which is the disjoint union of $L(w)$ and $R(w)$ with edges the pairs $(a,b) \in E(w)$. This graph is called the *extension graph* of w. If the extension graph $E(w)$ is acyclic, then $\ell(w) - r(w) + e(w)$ is the number of connected components of the graph $E(w)$. A biextendable set S is called a *tree set* of *characteristic* $\chi(S)$ if for any nonempty $w \in S$, the graph $E(w)$ is a tree (acyclic and connected) and if $E(\varepsilon)$ is a union of $\chi(S)$ trees.

A set of words $S \neq \{\varepsilon\}$ is *recurrent* if it is factorial and if for any $u, w \in S$, there is a $v \in S$ such that $uvw \in S$. An infinite factorial set is said to be *uniformly recurrent* if for any word $u \in S$ there is an integer $n \geq 1$ such that u is a factor of any word of S of length n. A uniformly recurrent set is recurrent. The converse is true for true for tree sets (see [9]).

An infinite word is *strict episturmian* if the set of its factors is closed under reversal and if it contains for each n exactly one right-special word u such that $r(u) = \mathrm{Card}(A)$ (see [2]). An *Arnoux-Rauzy set* is the set of factors of a strict episturmian word. Any Arnoux-Rauzy set is a recurrent tree set of characteristic 1 (see [5]).

Example 1. The *Fibonacci set* is the set of factors of the fixed-point $f^\omega(a)$ of the morphism $f : \{a,b\}^* \to \{a,b\}^*$ defined by $f(a) = ab$ and $f(b) = a$. It is an Arnoux-Rauzy set (see [13]), and thus a tree set of characteristic 1.

A *bifix code* is a set of nonempty words wich does not contain any proper prefix of proper suffix of its elements (see [3]). The *kernel* of a bifix code X is the set of words of X which are internal factors of X.

3 Specular sets

We consider an alphabet A with an involution $\theta : A \to A$, possibly with some fixed points. We also consider the group G_θ generated by A with the relations $a\theta(a) = 1$ for every $a \in A$. Thus $\theta(a) = a^{-1}$ for $a \in A$. When θ has no fixed point, we can set $A = B \cup B^{-1}$ by choosing a set of representatives of the orbits of θ for the set B. The group G_θ is then the free group on B. In general, we have $G_\theta = \mathbb{Z}^{*i} * (\mathbb{Z}/2\mathbb{Z})^{*j}$ where i is the number of orbits of θ with two elements and j the number of its fixed points. Such a group will be called a *specular group* of type (i, j). These groups are very close to free groups (see [4]).

Example 2. Let $A = \{a, b, c, d\}$ and let θ be the involution which exchanges b, d and fixes a, c. Then $G_\theta = \mathbb{Z} * (\mathbb{Z}/2\mathbb{Z})^2$ is a specular group of type $(1, 2)$.

A word on the alphabet A is *θ-reduced* if it has no factor of the form $a\theta(a)$ for $a \in A$. It is clear that any element of a specular group is represented by a unique θ-reduced word. A *specular set* on A is a biextendable set of θ-reduced words on A, closed under inverses, which is a tree set of characteristic 2. Thus, in a specular set, the extension graph of every nonempty word is a tree and the extension graph of the empty word is a union of two disjoint trees. Note that in a specular set the two trees forming $E(\varepsilon)$ are isomorphic ([4, Proposition 4.1]).

Example 3. Let $A = \{a, b\}$ and let θ be the identity on A. Then the set of factors of $(ab)^\omega$ is a specular set.

The following is a particular case of [9, Proposition 2.4].

Proposition 4. *The factor complexity of a specular set on the alphabet A is given by $p_0 = 1$ and $p_n = n(\mathrm{Card}(A) - 2) + 2$ for $n \geq 1$.*

Since a specular set is biextendable, any letter $a \in A$ occurs exactly twice as a vertex of $E(\varepsilon)$, one as an element of $L(\varepsilon)$ and one as an element of $R(\varepsilon)$. A letter $a \in A$ is said to be *even* if its two occurrences appear in the same tree. Otherwise, it is said to be *odd.* Observe that if a specular set is recurrent, there is at least one odd letter. A word $w \in S$ is said to be *even* if it has an even number of odd letters. Otherwise it is said to be *odd.*

Example 5. Let S be the set of Example 3. Both letters a and b are odd. Thus even words are exactly the words of even length.

4 Doubling maps

We now introduce a construction which allows one to build specular sets. This is a particular case of the multiplying maps introduced in [9].

A *doubling transducer* is a transducer $\mathcal{A}$ with set of states $Q = \{0, 1\}$ on the input alphabet Σ and the output alphabet A and such that:

1. the input automaton is a *group automaton*, that is, every letter of Σ acts on Q as a permutation
2. the output labels of the edges are all distinct.

We define two maps $\delta_0, \delta_1 : \Sigma^* \to A^*$ corresponding to initial states 0 and 1 respectively. Thus $\delta_0(u) = v$ (resp. $\delta_1(u) = v$) if the path starting at state 0 (resp. 1) with input label u has output v. The pair $\delta_\mathcal{A} = (\delta_0, \delta_1)$ is called a *doubling map.* The *image* of a set T on the alphabet Σ by the doubling map $\delta_\mathcal{A}$ is the set $S = \delta_0(T) \cup \delta_1(T)$. We denote by $i \overset{\alpha|a}{\to} j$ the edge of $\mathcal{A}$ from the state i to the state j having input label α and output label a. We define an involution $\theta_\mathcal{A}$ as the map such that $i \overset{\alpha|a}{\to} j$ and $1-j \overset{\alpha|\theta(a)}{\to} 1-i$ are the two edges of $\mathcal{A}$ having α as input label.

Theorem 6. *For any tree set T of characteristic* 1 *closed under reversal, the image of T by a doubling map $\delta_{\mathcal{A}}$ is a specular set relative to the involution $\theta_{\mathcal{A}}$.*

Example 7. Let $\Sigma = \{\alpha, \beta\}$ and let T be the Fibonacci set. Let $\delta_{\mathcal{A}}$ be the doubling map given by the transducer of Figure 1 on the left. The letter α acts as the transposition of the two states $0, 1$, while β acts as the identity.

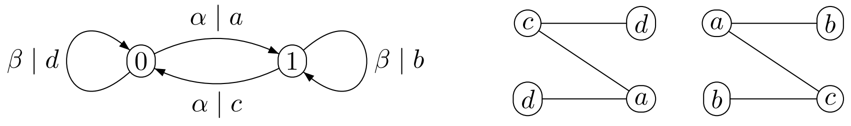

Figure 1: A doubling transducer and the extension graph $E(\varepsilon)$.

Then $\theta_{\mathcal{A}}$ is the involution θ of Example 2 and the image of T by δ is a specular set S on the alphabet $A = \{a, b, c, d\}$. The graph $E(\varepsilon)$ is represented in Figure 1 on the right. The letters a, c are odd while b, d are even.

5 Return words

Let S be a factorial set of words and let $X \subset S$ be a set of nonempty words. A *complete return word* to X is a word of S with a proper prefix in X, a proper suffix in X but no internal factor in X. We denote by $\mathcal{CR}(X)$ the set of complete return words to X. The set $\mathcal{CR}(X)$ is a bifix code. If S is uniformly recurrent, $\mathcal{CR}(X)$ is finite for any finite set X. For $w \in S$, we denote $\mathcal{CR}(w)$ instead of $\mathcal{CR}(\{w\})$. Thus $\mathcal{CR}(x)$ is the usual notion of a complete return word (see [11] for example).

Example 8. Let S be the specular set of Example 7. One can compute the sets $\mathcal{CR}(a) = \{abca, abcda, acda\}$, $\mathcal{CR}(b) = \{bcab, bcdacdab, bcdacdacdab\}$, $\mathcal{CR}(c) = \{cabc, cdabc, cdac\}$ and $\mathcal{CR}(d) = \{dabcabcabcd, dabcabcd, dacd\}$.

The following result is a direct consequence of [9, Theorem 5.2].

Theorem 9 (Cardinality Theorem for complete return words)**.** *Let S be a recurrent specular set on the alphabet A. For any finite nonempty bifix code $X \subset S$ with empty kernel, one has* $\mathrm{Card}(\mathcal{CR}(X)) = \mathrm{Card}(X) + \mathrm{Card}(A) - 2$.

Example 10. Let S be the specular set of Example 7. One has, for example, $\mathcal{CR}(\{a, c\}) = \{abc, ac, ca, cda\}$ and $\mathcal{CR}(\{b, d\}) = \{bcab, bcd, dab, dacd\}$. Both sets have four elements in agreement with Theorem 9.

Let S be a factorial set. For any nonempty word $w \in S$, a *right return word* to w in S is a word u such that wu is a complete return word to w. One defines symmetrically the *left return words*. We denote by $\mathcal{R}(x)$ the set of right return words to w in S and by $\mathcal{R}'(w)$ the corresponding set of left return words. Note that when S is closed under inverses, one has $\mathcal{R}(w)^{-1} = \mathcal{R}'(w^{-1})$. One can prove that in a specular set S, for every $w \in S$, all words in $\mathcal{R}(w)$ are even.

Theorem 11 (Cardinality Theorem for right return words)**.** *Let S be a recurrent specular set. For any $w \in S$, one has* $\mathrm{Card}(\mathcal{R}(w)) = \mathrm{Card}(A) - 1$.

Example 12. Let S be the specular set of Example 7. One has

$$\begin{aligned}
\mathcal{R}(a) &= \{bca, bcda, cda\},\\
\mathcal{R}(b) &= \{cab, cdacdab, cdacdacdab\},\\
\mathcal{R}(c) &= \{abc, dabc, dac\},\\
\mathcal{R}(d) &= \{abcabcd, abcabcabcd, acd\}.
\end{aligned}$$

Two words u, v are said to *overlap* if a nonempty suffix of one of them is a prefix of the other. In particular a nonempty word overlaps with itself. We now consider the return words to $\{w, w^{-1}\}$ with w such that w and w^{-1} do not overlap. This is true for every w in a specular set S where the involution θ has no fixed point. With a complete return word u to $\{w, w^{-1}\}$, we associate a word $N(u)$ obtained as follows: if u has w as prefix, we erase it and if u has a suffix w^{-1}, we also erase it. Note that these two operations can be made in any order since w and w^{-1} cannot overlap. The *mixed return words to w* are the words $N(u)$ associated with the words $u \in \mathcal{CR}(\{w, w^{-1}\})$. We denote by $\mathcal{MR}(w)$ the set of mixed return words to w in S. The reason for this definition comes from the study of natural codings of a linear involution (see [8]). Note that $\mathcal{MR}(w)$ is closed under inverses and that $w\mathcal{MR}(w)w^{-1} = \mathcal{MR}(w^{-1})$.

Theorem 13 (Cardinality Theorem for mixed return words)**.** *Let S be a recurrent specular set on the alphabet A. For any $w \in S$ such that w, w^{-1} do not overlap, one has* $\mathrm{Card}(\mathcal{MR}(w)) = \mathrm{Card}(A)$.

Example 14. Let S be the specular set of Example 7. One has $\mathcal{MR}(b) = \{cab, c, dac, dab\}$. Since b, d do not overlap, $\mathcal{MR}(b)$ has four elements in agreement with Theorem 13.

6 Palindromes

The notion of palindromic complexity originates in [10] where it is proved that a word of length n has at most $n + 1$ palindrome factors. A word of length n is *rich* (or full) if it has $n + 1$ palindrome factors and a factorial set is *rich* (or full) if all its elements are rich. By a result of [12], a recurrent set closed under reversal is rich if and only if every complete return word to a palindrome in S is a palindrome. It is known that all Arnoux-Rauzy sets are rich [10] and also all natural codings of interval exchanges defined by a symmetric permutation [1]. The following proposition generalizes results of [1, 10].

Proposition 15. *Let T be a recurrent tree set of characteristic* 1 *closed under reversal. Then T is rich.*

In [14], this notion was extended to that of G-rich, where G is a finite group of morphisms and antimorphisms of A^* containing at least one antimorphism. A set S closed under G is G-rich if for every $w \in S$, every complete return word to the G-orbit of w is fixed by a nontrivial element of G ([14, Theorem 29]).

Let S be a specular set obtained as the image of a tree set of characteristic 1 by a doubling map $\delta_{\mathcal{A}}$. Let us define the antimorphism $\sigma : u \mapsto u^{-1}$ for $u \in S$. From Section 4 it follows that both edges $i \overset{\alpha|a}{\rightarrow} j$ and $1-i \overset{\alpha|\sigma(a)}{\rightarrow} 1-j$ are in $\mathcal{A}$. Let us define the morphism τ obtained by replacing each letter $a \in A$ by $\tau(a)$ if there are edges $i \overset{\alpha|a}{\rightarrow} j$ and $1-j \overset{\alpha|\tau(a)}{\rightarrow} 1-i$ in $\mathcal{A}$. We denote by $G_{\mathcal{A}}$ the group generated by the σ and τ. Actually, we have $G_{\mathcal{A}} = (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$.

Example 16. Let S be the recurrent specular set defined in Example 7. One has $G_{\mathcal{A}} = \{id, \sigma, \tau, \sigma\tau\}$, where σ and τ are defined by $\sigma(a) = a, \sigma(b) = d, \sigma(c) = c, \sigma(d) = a$, and $\tau(a) = c, \tau(b) = d, \tau(c) = a, \tau(d) = b$. Note that $\sigma\tau = \tau\sigma$ is the antimorphism fixing b, d and exchanging a and c.

We now connect the notions of richness and G-richness, with an analogous result of Proposition 15 for specular sets.

Proposition 17. *Let T be a recurrent tree set of characteristic* 1 *on the alphabet Σ, closed under reversal and let S be the image of T under a doubling map $\mathcal{A}$. Then S is $G_{\mathcal{A}}$-rich.*

Example 18. Let S be the specular set of Example 7. S is $G_{\mathcal{A}}$-rich with respect to the group $G_{\mathcal{A}}$ of Example 16. The $G_{\mathcal{A}}$-orbit of a is the set $X = \{a, c\}$. The four words of $\mathcal{CR}(X)$ (see Example 10) are fixed by $\sigma\tau$.

References

[1] P. Baláži, Z. Masáková, and E. Pelantová. Factor versus palindromic complexity of uniformly recurrent infinite words. *Theoretical Computer Science*, 380(3):266–275, 2007.

[2] J. Berstel, C. De Felice, D. Perrin, C. Reutenauer, and G. Rindone. Bifix codes and Sturmian words. *Journal of Algebra*, 369:146–202, 2012.

[3] J. Berstel, D. Perrin, and C. Reutenauer. *Codes and Automata.* Cambridge University Press, 2009.

[4] V. Berthé, C. De Felice, V. Delecroix, F. Dolce, J. Leroy, D. Perrin, C. Reutenauer, and G. Rindone. Specular sets. In *Combinatorics on Words*, number 9304 in Springer LNCS, pages 210–222. 2015.

[5] V. Berthé, C. De Felice, F. Dolce, J. Leroy, D. Perrin, C. Reutenauer, and G. Rindone. Acyclic, connected and tree sets. *Monatshefte für Mathematik*, 176:521–550, 2015.

[6] V. Berthé, C. De Felice, F. Dolce, J. Leroy, D. Perrin, C. Reutenauer, and G. Rindone. The finite index basis property. *Journal of Pure and Applied Algebra*, 219:2521–2537, 2015.

[7] V. Berthé, C. De Felice, F. Dolce, J. Leroy, D. Perrin, C. Reutenauer, and G. Rindone. Maximal bifix decoding. *Dicrete Mathematics*, 338:725–742, 2015.

[8] V. Berthé, V. Delecroix, F. Dolce, D. Perrin, C. Reutenauer, and G. Rindone. Return words of linear involutions and fundamental groups. *Ergodic Theory and Dynamical Systems*, 2015. (to appear).

[9] F. Dolce and D. Perrin. Neutral and tree sets of arbitrary characteristic. *Theoretical Computer Science*, 2016. (to appear).

[10] X. Droubay, J. Justin, and G. Pirillo. Episturmian words and some constructions of de Luca and Rauzy. *Theoretical Computer Science*, 255(1-2):539–553, 2001.

[11] F. Durand. A characterization of substitutive sequences using return words. *Discrete Mathematics*, 179(1-3):89–101, 1998.

[12] A. Glen, J. Justin, S. Widmer, and L.Q. Zamboni. Palindromic richness. *European Journal of Combinatorics*, 30(2):510–531, 2009.

[13] M. Lothaire. *Algebraic Combinatorics on Words*. Cambridge University Press, 2002.

[14] E. Pelantová and Š. Starosta. Palindromic richness for languages invariant under more symmetries. *Theoretical Computer Science*, 518:42–63, 2014.

On the Density of Sets Defined by Sum-of-Digit Function in Base 2

Jordan Emme[1], Alexander Prikhod'ko[2]

[1] Aix-Marseille University, France

[2] Moscow Institute of Physics and Technology, Russia

In this talk we are interested in the statistic behaviour of the difference of the number of digits 1 in the binary expansion of an integer x before and after its summation with a. This kind of question can be linked with carry propagation problems developped by Knuth and Pippenger and has to do with computer arithmetics as in Muller or Ercegovac but our approach is different.

The main definitions are the following:

Definition 1. For any integer $x \in \mathbb{N}$ whose binary expansion is given by:

$$x = \sum_{k=0}^{n} x_k 2^k, \quad \forall k \in \{0, ..., n\} \quad x_k \in \{0, 1\},$$

we define the quantity

$$s_2(x) = \sum_{k=0}^{n} x_k$$

which is the number of digits 1 in the binary expansion of x.

Definition 2. For any integer x whose binary expansion is given by:

$$x = \sum_{k=0}^{n} x_k 2^k,$$

we denote by $\underline{x}$ the word $x_0 ... x_n$ in $\{0, 1\}^*$.

The function s_2 modulo 2 was extensively studied for its links with the Thue-Morse sequence (which was developped by Keane) for example or for arithmetic reason as in works of Mauduit and Rivat. But here our motivation is not of the same nature and we do not look at s_2 mod 2 but just at the function s_2 which is the sum of the digits in base 2.

Besineau studied the statistical indepence of sets defined via functions such as s_2, namely "sum of digits" functions. To that end he studied the correlation function defined in the following way:

Definition 3. Let $f : \mathbb{N} \to \mathbb{C}$. Its correlation $\gamma_f : \mathbb{N} \to \mathbb{C}$ is the function, if it exists, defined by:

$$\forall a \in \mathbb{N}, \ \gamma_f(a) = \lim_{N \to \infty} \frac{1}{N} \sum_{k=0}^{N} \overline{f(k)} f(k + a).$$

This correlation was studied by Besineau in this same article for functions of the form $k \mapsto e^{i\pi\alpha s(k)}$ where s is a sum-of-digits function in a given base and α is a real constant.

In the case of base 2, this motivates us to understand the following equation, with parameters $a \in \mathbb{N}$ and $d \in \mathbb{Z}$:

$$s_2(x+a) - s_2(x) = d. \tag{1}$$

Namely, we wish to understand, for given integers a and d, the behaviour of the density of set $\{x \in \mathbb{N} \mid s_2(x+a) - s_2(x) = d\}$ which always exists from works of Besineau or Morgenbesser and Spiegelhofer for instance. Remark that we can define in this way, for any integer a, a probability measure μ_a on $\mathbb{Z}$ defined for any d by:

$$\mu_a(d) := \lim_{N\to\infty} \frac{1}{N} \quad \#\{x \leq N \quad | \quad s_2(x+a) - s_2(x) = d\}.$$

The main results are the following:

Theorem 4. *The distribution μ_a is calculated via an infinite product of matrices whose coefficients are operators of $l^1(\mathbb{Z})$ applied to a vector whose coefficients are elements of $l^1(\mathbb{Z})$. In fact the expression is:*

$$\mu_a = (Id,\ Id)\ \cdots A_{a_n} A_{a_{n-1}} \cdots A_{a_1} A_{a_0} \begin{pmatrix} \delta_0 \\ 0 \end{pmatrix},$$

where the sequence $(a_n)_{n\in\mathbb{N}}$ is the binary expansion of a, δ_0 is the Dirac mass in 0

$$A_0 = \begin{pmatrix} Id & \frac{1}{2}S^{-1} \\ 0 & \frac{1}{2}S \end{pmatrix}, \qquad A_1 = \begin{pmatrix} \frac{1}{2}S^{-1} & 0 \\ \frac{1}{2}S & Id \end{pmatrix},$$

and S is the left shift transformation on $l^1(\mathbb{Z})$.

Such a result is proved by a combinatorial study of the family of solutions of Equation 1. To have the quantity μ_a expressed as a product of matrices allows an analytical study of these distributions as the binary expansion of a is more and more "complicated". Let us introduce this notion of complexity for a:

Definition 5. For any $a \in \mathbb{N}$, let us denote by $l(a)$ the number of subwords 01 in the binary expansion of a.

We are interested in what happens as there are more and more patterns 01 in the word $\underline{a}$. We can precisely estimate the asymptotic behaviour of the $l^2(\mathbb{Z})$ norm $\|\cdot\|_2$ of this distribution as a goes to infinity by increasing the number of subwords 01.

Namely, the theorem is as follows:

Theorem 6. *There exists a real constant C_0 such that for any integer a we have the following:*

$$\|\mu_a\|_2 \leq C_0 \cdot l(a)^{-1/4}.$$

This theorem states that the distributions μ_a uniformly converge towards zero as $l(a)$ goes to infinity.

We also study in which way the variance of the random variable of probability law μ_a is linked to the number of subwords 01 in the binary expansion of a.

We show that the mean and the variance of the probability measure μ_a do exist; in fact the mean in always zero. Moreover, we have bounds on this variance as shown in this result:

Theorem 7. *For any integer a such that $l(a)$ is large enough, the variance of μ_a denoted by $Var(a)$ has bounds:*

$$l(a) - 1 \leq Var(a) \leq 2(2l(a) + 1).$$

Numeration Systems and Their Uses

Aviezri S. Fraenkel

Dept. of Computer Science and Applied Mathematics, Weizmann Institute of Science, Israel

1 Introduction

We exhibit existence and uniqueness of several exotic numeration systems. In the three subsections of section 1 we show how they provide poly-time winning strategies to combinatorial games. In subsections 2 and 3 of section 1, they are the only known tools providing polynomial strategies. In sections 2 and 3 numeration systems provide elegant solutions to mathematical problems.

2 Efficient strategies for combinatorial games

We consider 2-player perfect information games without cycles (no repetitions) and without chance moves (no dice), played on two piles of finitely many tokens, on which the players move alternately. Unless otherwise specified, we employ *normal* play, that is, the player first unable to play loses, the opponent wins. An example is

2.1 Generalized Wythoff

Let t be a positive integer. The moves of the game Generalized Wythoff are of two types:

I. Remove any positive number of tokens from a *single* pile, possibly the entire pile.

II. Take $k > 0$ from one pile and $\ell > 0$ from the other, provided that $|k - \ell| < t$.

At their turn, a player chooses *one* of I, II.

The classical Wythoff game is the case $t = 1$ [11], [3], in which a player taking from both piles has to take the *same* number of tokens.

Positions from which the Previous player can win whatever the move the opponent makes are *P-positions*, and those from which the Next player can win, whatever move the opponent makes are *N-positions.* Thus $(0, 0)$ is a P-position for every $t > 0$, because the next (first) player is unable to move, so the previous (second) player wins; $(0, b)$, $b > 0$, is an N-position for every $t > 0$, because the next player moves to $(0, 0)$, winning. The reader can easily verify that for $t = 2$, $(1, 3)$ is a P-position. For $t = 2$, the first 14 P-positions are listed in Table 1 below.

The reader can easily verify that the table suggests that $B_n - A_n = 2n$ (tn in general) and A_n is the smallest nonnegative integer that did not yet appear in the table. This is proved to hold in general [4]. Thus, for $n = 14$, the smallest such number is 19, hence $(A_{14}, B_{14}) = (19, 47)$. This is a *recursive* construction of the P-positions.

Table 1: The first few P-positions of GNERALIZED WYTHOFF for $t = 2$.

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13
A_n	0	1	2	4	5	7	8	9	11	12	14	15	16	18
B_n	0	3	6	10	13	17	20	23	27	30	34	37	40	44

For any game of the type described in the first sentence of this paper, P-positions and N-positions have the following important properties:

- Every game position is either P or N.
- Every N-position has an *option* (direct follower) that is a P-position.
- All options of any P-position are N-positions.

Thus a player beginning from an N-position can win: (S)he moves to P, the opponent necessarily moves to N, and so on, until the beginning player moves to the P-position $(0, 0)$, winning.

Given any position (x, y) in GENERALIZED WYTHOFF, we can check whether (x, y) is P or N. This provides a *winning strategy* for the game. Alas, this recursive strategy is exponential in the input size $\log xy$ of the given position (x, y). However, there are two poly-time winning strategies: 1. Algebraic. Let $\alpha = (2-t+\sqrt{t^2+4})/2$, $\beta = \alpha+t$. Then $A_n = \lfloor n\alpha \rfloor$, $B_n = \lfloor n\beta \rfloor = A_n + tn$. These facts lead to a poly-time winning strategy.

2. Arithmetic. Construct the simple continued fraction $\alpha = [1, a_1, a_2, a_3 \ldots]$. The numerators of the *convergents* satisfy the recurrence:

$$p_{-1} = p_0 = 1, \qquad p_n = a_n p_{n-1} + p_{n-2} \quad (n \geq 1).$$

In [5] it was shown, inter alia, that every positive integer N has a unique representation $R(N)$ in the numeration system with basis elements p_i $(i \geq 0)$ and digits d_i satisfying:

$$R(N) = \sum_{i=0}^{k} d_i p_i, \;\; 0 \leq d_i \leq a_{i+1}; \;\; d_{i+1} = a_{+2} \implies d_i = 0.$$

For $a_i = 1$ for all i, the numeration system reduces to the Zeckendorf system [12].

It turns out that every number N in the set $\{\lfloor n\alpha \rfloor\}_{n\geq 1}$ has representation $R(N)$ ending in an even number (possibly 0) number of zeros; and every number N in the set $\{\lfloor n\beta \rfloor\}_{n\geq 1}$ has representation $R(N)$ ending in an odd number of zeros, where $\beta = \alpha/(\alpha-1)$. Moreover, if $a_i = t$ is fixed for all $i \geq 1$, then $\lfloor n\beta \rfloor$ is a *left shift* of $\lfloor n\alpha \rfloor$. These observations lead to a poly-time winning strategy. We illustrate for $t = 2$. Then $\alpha = [1, 2, 2, 2, \ldots]$, $p_0 = 1$, $p_1 = 3$, $p_2 = 7$, $p_3 = 17$, $\ldots$. The representation of the first 14 positive integers is given in Table 2. Thus $R(5) = 12$ ends in an even number of zeros, and its left shift $120 = R(13)$. In Table 1 we see that indeed $(5, 13)$ is P, namely, $(A_4, B_4) = (5, 13)$. In [4], where the above three winning strategies are given, a numeration system based on the denominators of the convergents is elucidated, from which one can see why $(A_n, B_n) = (5, 13)$ happens for $n = 4$.

To summarize, GENERALIZED WYTHOFF is a game for which three distinct winning strategies are known, one exponential, two polynomial, one of which depends on a continued fraction based numeration system. Is there a game for which the *only* known poly-time winning strategy is based on a numeration system? Enter

Table 2: Representation $R(N)$.

7	3	1	N
		1	1
		2	2
	1	0	3
	1	1	4
	1	2	5
	2	0	6
1	0	0	7
1	0	1	8
1	0	2	9
1	1	0	10
1	1	1	11
1	1	2	12
1	2	0	13
2	0	0	14

2.2 Heap Games

This family depends on two positive integer parameters s, t. There are again two types of moves.

I. Same as I in generalized Wythoff.

II. Remove $k > 0$ and $\ell > 0$ from the two piles, say $0 < k \leq \ell$. The move is constrained by the condition

$$0 < k \leq \ell < sk + t,$$

which is equivalent to $0 \leq \ell - k < (s-1)k + t$. Notice that the case $s = 1$ reduces to Generalized Wythoff. The P-positions $\{(A_n, B_n)_{n\geq 0}\}$ are given in [6] recursively, which again leads to an exponential-time winning strategy. For example, for $s = t = 2$, the first 14 P-positions are depicted in Table 3.

Table 3: The first few P-positions for $s = t = 2$.

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13
A_n	0	1	2	3	5	6	7	9	10	11	13	14	15	16
B_n	0	4	8	12	18	22	26	32	36	40	46	50	54	58

In [6], sect. 3, it was proved that there exist real numbers α, γ, β, δ such that $A_n = \lfloor n\alpha + \gamma \rfloor$ and $B_n = \lfloor n\beta + \delta \rfloor$ for all $n \geq 0$ if and only if $s = 1$. As remarked above, $s = 1$ is Generalized Wythoff, so for the case $s > 1$ there is no algebraic winning strategy of the form that exists for Generalized Wythoff.

Let $u_{-1} = 1/s$, $u_0 = 1$, $u_n = (s + t - 1)u_{n-1} + su_{n-2}$ $(n \geq 1)$. Let $\mathcal{U}$ denote the numeration system with bases u_0, $u_1, \ldots$ and digits $d_i \in \{0, \ldots, s + t - 1\}$ such that $d_{i+1} = s + t - 1 \implies d_i < s$ $(i \geq 0)$. It was shown there that every positive integer has a unique representation over $\mathcal{U}$. For $s = t = 2$, $u_1 = 4$, $u_2 = 14$, $u_3 = 50$, $\ldots$. The first few representations over $\mathcal{U}$ are displayed in Table 4.

Table 4: Representation $R(N)$.

14	4	1	N
		1	1
		2	2
		3	3
	1	0	4
	1	1	5
	1	2	6
	1	3	7
	2	0	8
	2	1	9
	2	2	10
	2	3	11
	3	0	12
	3	1	13
1	0	0	14

It was further proved there that $R(A_n), n \geq 1$ ends in an even number of 0s and $R(B_n), n \geq 1$ ends in an odd number of 0s for all $n \geq 1$. Moreover, $R(B_n)$ is a left shift of $R(A_n)$. These properties can be verified for the first few P-positions by comparing Tables 3 and 4. This observation leads to a poly-time winning strategy.

2.3 Restrictions of Heap Games

Let K be a positive integer, $\mathcal{M}_K = \{nK : n \in \mathbb{Z}_{\geq 0}\}$, $\Omega_K = \{0, 1, \ldots, K-1\}$. In [8] the following game Γ_K was defined:

I. Remove k tokens from a single pile, $0 < k \in \mathcal{M}_K$.

II. Remove $0 < k \in \mathcal{M}_K$ tokens from one pile and $0 < \ell \in \mathcal{M}_K$ from the other, constrained by $0 \leq \ell - k < (s-1)k + t$.

It is proved that its P-positions are given by

$$\P = \bigcup_{i \geq 0} \{(A_n + \alpha, B_n + \beta) : (\alpha, \beta) \in \Omega_K \times \Omega_K\},$$

where A_n is the smallest nonnegative integer that did not yet occur in

$$\{A_i + \alpha, B_i + \beta : 0 \leq i < n, (\alpha, \beta) \in \Omega_K \times \Omega_K\}, \quad B_n = sA_n + \lceil t/K \rceil Kn.$$

This result provides a recursive winning strategy which is exponential in the input size $\log xy$ of any game position $(x, y) \in \mathbb{Z}^2_{\geq 0}$. The main contribution of [8] is the proof that every Restricted Heap Game is equivalent to a judiciously chosen Heap Game, so the former has a poly-time winning strategy based on the numeration system defined in the previous subsection. Joint work with Haiyan Li, Sanyang Liu and Wen An Liu.

3 Dual numeration systems

For producing a generalization of Adamson's Wythoff wheel, used for phyllotaxis studies, we considered a dual numeration system, based on any simple continued fraction. We proved existence and uniqueness of such numeration systems. This generalizes the dual Zeckendorf representation. Joint work with Urban Larsson.

4 Numeration systems rescue congruence problems in the theory of partitions

Let $b_m(n)$ denote the number of m-ary partitions of n. An m-ary partition of n is a partition into parts restricted to powers of a fixed positive integer m. In [1] congruence properties of $b_m(n) \pmod{m}$ were determined based only on the base m numeration system of n. As stated there in the introduction, such characterizations in the world of integer partitions are rare. Secondly, the result depends on the base m representation of n and nothing else.

In [2], a similar (mod m) result is obtained for $c_m(n)$, where $c_m(n)$ counts the number of partitions of n into powers of m such that, if m^i is a part in a partition counted by $c_m(n)$, where i is a positive integer, then m^{i-1} must also be a part in the partition.

Joint work with George Andrews and James Sellers.

5 Conclusion

We have exhibited existence and uniqueness of some exotic numeration systems. Moreover, in the subsections of section 1, we have shown that judicious choices of numeration systems yield poly-time solutions to otherwise exponential-time problems. In this sense numeration systems fill in tasks analogous to data structures. The judicious selection of the latter has often been demonstrated to lead to efficient solutions to algorithmic problems. In section 2 numeration systems were applied to the study of theoretical phyllotaxis models, and in section 3 they were shown to produce elegant solutions to two congruence questions in the theory of partitions.

References

[1] G.E. Andrews, A.S. Fraenkel and J.A. Sellers, Characterizing the number of m-ary partitions modulo m. *Amer. Math. Monthly* **122** (2015) 880-–885.

[2] G.E. Andrews, A.S. Fraenkel and J.A. Sellers, m-ary partitions with no gaps: a characterization modulo m, *Discrete Math.* **339** (2016) 283-–287.

[3] H.S.M. Coxeter, The golden section, phyllotaxis, and Wythoff's game, *Scripta Math.* **19** (1953) 135—143.

[4] A.S. Fraenkel, How to beat your Wythoff games' opponent on three fronts, *Amer. Math. Monthly* **89** (1982) 353-–361.

[5] A.S. Fraenkel, Systems of numeration, *Amer. Math. Monthly* **92** (1985) 105–114.

[6] A.S. Fraenkel, Heap games, numeration systems and sequences, *Annals Combinatorics* **2** (1998) 197–210.

[7] A.S. Fraenkel, The vile, dopey, evil and odious game players, *Discrete Math.* **312** (2012) 42–46, special volume in honor of the 80th birthday of Gert Sabidussi.

[8] A.S. Fraenkel, H. Li, S. Liu and W A. Liu, Variants of (s,t)-Wythoff's game, Preprint.

[9] H. Li, S. Liu, Extensions and restrictions of a-Wythoff's game, Preprint.

[10] W.A. Liu, H. Li, General restriction of (s,t)-Wythoff's game, *Electr. J. Combinatorics* **21**(2) (2014) 29pp.

[11] W. Wythoff, A modification of the game of Nim, *Nieuw Arch. Wisk.* **7** (1907) 199–302.

[12] E. Zeckendorf, Représentation des nombres naturels par une somme de nombres de Fibonacci ou de nombres de Lucas. (French) *Bull. Soc. Roy. Sci. Liège* **41** (1972) 179-–182.

Beta-Representations of 0 and Pisot Numbers

Christiane Frougny[(1)], Edita Pelantová[(2)]

[(1)] IRIF, UMR 8243 CNRS and Université Paris-Diderot, France

[(2)] FNSPE, Czech Technical University in Prague, Czech Republic

In the following β is a real number > 1. The so-called *beta-numeration* has been introduced by Rényi in [10], and since then there have been many works in this domain, in connection with number theory, dynamical systems, and automata theory, see the survey [7] or more recent [11] for instance.

By a greedy algorithm each number of the interval $[0, 1]$ is given a β-expansion, which is an infinite word on a canonical alphabet of non-negative digits. When β is an integer, we obtain the classical numeration systems. When β is not an integer, a number may have different β-representations. The β-expansion obtained by the greedy algorithm is the greatest in the lexicographic ordering. The question of converting a β-representation into another one is equivalent to the study of the β-representations of 0. We focus on the question of the recognisability by a finite automaton of the set of β-representations of 0.

From this automaton it is possible to derive transducers, called digit-conversion transducers, that relate words with same values but written differently on the same or distinct alphabets of digits. The normalisation is a particular digit-conversion such that the result is the greedy expansion of the number considered.

Let d be a positive integer, and let

$$Z_{\beta,d} = \{z_1 z_2 \cdots \mid \sum_{i \geq 1} z_i \beta^{-i} = 0, \ z_i \in \{-d, \ldots, d\}\}$$

be the set of infinite words having value 0 in base β on the alphabet $\{-d, \ldots, d\}$.

If $d < \lceil \beta \rceil - 1$, then 0 has in the alphabet $\{-d, \ldots, d\}$ only the trivial β-representation. On the other hand, if the β-expansion of 1 is denoted $d_\beta(1) = (t_i)_{i \geq 1}$, then $(-1)t_1 t_2 \cdots$ is a nontrivial β-representation of 0 on the alphabet $\{-\lceil \beta \rceil + 1, \ldots, \lceil \beta \rceil - 1\}$, and thus we consider only alphabets $\{-d, \ldots, d\}$ with $d \geq \lceil \beta \rceil - 1$.

The following result has been formulated in [7]:

Theorem 1. *The following conditions are equivalent:*

1. *the set $Z_{\beta,d}$ is recognisable by a finite Büchi automaton for every integer d,*
2. *the set $Z_{\beta,d}$ is recognisable by a finite Büchi automaton for one integer $d \geq \lceil \beta \rceil$,*
3. *β is a Pisot number.*

(3) implies (1) is proved in [5], (1) implies (3) is proved in [1] and (2) implies (1) is proved in [6].

Note that, if $Z_{\beta,d}$ is recognisable by a finite Büchi automaton, then, for every $c < d$, $Z_{\beta,c} = Z_{\beta,d} \cap \{-c, \ldots, c\}^{\mathbb{N}}$ is recognisable by a finite Büchi automaton as well.

Example 2. Take $\beta = \varphi = \frac{1+\sqrt{5}}{2}$ the Golden Ratio. It is a Pisot number, with $d_\varphi(1) = 11$. A finite Büchi automaton recognising $Z_{\varphi,1}$ is designed in Figure 1. The initial state is 0, and all the states are terminal.

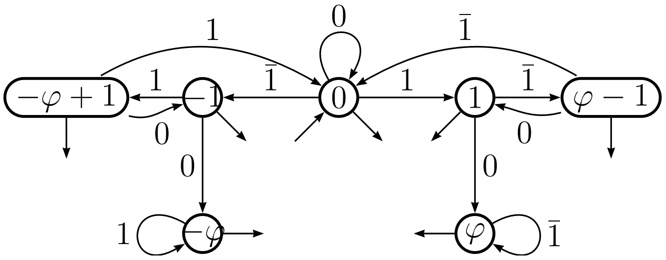

Figure 1: Finite Büchi automaton recognising $Z_{\varphi,1}$ for $\varphi = \frac{1+\sqrt{5}}{2}$.

Notation: In the sequel $y_{m-1} \cdots y_0 {\scriptstyle\bullet} y_{-1} y_{-2} \cdots$ denotes the numerical value $y_{m-1}\beta^{m-1} + \cdots + y_0 + y_{-1}\beta^{-1} + y_{-2}\beta^{-2} + \cdots$.

A number β such that $d_\beta(1)$ is eventually periodic is a *Parry number*. It is a *simple* Parry number if $d_\beta(1)$ is finite.

A *Pisot number* is an algebraic integer greater than 1 such that all its Galois conjugates have modulus less than 1. Every Pisot number is a Parry number, see [2] and [12]. The converse is not true, see for instance Example 9 below.

Recently Feng answered an open question raised by Erdős on accumulation points of the set

$$Y_d(\beta) = \{\sum_{i=0}^{n} z_i \beta^i \mid n \in \mathbb{N},\ z_i \in \{-d, \ldots, d\}\}\,.$$

Theorem 3 ([4]). *Let $\beta > 1$. Then $Y_d(\beta)$ is dense in $\mathbb{R}$ if and only if $\beta < d+1$ and β is not a Pisot number.*

In the present work we use Feng's result to simplify the proof of the implication (2) ⇒ (3) of Theorem 1 and moreover to replace the inequality $d \geq \lceil\beta\rceil$ by $d \geq \lceil\beta\rceil - 1$. In particular, we prove the conjecture stated in [7]:

If the set $Z_{\beta,\lceil\beta\rceil-1}$ is recognisable by a finite Büchi automaton then β is a Pisot number.

Note that the value $d = \lceil\beta\rceil - 1$ is the best possible as $Z_{\beta,d}$ is reduced to the infinite string of 0's if $d < \lceil\beta\rceil - 1$.

We thus obtain the following result.

Theorem 4. *The following conditions are equivalent:*

1. *the set $Z_{\beta,d}$ is recognisable by a finite Büchi automaton for every positive integer d,*
2. *the set $Z_{\beta,d}$ is recognisable by a finite Büchi automaton for one $d \geq \lceil\beta\rceil - 1$,*
3. *β is a Pisot number.*

Now we enlarge a definition originally given in [8] for $1 < \beta < 2$.

Definition 5. A number $\beta > 1$ is a *F-number* if

$$Y_{(\lceil\beta\rceil-1)}(\beta) \cap \big[-\frac{\lceil\beta\rceil-1}{\beta-1}, \frac{\lceil\beta\rceil-1}{\beta-1}\big]$$

is finite.

From Theorem 4 we obtain

Corollary 6. *A number β is a F-number if and only if it is a Pisot number.*

Normalisation in base β is the function which maps a β-representation on the canonical alphabet $A_\beta = \{0, \ldots, \lceil\beta\rceil - 1\}$ of a number $x \in [0, 1]$ onto the greedy β-expansion of x. Since the set of β-expansions of the elements of $[0, 1]$ is recognisable by a finite Büchi automaton when β is a Pisot number, see [3], the following result holds true.

Corollary 7. *Normalisation in base β is computable by a finite Büchi transducer if and only if β is a Pisot number.*

⋆ ⋆ ⋆

One can also ask the following question: what are the results in case we consider only finite representations of numbers, and the base β is a complex number. The situation is quite different.

Let

$$W_{\beta,d} = \{z_1 z_2 \cdots z_n \mid n \geq 1, \sum_{i\geq 1}^{n} z_i \beta^{-i} = 0, \ z_i \in \{-d, \ldots, d\}\}.$$

Theorem 8 ([5])**.** *Let β be in $\mathbb{C}$. The set $W_{\beta,d}$ is recognisable by a finite automaton for every d if and only if β is an algebraic number with no conjugate of modulus 1.*

If β is real, $\beta > 1$, we have that $W_{\beta,d}$ is recognisable by a finite automaton for every d if and only if $W_{\beta,d}$ is recognisable by a finite automaton for one $d \geq \lceil\beta\rceil$ ([6]).

Example 9 ([7])**.** Let β be the root > 1 of the polynomial $X^4 - 2X^3 - 2X^2 - 2$. Then $d_\beta(1) = 2202$ and β is a simple Parry number which is not a Pisot number and has no root of modulus 1. The set $Z_{\beta,2}$ is not recognisable by a finite Büchi automaton, but $W_{\beta,2}$ is recognisable by a finite automaton.

Example 10 ([9])**.** Let β be the root > 1 of $X^4-2X^3+X^2-2X+1$. Then $d_\beta(1) = 1(1100)^\omega$. β is a Salem number. It can be shown that $W_{\beta,1}$ is not recognisable by a finite automaton.

In view of these examples we set the following conjecture.

Conjecture 11. *Let $\beta > 1$ be an algebraic number such that $W_{\beta,\lceil\beta\rceil-1} \neq \{0^*\}$. If β has a conjugate of modulus 1 then $W_{\beta,\lceil\beta\rceil-1}$ is not recognisable by a finite automaton.*

Acknowledgements

E.P. acknowledges financial support by the Czech Science Foundation grant GAČR 13-03538S.

References

[1] D. Berend and Ch. Frougny, Computability by finite automata and Pisot bases, *Math. Systems Theory* **27** (1994) 274–282.

[2] A. Bertrand, Développements en base de Pisot et répartition modulo 1, *C. R. Acad. Sci. Paris, Sér. A* **285** (1977) 419–421.

[3] A. Bertrand-Mathis, Développements en base θ, répartition modulo un de la suite $(x\theta^n)_{n\geq 0}$, langages codés et θ-shift, *Bull. Soc. Math. Fr.* **114** (1986) 271–323.

[4] D.-J. Feng, On the topology of polynomials with bounded integer coefficients, to appear in *J. Eur. Math. Soc.* arXiv:1109.1407.

[5] Ch. Frougny, Representation of numbers and finite automata, *Math. Systems Theory* **25** (1992) 37–60.

[6] Ch. Frougny and J. Sakarovitch, Automatic conversion from Fibonacci representation to representation in base φ, and a generalization. *Internat. J. Algebra Comput.* **9** (1999) 351–384.

[7] Ch. Frougny and J. Sakarovitch, Number representation and finite automata, Chapter 2 in *Combinatorics, Automata and Number Theory*, V. Berthé, M. Rigo (Eds), Encyclopedia of Mathematics and its Applications 135, Cambridge University Press (2010).

[8] K. S. Lau, Dimension of a family of singular Bernoulli convolutions, *J. Funct. Anal.* **116** (1993) 335–358.

[9] P. Mercat, Semi-groupes fortement automatiques, *Bull. SMF* **141**, fascicule 3 (2013).

[10] A. Rényi, Representations for real numbers and their ergodic properties, *Acta Math. Acad. Sci. Hungar.* **8** (1957) 477–493.

[11] M. Rigo, *Formal languages, automata and numeration systems, volume 1: Introduction to combinatorics on words*, ISTE-Wiley, 2014.

[12] K. Schmidt, On periodic expansions of Pisot numbers and Salem numbers, *Bull. London Math. Soc.* **12** (1980) 269–278.

Base d expansions with digits 0 to $q - 1$

Kevin G. Hare*

Department of Pure Mathematics, University of Waterloo, Canada

This talk is primarily based on [3]. Let $f_{d,q}(n)$ be the number of ways we can represent n in base d with digits $0, 1, \cdots, q-1$. That is:

$$f_{d,q}(n) = \# \left\{ (a_k a_{k-1} \cdots a_0)_d \mid \sum_{i=0}^{k} a_i d^i = n, a_i \in \{0, 1, \cdots, q-1\} \right\}.$$

We define $f_{d,Q}$ similarly, where Q is a generic subset of the integers.

This has been looked at by [2, 4, 5]. For example, if $d = 2$ and $q = 7$ then we might represent 6 as $(110)_2 = 1 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0$ as well as $(102)_2 = 1 \cdot 2^2 + 0 \cdot 2^1 + 2 \cdot 2^0$. In this case there are six representations, $(110)_2, (102)_2, (30)_2, (22)_2, (14)_2$ and $(6)_2$, hence $f_{2,7}(6) = 6$. Similarly we see that $f_{2,\{0,1,2,4\}}(6) = 4$.

The case with base $d = 2$ has a long history. Euler showed that $f_{2,2}(n) = 1$ for all $n \geq 0$. Reznick [5] showed that $f_{2,3}(n) = s(n+1)$ where $s(n)$ is the Stern sequence. The case of $f_{2,4}(n) = \lfloor n/2 \rfloor + 1$ was done on the 1983 Putnam competition. The function $f_{2,\mathbb{N}}(n)$ has been studied by numerous people (see [5] and citations within).

The more general case for d was studied in [2] where a precise asymptotic for $f_{d,q}(n)$ was given when $q \leq d^2$.

The basic questions that we wish to look at are:

1. What can be said about the asymptotics of $f_{d,q}(n)$?

2. How fast does $f_{d,q}(n)$ grow at best? At worst?

3. How does this change if we replace $\{0, 1, 2, \ldots, q-1\}$ with a generic subset Q of the integers?

A simple counting argument shows that, on average, $f_{d,q}(n)$ is $O\left((q/d)^{\log_d(n)}\right) = O(n^{\log_d(q/d)})$. A similar argument can be used for a generic subset, assuming the subset is finite. What is surprising is that the maximal rate and the minimal rate of growth will often differ from this average value.

Definition 1. Let $\hat{\rho} := \hat{\rho}(d, q)$ be such that $\log_d \hat{\rho}$ is the exponent of the maximal rate of growth. That is

$$\log_d \hat{\rho} = \limsup_{n \to \infty} \frac{\log f_{d,q}(n)}{\log n}.$$

Let $\check{\rho} := \check{\rho}(d, q)$ be such that $\log_d \check{\rho}$ is the exponent of the minimal rate of growth. That is

$$\log_d \hat{\rho} = \liminf_{n \to \infty} \frac{\log f_{d,q}(n)}{\log n}.$$

*Research of K. G. Hare supported, in part by NSERC of Canada. Computational support provided in part by the Canadian Foundation for Innovation, and the Ontario Research Fund.

Alternately we could define $\hat{\rho}$ and $\check{\rho}$ such that for all n sufficiently large there exist C and D with

$$Cn^{\log_d \check{\rho}} \leq f_{d,q}(n) \leq Dn^{\log_d \hat{\rho}}$$

and with $\check{\rho}$ and $\hat{\rho}$ being sharp. For finite sets Q we can define $\hat{\rho}(d,Q)$ and $\check{\rho}(d,Q)$ similarly.

We know from [2] that $f_{d,q}(n)$ is a d-regular sequence. This implies that there exist d matrices, say $M_0, M_1, \cdots, M_{d-1}$ and vectors v_1 and v_2 such that if $n = (a_k a_{k-1} \cdots a_0)_d$ in base d with digits $\{0, 1, \cdots, d-1\}$, then

$$f_{d,q}(n) = v_1^T M_{a_0} M_{a_1} \cdots M_{a_{k-1}} M_{a_k} v_2.$$

These matrices will play an important role in the asymptotics of $f_{d,q}(n)$. The matrices arising from $f_{d,q} = f_{d,\{0,1,\ldots,q-1\}}$ are related to those coming from $f_{d,\{-k,-k+1,\ldots,q-k-1\}}$, allowing a precise relationship between the associated $\hat{\rho}$ and $\check{\rho}$ to be given. Many of these conjectures and results carry over to this more general $Q = \{-k, -k+1, \ldots, q-1-k\}$. It is not currently clear what is happening for generic Q that are not as "nice". (Although this may be clear by the time of the conference.)

It is shown in [2] that:

Theorem 2 (Dumont, Sidorov, Thomas, 99)**.** *If* $d \mid q$ *then*

$$f_{d,q}(n) = f_{d,q}(n) = \sum_{j=0}^{\lfloor q/d^2 \rfloor} f_{d,q/d}(j).$$

The exact order of $f_{d,q}(n)$ *is* $n^{\log_d(q/d)}$. *That is,* $\hat{\rho}(d,q) = \check{\rho}(d,q) = q/d$.

As a consequence we need not consider the case $d \mid q$. Further, a precise formula for $\hat{\rho}$ was given for $d < q < d^2$ with $d \nmid q$.

Theorem 3 (Dumont, Sidorov, Thomas, 99)**.** *Let* $r = \left\lfloor \frac{q-1}{d} \right\rfloor$ *and* $s := d\left\{\frac{q-1}{d}\right\}$, *where* $\{x\} = x - \lfloor x \rfloor$ *is the fractional part of* x. *If* $q \leq d^2$ *then*

1. *For* $r \leq s$ *we have* $f_{d,q}(n) = O\left(n^{\log_d(r+1)}\right)$, *or equivalently* $\hat{\rho}(d,q) = r+1$.
2. *For* $r > s$ *we have* $f_{d,q}(n) = O\left(n^{\log_d\left(\frac{r+\sqrt{r^2+4s+4}}{2}\right)}\right)$ *for* $r > s$, *or equivalently* $\hat{\rho}(d,q) = \frac{r+\sqrt{r^2+4s+4}}{2}$.

In Table 1 we give the values for $\hat{\rho}$ for $d = 2, 3, 4$ and $d < q < d^2$, where $d \nmid q$. The last column indicates the useful observation that $\hat{\rho}$ arises from the spectral radius ρ of short products of matrices in the set $\{M_0, \cdots, M_{d-1}\}$. Here $\rho(M) := \max |\lambda_i|$ where the λ_i range over the eigenvalues of M.

In the special case of $d = 2$, we have a conjecture from [4] that both $\hat{\rho}$ and $\check{\rho}$ arise from short products of $\{M_0, M_1\}$. More precisely:

Conjecture 4 (Protasov, 2000)**.** *For* $d = 2$ *and* q *odd, then*

$$\hat{\rho}(2,q) = \max(\rho(M_0), \sqrt{\rho(M_0 M_1)})$$

and

$$\check{\rho}(2,q) = \min(\rho(M_0), \sqrt{\rho(M_0 M_1)}).$$

Here M_0 *and* M_1 *depend on* d *and* q.

d	q	$\hat{\rho}$	$\hat{\rho}$ value
2	3	1.6180339	$\sqrt{\rho(M_0M_1)}$
3	4	1.6180339	$\sqrt{\rho(M_0M_1)}$
3	5	2	$\rho(M_1)$
3	7	2.4142135	$\sqrt{\rho(M_0M_2)} = \rho(M_1)$
3	8	2.7320508	$\sqrt{\rho(M_1M_2)}$
4	5	1.61803398	$\sqrt{\rho(M_0M_1)}$
4	6	2.	$\rho(M_1)$
4	7	2.	$\rho(M_1) = \sqrt{\rho(M_1M_2)} = \rho(M_2)$
4	9	2.41421356	$\sqrt{\rho(M_0M_2)} = \rho(M_1)$
4	10	2.73205080	$\sqrt{\rho(M_1M_2)}$
4	11	3.	$\rho(M_2)$
4	13	3.30277563	$\sqrt{\rho(M_0M_3)} = \rho(M_1) = \sqrt{\rho(M_1M_2)} = \rho(M_2)$
4	14	3.56155281	$\sqrt{\rho(M_1M_3)} = \rho(M_2)$
4	15	3.79128784	$\sqrt{\rho(M_2M_3)}$

Table 1: $\hat{\rho}$ for $f_{d,q}(n)$

Protasov proved this for the case when $d = 2$ and $q \leq 13$. In particular, he showed:

Theorem 5 (Protasov, 2000). *Let $d = 2$.*

- *For $q = 3, 5, 9$ we have $\hat{\rho}(2, q) = \sqrt{\rho(M_0M_1)}$ and $\check{\rho}(2, q) = \rho(M_0)$.*
- *For $q = 7, 11, 13$ we have $\hat{\rho}(2, q) = \rho(M_0)$ and $\check{\rho}(2, q) = \sqrt{\rho(M_0M_1)}$.*

Here M_0 and M_1 depend on d and q.

Let $s_2(n)$ be the sum of the binary digits of n. Using the techniques of Protasov, we can extend this data for all $\hat{\rho}$ and $\check{\rho}$ for $q \leq 55$. We present the data for $q \leq 40$ in Table 2 below. We divide this data into the two possible values for $\hat{\rho}$ and $\check{\rho}$. We also provide the value of $s_2(q)$, and observe a potential relationship between $s_2(q)$ and the value of $\hat{\rho}$ and $\check{\rho}$. This observation holds for all $q \leq 55$.

It appears that if $s_2(q)$ is even, then $\hat{\rho} = \sqrt{\rho(M_0M_1)}$ and $\check{\rho} = \rho(M_0)$, whereas if $s_2(q)$ is odd, then $\hat{\rho} = \rho(M_0)$ and $\check{\rho} = \sqrt{\rho(M_0M_1)}$.

Based on this data, we make the following conjecture:

Conjecture 6. *Let $d = 2$ and q odd.*

- *If $s_2(q) \equiv 0 \mod 2$, then $\hat{\rho}(2, q) = \sqrt{\rho(M_0M_1)}$ and $\check{\rho}(2, q) = \rho(M_0)$.*
- *If $s_2(q) \equiv 1 \mod 2$, then $\hat{\rho}(2, q) = \rho(M_0)$ and $\check{\rho}(2, q) = \sqrt{\rho(M_0M_1)}$.*

Here $M_0, M_1, \cdots, M_{d-1}$ depend on d and q.

$\hat\rho = \sqrt{\rho(M_0M_1)}$		$\hat\rho = \rho(M_0)$	
$\check\rho = \rho(M_0)$		$\check\rho = \sqrt{\rho(M_0M_1)}$	
q	$s_2(q)$	q	$s_2(q)$
3	2	7	3
5	2	11	3
9	2	13	3
15	4	19	3
17	2	21	3
23	4	25	3
27	4	31	5
29	4	35	3
33	2	37	3
39	4		

Table 2: $\hat\rho$ for $f_{2,q}$ with $q \le 40$ and odd.

Note that $\{s_2(n) \mod 2\}$ has a long history in the mathematical literature. This is the Thue-Morse sequence. See [1] and references within.

We now repeat this exercise for $d = 3$. Similar to Table 2, in Table 3 we partition $f_{3,q}(n)$ based on the value of $\hat\rho(3, q)$. We include information for $s_3(q)$, the sum of digits of the base 3 expansion of q.

$\hat\rho = \sqrt{\rho(M_0M_1)}$		$\hat\rho = \rho(M_1)$		$\hat\rho = \sqrt{\rho(M_1M_2)}$		$\hat\rho = \rho(M_0) = \rho(M_2)$	
$\check\rho = \sqrt{\rho(M_1M_2)}$		$\check\rho = \rho(M_0) = \rho(M_2)$		$\check\rho = \sqrt{\rho(M_0M_1)}$		$\check\rho = \rho(M_1)$	
q	$s_3(q)$	q	$s_3(q)$	q	$s_3(q)$	q	$s_3(q)$
4_*	2	5	3	8_*	4	17	5
10_*	2	7^*_*	3	14	4	23	5
26^*	6	11	3	16	4	25	5
28_*	2	13	3	20	4		
		19	3	22	4		
		29	3				

Table 3: $\hat\rho$ for $f_{3,q}$ with $q \le 30$, $3 \nmid n$

Again, we observe a potential relationship between $\hat\rho$, $\check\rho$. and $s_3(q)$. Similar tables can be constructed for $d = 4, 5, \ldots$.

We can extend Conjecture 4 to a more generalized setting as:

Conjecture 7. *For all pairs $d \nmid q$ we have*

$$\begin{aligned}
\hat\rho(d,q) &= \max\Big(\rho(M_0), \sqrt{\rho(M_0M_1)}, \rho(M_1), \sqrt{\rho(M_1M_2)}, \cdots, \\
&\qquad \sqrt{\rho(M_{d-2}M_{d-1})}), \rho(M_{d-1}), \sqrt{\rho(M_{d-1}M_0)}\Big) \\
\check\rho(d,q) &= \min\Big(\rho(M_0), \sqrt{\rho(M_0M_1)}, \rho(M_1), \sqrt{\rho(M_1M_2)}, \cdots, \\
&\qquad \sqrt{\rho(M_{d-2}M_{d-1})}), \rho(M_{d-1}), \sqrt{\rho(M_{d-1}M_0)}\Big).
\end{aligned}$$

Here $M_0, M_1, \cdots, M_{d-1}$ depend on d and q.

With this, we can generalize Conjecture 6 to get:

Conjecture 8. *Let $d \nmid q$. We have*

$$\hat{\rho}(d,q) = \begin{cases} \sqrt{\rho(M_{i-1}M_i)} & \text{if } s_d(q) \equiv 2i \mod 2d-2 \text{ is even} \\ \rho(M_i) & \text{if } s_d(q) \equiv 2i+1 \mod 2d-2 \text{ is odd} \end{cases}$$

and

$$\check{\rho}(d,q) = \begin{cases} \sqrt{\rho(M_{i-1}M_i)} & \text{if } s_d(q)+d-1 \equiv 2i \mod 2d-2 \text{ is even} \\ \rho(M_i) & \text{if } s_d(q)+d-1 \equiv 2i+1 \mod 2d-2 \text{ is odd.} \end{cases}$$

Here $M_0, M_1, \cdots, M_{d-1}$ depend on d and q.

We show that

Theorem 9. *Conjecture 8 holds all (d,q) with $d < q < d^2$.*

Theorem 10. *Conjecture 8 holds for all (d,q) where $q \leq 33$.*

Theorem 11. *Assuming Conjecture 7, Conjecture 8 holds for all (d,q) where $q \leq 200$.*

References

[1] Allouche, J.-P. and Shallit, J. (2003). *Automatic sequences.* Cambridge University Press, Cambridge. Theory, applications, generalizations.

[2] Dumont, J. M., Sidorov, N., and Thomas, A. (1999). Number of representations related to a linear recurrent basis. *Acta Arith.*, 88(4):371–396.

[3] Hare, K. G. Base-d expansions with digits 0 to $q-1$. *Exp. Math.*, 24(3):295–303, 2015.

[4] Protasov, V. Y. (2000). Asymptotics of the partition function. *Mat. Sb.*, 191(3):65–98.

[5] Reznick, B. (1990). Some binary partition functions. In *Analytic number theory (Allerton Park, IL, 1989)*, volume 85 of *Progr. Math.*, pages 451–477. Birkhäuser Boston, Boston, MA.

The Numbers of Distinct Squares and Cubes in the Tribonacci Sequence*

Yuke Huang(1), Zhiying Wen(2)

(1) School of Mathematics and Systems Science, Beihang University (BUAA), P. R. China

(2) Department of Mathematical Sciences, Tsinghua University, P. R. China

Abstract

The Tribonacci sequence $\mathbb{T}$ is the fixed point of the substitution $\sigma(a,b,c)=(ab,ac,a)$. In this note, we give the explicit expressions of the numbers of distinct squares and cubes in $\mathbb{T}[1,n]$ (the prefix of $\mathbb{T}$ of length n).

1 Introduction

Let $\mathcal{A}=\{a,b,c\}$ be a three-letter alphabet. The concatenation of factors ν and ω denoted by $\nu*\omega$ or $\nu\omega$. The Tribonacci sequence $\mathbb{T}$ is the fixed point beginning with a of the substitution σ defined by $\sigma(a)=ab$, $\sigma(b)=ac$, $\sigma(c)=a$. The Tribonacci sequence, which is a natural generalization of the Fibonacci sequence, has been studied extensively by many authors, see [2, 8, 9, 10, 11].

Let ω be a factor of $\mathbb{T}$, denoted by $\omega\prec\mathbb{T}$. Let ω_p be the p-th occurrence of ω. If the factor ω and integer p such that $\omega_p\omega_{p+1}$ (resp. $\omega_p\omega_{p+1}\omega_{p+2}$) is the factor of $\mathbb{T}$, we call it a square (resp. cube) of $\mathbb{T}$. As we know, $\mathbb{T}$ contains no fourth powers. The properties of squares and cubes are objects of a great interest in many aspects of mathematics and computer science etc.

We denote by $|\omega|$ the length of ω. Let $\tau=x_1\cdots x_n$ be a finite word (or $\tau=x_1x_2\cdots$ be a sequence). For any $i\leq j\leq n$, define $\tau[i,j]:=x_ix_{i+1}\cdots x_{j-1}x_j$. By convention, denote $\tau[i]:=\tau[i,i]=x_i$, $\tau[i,i-1]:=\varepsilon$(empty word). Denote $T_m=\sigma^m(a)$ for $m\geq 0$, $T_{-2}=\varepsilon$, $T_{-1}=c$, then $T_0=a$, $T_1=ab$ and $T_m=T_{m-1}T_{m-2}T_{m-3}$ for $m\geq 2$. Denote $t_m=|T_m|$ for $m\geq -2$, called the m-th Tribonacci number. Then $t_{-2}=0$, $t_{-1}=t_0=1$, $t_m=t_{m-1}+t_{m-2}+t_{m-3}$ for $m\geq 1$. Denote by δ_m the last letter of T_m, then $\delta_m=a$ (resp. b, c) for $m\equiv 0$, (resp. 1, 2) mod 3, $m\geq -1$.

In 2006, A.Glen gave the number of distinct squares in T_m in her PhD thesis, see Theorem 6.30 in [3]. She also gave some properties about cubes. In 2014, H.Mousavi and J.Shallit[8] gave some properties of the Tribonacci word, such as the lengths of squares and cubes. All of these results above only consider the squares or cubes in the prefixes of some special lengths: the Tribonacci numbers. The main aim of this article is to give the explicit expressions of the numbers of distinct squares and cubes in $\mathbb{T}[1,n]$. This topic has been studied not only for the Tribonacci sequence. We gave the expressions of the numbers of distinct squares and cubes in each prefix of the Fibonacci sequence, see [7].

*Supported by the Grant NSFC No.11431007, No.11271223 and No.11371210.

The main tools of the paper are "kernel word" and the unique decomposition of each factor with respect to its kernel, which introduced and studied in Huang and Wen[5]. In this paper, Section 2 presents some basic notations and known results. Section 3 proves some basic properties of squares. We determine the numbers of distinct squares and cubes in $\mathbb{T}[1,n]$ in Section 4 and 5 respectively. In Section 6, we give some open problems.

2 Preliminaries

We define the kernel numbers that $k_0=0$, $k_1=k_2=1$, $k_m=k_{m-1}+k_{m-2}+k_{m-3}-1$ for $m\geq 3$. The kernel word with order m is defined as $K_1=a$, $K_2=b$, $K_3=c$, $K_m=\delta_{m-1}T_{m-3}[1,k_m-1]$ for $m\geq 4$. By Proposition 2.7 in [5], all kernel words are palindromes. Let $Ker(\omega)$ be the maximal kernel word occurring in factor ω, then by Theorem 4.3 in [5], $Ker(\omega)$ occurs in ω only once.

Property 1 (Theorem 4.11 in [5]). *$\forall\omega\in\mathbb{T}$, $p\geq 1$, $Ker(\omega_p)=Ker(\omega)_p$.*

This means, let $Ker(\omega)=K_m$, then the maximal kernel word occurring in ω_p is just $K_{m,p}$. For instance, $Ker(aba)=b$, $(aba)_3=\mathbb{T}[8,10]$, $(b)_3=\mathbb{T}[9]$, so $Ker((aba)_3)=(b)_3$, $(aba)_3=a(b)_3a$.

The next three properties can be proved easily by induction.

Property 2. *For $m\geq 3$, (1) $k_m=k_{m-3}+t_{m-4}=\frac{t_{m-3}+t_{m-5}+1}{2}$;*
(2) $K_m=\delta_{m-1}T_{m-4}K_{m-3}[2,k_{m-3}]=\delta_{m-1}T_{m-4}T_{m-5}[1,k_{m-3}-1]$.

Property 3. *(1) $\sum_{i=0}^{m}t_i=\frac{t_m+t_{m+2}-3}{2}$ for $m\geq 0$, (see Lemma 6.7 in [3]);*
(2) $\sum_{i=1}^{m}k_i=\frac{k_m+k_{m+2}+m-1}{2}=\frac{t_{m-2}+t_{m-3}+m}{2}$ for $m\geq 1$.

Property 4. *For $m\geq 0$, (1) $T_mT_{m+1}[1,k_{m+4}-2]=T_{m+2}[1,k_{m+5}-2]$;*
(2) $T_{m+3}[1,k_{m+6}-2]=T_{m+1}T_mT_{m+1}[1,k_{m+4}-2]$.

3 Basic properties of squares

We denote the gap between ω_p and ω_{p+1} by $G_p(\omega)$. The sequence $\{G_p(\omega)\}_{p\geq 1}$ is called the gap sequence of factor ω. By Lemma 4.7, Definition 4.12 and Corollary 4.13 in [5], any factor ω with kernel K_m can be expressed uniquely as

$$\omega=T_{m-1}[i,t_{m-1}-1]K_mT_m[k_m,k_m+j-1],$$

where $1\leq i\leq t_{m-1}$ and $0\leq j\leq t_{m-1}-1$. By Theorem 3.3, Corollary 3.12 and Proposition 6.7(1) in [5], $\omega_p\omega_{p+1}\prec\mathbb{T}$ has three cases.

Case 1. $G_p(K_m)=G_1(K_m)$ and $|G_1(K_m)|=t_m-k_m$.

Since $|G_p(K_m)|=|T_{m-1}[i,t_{m-1}-1]|+|T_m[k_m,k_m+j-1]|=t_{m-1}-i+j$, $j=t_{m-2}+t_{m-3}-k_m+i$. So $0\leq j\leq t_{m-1}-1$ gives a range of i. Comparing this range with $1\leq i\leq t_{m-1}$, we have $1\leq i\leq k_{m+1}-1$ and $m\geq 3$. Furthermore,

$$\begin{aligned}\omega=&T_{m-1}[i,t_{m-1}]T_m[1,t_{m-2}+t_{m-3}+i-1]\\=&T_{m-1}[i,t_{m-1}]T_{m-2}T_{m-3}T_{m-2}[1,i-1];\\\omega\omega=&T_m[i,t_m-1]\underline{\delta_mT_{m-1}[1,k_{m+1}-1]}T_{m+1}[k_{m+1},t_m+i-1].\end{aligned}$$

Thus $K_{m+1}=\delta_m T_{m-1}[1,k_{m+1}-1]\prec\omega\omega$. Similarly, $K_{m+2},K_{m+3},K_{m+4}\not\prec\omega\omega$ and $|\omega\omega|<K_{m+5}$, so K_{m+1} is the largest kernel word in $\omega\omega$, i.e. $Ker(\omega\omega)=K_{m+1}$ for $m\geq 3$. Moreover, since $|\omega|=|G_p(K_m)|+k_m$, $|\omega|=t_m$.

By analogous arguments, we have

Case 2. $G_p(K_m)=G_2(K_m)$ and $|G_2(K_m)|=t_{m-2}+t_{m-1}-k_m$.

$$\omega\omega=T_m[i,t_{m-1}+t_{m-2}-1]\underline{K_{m+2}}T_{m+1}[k_{m+2},t_{m-1}+t_{m-2}+i-1],$$

where $1\leq i\leq k_{m+2}-1$, $m\geq 2$, $Ker(\omega\omega)=K_{m+2}$ and $|\omega|=t_{m-2}+t_{m-1}$.

Case 3. $G_p(K_m)=G_4(K_m)$ and $|G_4(K_m)|=t_{m-1}-k_m$.

$$\omega\omega=T_{m-1}[i,t_{m-1}-1]\underline{K_{m+3}}T_{m+1}[k_{m+3},t_{m-1}+i-1],$$

where $k_m\leq i\leq t_{m-1}$, $m\geq 1$, $Ker(\omega\omega)=K_{m+3}$ and $|\omega|=t_{m-1}$.

Remark 5. By the three cases of squares, we have: (1) all squares in $\mathbb{T}$ are of length $2t_m$ or $2t_m+2t_{m-1}$ for some $m\geq 0$; (2) for all $m\geq 0$, there exists a square of length $2t_m$ and $2t_m+2t_{m-1}$ in $\mathbb{T}$. These are known results of H.Mousavi and J.Shallit, see Theorem 5 in [8].

Denote $P(\omega,1)$ (resp. $L(\omega,1)$) the position of the last (resp. first) letter of ω_1. By Theorem 6.1, Remark 6.2 in [5] and $P(\omega,1)=L(\omega,1)+|\omega|-1$, we have

Property 6. $P(K_m,1)=t_{m-1}+k_m-1=k_{m+3}-1$ *for* $m\geq 1$.

We define three sets for $m\geq 4$,

$$\begin{cases}\langle 1,K_m\rangle:=\{P(\omega\omega,1):Ker(\omega\omega)=K_m,|\omega|=t_{m-1},\omega\omega\prec\mathbb{T}\}\\ \langle 2,K_m\rangle:=\{P(\omega\omega,1):Ker(\omega\omega)=K_m,|\omega|=t_{m-4}+t_{m-3},\omega\omega\prec\mathbb{T}\}\\ \langle 3,K_m\rangle:=\{P(\omega\omega,1):Ker(\omega\omega)=K_m,|\omega|=t_{m-4},\omega\omega\prec\mathbb{T}\}\end{cases}$$

Obviously these sets correspond the positions $P(\omega\omega,1)$ for the three cases of squares respectively. By Property 6, $\langle 1,K_m\rangle$ is equal to

$$\begin{aligned}&\{P(\omega,1):\omega=T_{m-1}[i,t_{m-1}-1]K_mT_m[k_m,t_{m-1}+i-1],1\leq i\leq k_m-1\}\\ =&\{P(K_m,1)+t_{m-1}-k_m+i,1\leq i\leq k_m-1\}=\{2t_{m-1},\cdots,k_{m+4}-2\}.\end{aligned}$$

Moreover $\sharp\langle 1,K_m\rangle=\sharp\{1\leq i\leq k_m-1\}=k_m-1$. Similarly

Property 7. *For* $m\geq 4$,

$$\begin{cases}\langle 1,K_m\rangle=\{2t_{m-1},\cdots,k_{m+4}-2\};\\ \langle 2,K_m\rangle=\{2t_{m-1}-t_{m-2},\cdots,t_{m-1}+k_{m+2}-2\};\\ \langle 3,K_m\rangle=\{k_{m+3}-1,\cdots,t_{m-1}+2t_{m-4}-1\}.\end{cases}$$

Moreover $\sharp\langle 1,K_m\rangle=\sharp\langle 2,K_m\rangle=k_m-1$, $\sharp\langle 3,K_m\rangle=t_{m-4}-k_{m-3}+1$.

For $m\geq 3$, denote

$$\Delta_m:=\sum_{i=4}^{m}\sharp\langle 1,K_i\rangle=\sum_{i=4}^{m}\sharp\langle 2,K_i\rangle,\ \Theta_m:=\sum_{i=4}^{m}\sharp\langle 3,K_i\rangle.$$

Obviously $\Delta_3=\Theta_3=0$. For $m\geq 4$, by $\sum_{i=0}^{m}t_i=\frac{t_m+t_{m+2}-3}{2}$ and $\sum_{i=1}^{m}k_i=\frac{t_{m-2}+t_{m-3}+m}{2}$, we have $\Delta_m=\frac{t_{m-2}+t_{m-3}-m}{2}$ and $\Theta_m=\frac{t_{m-2}-t_{m-3}+2t_{m-4}+m-6}{2}$.

4 The number of distinct squares in $\mathbb{T}[1, n]$

By Property 7, $\langle i, K_m\rangle$ are pairwise disjoint, and each set contains some consecutive integers. Therefore we get a chain

$$\langle 3, K_4\rangle, \langle 2, K_4\rangle, \langle 1, K_4\rangle, \langle 3, K_5\rangle, \cdots, \langle 3, K_m\rangle, \langle 2, K_m\rangle, \langle 1, K_m\rangle, \cdots$$

Denote $a(n) := \sharp\{\omega : \omega\omega \prec \mathbb{T}[1, n], \omega\omega \not\prec \mathbb{T}[1, n-1]\}$, then $a(n) = 1$ iff $n \in \cup_{m\geq 4}(\langle 3, K_m\rangle \cup \langle 2, K_m\rangle \cup \langle 1, K_m\rangle)$. The "$\cup$" in this note always means disjoint union. Since $\max\langle 1, K_m\rangle + 1 = \min\langle 3, K_{m+1}\rangle$, sets $\langle 1, K_m\rangle$ and $\langle 3, K_{m+1}\rangle$ are consecutive. We have $\langle 1, K_m\rangle \cup \langle 3, K_{m+1}\rangle = \{2t_{m-1}, \cdots, t_m + 2t_{m-3} - 1\}$.

Property 8. *For $n < 14$, $a(n) = 1$ iff $n \in \{8, 10\}$; for $n \geq 14$, let m such that $2t_{m-1} \leq n < 2t_m$, then $m \geq 4$ and $a(n) = 1$ iff*

$$n \in \{2t_{m-1}, \cdots, t_m + 2t_{m-3} - 1\} \cup \{2t_m - t_{m-1}, \cdots, t_m + k_{m+3} - 2\}.$$

Denote $A(n) := \sharp\{\omega : \omega\omega \prec \mathbb{T}[1, n]\}$, which is the number of distinct squares in $\mathbb{T}[1, n]$. Then $A(n) = \sum_{i=1}^{n} a(i)$. For $n \geq 14$, find the m such that $2t_{m-1} \leq n < 2t_m$, then $m \geq 4$. Denote

$$\begin{cases} \alpha_m := \min\langle 1, K_m\rangle = 2t_{m-1}, \ \beta_m := \max\langle 3, K_{m+1}\rangle = t_m + 2t_{m-3} - 1, \\ \gamma_m := \min\langle 2, K_{m+1}\rangle = 2t_m - t_{m-1}, \\ \theta_m := \max\langle 2, K_{m+1}\rangle = t_m + k_{m+3} - 2 = \frac{3t_m + t_{m-2} - 3}{2}. \end{cases}$$

By Property 8 and the definition of Δ_m, Θ_m, for $m \geq 4$

$$\begin{cases} A(\alpha_m) = \Delta_{m-1} + \Delta_m + \Theta_m + 1 = \frac{2t_{m-2} + t_{m-3} + 3t_{m-4} - m - 3}{2}, \\ A(\beta_m) = \Delta_m + \Delta_m + \Theta_{m+1} = \frac{t_{m-1} + t_{m-2} + 4t_{m-3} - m - 5}{2}, \\ A(\gamma_m) = \Delta_m + \Delta_m + \Theta_{m+1} + 1 = A(\beta_m) + 1, \\ A(\theta_m) = \Delta_m + \Delta_{m+1} + \Theta_{m+1} = A(\alpha_{m+1}) - 1. \end{cases}$$

Obviously, when $\alpha_m \leq n < \beta_m$, $A(n) = A(\alpha_m) + n - \alpha_m$; when $\beta_m \leq n < \gamma_m$, $A(n) = A(\beta_m)$; when $\gamma_m \leq n < \theta_m$, $A(n) = A(\gamma_m) + n - \gamma_m$; when $\theta_m \leq n < \alpha_{m+1}$, $A(n) = A(\theta_m)$. So

Theorem 9 (The numbers of distinct squares, $A(n)$)**.** *$A(n) = 0$ for $n \leq 7$; $A(n) = 1$ for $n = 8, 9$; $A(n) = 2$ for $10 \leq n \leq 13$. For $n \geq 14$, let m such that $\alpha_m \leq n < \alpha_{m+1}$, then $m \geq 4$,*

$$A(n) = \begin{cases} n - \frac{1}{2}(t_m + t_{m-3} + m + 3), & \alpha_m \leq n < \beta_m; \\ \frac{1}{2}(t_{m-1} + t_{m-2} + 4t_{m-3} - m - 5), & \beta_m \leq n < \gamma_m; \\ n - \frac{1}{2}(t_{m-1} + 3t_{m-2} + m + 3), & \gamma_m \leq n < \theta_m; \\ \frac{1}{2}(2t_{m-1} + t_{m-2} + 3t_{m-3} - m - 6), & \theta_m \leq n < \alpha_{m+1}. \end{cases}$$

Example. Count the numbers of distinct squares in $\mathbb{T}[1, 355]$, i.e. $A(355)$.

Since $n = 355 \geq 14$ and $2t_8 = 298 \leq n = 355 < 2t_9 = 548$, $m = 9$. Moreover $n < \beta_9 = t_9 + 2t_6 - 1 = 361$, so $C(355) = 355 - \frac{1}{2}(t_9 + t_6 + 12) = 190$.

For $m \geq 3$, since $\theta_{m-1} = \frac{3t_{m-1} + t_{m-3} - 1}{2} \leq t_m < \alpha_m$, by Theorem 9, we have $A(t_m) = A(\theta_{m-1})$ for $m \geq 5$. It is easy to check the expression holds also for $m = 3, 4$. Thus for $m = 0, 1, 2$, $A(t_m) = 0$, and

Theorem 10. *For $m \geq 3$, $A(t_m) = \frac{1}{2}(2t_{m-2} + t_{m-3} + 3t_{m-4} - m - 5)$.*

Remark 11. A.Glen show the number of distinct squares in T_m, i.e. $A(t_m)$ in Theorem 6.30 in [3], that $A(t_m) = \sum_{i=0}^{m-2}(d_i+1)+d_{m-4}+d_{m-5}+1$ for $m \geq 3$, where $d_{-2} = d_{-1} = -1$, $d_0 = 0$ and $d_m = \frac{t_{m+1}+t_{m-1}-3}{2}$ for $m \geq 1$. By the expression of $\sum_{i=0}^{m} t_i$, we know the two expressions of $A(t_m)$ are same.

5 The number of distinct cubes in $\mathbb{T}[1, n]$

Let ω be a factor with kernel K_m, by analogous arguments as Section 3 and 4, we have: (1) all cubes in $\mathbb{T}$ are of length $3t_m$ for some $m \geq 3$; (2) for all $m \geq 3$, there exists a cube of length $3t_m$, which is Theorem 7 in [8]. Moreover,

Theorem 12 (The numbers of distinct cubes, $B(n)$)**.** *$B(n) = 0$ for $n \leq 57$. For $n \geq 58$, let m such that $t_{m-1} + 2t_{m-4} \leq n < t_m + 2t_{m-3}$, then $m \geq 7$,*

$$B(n) = \begin{cases} n - \frac{1}{2}(4t_{m-1} - t_{m-2} - 3t_{m-3} + m - 6), & n \leq \frac{3t_{m-1}-t_{m-3}-3}{2}; \\ \frac{1}{2}(t_{m-5} + t_{m-6} - m + 3), & \textit{otherwise}. \end{cases}$$

Example. Count the numbers of distinct cubes in $\mathbb{T}[1, 365]$, i.e. $B(365)$.

Since $n = 365 \geq 58$ and $t_9 + 2t_6 = 362 \leq n = 365 < t_{10} + 2t_7 = 666$, $m = 10$. Moreover $n < t_9 + k_{11} - 2 = 369$, $B(365) = 365 - \frac{4t_9-t_8-3t_7+4}{2} = 11$.

For $m \geq 7$, since $t_m > \frac{3t_{m-1}-t_{m-3}-3}{2}$, by Theorem 12, we have

Theorem 13. *For $m \leq 6$, $B(t_m) = 0$, for $m \geq 7$, $B(t_m) = \frac{t_{m-5}+t_{m-6}-m+3}{2}$.*

6 Open Problems

In 2014, H.Mousavi and J.Shallit[8] gave explicit expressions about the numbers of repeated squares and cubes in the Tribonacci word T_m, which they proved by mechanical way. In [7], we give fast algorithms for counting the numbers of repeated squares and cubes in each prefix of the Fibonacci sequence. But we have not yet succeeded in giving fast algorithms for counting the numbers of repeated squares and cubes in $\mathbb{T}[1, n]$ for all n by our method.

References

[1] C.-F.Du, H.Mousavi, L.Schaeffer, J.Shallit. Decision Algorithms for Fibonacci-Automatic Words, with Applications to Pattern Avoidance. Eprint Arxiv, 2014.

[2] E.Duchêne, M.Rigo. A morphic approach to combinatorial games: the Tribonacci case, RAIRO-Theoretical Informatics and Applications. 42 (2008) 375-393.

[3] A.Glen. On Sturmian and Episturmian Words, and Related Topics, PhD thesis, The University of Adelaide, Australia. 2006.

[4] Y.-K.Huang, Z.-Y.Wen. The sequence of return words of the Fibonacci sequence, Theoretical Computer Science. 593 (2015) 106-116.

[5] Y.-K.Huang, Z.-Y.Wen. Kernel words and gap sequence of the Tribonacci sequence, Acta Mathematica Scientia (Series B). 36.1 (2016) 173-194.

[6] Y.-K.Huang, Z.-Y.Wen. The structure of palindromes in the Fibonacci sequence. arXiv:1601.04391.

[7] Y.-K.Huang, Z.-Y.Wen. The number of distinct and repeated squares and cubes in the Fibonacci sequence. arXiv:1603.04211.

[8] H.Mousavi, J.Shallit. Mechanical proofs of properties of the Tribonacci word. Combinatorics on Words. Springer International Publishing. 2014, 170-190.

[9] S.W.Rosema, R.Tijdeman. The Tribonacci substitution. INTEGERS: Elect J of Combin Number Theory, 5.3 (2005) ♯A13.

[10] G.Richomme, K.Saari, L.Q.Zamboni. Balance and Abelian complexity of the Tribonacci word. Advance Applied Mathematic, 45 (2010) 212-231.

[11] B.Tan, Z.-Y.Wen. Some properties of the Tribonacci sequence. European J Combin, 28 (2007) 1703-1719.

[12] Z.-X.Wen, Z.-Y.Wen. Some properties of the singular words of the Fibonacci word. European J Combin, 15 (1994) 587-598.

Some Improvements on Number Expansion Computations

Péter Hudoba, Attila Kovács

Eötvös Loránd University, Hungary

Let Λ be a lattice in $\mathbb{R}^n$ and let $M : \Lambda \to \Lambda$ be a linear operator such that $\det(M) \neq 0$. Let furthermore $0 \in D \subseteq \Lambda$ be a finite subset. Lattices can be seen as finitely generated free abelian groups or set of points in euclidean spaces.

Lattices have many significant applications in pure mathematics (Lie algebras, number theory and group theory), in applied mathematics (coding theory, cryptography) because of conjectured computational hardness of several lattice problems, and are used in various ways in the physical sciences.

We consider number expansions in lattices.

Definition 1. The triple (Λ, M, D) is called a *number system* (GNS) if every element x of Λ has a unique, finite representation of the form

$$x = \sum_{i=0}^{L} M^i d_i \ ,$$

where $d_i \in D$ and $L \in \mathbb{N}$. L is the *length of the expansion.*

Here M is called the *base* and D is the *digit set.* It is easy to see that similarity preserves the number system property, i.e., if M_1 and M_2 are similar via the matrix Q then (Λ, M_1, D) is a number system if and only if $(Q\Lambda, M_2, QD)$ is a number system at the same time. If we change the basis in Λ a similar integer matrix can be obtained, hence, no loss of generality in assuming that M is integral acting on the lattice $\mathbb{Z}^n$.

If two elements of Λ are in the same coset of the factor group $\Lambda/M\Lambda$ then they are said to be *congruent* modulo M. The following theorem is well-known.

Theorem 2. *If* (Λ, M, D) *is a number system then*

1. *D must be a full residue system modulo M,*
2. *M must be expansive,*
3. $\det(I_n - M) \neq \pm 1$. (unit condition)

If a system fulfills the first two conditions then it is called a radix system.

Let $\varphi : \Lambda \to \Lambda$, $x \overset{\varphi}{\mapsto} M^{-1}(x - d)$ for the unique $d \in D$ satisfying $x \equiv d \pmod{M}$. Since M^{-1} is contractive and D is finite, there exists a norm $\|.\|$ on Λ and a constant C such that the orbit of every $x \in \Lambda$ eventually enters the finite set $S = \{x \in \Lambda \mid \|x\| < C\}$ for the repeated application of φ. This means that the sequence $x, \varphi(x), \varphi^2(x), \dots$ is eventually periodic for all $x \in \Lambda$. Clearly, (Λ, M, D) is a number system iff for every $x \in \Lambda$ the orbit of x eventually reaches 0.

A point p is called *periodic* if $\varphi^k(p) = p$ for some $k > 0$. The orbit of a periodic point p is a *cycle*. The set of all periodic points is denoted by $\mathcal{P}$.

The following problem classes are in the mainstream of the research: for a given (Λ, M, D)

- the *decision problem* asks if the triple form a number system or not.
- the *classification problem* means finding all cycles (*witnesses*).
- the *parametrization problem* means finding parametrized families of number systems.
- the *construction problem* aims at constructing a digit set D to M for which (Λ, M, D) is a number system.

The algorithmic complexity of the decision and classification problems is still unknown. We summarize the earlier results of the known algorithmic approaches and we suggest new methods improving the running time of the computations. The measurements are performed using the computer algebra system Sage. We show how to compute efficiently the discrete dynamics of the expansions, how to construct the appropriate norm which is indispensable for constructing dense digit sets.

References

[1] Kovács, A., *On computation of attractors for invertible expanding linear operators in* $\mathbb{Z}^k$, Publ. Math. Debrecen **56**/1–2, (2000), 97–120.

[2] Burcsi, P., Kovács, A., Papp-Varga, Zs., *Decision and Classification Algorithms for Generalized Number Systems*, Annales Univ. Sci. Budapest, Sect. Comp., **28**, (2008), 141–156.

Simultaneous Approximation Problems and Knapsack Cryptosystems in p-Adic Numberlands

Hirohito Inoue, Shoichi Kamada, Koichiro Naito, Keisuke Shiromoto

Graduate School of Science and Technology, Kumamoto University, Japan

1 Introduction

In the usual real numbers case the shortest vector problems (SVP) and the simultaneous approximation problems (SAP) have the computational complexity, NP-hardness or NP-completeness (cf. [5], [2]). The security of some modern cryptosystems is based on the hardness of these problems and the lattice-based cryptography is considered as one of the most powerful post-quantum cryptography.

In the first part of this paper, extending the two-dimensional p-adic approximation lattices given by de Weger in [7] to multi-dimensional cases, we construct the multi-dimensional p-adic approximation lattices by using the SAP of p-adic numbers. Here the strong triangle inequality condition, which gives the significant properties in a field or a ring of p-adic numbers, plays the most essential role. We estimate the l_∞ norm of the p-adic SAP solutions theoretically by applying Dirichlet's principle and numerically by using the LLL algorithm (cf. [4]).

In the second part, using the results in the first part, we propose new lattice based cryptosystems. First we introduce a p-adic knapsack cryptosystem in which we use a p-adic decreasing sequence instead of a super increasing sequence of usual integers. Knapsack cryptosystems of usual real numbers have been broken by several attacks. Our p-adic knapsack system can resist Shamir's method in [6], which attacks against the super increasing properties, but our system is not sufficiently secure against the low density attacks in [3] by using LLL algorithms. Next we propose a p-adic knapsack cryptosystem with commitment schemes, a typical example of which is a digital signature. Since we implement our p-adic cryptosystem in the open software Sage, we prepare the sets of p-adic numbers, described by the computational style in Sage and the transformations between these p-adic numbers and the usual integers. We call the set of the numbers with these transformations a p-adic numberland. We give the two p-adic numberlands, one is for Bob, a receiver, and the other is for Alice, a sender. The encryption and the decryption procedures are performed in each p-adic numberland and the opening or the public keys and the ciphertexts in the communication procedures are constructed by using the usual integers. Finally, we give a numerical example with small parameters to show the outline of our system.

2 Multi-dimensional p-adic approximation lattice

Let p be a fixed rational prime number and $|\cdot|_p$ be the corresponding p-adic absolute value, normalized so that $|p|_p = p^{-1}$. The completion of $\mathbb{Q}$ w.r.t. $|\cdot|_p$ is called the field of p-adic numbers, denoted by $\mathbb{Q}_p$. The set of p-adic integers is defined by

$$\mathbb{Z}_p = \{z \in \mathbb{Q}_p : |z|_p \leq 1\}.$$

We introduce p-adic approximation lattices and investigate simultaneous rational approximation problems of p-adic numbers. Let $n \geq 1$ be an integer and let $\Xi = \{\xi_1, \xi_2, \dots, \xi_n\}$ be the n-tuple of p-adic integers. For a positive integer m we define the p-adic approximation lattice Γ_m by

$$\Gamma_m = \{(a_0, a_1, \dots, a_n) \in \mathbb{Z}^{n+1} : |a_0 + a_1\xi_1 + \cdots + a_n\xi_n|_p \leq p^{-m}\}.$$

When a p-adic integer ξ_i has the p-adic expansion

$$\xi_i = \sum_{k=0}^{\infty} x_{i,k}p^k, \ x_{i,k} \in \{0, 1, \dots, p-1\},$$

let $\xi_{i,m}$ be the m-th order approximation of ξ_i defined by $\xi_{i,m} = \sum_{k=0}^{m-1} x_{i,k}p^k$. Using the basis $\{\mathbf{b}_{0,m}, \mathbf{b}_{1,m}, \dots, \mathbf{b}_{n,m}\} \subset \mathbb{Z}^{n+1}$ of the lattice Γ_m given by $\mathbf{b}_{0,m} = (p^m, 0, 0, \dots, 0)^t$, $\mathbf{b}_{i,m} = (\xi_{i,m}, -1, 0, \dots, 0)^t$, $i = 1, ..., n$, we define the matrix $B_m = (\mathbf{b}_{0,m}\mathbf{b}_{1,m} \dots \mathbf{b}_{n,m})$,

$$B_m = \begin{pmatrix} p^m & \xi_{1,m} & \xi_{2,m} & \cdots & \xi_{n,m} \\ 0 & -1 & 0 & \dots & 0 \\ 0 & 0 & -1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & -1 \end{pmatrix}. \tag{1}$$

By applying the LLL algorithm for B_m with $\delta \in (1/4, 1)$, we can obtain a reduced basis $\{\mathbf{b}_0, \dots, \mathbf{b}_n\}$ and for the minimum vector $\mathbf{b}_0$ in this basis it is known (cf. [5]) that

$$\|\mathbf{b}_0\|_2 \leq \sqrt{n+1}\, p^{\frac{m}{n+1}} \left(\frac{2}{\sqrt{4\delta - 1}}\right)^n$$

holds.

Let $\lambda_1^{(\infty)}(\Gamma_m)$ be the length of the shortest vector of the lattice Γ_m in the l_∞ norm. In our previous paper [1] we have given the upper bound of $\lambda_1^{(\infty)}(\Gamma_m)$ by using the famous Dirichlet principle,

$$\lambda_1^{(\infty)}(\Gamma_m) \leq p^{\frac{m}{n+1}} = \det(\Gamma_m)^{\frac{1}{n+1}}.$$

Also, using the LLL algorithms, we have numerically shown that this estimate holds if the dimension n is under 60.

3 Knapsack Cryptosystem with Commitment Schemes

We give a p-adic knapsack cryptosystem, which is a public key cryptosystem, using the isosceles principle of p-adic numbers as a trapdoor. Since we implement our cryptosystems of p-adic numbers in Sage, we introduce the following notations.

For a prime number p, an approximation order m and a precision M, a precise description order of each p-adic number used in Sage, we consider the following mathematical and practically computational objects. Let $\mathbb{Z}_p^{(M)}$ be a set of p-adic integers such that each $\xi \in \mathbb{Z}_p^{(M)}$ has the description

$$\xi = a_0 + a_1 p + a_2 p^2 + \cdots + a_{M-1} p^{M-1} + O(p^M)$$

as in Sage. For a p-adic number ξ given by $\xi = \sum_{k=0}^{\infty} a_k p^k$, we define an integer-valued function $To\_int(p, m, \xi)$ by

$$To\_int(p, m, \xi) = \sum_{k=0}^{m-1} a_k p^k := \xi_m \in \mathbb{Z}.$$

On the contrary, for $z = \sum_{k=0}^{l} b_k p^k \in \mathbb{Z}$, we introduce a p-adic number valued function $To\_pad(p, z)$ defined by

$$To\_pad(p, z) = \sum_{k=0}^{M-1} b_k p^k + O(p^M) \in \mathbb{Z}_p^{(M)}$$

where $b_k = 0,\ k \geq l + 1$. Then we call the set $\mathbb{Z}_p^{(M)}$ with these transformations $To\_int(p, m, \xi), To\_pad(p, z)$ a p-adic numberland $\{p, m, M\}$.

We consider a knapsack cryptosystem with commitment schemes, where we provide a p-adic numberland $\{p, m, M\}$ for Bob and the other p-adic numberland $\{p_0, m_0, M_0\}$ for Alice. Hereafter we set $M = M_0$ for simplicity.

Key Generation

Bob chooses the following private keys; a prime number p, an approximation order m, and a p-adic decreasing sequence $\eta = (\eta_{1,m}, \ldots, \eta_{n,m}) :\ |\eta_{i,m}|_p > |\eta_{i+1,m}|_p$. Furthermore, he sets a sufficiently large prime number q as a modulus, such that $q > np^m$, and a large random integer r which satisfies $\gcd(p, r) = 1$ and $rp^m > q$. Let s be the inverse of r modulo q, that is, $sr \equiv 1 \pmod{q}$.

Bob calculates $\beta = (\beta_1, \beta_2, \ldots, \beta_n) \in \mathbb{Z}^n$ as a public key defined by $\beta_i \equiv r\eta_{i,m} \pmod{q}$.

Alice chooses one of the components of the public key $\beta = (\beta_1, \beta_2, \ldots, \beta_n)$, say β_{k_0}, and by using its powers she constructs a vector $\gamma = (\gamma_1, \gamma_2, ..., \gamma_n) \in \mathbb{Z}^n$ given by $\gamma_i = \beta_{k_0}^i,\ i = 1, ..., n$. Next she calculates their p-adic numbers $\xi = (\xi_1, \xi_2, \ldots, \xi_n) \in \mathbb{Z}_p^n$ given by $\xi_i = To\_pad(p_0, \gamma_i),\ \ i = 1, ..., n$. Then she can obtain the m_0-th order approximation vector $\xi_{m_0} = (\xi_{1,m_0}, \cdots, \xi_{n,m_0})$ given by

$$\xi_{i,m_0} = To\_int(p_0, m_0, \xi_i) \in \mathbb{Z}, \quad i = 1, ..., n.$$

Alice produces a secret key $(a_0, a_1, ..., a_n) \in \mathbb{Z}^n$, which can be obtained by applying LLL for B_{m_0} in the suitably partitioned SAP and combining these solutions in her p-adic numberland. Then, due to the strong triangle inequality,

$$|\sum_{i=0}^{n} a_i \xi_{i,m_0}|_{p_0} \leq p_0^{-m_0}, \quad \max_i |a_i| \leq p_0^{m_0/(n_0+1)} := K, \tag{2}$$

hold where $\xi_0 = \xi_{0,m_0} = 1$ and n_0 is the dimension of the smallest partitioned SAP.

Next Alice randomly constructs her private key $\{\sigma_i\}$ and her opening key $\{\rho_i\}$ from the secret key $\{a_i\}$, which satisfy

$$a_i = \sigma_i + \rho_i, \ \sigma_i, \rho_i \in \mathbb{Z} : \ |\sigma_i|, |\rho_i| \leq K, \quad i = 0, 1, ..., n.$$

Encryption

For a plaintext $\mathbf{x} = (x_1, \ldots, x_n) \in \{0, 1\}^n$, Alice computes a ciphertext C given by

$$C = \sum_{i=0}^{n} \sigma_i \xi_{i,m_0} + \sum_{i=1}^{n} x_i \beta_i.$$

At the first stage she sends (C, p_0, m_0, k_0), the ciphertext C with the opening keys p_0, m_0, k_0, to Bob. Bob checks the inequality condition $q < p_0^{m_0}$, then if this condition is satisfied, he returns the number 0 as his check message to Alice. Otherwise, he returns the minimum positive integer d, which satisfies $q < p_0^{m_0+d}$.

At the second stage she sends the opening key $\{\rho_i\}$ if she receives the check message 0. Otherwise, if she receives a positive integer d, she chooses a pair of small nonnegative integers (c_0, d_0) such that $p_0^{m_0+d} < (p_0 + c_0)^{m_0+d_0}$ and $p_0 + c_0$ is a prime number. By putting $p_1 = p_0 + c_0, m_1 = m_0 + d_0$ and following the key generation procedure in her new p-adic numberland $\{p_1, m_1, M\}$, Alice reconstructs the new m_1-th order approximation vector $\xi'_{m_1} = (\xi'_{1,m_1}, ..., \xi'_{n,m_1}) \in \mathbb{Z}^n$ from the public key $\beta \in \mathbb{Z}^n$ by choosing the k_1-th component β_{k_1}. By the same way as in the previous key generation steps she can obtain her secret key $\{a'_i\}$ by applying LLL and randomly, her private key $\{\sigma'_i\}$ and her opening key $\{\rho'_i\}$, which satisfies $a'_i = \sigma'_i + \rho'_i$. Then she reconstructs the ciphertext C_1 given by

$$C_1 = \sum_{i=0}^{n} \sigma'_i \xi'_{i,m_1} + \sum_{i=1}^{n} x_i \beta_i$$

where $\xi'_{0,m_1} = 1$ and she sends her cipher-vector (C_1, p_1, m_1, k_1) to Bob.

At the third stage, after the check message 0 from Bob, she sends the opening key $\{\rho'_i\}$.

Decryption

Since the decryption procedure can be performed by the same manner in each case, here we treat the case where the first stage is successful without Alice's reconstructions. Using Alice's opening keys $p_0, m_0, k_0, \{\rho_i\}$, Bob first computes ξ_{i,m_0} by

$$\xi_{i,m_0} = To\_int(p_0, m_0, To\_pad(p_0, \beta^i_{k_0})) \in \mathbb{Z}, \quad i = 1, .., n.$$

Now he can compute C' given by

$$C' := C + \sum_{i=0}^{n} \rho_i \xi_{i,m_0} = \sum_{i=0}^{n} a_i \xi_{i,m_0} + \sum_{i=1}^{n} x_i \beta_i$$

and, taking modulo $p_0^{m_0}$, he obtains C''

$$C'' := \sum_{i=1}^{n} x_i \beta_i \equiv C' \pmod{p_0^{m_0}}.$$

Using the private key s, he can computes C''' given by

$$C''' := \sum_{i=1}^{n} x_i \eta_{i,m} \equiv sC'' \pmod{q},$$

since the inequality condition $q < p_0^{m_0}$ holds. Using the decreasing property of η and the isosceles principle on p-adic numbers, Bob obtains the original message by the following steps in his p-adic numberland $\{p, m, M\}$.

1st-step
If $|C'''|_p = |\eta_{1,m}|_p$, then $x_1 = 1$, otherwise $x_1 = 0$.

2nd-step
If $|C''' - x_1\eta_{1,m}|_p = |\eta_{2,m}|_p$, then $x_2 = 1$, otherwise $x_2 = 0$.

$\vdots$

n**th-step**
If $|C''' - (x_1\eta_{1,m} + \cdots + x_{n-1}\eta_{n-1,m})|_p = |\eta_{n,m}|_p$, then $x_n = 1$, otherwise $x_n = 0$.

By the above n steps Bob can correctly decrypt the message x from Alice.

4 Concluding remark

In the most recent post-quantum cryptography (PQC) multi-sender-multi-receiver cryptosystems provide most attractive research topics. Since so many p-adic numberlands in a network cloud must be prepared in these multiple cases, the ring of adeles or the group of ideles will become significant mathematical objects, which will be able to provide sufficiently many and useful p-adic numberlands to Alice's and Bob's groups, in a post-quantum world.

References

[1] H. Inoue, K. Naito, *The shortest vector problems in p-adic lattices and simultaneous approximation problems of p-adic numbers*, to appear in proc. of ICM Satellite Conference 2014: The 4th Asian Conf. on Nonlinear Analysis and Optim.

[2] J. C. Lagarias, *The computational complexity of simultaneous Diophantine approximation problems*, SIAM Journal on Computing **14** (1985), 196–209.

[3] J. C. Lagarias, A. M. Odlyzko, *Solving low-density subset sum problems*, Journal of the ACM **32** (1985), 229–246.

[4] A. K. Lenstra, H. W. Lenstra, and L. Lovász. *Factoring polynomials with rational coefficients*, Mathematische Annalen **261** (1982), 515–534.

[5] D. Micciancio and S. Goldwasser, “Complexity of Lattice Problems, a Cryptographic Perspective", Springer International Series in Engineering and Computer Science **671**, Springer 2002.

[6] A. Shamir, *A polynomial time algorithm for breaking the basic Merkle-Hellman cryptosystem*, 23rd Annual Symposium on Foundations of Computer Science 1982, 145–152.

[7] B.M.M. de Weger, *Approximation Lattices of p-adic Numbers*, Journal of Number Theory. **24** (1986), 70–88.

Two Properties Related to β-Expansions*

Maria Rita Iacò[(1)], Wolfgang Steiner[(1)], Robert Tichy[(2)]

[(1)] Université Paris Diderot – Paris 7

[(2)] Graz University of Technology

Let $(G_n)_{n\in\mathbb{N}}$ be an increasing sequence of positive integers, with initial value $G_0 = 1$. Then every positive integer can be greedly expanded as

$$n = \sum_{k=0}^{\infty} \varepsilon_k(n) G_k \ ,$$

where $\varepsilon_k(n) \in \{0, \dots, \lceil G_{k+1}/G_k \rceil - 1\}$. This expansion (called G-expansion) is uniquely determined and finite, provided that for every K

$$\sum_{k=0}^{K-1} \varepsilon_k(n) G_k < G_K \ . \tag{1}$$

We denote by $\mathcal{K}_G$ the subset of sequences that satisfy (1) and we call its elements G-admissible. The addition-by-one map τ defined on $\mathbb{N}$ can be naturally extended to $\mathcal{K}_G$ and the dynamical system $(\mathcal{K}_G, \tau)$ is called odometer (or G-odometer). In particular, we are interested in the digit expansion of integers with respect to the linear recurrence

$$G_{n+1} = \sum_{k=0}^{n} a_{n-k} G_k + 1 \ , \qquad G_0 = 1 \ .$$

It has been shown in [1] that G-odometers on systems $\mathcal{K}_G$, where the base sequence is a finite linear recurrence are continuous and $(\mathcal{K}_G, \tau)$ is uniquely ergodic. In [1, Theorem 5], the authors provide also an explicit formula for the unique invariant measure μ defined on $\mathcal{K}_G$. Moreover, they use the following condition to prove that $\mathcal{K}_G$ has purely discrete spectrum. - There exists an integer $b > 0$ such that for all k and

$$N = \sum_{i=0}^{k-1} \epsilon_i(N) G_i + \sum_{j=k+b+1}^{\infty} \epsilon_j(N) G_j,$$

the addition of G_m to N, where $m \geq k + b + 1$, does not change the first k digits in the greedy representation i.e.

$$N + G_m = \sum_{i=0}^{k-1} \epsilon_i(N) G_i + \sum_{j=k}^{\infty} \epsilon_j(N + G_m) G_j.$$

*The authors are participants in the ANR/FWF project FAN "Fractals and Numeration" (ANR-12-IS01-0002, FWF grant I1136).

The sequence of integers G_n is strongly connected with the expansion in an non-integer base β. More precisely, let $\beta > 1$ be a fixed real number. A β-expansion of a positive real number x in $[0,1)$ can be obtained via the iteration of the so-called β-transformation T_β defined by

$$T_\beta \colon [0,1) \to [0,1)\ , \quad x \mapsto \beta x - \lfloor \beta x \rfloor\ ,$$

where $\lfloor x \rfloor$ is the largest integer not exceeding x. Taking at each iteration of T_β $\epsilon_i = \lfloor \beta T_\beta^{i-1}(x) \rfloor$, we obtain the following greedy expansion of x

$$x = \sum_{k=1}^{\infty} \epsilon_k \beta^{-k} = 0.\epsilon_1\epsilon_2\epsilon_3 \dots\ .$$

Then the sequence $(G_n)_{n\geq 0}$ associated to β is defined

$$G_j = \sum_{k=1}^{j} a_k G_{j-k} + 1, \quad \text{with} \quad a_k = \lceil \beta\, \tilde{T}_\beta^{k-1}(1) \rceil - 1.$$

For $\beta > 1$, we can also define the *quasi-greedy β-transformation* as

$$\tilde{T}_\beta :\ (0,1] \to (0,1], \quad x \mapsto \beta x - \lceil \beta x \rceil + 1.$$

It differs from T_β only at the points of discontinuity. Let

$$V_\beta = \big\{ \tilde{T}_\beta^k(1) : k \geq 0 \big\}.$$

If V_β is finite, then β is called a *Parry number*. Il β is such that

$$\forall\, x \in \mathbb{Z}_+[\beta^{-1}] \cap [0,1)\ \exists\, k \geq 0 : T_\beta^k(x) = 0\ , \tag{PF}$$

where $\mathbb{Z}_+ = \mathbb{Z} \cap [0,+\infty)$, we say that β has the positive finiteness property (PF).

We will now briefly describe a property introduced in the framework of tilings associated to Pisot β-numerations. Let σ be a primitive substitution on the alphabet $A = \{1,2,\dots,m\}$ and $M_\sigma = (|\sigma(j)|_i)_{i,j\in A}$ its incidence matrix with dominant eigenvalue $\beta > 1$. Let $\mathbf{v} = (v_1, v_2, \dots, v_n)$ be a left eigenvector of M_σ to the eigenvalue β, with $v_i \in \mathbb{Q}(\beta)$, and

$$L_\sigma = \langle v_i - v_j :\ i,j \in A \rangle_{\mathbb{Z}}$$

be the $\mathbb{Z}$-module generated by the differences of coordinates of $\mathbf{v}$. Note that $\mathbf{v}$ and L_σ are only defined up to a constant factor, which plays no role in the following. The *quotient mapping condition* states that

$$\operatorname{rank}(L_\sigma) = \deg(\beta) - 1 \tag{QM}$$

This definition is equivalent to Definition 3.13 in [2].

In the first of our main results in this paper we show that (QM) is a necessary condition for the discreteness of the spectrum of the β-odometer of β-admissible sequences

$$\mathcal{K}_\beta = \Big\{ (\epsilon_j)_{j\geq 0} \in \{0,1,\dots,\lceil\beta\rceil - 1\}^{\mathbb{N}} : \sum_{j=1}^{k} \frac{\epsilon_{k-j}}{\beta_j} \in [0,1) \text{ for all } k \geq 1 \Big\}.$$

Theorem 1. *Let β be a Pisot number satisfying* (QM). *Then the odometer $(\mathcal{K}_\beta, \tau_\beta)$ has pure discrete spectrum.*

Theorem 2. *Let β be a Parry number. Hypothesis B holds for the sequence $(G_j)_{j\geq 0}$ associated to β if and only if conditions* (PF) *and* (QM) *hold.*

References

[1] P. J. Grabner, P. Liardet, and R.F. Tichy. Odometers and systems of numeration. Acta Arith, 70(2), 103-123 (1995).

[2] A. Siegel, and J. M. Thuswaldner. Topological properties of Rauzy fractals. Mem. Soc. Math. Fr. (N.S.), 118- 140 (2009).

Pisot-Salem Numbers, Interlacing and $\{0, 1\}$-Words

Jonas Jankauskas

Montanuniversität Leoben, Austria

In 2012, C. Smyth and J. McKee established the necessary and sufficient condition for the pair of self-inversive polynomials $Q(z)$ and $R(z)$ in $\mathbb{Q}[z]$ to give a rise to the minimal polynomial $P(z)$ of a Pisot number. This condition is given in terms of the interlacing pattern for the roots of $Q(z)$ and $R(z)$ on the unit circle.

The main purpose of my talk is to provide a combinatorial proof of this result and to point out a possible generalization: such patterns correspond to binary words on $\{0, 1\}$ having *almost maximal* reduced lenght $l(w)$ - a certain function that measures the winding number of the polynomial $P(z)$ on the unit circle. A general root-counting formula for $P(z)$ that is based on the same function $l(w)$ can be used to establish the interlacing patterns that give rise to complex-Pisot numbers.

This talk is based on the manuscript *Binary words, winding numbers and polynomials with interlaced roots* (submitted).

Multiple Expansions of Real Numbers Over Digit Set $\{0, 1, q\}$

Kan Jiang

Utrecht University, Netherlands

For $q > 1$ we consider expansions in base q over the alphabet $\{0, 1, q\}$. Let U_q be the set of x which have a unique q-expansions. For $k = 2, 3, \ldots, \aleph_0$ let $\mathbb{B}_k$ be the set of bases q for which there exists x having k different q-expansions, and for $q \in \mathbb{B}_k$ let $U_q^{(k)}$ be the set of all such x's which have k different q-expansions. In this paper we show that

$$\mathbb{B}_{\aleph_0} = [2, \infty), \quad \mathbb{B}_k = (q_c, \infty) \quad \text{for any} \quad k \geq 2,$$

where $q_c \approx 2.32472$ is the appropriate root of $x^3 - 3x^2 + 2x - 1 = 0$. Moreover, we show that for any positive integer $k \geq 2$ and any $q \in \mathbb{B}_k$ the Hausdorff dimensions of $U_q^{(k)}$ and U_q are the same, i.e.,

$$\dim_H U_q^{(k)} = \dim_H U_q \quad \text{for any} \quad k \geq 2.$$

Finally, we conclude that the set of x having a continuum of q-expansions has full Hausdorff dimension. This is joint work with Karma Dajani, Derong Kong and Wenxia Li.

Critical Bases for Ternary Alphabets

Vilmos Komornik[1], Marco Pedicini[2]

[1] IRMA, Université de Strasbourg

[2] Department of Mathematics and Physics, Roma Tre University

Glendinning and Sidorov discovered an important feature of the Komornik-Loreti constant $q' \approx 1.78723$ in non-integer base expansions on two-letter alphabets: in bases $1 < q < q'$ only countably numbers have unique expansions, while for $q \geq q'$ there is a continuum of such numbers. We investigate the analogous question for ternary alphabets.

From Redundant Digit Expansions via Continued Fractions to (Non-)Minimal Expansions*

Daniel Krenn

Institut für Mathematik, Alpen-Adria-Universität Klagenfurt, Austria

Abstract

This talk will be about redundant digit expansions with an imaginary quadratic algebraic integer with trace ±1 as base and a minimal norm representatives digit set. We will consider the width-w non-adjacent form and its (non-)minimizing property of the Hamming-weight among all possible expansions with the same digit set. One main part in the proof of the presented results is to show that a certain inequality does not have any integer solutions. Furthermore, approximation properties of continued fractions are used (by a variant of the Baker–Davenport reduction method).

1 Introduction

Let τ be an (imaginary quadratic) algebraic integer and $\mathcal{D}$ a finite subset of $\mathbb{Z}[\tau]$ including zero. Choosing the digit set $\mathcal{D}$ properly, we can represent $z \in \mathbb{Z}[\tau]$ by a finite sum

$$\sum_{\ell=0}^{L-1} \sigma_\ell \tau^\ell,$$

where the digits σ_ℓ lie in $\mathcal{D}$. Using a redundant digit set $\mathcal{D}$, i.e., taking more digits than needed to represent all elements of $\mathbb{Z}[\tau]$, each element can be written in different ways. Of particular interest are expansions which have the lowest number of non-zero digits. We call these expansions *optimal* or *minimal expansions*.

The motivation looking at such expansions comes from elliptic curve crypography. There the scalar multiplication of a point on the curve is a crucial operation and has to be performed as efficiently as possible. The standard double-and-add algorithm can be extended by windowing methods. Translating this into the language of digit expansions means the usage of redundant digit expansions with base 2. However, using special elliptic curves, for example Koblitz curves, see [6, 7, 9, 10], the "expensive" doublings can be replaced by the "cheap" application of the Frobenius endomorphism over finite fields. In the world of digit expansions this means taking an imaginary quadratic algebraic integer as base. This leaves us with the additions of points of the elliptic curve as an "expensive" operation. The number of such additions is basically the number of non-zero digits in an expansion. Therefore minimizing this number is an important goal.

[*] This talk is based on a joint work with Volker Ziegler. The author of this talk is supported by the Austrian Science Fund (FWF): P24644-N26.

Let the parameter $w \geq 2$ be an integer. Then one special expansion is the width-w non-adjacent form (w-NAF), where in each block of width w at most one digit is not equal to zero. This expansion contains, by construction, only few non-zero digits. When we use a digit set consisting of zero and of representatives with minimal norm of the residue classes modulo τ^w excluding those which are divisible by τ, the w-NAF-expansion is minimal in a lot of cases. We call such a digit set a *minimal norm representative digit set modulo* τ^w. Note that each element of $\mathbb{Z}[\tau]$ admits a unique w-NAF expansion with this digit set.

A general criterion for minimality of the w-NAF-expanions can be found in [5]: The w-NAF of each element is minimal, if expansions of weight 2 are minimal.

In this extended abstract we are interested in bases τ with $\tau^2 - p\tau + q = 0$ and $p \in \{-1, 1\}$. Note that the case $q = 2$ is related to Koblitz curves in characteristic 2. A few results are already known: If $w = 2$ or $w = 3$ minimality was shown in [1]. In contrast, for $w \in \{4, 5, 6\}$, the w-NAF-expansion is not minimal anymore. This was shown in [4]. These results rely on transducer automata rewriting arbitrary expansions (with given base and digit set) to a w-NAF-expansion and on a search of cycles of negative “weight”.

2 Results

Theorem 1. *Let q be an integer with $q \geq 2$ and let $p \in \{-1, 1\}$. Let τ be a root of $X^2 - pX + q$ and $\mathcal{D}$ a minimal norm representative digit set modulo τ^w. Then there exists an explicitly/effectively computable bound w_q such that for all $w \geq w_q$ the width-w non-adjacent form expansion is not minimal with respect to τ and to $\mathcal{D}$.*

It turns out that the bounds w_q are rather huge. However, for small q we can reduce this bound dramatically (for example from $w_2 = 2.885 \cdot 10^{16}$ to $\widetilde{w}_2 = 147$) and get the following much stronger result.

Theorem 2. *Let q and w be integers with*

- *either*[1] $2 \leq q \leq 306$ *and* $w \geq 2$
- *or* $q \geq 2$ *and* $w \in \{2, 3\}$,

and let $p \in \{-1, 1\}$. Let τ be a root of $X^2 - pX + q$ and $\mathcal{D}$ a minimal norm representative digit set modulo τ^w. Then the width-w non-adjacent form expansion with respect to τ and to $\mathcal{D}$ is minimal if and only if $q = 2$ and $w \in \{2, 3\}$.

Formulated differently, this means that the w-NAF is **not** minimal/optimal for all the given parameter configurations except for the four cases with $w \in \{2, 3\}$, $p \in \{-1, 1\}$ and $q = 2$.

The main part of the proof of Theorem 2 provides an algorithm which takes q (and p) as input and outputs a list of values for w for which no counterexample to the minimality of the w-NAF can be found.

[1] The upper bound $q \leq 306$ in Theorem 2 is determined by an ongoing calculation.

3 Overview on the Proof

The algorithm to test for fixed q grows out of an intuition on how counterexample to minimality of the w-NAF are constructed. To do so, we have to find certain lattice point configurations located near the boundary of the digit set: We have to find a lattice point located in some rectangle which additionally avoids some smaller lattice.

Using the theory of the geometry of numbers will allow us to construct such a lattice point, but unfortunately not "for free"; we have to ensure that there is no lattice point in some smaller rectangle. This problem can be reformulated as an inequality and we have to show that it does not have any integer solutions. This is a task of Diophantine analysis. In particular and because of the structure of the inequality, we use the theory of linear forms in logarithms. This provides, for given q, a rather huge bound on w (based on a result due to Matveev [8]). From this Theorem 1 can be proven. However, using the convergents of continued fractions we are able to reduce this bound significantly. Therefore, we are able to check all the remaining w directly. In particular, we use a variant of the Baker–Davenport method [2].

With the above found lattice point, we construct counterexamples to the minimality of the w-NAF. In particular, this gives us a minimal non-w-NAF expansion, whose most significant digit is perturbated a little bit. This is compensated by a large change in the least significant digit. Gluing everything together results in the actual counterexamples (thereby proving Theorem 2).

The actual algorithm is implemented in SageMath [3].

References

[1] Roberto Avanzi, Clemens Heuberger, and Helmut Prodinger, *Scalar multiplication on Koblitz curves. Using the Frobenius endomorphism and its combination with point halving: Extensions and mathematical analysis*, Algorithmica **46** (2006), 249–270.

[2] Alan Baker and Harold Davenport, *The equations* $3x^2 - 2 = y^2$ *and* $8x^2 - 7 = z^2$, Quart. J. Math. Oxford **20** (1969), 129–137.

[3] The SageMath Developers, *SageMath Mathematics Software (Version 7.0)*, 2016, `http://www.sagemath.org`.

[4] Clemens Heuberger, *Redundant* τ*-adic expansions II: Non-optimality and chaotic behaviour*, Math. Comput. Sci. **3** (2010), 141–157.

[5] Clemens Heuberger and Daniel Krenn, *Optimality of the width-*w *non-adjacent form: General characterisation and the case of imaginary quadratic bases*, J. Théor. Nombres Bordeaux **25** (2013), no. 2, 353–386.

[6] Neal Koblitz, *CM-curves with good cryptographic properties*, Advances in cryptology—CRYPTO '91 (Santa Barbara, CA, 1991) (J. Feigenbaum, ed.), Lecture Notes in Comput. Sci., vol. 576, Springer, Berlin, 1992, pp. 279–287.

[7] Neal Koblitz, *An elliptic curve implementation of the finite field digital signature algorithm*, Advances in cryptology—CRYPTO '98 (Santa Barbara, CA, 1998), Lecture Notes in Comput. Sci., vol. 1462, Springer, Berlin, 1998, pp. 327–337.

[8] Eugene M. Matveev, *An explicit lower bound for a homogeneous rational linear form in logarithms of algebraic numbers. II*, Izv. Ross. Akad. Nauk Ser. Mat. **64** (2000), no. 6, 125–180.

[9] Jerome A. Solinas, *An improved algorithm for arithmetic on a family of elliptic curves*, Advances in Cryptology — CRYPTO '97. 17th annual international cryptology conference. Santa Barbara, CA, USA. August 17–21, 1997. Proceedings (B. S. Kaliski, jun., ed.), Lecture Notes in Comput. Sci., vol. 1294, Springer, Berlin, 1997, pp. 357–371.

[10] Jerome A. Solinas, *Efficient arithmetic on Koblitz curves*, Des. Codes Cryptogr. **19** (2000), 195–249.

On Simultaneous Number Systems with 3 Bases

Tamás Krutki, Gábor Nagy

ELTE IK, Hungary

Indlekofer, Kátai and Racskó examined in [1], for what N_1, N_2 is $(-N_1, -N_2, \mathcal{A}_c)$ a simultaneous number system, where $2 \leq N_1 < N_2$ are rational integers and $\mathcal{A}_c = \{0, 1, \ldots, |N_1||N_2| - 1\}$. The triplet $(-N_1, -N_2, \mathcal{A}_c)$ is called a simultaneous number system, if there exist $a_j \in \mathcal{A}_c$ $(j = 0, 1, \ldots, n)$ for all z_1, z_2 rational integers so that

$$z_1 = \sum_{j=0}^{n} a_j(-N_1)^j, \quad z_2 = \sum_{j=0}^{n} a_j(-N_2)^j.$$

Analogous definition can be used for the Gaussian integers. One of the authors showed in [6] that there is no simultaneous number system of Gaussian integers with the canonical digit set, furthermore the construction of a new digit set was given by which simultaneous number systems of Gaussian integers exist. A. Kovács gave the complete description of Gaussian integers that can serve as bases of simultaneous number systems in [3] and [4], moreover he examined the case of the lattice of the Eisenstein integers in [5]. Simultaneous expansion of real numbers was studied by V. Komornik and A. Pethő in [2].

One way of generalization is using 3 bases instead of 2. Unfortunately the ring of Gaussian integers is not appropriate for this, but the ring of integers of the quadratic field $\mathbb{Q}(\sqrt{5})$ is suitable. The difficulty is the amount of triplets we have to check to validate a given system is number system. So the development of a software which can check these sets in acceptable times (using parallelization, GPU computing) was necessary. The existence of simultaneous number systems with three bases was confirmed by the finished software for some concrete choices of bases (both with dense and K-type digit sets).

References

[1] Indlekofer K.-H., I. Kátai and P. Racskó, Number systems and fractal geometry, *Probability Theory and Applications*, Kluwer Academic Publishers, The Netherlands, (1992), 319–334.

[2] Komornik, V. and A. Pethő. Common expansions in noninteger bases, *Publ. Math. Debrecen, to appear*, Available at `http://www.inf.unideb.hu/pethoe/cikkek/163-KomPet-Commonexpansions-2014-05-08-a.pdf` (2014).

[3] Kovács A. Number System Constructions with Block Diagonal Bases, *submitted to RIMS Kôkyûroku Bessatsu*, (2012).

[4] Kovács A. Algorithmic construction of simultaneous number systems in the lattice of Gaussian integers, *Annales Univ. Sci. Budapest, Sect. Comp.*, **41** (2013), 43–55.

[5] Kovács A. Simultaneous number systems in the lattice of Eisenstein integers, *Annales Univ. Sci. Budapest, Sect. Comp.*, **39** (2013), 279–290.

[6] Nagy G. On the simultaneous number systems of Gaussian integers, *Annales Univ. Sci. Budapest, Sect. Comp.*, **35** (2011), 223–238.

Sturmian Word, Cantor Set, and Unique Expansions over Ternary Alphabets

DoYong Kwon

Department of Mathematics, Chonnam National University, Republic of Korea

Komornik, Lai, and Pedicini [1] studied unique expansions over a ternary alphabet $\{a_1, a_2, a_3\}$ with $a_1 < a_2 < a_3$. Without loss of generality, the alphabet is assumed, after a normalizing process, to be $A_m := \{0, 1, m\}$ with $m \geq 2$. What they proved includes the following: for a given $m \geq 2$, there continuously exists p_m such that

(a) $2 \leq p_m \leq P_m := 1 + \sqrt{\frac{m}{m-1}}$,

(b) if $q < p_m$, then unique expansions in base q are only 0^∞ and m^∞, the trivial unique expansions,

(c) if $q > p_m$, then there are nontrivial unique expansions in base q,

(d) the set $C := \{m \geq 2 : p_m = P_m\}$ is a Cantor set, i.e., a nowhere dense perfect set.

The above p_m was called a generalized golden ratio for A_m. During determining p_m, they exhibited that there emerge, curiously enough, Sturmian words.

Now we focus on Sturmian words under this context. For a given $m \geq 2$, we decide the corresponding Sturmian word effectively and algorithmically, from which we investigate the generalized golden ratio and the Cantor set in more detail.

References

[1] V. Komornik, A.C. Lai, and M. Pedicini. Generalized golden ratios of ternary alphabets. *J. Eur. Math. Soc. (JEMS)* **13** (2011), no. 4, 1113-1146.

The Hausdorff Dimension of Non-Normal Numbers

Manfred Madritsch[(1)], Izabela Petrykiewicz[(2)]

[(1)] Institute Elie Cartan Nancy, France

[(2)] Max Planck Institute for Mathematics, Bonn, Germany

Let $\beta > 1$ be a Pisot number. Then every elements $x \in [0,1]$ admits an expansion of the form

$$x = \sum_{k \geq 1} a_k \beta^{-k}.$$

This expansion is called the β-expansion of x. A way to obtain the digits a_k of such an expansion is to consider the transformation (X, T) where $X = [0,1]$ and $T\colon X \to X, x \mapsto \beta x \bmod 1$. Furthermore let $\mathcal{P} = \{P_0, P_1, \ldots, P_{\lfloor \beta \rfloor}\}$ with

$$P_i = \left(\frac{i}{\beta}, \frac{i+1}{\beta}\right) \text{ for } i = 0, \ldots, \lfloor \beta \rfloor - 1 \quad \text{and} \quad P_{\lfloor \beta \rfloor} = \left(\frac{\lfloor \beta \rfloor}{\beta}, 1\right)$$

be a topological partition of X. Then we get that $a_k = i$ such that $T^{k-1}(x) \in P_i$ is a suitable choice.

Rényi (1957) already showed that the system (X, T) admits a unique maximal ergodic measure μ. Let $\mathfrak{B}$ be the sigma algebra of Borel sets generated by the cylinder sets and $\mathcal{A}_\beta := \{0, 1, \ldots, \lfloor \beta \rfloor\}$ be the set of digits. We call a $x \in X$ normal with respect to $(X, \mu, \mathfrak{B}, T)$, if for each $k \geq 1$ and each $\mathbf{b} = (b_1, \ldots, b_k) \in \mathcal{A}_\beta^k$ we have that

$$\frac{1}{N} \# \left\{0 \leq n < N \colon T^n(x) \in P_{b_1}, \ldots, T^{n+k-1}(x) \in P_{b_k}\right\} \xrightarrow[N \to \infty]{} \mu(\mathbf{b}).$$

By Birkhoff's Ergodic Theorem we get that almost all $x \in X$ are normal with respect to the maximal ergodic measure μ.

Now we turn our attention to non-normal numbers. If we take $\beta = 3$ then we obviously get the ternary expansion. Furthermore let C be the set of $x \in [0,1]$ such that the digit 1 does not occur in the ternary expansion of x. Then C is the middle third Cantor sets. This set has measure zero, but has Hausdorff dimension $\log 2 / \log 3 > 0$. In order to get this result we define a measure μ_C such that $\mu_C(0) = \mu_C(2) = \frac{1}{2}$ and $\mu_C(1) = 0$. It is easy to see that the Hausdorff dimension of a set with no 1s and with only finitely many 1s is the same. Therefore the Theorem of Besicovitch and Eggleston (see Billingsley (1965)) yields the desired estimate. This theorem is applicable if we have a measure (we could say "distribution of digits"). A generalization to shift spaces fulfilling the specification property was shown by Pfister and Sullivan (2003). In particular, this holds for every β-expansion with β being Pisot.

In the present talk we want to consider stronger forms of non-normal numbers. First we consider particularly non-normal numbers, where we have a pair of digits one of which has a limiting frequency whereas the other one has no limiting frequency. Then we consider essentially non-normal numbers. These are numbers where for each digit in $\mathcal{A}_\beta$ there exists no limiting frequency. Finally we consider extremely non-normal numbers where all possible frequency vectors occur as limit points. In all three cases we consider the constructions as well as the Hausdorff dimension of the sets.

On Distribution of Subsequences of the Natural Numbers on the p-Adic Integers

Radhakrishnan Nair

Department of Mathematical Sciences, University of Liverpool

The Van der Corput sequence is the projection of the natural numbers from the p-adic integers onto the unit interval under the Monna map. The sequence is well known to be uniformly distributed modulo one. It is in fact a low discrepancy sequence which means it is about as uniformly distributed as you can get. This property is fundamental to Quasi-Monti Carlo Estimation, which gives us a large audience for its properties. In this talk we will study arithmetic subsequences of the Van der Corput sequence and discuss the uniform distribution properties of these sequences. Generically these subsequences are uniform distributed, though some interesting examples are not. An initial approach to this issue is to use the fact that the p-adic integers are a compact abelian topological group, with a well developed character theory and use Weyl's criterion on this group to prove the uniform distribution. We then push the uniform distribution down to the unit interval using the Monna map, a natural structure preserving map between the two sets. This reduces the problem to one on exponential sums. Clearly this kind of argument is no use in situations where this group structure is not available. Another approach to this question is one based on Birkhoff's ergodic theorem the fact the natural numbers are a group rotation of the origin under the rotation map $Tx = x + 1$ and Oxtoby's characterisation of unique ergodicity. Group rotations are of course uniquely ergodic. The advantage of this approach is that it allows generalisations to situations where there is no group structure, no character theory or indeed no Weyl's criterion. In this talk I will give a new approach to this question, not based on Birkhoff's ergodic theorem but on good universality, which is the extention of Birkhoff's theorem to times that are subsequences of the integers. To do this we have to introduce a new characterization of unique ergodicity which is much more powerful than that of Oxtoby and subsumes Oxtoby's characterisation as a special case. This may be of independent interest in its own right.

References

[1] N. H. Asmar and R. Nair: Certain averages on the a-adic numbers. Proc. Amer. Math. Soc. 114 (1992), no. 1, 21–28.

[2] R. Nair: On asymptotic distribution of the a-adic integers. Proc. Indian Acad. Sci. Math. Sci. 107 (1997), no. 4, 363–376.

[3] P. Lertchoosakul and R. Nair: Distribution functions for subsequences of the van der Corput sequence. Indag. Math. (N.S.) 24 (2013), no. 3, 593–601.

[4] A. Jassova, P. Lertchoosakul and R. Nair : On variants of the Halton sequence, Monat. Math (2015), DOI: 10.1007/s00605-015-0794-8.

[5] A. Jassova, P. Lertchoosakul M. Weber and R. Nair: Distribution functions for Subsequences of Generalised Van der Corput sequence (in submission).

Algorithmic Theoretical Questions on Canonical Number Systems and Shift Radix Systems

Attila Pethő

University of Debrecen, Debrecen, Hungary

Let $CNS(d,H)$ denote the complexity of the problem whether a monic polynomial with integer coefficients of degree d and height H is CNS. Similarly denote $SRS(d,H)$ the complexity of the problem whether a vector with rational coefficients of dimension d and height H is SRS with boundedness condition. In this talk we give an overview on known results and problems on both functions.

It is known, for example that $CNS(d,H) \leq SRS(d-1,H)$, moreover the backward division algorithm and Brunotte's algorithm solves CNS in H exponential time. However it is not known whether CNS can be solved in polynomial time or even whether CNS lie in the NP complexity class. Long cycles appear if one of the roots of the polynomial is near to a critical point. Brunotte's algorithm solves $SRS(d,H)$ in exponential time in H, but only if the companion polynomial has no roots on the unit circle. In the later case we do not know whether the SRS with boundedness condition is algorithmically decidable.

Distribution Modulo 1
and the Cardinality Gap Phenomenon

Johannes Schleischitz

BOKU Vienna, Austria

The talk is about special aspects of distribution modulo 1. The distribution of the sequence $a_n = \alpha\zeta^n$ modulo 1 for fixed real numbers α and $\zeta > 1$ has been intensely studied, in particular for the reason that when ζ is a Pisot number and $\alpha = 1$ then the sequence tends to 0 modulo 1. This behavior is very untypical since the "normal case" is that $(a_n)_{n\geq 1}$ is equidistributed in $[0, 1)$. The focus of the talk is on the following aspect. For given $\zeta > 1$, how large must a subinterval I of $[0, 1)$ be such that there are (un)countably many α such that a_n mod 1 belongs to I for all large n. We are particularly interested in the case that ζ is rational, connected to Mahler's 3/2-problem. A similar question is dealt with in the reverse case of fixed α. In combination with a result due to Dubickas the study of these questions leads to a simple characterization of Pisot and Salem numbers among the algebraic numbers.

Exploring the Intersection of the Pieces of Rauzy Fractals

Bernd Sing

Department of Mathematics, University of the West Indies, Barbados

G. Rauzy studied the dynamical system generated by the tribonacci substitution $a \to ab$, $b \to ac$, $c \to a$ via its geometric realization, now also known as "Rauzy fractal". This Rauzy fractal consists of three pieces – one associated to each letter a, b or c – that can be obtained as solution of a graph-directed iterated function system (GIFS) that can be derived from the substitution.

In this joint work with Tarek Sellami, we look at the fractal boundary of such Rauzy fractals and, in particular, at the part of the boundary where two pieces of the Rauzy fractal intersect. Interestingly, these parts can again be obtained as solutions of a GIFS. But while the directed graph representing the GIFS for the pieces of the Rauzy fractal is strongly connected for a Pisot substitution, this is no longer true for the directed graph representing the GIFS for the boundary pieces and thus this digraph may consist of several strongly connected components. However, one can concentrate on each such strongly connected component by breaking the GIFS into a GIFS "with condensation".

As an example, we consider the flipped tribonacci substitution $a \to ab$, $b \to ca$, $c \to a$. Here, the aforementioned condensation in the GIFS for the boundary sets lead to sets containing isolated points (even countably infinitly many isolated points). As another example, not least to show how complicated the situation can become, we also consider the "common part" of the usual and the flipped tribonacci substitution, a primitive substitution on 11 letters derived from the balanced pairs of the two tribonacci substitutions. In this case, the boundaries of the pieces of the corresponding Rauzy fractal are no longer of uniform Hausdorff dimension, and we analyse the parts involved.

Divisibility of Binomial Coefficients by Powers of Primes

Lukas Spiegelhofer

Université de Lorraine, Vandœuvre-lès-Nancy, France

For a prime p and nonnegative integers j and n let $\vartheta_p(j,n)$ be the number of entries in the n-th row of Pascal's triangle that are exactly divisible by p^j. Moreover, for a finite sequence $w=(w_{r-1}\cdots w_0)\neq(0,\ldots,0)$ in $\{0,\ldots,p-1\}$ we denote by $|n|_w$ the number of times that w appears as a factor (contiguous subsequence) of the base-p expansion $n=\sum_{i=0}^{\infty}\varepsilon_i p^i$ of n.

It follows from the work of Barat and Grabner (*Digital functions and distribution of binomial coefficients*, J. London Math. Soc. (2) 64(3), 2001) that $\vartheta_p(j,n)/\vartheta_p(0,n)$ is given by a polynomial P_j in the variables X_w, where w are certain finite words in $\{0,\ldots,p-1\}$, and each variable X_w is set to $|n|_w$. This was later made explicit by Rowland (*The number of nonzero binomial coefficients modulo* p^α, J. Comb. Number Theory 3(1), 2011), independently from Barat and Grabner's work. Rowland described and implemented an algorithm computing these polynomials P_j. For the prime $p=2$ and $j\leq 4$, formulas of this kind had been known before, for example,

$$\begin{aligned}
\vartheta_2(1,n)/\vartheta_2(0,n) &= \tfrac{1}{2}|n|_{10},\\
\vartheta_2(2,n)/\vartheta_2(0,n) &= -\tfrac{1}{8}|n|_{10}+|n|_{100}+\tfrac{1}{4}|n|_{110}+\tfrac{1}{8}|n|_{10}^2,\\
\vartheta_2(3,n)/\vartheta_2(0,n) &= \tfrac{1}{24}|n|_{10}-\tfrac{1}{8}|n|_{110}-\tfrac{1}{2}|n|_{100}+\tfrac{1}{8}|n|_{1110}+\tfrac{1}{2}|n|_{1100}+\tfrac{1}{2}|n|_{1010}\\
&\qquad +2|n|_{1000}-\tfrac{1}{16}|n|_{10}^2+\tfrac{1}{8}|n|_{10}|n|_{110}+\tfrac{1}{2}|n|_{10}|n|_{100}+\tfrac{1}{48}|n|_{10}^3.
\end{aligned}$$

In this talk, we present a method for obtaining the coefficients of a given monomial in P_j as a generating function. For example, for $p=2$ the monomial X_{10}, corresponding to the term $|n|_{10}$, we obtain the generating function $\log(1+x/2)$, which has the coefficients $0, 1/2, -1/8, 1/24, -1/64, \ldots$. To give another, more generic, example, the coefficients of the monomial $X_{10}^2X_{1010}^3$ are given by the generating function

$$\frac{1}{2!}\bigl(\log(1+x/2)\bigr)^2\frac{1}{3!}\bigl(\log\bigl(1+\tfrac{1}{2}x^3/(1+x/2)^2\bigr)\bigr)^3.$$

In particular, the monomial $X_{10}^2X_{1010}^3$ occurs first in the polynomial P_{11}. Besides providing insight into the structure of the polynomials P_j, these results allow us to compute the polynomials P_j in a very efficient way. This is joint work with Michael Wallner (TU Vienna).

Continued Fractions and Spectra of Certain Operators

Štěpán Starosta

FIT, Czech Technical University in Prague, zech Republic

1 Introduction

In [6] and [7], the authors study certain stable quantum systems that live on rectangular and hexagonal lattices, respectively. It turns out that the spectral properties of the studied systems depend on number theoretical properties of some of its parameters. These properties are intimately related to continued fraction expansion of these parameters, namely to the Markov constant $\mu(\alpha)$ of a real number α (see below for an exact definition or [3]).

In this contribution, we present the study of the spectrum of a certain differential operator. It is again connected to the Markov constant of one of its parameters, this time in a certain broader sense. Using continued fraction expansion of this parameter, we exhibit different behaviours of the spectrum in question.

First, we give a short overview of how the mathematical question is derived. See [9] for more details. The studied model is given by the following hyperbolic partial differential equation

$$\Box f(x,y) = \lambda f(x,y)\,, \qquad \Box = \frac{\partial^2}{\partial x^2} - \frac{\partial^2}{\partial y^2}\,, \qquad f|_{\partial R} = 0. \tag{1}$$

The eigenfunctions are required to satisfy the most common Dirichlet boundary conditions, i.e., they are expected to vanish along the boundary of the two-dimensional rectangle

$$R = \{(x,y) \colon 0 \le x \le a, 0 \le y \le b\}. \tag{2}$$

Separating the variables, one may find that the spectrum of the operator $\Box$ satisfies

$$\sigma(\Box) = \overline{\{\lambda_{k,m} \colon k,m \in \mathbb{Z}\}},$$

where

$$\lambda_{k,m} = \frac{\pi^2 m^2}{a^2}\left(\frac{k}{m} - \frac{a}{b}\right)\left(\frac{k}{m} + \frac{a}{b}\right).$$

Thus, up to a multiplicative factor, the singular part of the spectrum $\sigma(\Box)$ coincides with the set

$$\S(\alpha) = \text{set of all accumulation points of } \left\{ m^2\left(\frac{k}{m} - \alpha\right) \colon k,m \in \mathbb{Z} \right\}$$

where $\alpha = a/b$.

In what follows, we study the set $\S(\alpha)$ based on the properties of α.

2 Simple properties of $\S(\alpha)$

Let us rephrase the definition of $\S(\alpha)$: a number x belongs to $\S(\alpha)$ if there exist strictly monotone sequences of integers (k_n) and (m_n) such that $x = \lim\limits_{n\to\infty} m_n^2\Big(\frac{k_n}{m_n} - \alpha\Big)$.

We list several simple properties of $\S(\alpha)$.

1. The set $\S(\alpha)$ is a topologically closed subset of $\mathbb{R}$.
2. If $\alpha \in \mathbb{Q}$, then $\S(\alpha)$ is empty.
3. If $\alpha \notin \mathbb{Q}$, then $\S(\alpha)$ has at least one element in the interval $[-1, 1]$.

   Proof. According to Dirichlet's theorem, there exist infinitely many rational numbers $\frac{k}{m}$ such that $\left|\frac{k}{m} - \alpha\right| < \frac{1}{m^2}$. □

The next property, stated as a proposition, follows from the definition of $\S(\alpha)$.

Proposition 1. *Let $\alpha \in \mathbb{R}$ and $a, b, c, d \in \mathbb{Z}$ such that $ad - bc = \Delta \neq 0$. We have*

$$\Delta \cdot \S(\alpha) \subset \S\left(\frac{a\alpha + b}{c\alpha + d}\right).$$

In particular, $\S\left(\frac{a\alpha+b}{c\alpha+d}\right) = \S(\alpha)$ if $\Delta = 1$.

Let us mention two immediate consequences of the last proposition. Setting $0 \neq a = d \in \mathbb{Z}$ and $b = c = 0$, we obtain that $\S(\alpha)$ is closed under multiplication by a^2 for each nonzero $a \in \mathbb{Z}$. Setting $a = d = 1$, $b = \lfloor\alpha\rfloor$ and $c = 0$, we obtain that $\S(\alpha) = \S(\alpha - \lfloor\alpha\rfloor)$.

Another corollary follows when one uses the continued fraction expansion of α, which is denoted $[a_0, a_1, a_2, a_3, \ldots]$ where $a_0 \in \mathbb{Z}$ and $a_i \in \{1, 2, \ldots\}$ for $i > 0$. We also identify the expansion of α with the value of α itself, i.e., we write $\alpha = [a_0, a_1, a_2, a_3, \ldots]$. Using this convention, Proposition 1 yields the following.

Corollary 2. *Let $[a_0, a_1, a_2, a_3, \ldots]$ be a continued fraction. We have*

$$\S([a_{n+k}, a_{n+1+k}, a_{n+2+k}, \ldots]) = (-1)^k \S([a_n, a_{n+1}, a_{n+2}, \ldots]) \text{ for any } k, n \in \mathbb{N}.$$

Using the basic properties of convergents of α, we obtain another corollary.

Corollary 3. *Let α be an irrational number and I be an interval. There exists $\beta \in I$ such that $\S(\alpha) = \S(\beta)$.*

Let α be an irrational number and $\frac{p}{q} \in \mathbb{Q}$. The famous Legendre's theorem (see for instance [3], Theorem 5.12) states that if $\left|\frac{p}{q} - \alpha\right| < \frac{1}{2q^2}$, then $\frac{p}{q}$ is a convergent of α. It allows us to understand the part of $\S(\alpha)$ near 0 completely via convergents of α:

Theorem 4. *Let α be an irrational number and $(\frac{p_N}{q_N})_{N\in\mathbb{N}}$ be the sequence of its convergents. If x belongs to $\S(\alpha) \cap (-\frac{1}{2}, \frac{1}{2})$, then x is an accumulation point of the sequence*

$$\left(q_N^2\left(\frac{p_N}{q_N} - \alpha\right)\right)_{N\in\mathbb{N}}. \tag{3}$$

Therefore, we start to investigate the accumulation points of the sequence (3). The following result is due to Perron (see for instance [4]).

Lemma 5. *Let α be an irrational number and $(\frac{p_N}{q_N})_{N\in\mathbb{N}}$ be the sequence of its convergents. For any $N \in \mathbb{N}$ we have*

$$q_N^2\left(\frac{p_N}{q_N}-\alpha\right) = (-1)^{N+1}\Big([a_{N+1}, a_{N+2}, \ldots] + [0, a_N, a_{N-1}, \ldots, a_1]\Big)^{-1}.$$

In particular, for any $N \in \mathbb{N}$

$$\frac{1}{2+a_{N+1}} < \left|q_N^2\left(\frac{p_N}{q_N}-\alpha\right)\right| < \frac{1}{a_{N+1}}.$$

The last property that we mention in this section follows from a stronger result. In [2], the authors describe the distribution of the sequence $q_N|p_N - \alpha q_N|$, where $\frac{p_N}{q_N}$ are again convergents of α. A consequence of their result is that $\S(\alpha) = \mathbb{R}$ for almost all $\alpha \in \mathbb{R}$.

3 Well and badly approximable numbers

Lemma 5 allows us to exhibit various possibilities for α such that $\S(\alpha) \neq \mathbb{R}$. Before doing that, we introduce the notions of Markov constant and well and badly approximable numbers.

Definition 6. Let α be an irrational number. The number

$$\mu(\alpha) = \inf\left\{c > 0\colon \left|\alpha - \frac{k}{m}\right| < \frac{c}{m^2} \text{ has infinitely many solutions } k, m \in \mathbb{Z}\right\}$$

is the *Markov constant of* α.

The number α is said to be *well approximable* if $\mu(\alpha) = 0$ and *badly approximable* otherwise.

We give several comments on the value $\mu(\alpha)$:

1. Theorem of Hurwitz implies $\mu(\alpha) \leq \frac{1}{\sqrt{5}}$ for any irrational real number α.
2. A pair (k, m) which is a solution of $\left|\alpha - \frac{k}{m}\right| < \frac{c}{m^2}$ with $c \leq \frac{1}{\sqrt{5}}$ satisfies $k = \|m\alpha\|$, where we use the notation $\|x\| = \min\{|x-n|\colon n \in \mathbb{Z}\}$. Therefore,

$$\mu(\alpha) = \liminf_{m\to+\infty} m\|m\alpha\| \qquad \text{and} \qquad \mu(\alpha) = \min|\S(\alpha)|$$

   as the set $\S(\alpha)$ is topologically closed.
3. The inequality in Lemma 5 implies

$$\mu(\alpha) = 0 \qquad \Longleftrightarrow \qquad (a_N) \quad \text{is not bounded} \qquad \Longleftrightarrow \qquad 0 \in \S(\alpha).$$

   In other words, an irrational number α is well approximable if and only if the sequence (a_N) of its partial quotients is bounded.

3.1 Well approximable numbers

It follows immediately from the definition of well approximable numbers and the equality $\mu(\alpha) = \min|\S(\alpha)|$ that if $\S(\alpha) = \mathbb{R}$, then α is well approximable. The converse is not true. It can be seen for the Euler constant whose continued fraction has the following structure:

$$\mathrm{e} = [2, 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, 1, 1, 10, \ldots].$$

Theorem 4 allows us to show that

$$(-\tfrac{1}{2}, \tfrac{1}{2}) \cap \S(\mathrm{e}) = \{0\}.$$

Moreover, using so-called secondary convergents, it can be shown that

$$\{a + \tfrac{1}{2} : a \in \mathbb{Z}\} \subset \S(\mathrm{e}).$$

Secondary convergents allow for the following general result for well approximable numbers.

Proposition 7. *Let α be an irrational well approximable number. For any $n \in \mathbb{N}$ the interval $[n, n+1]$ or the interval $[-n-1, -n]$ has a non-empty intersection with $\S(\alpha)$.*

3.2 Badly approximable numbers

Theorems 8 and 9 give two examples of spectra of badly approximable numbers of different kinds.

Theorem 8. *There exists a badly approximable irrational number α such that $\S(\alpha) = (-\infty, -\varepsilon] \cup [\varepsilon, +\infty)$, where $\varepsilon = \frac{\sqrt{2}}{8} \approx 0.18$.*

Theorem 9. *There exists a badly approximable irrational number α such that the Hausdorff dimension of $\S(\alpha) \cap \left(-\frac{1}{2}, \frac{1}{2}\right)$ is positive but less than 1. In particular, $\S(\alpha) \cap \left(-\frac{1}{2}, \frac{1}{2}\right)$ is an uncountable set and its Lebesgue measure is 0.*

Proofs of both theorems are based on Lemma 5 and results concerning the following set defined for $r \in \mathbb{N}$:

$$F(r) = \{[t, a_1, a_2, \ldots] : t \in \mathbb{Z}, 1 \le a_i \le r\}.$$

A crucial result is due to [8] (see also [1]):

$$F(4) + F(4) = \mathbb{R}. \tag{4}$$

It is worth mentioning that $r = 4$ is the least integer for which $F(r) + F(r) = \mathbb{R}$, i.e., in particular, $F(3) + F(3) \neq \mathbb{R}$ (see [5]).

A number α is a *quadratic* irrational number if it is an irrational root of a quadratic polynomial with integer coefficients. A famous theorem of Lagrange says that α is a quadratic irrational number if and only if the continued fraction of α is eventually periodic, i.e., $\alpha = [a_0, a_1, \ldots, a_s, \overline{a_{s+1}, \ldots, a_{s+\ell}}]$, where the overline symbol indicates infinite repetition of the partial quotients $a_{s+1}, \ldots, a_{s+\ell}$. As the partial quotients of such α are bounded, quadratic irrational numbers are badly approximable. The ultimate periodicity of their continued fraction allows us to obtain more insight into $\S(\alpha)$.

Theorem 10. *Let α be a quadratic number and $\left(\frac{p_N}{q_N}\right)$ be the sequence if its convergents. Let ℓ be the smallest period of the repeating part of the continued fraction of α. The sequence $\left(q_N^2\left(\frac{p_N}{q_N} - \alpha\right)\right)_{N\in\mathbb{N}}$ has at most*

- *ℓ accumulation points if ℓ is even;*
- *2ℓ accumulation points if ℓ is odd.*

Moreover, at least one of the accumulation points belongs to the interval $\left(-\frac{1}{2}, \frac{1}{2}\right)$.

For quadratic irrational numbers having a special form, we can describe the whole set $\S(\alpha)$.

Theorem 11. *If $\alpha = s + \sqrt{D}$ with $s \in \mathbb{Z}$ and $D \in \mathbb{N}$ being nonsquare, then there exists $C \in \mathbb{R}$ such that*

$$C \cdot \S(\alpha) = \{N(k + m\sqrt{D}) \colon k, m \in \mathbb{Z}\}$$

where N is the norm on $\mathbb{Q}(\sqrt{D})$, i.e., $N(k + m\sqrt{D}) = (k + m\sqrt{D})(k - m\sqrt{D})$.

References

[1] S. Astels, *Cantor sets and numbers with restricted partial quotients*, T. Am. Math. Soc., 352 (1999), pp. 133–170.

[2] W. Bosma, H. Jager, and F. Wiedijk, *Some metrical observations on the approximation by continued fractions*, Indagat. Math. (Proceedings), 86 (1983), pp. 281–299.

[3] E. B. Burger, *Exploring the Number Jungle: A Journey Into Diophantine Analysis*, American Mathematical Soc., 2000.

[4] T. Cusick and M. Flahive, *The Markoff and Lagrange Spectra*, Mathematical surveys and monographs, American Mathematical Society, 1989.

[5] B. Diviš, *On the sums of continued fractions*, Acta Arith., 22 (1973), pp. 157–173.

[6] P. Exner and R. Gawlista, *Band spectra of rectangular graph superlattices*, Phys. Rev. B, 53 (1996), pp. 7275–7286.

[7] P. Exner and O. Turek, *Spectrum of a dilated honeycomb network*, Integr. Equat. Oper. Th., 81 (2015), pp. 535–557.

[8] M. Hall, Jr., *On the sum and product of continued fractions*, Ann. of Math., 48 (1947), pp. 966–993.

[9] E. Pelantová, Štěpán Starosta, and M. Znojil, *Markov constant and quantum instabilities*, J. Phys. A: Math. Theor., 49 (2016), p. 155201.

Substitutions, Shifts of Finite Type, and Numeration[*]

Paul Surer

BOKU Vienna, Austria

Let $\mathcal{A}$ be a finite set (alphabet), $\mathcal{A}^*$ the free monoid over $\mathcal{A}$, and $\mathcal{A}^{\mathbb{Z}}$ the set of bi-infinite words over $\mathcal{A}$. For a sequence $w = (w_i)_{i\in\mathbb{Z}} \in \mathcal{A}^{\mathbb{Z}}$ we especially tag the *central pair* $w_{-1}w_0$ which will be denoted by a point, *i.e.* $w = \cdots w_{-3}w_{-2}w_{-1}.w_0w_1w_2\cdots$.

Denote by $\sigma : \mathcal{A}^* \longrightarrow \mathcal{A}^*$ a non-erasing morphism (substitution). Suppose that σ is primitive, that is there exists an $n \in \mathbb{N}$ such that for all $a, b \in \mathcal{A}$ the letter b appears in $\sigma^n(a)$ at least once. Extend σ to $\mathcal{A}^{\mathbb{Z}}$ by defining

$$\sigma(\cdots w_{-3}w_{-2}w_{-1}.w_0w_1w_2\cdots) = \cdots\sigma(w_{-3})\sigma(w_{-2})\sigma(w_{-1}).\sigma(w_0)\sigma(w_1)\sigma(w_2)\cdots.$$

Denote by $\mathfrak{L}$ the induced language given by

$$\mathfrak{L} := \{A \in \mathcal{A}^* \,|\, \exists a \in \mathcal{A}, n \in \mathbb{N} \text{ such that } A \text{ is a subword of } \sigma^n(a)\}.$$

The *substitution dynamical system induced by* σ is the pair (Ω, S), where

$$\Omega = \left\{(w_i)_{i\in\mathbb{Z}} \in \mathcal{A}^{\mathbb{Z}} \,|\, \forall i \in \mathbb{Z}, k \in \mathbb{N} : w_i\cdots w_{i+k} \in \mathfrak{L}\right\}$$

and S is the left shift

$$S : \cdots w_{-3}w_{-2}w_{-1}.w_0w_1w_2\cdots \mapsto \cdots w_{-3}w_{-2}w_{-1}w_0.w_1w_2\cdots.$$

The principle aim of the talk is to present how to code substitution dynamical systems as shifts of finite type with respect to a so-called *coding prescription.* According to [4], a coding prescription is a function c with source $\mathcal{A}$ that assigns to each letter $a \in \mathcal{A}$ a complete set of representatives modulo $|\sigma(a)|$ whose absolute values are smaller than $|\sigma(a)|$ (where $|\sigma(a)|$ denotes the length of the word $\sigma(a)$). We extend c to $\mathcal{A}^2$ by

$$c(ab) := \{k \in c(a) \,|\, k \le 0\} \cup \{k \in c(b) \,|\, k \ge 0\}.$$

A coding prescription induces in a natural way a finite graph $G(c)$. The vertices are given by $\mathfrak{L}_2 := \mathfrak{L} \cap \mathcal{A}^2$. There is an edge from $a'b'$ to ab labelled by (ab, k) if $k \in c(ab)$ and $a'b'$ appears at the $(k + |\sigma(a)|)$th position in $\sigma(ab)$. We will see that Ω can be coded continuously and surjectively as the shift of finite type given by the infinite walks on $G(c)$. Depending on the actual coding prescription, several interesting effects may occur (for example in context with the injectivity). The special case where $c(a)$ does not contain negative integers for all $a \in \mathcal{A}$ corresponds to the well-known prefix-suffix coding (see [1, 3]).

It is well known that substitutions are intimately related with numeration (Dumont-Thomas numeration [2]). The concept of coding prescriptions allows us to generalise these results. We will see that different coding prescriptions correspond to different sets of digits.

[*] Supported by the FWF.

References

[1] V. Canterini and A. Siegel, *Automate des préfixes-suffixes associé à une substitution primitive*, J. Théor. Nombres Bordeaux, 13 (2001), pp. 353–369.

[2] J.-M. Dumont and A. Thomas, *Systemes de numeration et fonctions fractales relatifs aux substitutions*, Theoret. Comput. Sci., 65 (1989), pp. 153–169.

[3] C. Holton and L. Q. Zamboni, *Directed graphs and substitutions*, Theory Comput. Syst., 34 (2001), pp. 545–564.

[4] P. Surer, *Coding of substitution dynamical systems as shifts of finite type*, Ergodic Theory Dynam. Systems, 36 (2016), pp. 944–972.

On Height One Trinomials and Limit Dynamical Zeta Functions

Jean-Louis Verger-Gaugry

LAMA, CNRS UMR 5127, University Savoie Mont Blanc, France

Let $\chi_3(m)$ be the Jacobi symbol $\left(\frac{m}{3}\right)$ ($\chi_3(m)$ is equal to $0, 1, -1$ according to whether $m \equiv 0, 1$ or $2 \pmod 3$). Let $L(s, \chi_3(m)) = \sum_{m \geq 1} \frac{\chi_3(m)}{m^s}$ be the Dirichlet L-series. Denote by

$$\Lambda = 1.38135\ldots = \exp\left(\frac{3\sqrt{3}}{4\pi} L(2, \chi_3(m))\right).$$

The Mahler measure of a polynomial P is denoted by $\mathrm{M}(P)$. Due to the invariance properties of M , the following conjecture covers all cases of height one trinomials.

Conjecture (Smyth)**.** *For all integers $n \geq 4,\ k \geq 1$ such that $\gcd(n,k) = 1,\ k < n/2$,*

- *$M(z^n + z^k + 1) < \Lambda$ if and only if 3 divides $n + k$,*
- *$M(z^n - z^k + 1) < \Lambda$ with n odd if and only if 3 does not divide $n + k$,*
- *$M(z^n - z^k - 1) < \Lambda$ with n even if and only if 3 does not divide $n + k$.*

Flammang (2014) proved this conjecture for large n. Verger-Gaugry (2015) proved it for the family $(-1 + z + z^n)_{n \geq 4}$ using Poincaré asymptotic expansions and Smyth's and Boyd's techniques dedicated to trinomials.

We reinvestigate these results by the dynamics of the β-shift and its dynamical zeta function.