Yaroslav-the-Wise
Novgorod State University

Fifth Russian Finnish Symposium on Discrete Mathematics

19-22 May, 2019

Veliky Novgorod, Russia

Yaroslav-the-Wise Novgorod State University

Fifth Russian Finnish Symposium on Discrete Mathematics

19-22 May, 2019

Veliky Novgorod, Russia

Veliky Novgorod

2019

УДК 519.1(063)

ББК 22.176

Т45

Научные редакторы / Editors

Yuri Matiyasevich, Juhani Karhumäki, Vladimir Edemskiy

Пятый российско-финский симпозиум по дискретной математике.
Великий Новгород, Новгородский государственный университет, 2019.
199 с.
ISBN 978-5-89896-704-8

ISBN 978-5-89896-704-8

Scientific committee

Yuri Matiyasevich
Juhani Karhumki
Alexander Okhotin
Mikhail Volkov
Dmitry Karpov
Ilya Ponomarenko
Vladimir Edemskiy
Vesa Halava
Jarkko Kari
Tero Laihonen

Organizing committee Novgorod State University, Velikiy Novgorod, Russia

Yuri Matiyasevich
Vladimir Edemskiy
Alexander Kolnogorov
Stefan Eminov
Sergey Garbar
Nikita Sokolovskii
Tatyana Zhgun
Tatyana Shelonina

Preface

The fifth RuFiDiM conference, Russian-Finnish Symposium on Discrete Mathematics, took place in Velikiy Novgorod in May, from 19th till 22nd, 2019.

The goal of the conference series is to increase cooperation between Finnish and Russian mathematicians in discrete mathematics, but the symposium is open for a broader international audience.

Abstracts or extended abstracts of the lectures are presented in these proceedings.

Acknowledgements

The organizers are grateful to Yaroslav-the-Wise Novgorod State University for support.

Veliky Novgorod, April 2019

Juhani Karhumki, Yuri Matiyasevich, Vladimir Edemskiy

Contents

Invited speakers

Group rings in combinatorics

Fedor Petrov
St. Petersburg Department of V.A.Steklov Institute
of Mathematics of the Russian Academy of Science

The first application of computations in group rings to additive combinatorics belongs to Olson, who managed to find the Davenport constant of finite abelian p-groups. We discuss several old and new results in the combinatorics of finite groups (not necessarily abelian) which rely on structural properties of zero divisors in their group rings over appropriate field. In particular, this covers the recent breakthrough results of Croot, Lev and Pach (the exponential bounds for sets without 3-progressions in $(\mathbb{Z}/4\mathbb{Z})^n$) and its extensions by Ellenberg, Gijswijt and others which were obtained using polynomial method. The crucial concrete property of the group ring is the existence of a huge nilpotent subspace of low exponent.

A fast algorithm for computing the geometric intersection index of curves on a triangulated surface and the word problem for the mapping class groups

Ivan Dynnikov
V.A. Steklov Mathematical Institute of Russian Academy of Science
dynnikov@mech.math.msu.su

The word length function used to be the default option for the complexity measure of an element of a finitely presented group but it is not always the most natural choice. For instance, the nth power of a prabolic element of $\mathrm{SL}(2,\mathbb{Z})$ has word length $O(n)$ whereas its conventional matrix presentation has size as small as $O(\log(n))$.

A similar situation occurs for the mapping class groups of punctured surfaces, in which, for the geometrical nature of the groups, it is more appropriate to regard the complexity of the nth power of a Dehn twist as having order $O(\log(n))$, not $O(n)$.

A quadratic-time solution of the word problem for the mapping class groups of punctured surfaces was given by Lee Mosher in [11], but in his approach the complexity was measured by word length. This means, that, with respect to the complexity of the geometric presentation described below, this solution is actually exponential-time (in worst case).

For two non-negative functions c_1 and c_2 on a group G, we say that c_1 and c_2 are *comparable* if there exists a constant C such that $c_1(g) < C \cdot c_2(g)$ and $c_2(g) < C \cdot c_1(g)$.

We say that $c : G \to \mathbb{R}_{\geqslant 0}$ is a *complexity function* if there exists a finite alphabet $\mathcal{A}$ and a language $\mathcal{L} \subset \mathcal{A}^*$ with an onto mapping $\pi : \mathcal{L} \to G$ such that

(i) if $w_1, w_2 \in \mathcal{L}$, then $w_1 w_2 \in \mathcal{L}$ and $\pi(w_1 w_2) = \pi(w_1)\pi(w_2)$;

(ii) c is comparable to the following function f:

$$f(g) = \inf_{\pi(w)=g} |w|,$$

where $|w|$ denote the word length.

A couple $(\mathcal{L}, \pi)$ satisfying (i) will be referred to as *a G-presentation*, and if (ii) also holds then it will be said to be *appropriate* for c.

For a finite generating set $\mathcal{A}$ of a group G we define *the zipped word length function* $\mathrm{zwl}_{\mathcal{A}}$ as follows:

$$\mathrm{zwl}_{\mathcal{A}}(g) = \min_{\substack{g = a_1^{k_1} \ldots a_m^{k_m}, \\ a_1, \ldots, a_m \in \mathcal{A}, \\ k_1, \ldots, k_m \in \mathbb{Z}}} \sum_{i=1}^{m} \log_2(|k_i| + 1).$$

Obviously, this is a complexity function, for which an appropriate G-presentation is obtained by choosing a reasonable encoding for sequences of the form $((a_1, k_1), \ldots, (a_m, k_m))$, where $a_i \in \mathcal{A}$, $k_i \in \mathbb{Z}$, and interpreting such a sequence as the product $a_1^{k_1} \ldots a_m^{k_m} \in G$. We call it *the zipped word presentation.*

For a complexity function c on a group G, we call *an efficient solution of the word problem for G with respect to c* an appropriate G-presentation $(\mathcal{L}, \pi)$ together with

(i) a mapping $\mathrm{nf} : G \to \mathcal{L}$ (the word $\mathrm{nf}(g)$ is thought of as the normal form of g) such that we have $\pi \circ \mathrm{nf} = \mathrm{id}_G$ and the function $g \mapsto |\mathrm{nf}(g)|$ is comparable to c, and

(ii) polynomial-time algorithms to decide wether $w \in \mathcal{L}$ or not and to compute $\mathrm{nf}(\pi(w))$ from w if $w \in \mathcal{L}$.

Let a, b be elements of a group G. We say that a is *a fractional power of b* if $a^k = b^l$ for some $k, l \in \mathbb{Z}$, $k > 0$.

Theorem 1. *Let M be a compact surface, $P_1, \ldots, P_n \in M$ a non-empty collection of pairwise distinct points such that the mapping class group $G = \mathrm{MCG}(M; \{P_1, \ldots, P_n\})$ is infinite. Let $\mathcal{A}$ be a finite generating set for G such that*

(i) every element in $\mathcal{A}$ is a fractional power of a Dehn twist;

(ii) every Dehn twist in G is conjugate to a fractional power of an element from $\mathcal{A}$.

Then the word problem in G is efficiently solvable with respect to $\mathrm{zwl}_{\mathcal{A}}$.

There are various generating sets known for mapping class groups that satisfy Condition (i) of the theorem, see [2,3,5–9].

The idea behind the proof is to switch from the word presentation of the elements of the mapping class groups to a geometric presentation, which is more natural and equivalent to the zipped word approach from the complexity point of view. Theorem 1 generalizes the results of [4], but the approach to the construction of the algorithm is different.

We fix a connected compact surface M, orientable or not, and a non-empty set of *punctures* $\mathcal{P} = \{P_1, \ldots, P_n\} \subset M$. If M is a sphere we require $n \geqslant 4$; if M is a projective plane, a disk, an annulus, or a Möbius band we require $n \geqslant 3$; and if M is a torus or a Klein bottle we require $n \geqslant 2$.

By G we will denote *the mapping class group* $\mathrm{MCG}(M, \mathcal{P})$ that is the quotient of the group $\mathrm{Homeo}(M, \mathcal{P})$ of homeomorphisms of M onto itself preserving the subset $\mathcal{P}$ by the connected component $\mathrm{Homeo}_0(M, \mathcal{P})$ of $\mathrm{Homeo}(M, \mathcal{P})$ containing the identity homeomorphism.

We assume that every boundary component γ of M contains at least one of P_i's, which is not a loss of generality.

By *a proper arc* on M we mean an open simple arc α in $M \setminus \mathcal{P}$ approaching some punctures P_i, P_j at the ends such that the closure $\overline{\alpha}$ of α does not bound an *empty* disk, i.e. a disk with no puncture inside. It is allowed, however, that $\overline{\alpha}$ forms a loop.

By *a simple curve* on M we mean a smooth simple closed curve in $M \setminus \mathcal{P}$ that does not bound an empty disk.

By *a multiple curve* on M we mean a possibly empty union of pairwise disjoint simple curves and proper arcs on M.

Two proper arcs are *parallel* if they coincide or enclose an empty disk. Two simple curves are *parallel* if they enclose an empty annulus.

Two curves γ_1, γ_2 are said to be *tight* (with respect to each other) if they either do not intersect or intersect transversely, and there is no empty disk $D \subset M$ bounded by two subarcs $\alpha_1 \subset \overline{\gamma_1}$ and $\alpha_2 \subset \overline{\gamma_2}$ such that at least one of the common endpoints of α_1 and α_2 is not a puncture.

Let γ and γ' be two multiple curves. We write $\gamma \sim \gamma'$ if they are isotopic relative to $\mathcal{P}$.

If two multiple curves γ_1 and γ_2 are tight we define their *geometric intersection index* $\langle \gamma_1, \gamma_2 \rangle$ to be the number of intersections $|\gamma_1 \cap \gamma_2|$ less the number of pairs of parallel proper arcs (α_1, α_2) such that $\alpha_i \subset \gamma_i$, and the number of pairs of isotopic one-sided simple curves (β_1, β_2) such that $\beta_i \subset \gamma_i$. For arbitrary multiple curves γ_1, γ_2, the geometric intersection index $\langle \gamma_1, \gamma_2 \rangle$ is defined as $\langle \gamma_1', \gamma_2' \rangle$ with any tight pair (γ_1', γ_2') of multiple curves such that $\gamma_i' \sim \gamma_i$, $i = 1, 2$ (this number is well defined).

By *a triangulation of M with vertices at $\mathcal{P}$* we mean a maximal collection of proper arcs $\{e_1, \ldots, e_N\}$ such that they are pairwise disjoint and nonparallel. The arcs e_i are called *edges* of the triangulations. We assume additionally that the boundary ∂M is covered by $\bigcup_{i=1}^N \overline{e_i}$.

Let $T = \{e_1, \ldots, e_N\}$ and $T' = \{e'_1, \ldots, e'_N\}$ be two triangulations of M with vertices at $\mathcal{P}$. We denote by $\langle T, T'\rangle$ the $N \times N$ matrix whose (ij)th entry is

$$\langle T, T'\rangle_{ij} = \langle e_i, e'_j\rangle.$$

The point now is that an element $g \in G$ can be recovered uniquely from the matrix $\langle T, g(T)\rangle$. Thus, by choosing a proper encoding for $N \times N$-matrices we get a G-presentation in which an element $g \in G$ can be presented by any sequence of matrices $(m_1, \ldots, m_k)$ such that $m_i = \langle T, g_i(T)\rangle$ with $g_1, \ldots, g_k \in G$, $g_1 \cdot \ldots \cdot g_k = g$. It is then natural to nominate $\langle T, g(T)\rangle$ for being the normal form $\mathrm{nf}(g)$ of g and to measure the complexity of g by the amount of space needed to record $\langle T, g(T)\rangle$, which is comparable to

$$c_T(g) = \sum_{i,j=1}^{N} \log_2(|\langle T, g(T)\rangle_{ij} + \delta_{ij}| + 1),$$

where δ_{ij} is the Kroneker delta. We call *$c_T(g)$ the matrix complexity of g*.

Proposition 1. *Let $\mathcal{A} \subset G$ be a generating set as in Theorem 1 and T a triangulation of M. Then the zipped word length funciton $\mathrm{zwl}_{\mathcal{A}}$ is comparable to the matrix complexity function c_T.*

The key question about the efficiency of the matrix approach is how to compute $\langle T, g_1(g_2(T))\rangle$ from $\langle T, g_1(T)\rangle$ and $\langle T, g_2(T)\rangle$ for arbitrary $g_1, g_2 \in G$. It turns out that this computation has much in common with the ordinary matrix multiplication.

Proposition 2. *The matrix element $\langle T, g_1(g_2(T))\rangle_{ij}$ equals $\langle \gamma, \gamma'\rangle$, where γ and γ' are multiple curves whose geometric intersection indices with the edges of T form the ith row of $\langle T, g_1(T)\rangle$ and the jth column of $\langle T, g_2(T)\rangle$, respectively.*

Now the key result is the following one.

Proposition 3. *There exists an algorithm that, given the geometric intersection indices of two multiple curves γ_1 and γ_2 with the edges of a fixed triangulation $T = (e_1, \ldots, e_N)$, computes $\langle \gamma_1, \gamma_2\rangle$ in time $O\big(|\gamma_1|_T \cdot |\gamma_2|_T\big)$, where by $|\gamma|_T$ we denote the following complexity measure:*

$$|\gamma|_T = \sum_i \log_2(|\langle \gamma, e_i\rangle| + 1).$$

The proof uses a technique based on train tracks and their splittings [1,10].

References

[1] M.Bestvina; M.Handel. Train-tracks for surface homeomorphisms. *Topology* **34** (1995), no. 1, 109–140.

[2] T.E.Brendle, B.Farb. Every mapping class group is generated by 6 involutions. *J. Algebra* **278** (2004), no. 1, 187–198.

[3] D.R.J.Chillingworth. A finite set of generators for the homeotopy group of a non-orientable surface, *Proc. Cambridge Philos. Soc.* **65** (1969), 409-430.

[4] I. Dynnikov, B. Wiest. On the complexity of braids. *J. Eur. Math. Soc.* **9** (2007), no. 4, 801–840.

[5] M.Korkmaz. Mapping class groups of nonorientable surfaces. *Geom. Dedicata* **89** (2002), 109-133.

[6] W.B.R.Lickorish. Homeomorphisms of non-orientable two-manifolds, *Proc. Cambridge Philos. Soc.* **59** (1963), 307-317.

[7] W.B.R.Lickorish. Afinite set of generators for the homeotopy group of a 2-manifold, *Proc. Cambridge Philos. Soc.* **60** (1964), 769-778.

[8] W.B.R.Lickorish. Corrigendum: On the homeotopy group of a 2-manifold, *Proc. Cambridge Philos. Soc.* **62** (1966), 679-681.

[9] B.Szepietowski. The mapping class group of a nonorientable surface is generated by three elements and by four involutions. *Geom. Dedicata* **117** (2006), 1–9.

[10] H. Masur, L. Mosher, S. Schleimer. On train-track splitting sequences. Duke Math. J. **161** (2012), no. 9, 161–1656.

[11] L.Mosher. Mapping class groups are automatic. *Ann. of Math.* (2) **142** (1995), no. 2, 303–384.

Yet another proof of Parikh's Theorem

Manfred Kufleitner
Loughborough University

Parikh's Theorem is a classical tool in formal language theory. It shows that context-free languages admit a simple structure regarding the number of occurrences of the letters in the alphabet. More precisely, the theorem says that the so-called Parikh image of a context-free language is semilinear. There is a ”logic” version of Parikh's theorem due to Verma, Seidl, and Schwentick. They showed that, for a context-free grammar, one can construct an existential formula in Presburger arithmetic defining the Parikh image. Since Presburger arithmetic has the same expressive power as semilinear sets, this also yields Parikh's Theorem. During the talk, we give a new and simple proof of Verma, Seidl, and Schwentick's theorem.

Physical Universality in Cellular Automata, Turing Machines and Beyond

Ilkka Törmä
University of Turku

A deterministic dynamical system is called physically universal, if one can perform an arbitrary manipulation of any bounded region of the configuration space using only the dynamical rules of the system. Intuitively, in such a system there exist ”machines” that can analyze and alter all objects of bounded size in any desired manner. Janzing defined the notion of physical universality in 2010 and left open the existence of systems with the property. Schaeffer was the first to construct a two-dimensional physically universal cellular automaton, and later Salo and I produced a one-dimensional version of it. We have also discovered a two-dimensional Turing machine with a similar property. I present these examples, some other results and possible extensions of the concept.

The geography of multitape automata

Reino Niskanen
University of Oxford

Finite automata is a well-studied and understood model of computation. An extension where the automaton has several input tapes was introduced in the late 1950's. It turned out that understanding the behaviour of multitape automata is a more challenging problem than for one-tape automata. For example, non-deterministic automata are more expressive than deterministic ones if there are at least two tapes present, while for one-tape automata they define the same language family. Similarly, some problems have significantly different complexities depending on the formalism. For example, the equivalence problem (i.e., whether two given automata accept the same language) is undecidable for non-deterministic two-tape automata but decidable for deterministic k-tape automata.

In this talk, we further investigate the geography of multitape automata with respect to the behaviour of the head. We consider the expressive power of relations recognized by different multitape automata families. It is known that there exists a strict hierarchy of relations: rational relations, deterministic rational relations, synchronous relations (also called regular or automatic) and recognizable relations (also called monadic decomposable). Our main focus is on the so-called relative decidability, where we are asked to decide whether a relation from one family (say a rational relation) can also be expressed by a less expressive family (say by a deterministic rational relation). We will talk about the recent advancements in deciding whether a given synchronous relation is a recognizable relation, that is, the relative decidability for the two of the simplest families in the above hierarchy.

Decision Problems for Finite Automata and Semigroups

Lukas Fleischer

FMI, University of Stuttgart*
Universitstra 38, 70569 Stuttgart, Germany
fleischer@fmi.uni-stuttgart.de

Abstract

Both automata theory and complexity theory play an important role in computer science. We investigate the computational complexity of classical decision problems for regular languages: emptiness, universality, inclusion, equivalence, and intersection non-emptiness. For each of these problems three different representations of the languages are considered:

1. deterministic finite automata (DFA),
2. non-deterministic finite automata (NFA) and
3. morphisms to finite semigroups, where the semigroups are given as multiplication tables.

Naturally, the complexity of these problems decreases when imposing constraints on the inputs. These constraints can often be expressed in terms of membership (of the transition semigroup or the semigroup itself) to a certain variety of finite semigroups. The full classification of the complexity of language decision problems for varieties of finite monoids is an interesting open problem with connections to many other decision problems in algebra. We give a brief overview on existing results and known relationships.

It is well-known that the emptiness problem for DFA is NL-complete [10], whereas intersection non-emptiness is PSPACE-complete [11]. The same completeness results hold for languages given as NFA and for languages given as recognizing morphisms to finite semigroups. Moreover, for DFA and for finite semigroups, one can show that the emptiness, universality, inclusion and equivalence problems are equivalent under very weak reductions if a suitable input

*This work was supported by the DFG grant DI 435/5–2.

encoding is chosen. These reductions are *variety-preserving* in the sense that every instance from a variety of finite semigroups $\mathbf{V}$ is mapped to an instance that again belongs to $\mathbf{V}$. Thus, the universality, inclusion and equivalence problems for DFA and finite semigroups are also NL-complete. Beyond that, in order to analyze the complexity of these problems for a specific variety, it suffices to investigate the emptiness problem. It is important to note that these equivalences do not hold for NFA. In the NFA setting, there are reductions from intersection non-emptiness to universality, inclusion and equivalence, and each of these problems is PSPACE-complete.

When it comes to considering specific varieties of finite semigroups, the case of finite groups is particularly interesting. Here, the DFA emptiness problem is known to be decidable in deterministic logarithmic space using Reingold's algorithm for undirected graph reachability [12] and L-hard by results from [5]. It was conjectured in [2] that L-completeness also holds in the semigroup setting. Partial progress towards a refutation of this conjecture was made by Barrington, Kadau, Lange and McKenzie in 2001, who obtained results for Abelian groups, nilpotent groups and solvable groups [3]. However, the original conjecture remained open for more than 25 years. It was refuted only recently [6] with a proof that can be divided into three steps:

1. Proving that the variety of finite groups has the *poly-logarithmic circuits property*: for a subset X of a finite group G and an element $s \in \langle X \rangle$, there always exists a straight-line program (SLP, for short) over X that computes s and has poly-logarithmic size (in $|G|$). The terminology *poly-logarithmic circuits property* is inspired by the fact that an SLP can also be viewed as an algebraic circuit.

2. Proving that having the poly-logarithmic circuits property implies decidability of the emptiness problem by quasi-polynomial-size constant-depth Boolean circuits.

3. Applying known lower bounds from circuit complexity [9, 13] to obtain the non-hardness result.

The first step was actually already obtained much earlier by Babai and Szemerédi in a different context [1]. In his doctoral thesis, the author of this note improved and generalized these results. He showed that a variety of finite monoids has the poly-logarithmic circuits property if and only if it contains only commutative monoids or only Clifford monoids. He proved that the emptiness problem for such varieties is decidable in poly-logarithmic time on non-deterministic random-access Turing machines, thereby improving and simplifying the circuit-based algorithm from [6]. He also showed that the problem is NL-complete for all varieties containing a monoid that is not completely regular. For the variety of completely regular monoids, only partial results are known.

The idea of using the existence of succinct representations of semigroup elements and random-access Turing machines led to several additional interesting results. For example, the intersection non-emptiness problem for semigroups is NP-complete for every variety obtained by starting with the variety of finite groups $\mathbf{G}$ and repeatedly iterating Mal'cev products of the form $\mathbf{K} \textcircled{m} \mathbf{V}$ and $\mathbf{D} \textcircled{m} \mathbf{V}$ where $\mathbf{K}$ denotes the variety of all reverse definite semigroups and $\mathbf{D}$ denotes the variety of definite semigroups [7]. In the automaton setting, NP-completeness is known to hold for group DFA [8] and for DFA with $\mathcal{R}$-trivial transition semigroups [4] but is still open even for $\mathcal{L}$-trivial transition semigroups.

Lastly, there also exists an algorithm for group isomorphism that relies on very similar techniques and can be implemented on an alternating random-access Turing machine with a bounded number of alternations and poly-logarithmic running time, thereby simplifying several earlier results on group isomorphism.

References

[1] L. Babai and E. Szemeredi. On the complexity of matrix group problems I. In *25th Annual Symposium on Foundations of Computer Science*, pages 229–240, Oct 1984.

[2] D. A. M. Barrington and P. McKenzie. Oracle branching programs and Logspace versus P. *Information and Computation*, 95(1):96–115, 1991.

[3] D. M. Barrington, P. Kadau, K.-J. Lange, and P. McKenzie. On the complexity of some problems on groups input as multiplication tables. *Journal of Computer and System Sciences*, 63(2):186–200, 2001.

[4] M. Beaudry, P. McKenzie, and D. Thérien. The membership problem in aperiodic transformation monoids. *J. ACM*, 39(3):599–616, 1992.

[5] S. A. Cook and P. McKenzie. Problems complete for deterministic logarithmic space. *Journal of Algorithms*, 8(3):385–394, 1987.

[6] L. Fleischer. On the Complexity of the Cayley Semigroup Membership Problem. In R. A. Servedio, editor, *CCC 2018, Proceedings*, volume 102 of *LIPIcs*, pages 25:1–25:12. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2018.

[7] L. Fleischer and M. Kufleitner. The Intersection Problem for Finite Monoids. In *STACS 2018, Proceedings*, volume 96 of *LIPIcs*, pages 30:1–30:14. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2018.

[8] M. Furst, J. Hopcroft, and E. Luks. Polynomial-time algorithms for permutation groups. In *21st Annual Symposium on Foundations of Computer Science (SFCS 1980)*, pages 36–41, Oct 1980.

[9] J. Hastad. Almost optimal lower bounds for small depth circuits. In *Proceedings of the Eighteenth Annual ACM Symposium on Theory of Computing*, STOC '86, pages 6–20, New York, NY, USA, 1986. ACM.

[10] M. Holzer and M. Kutrib. Descriptional and computational complexity of finite automata — a survey. *Inf. Comput.*, 209(3):456–470, 2011.

[11] D. Kozen. Lower bounds for natural proof systems. In *Proc. of the 18th Ann. Symp. on Foundations of Computer Science, FOCS'77*, pages 254–266, Providence, Rhode Island, 1977. IEEE Computer Society Press.

[12] O. Reingold. Undirected connectivity in log-space. *J. ACM*, 55(4):17:1–17:24, Sept. 2008.

[13] A. C.-C. Yao. Separating the polynomial-time hierarchy by oracles. In *Proceedings of the 26th Annual Symposium on Foundations of Computer Science*, SFCS '85, pages 1–10, Washington, DC, USA, 1985. IEEE Computer Society.

Exhaustive search of polygons than tile the plane

Michael Rao
Charge de recherche CNRS au LIP

An "ein-stein" tile is a tile that tessellate the plane, but only in a non-periodic way. The "Taylor-Socolar" tile (2011) has this property, but is not connected. One can ask if a connected ein-stein tile exists.

In order to solve this problem, one can look at on a first time polygons In 1918, Karl Reinhardt asked which convex polygon can tile the plane, and the pentagon was the only opened case. Fifteen types of such pentagons have been found between 1918 and 2015.

I show that, for every k, one can classify k-gones which tiles the plane into a finite set of families. For convex pentagons, there are 371 families to consider, and among these families, there are no new pentagon that tiles the plane. In particular, this implies that there is no convex ein-stein tile.

Contributed talks

On the modularity of configuration graphs

Marina Leri, Yuri Pavlov

Institute of Applied Mathematical Research, Karelian Research Centre RAS
e-mail: leri@krc.karelia.ru, pavlov@krc.karelia.ru

We consider configuration graphs [1] with N vertices. The vertex degrees $1, \ldots, N$ are independent identically distributed random variables $\xi_1, \ldots, \xi_N$ drawn from the following distribution:

$$p_k = \mathbf{P}\{\xi_i = k\}, \quad k = 1, 2, \ldots, \quad i = 1, \ldots, N. \tag{1}$$

We denote $\zeta_N = \xi_1 + \ldots, \xi_N$. The degree of each vertex equals to the number of incident half-edges, i.e. edges for which the adjacent vertices are not defined yet. All the half-edges are numbered in an arbitrary order. Since the sum of vertex degrees has to be even, one half-edge is added to an equiprobably chosen vertex if the sum is odd. The graph is constructed by joining each half-edge to another equiprobably to form edges. Because the paring is done without any restrictions, multiple edges and loops can appear in the graph. It is well known (see e.g. [2]) that configuration random graphs are being a good representation of various complex networks such as Internet, social and telecommunication networks.

Let the distribution (1) has finite mathematical expectation:

$$m = \sum_{k=1}^{\infty} k p_k. \tag{2}$$

We denote by $F(z)$ the generating function for the distribution (1):

$$F(z) = \sum_{k=1}^{\infty} p_k z^k.$$

Further we will consider the Galton-Watson branching process $Z(t)$, $t = 0, 1, 2, \ldots$, starting with one particle with offspring distribution:

$$q_k = \frac{(k+1)p_{k+1}}{m}, \quad k = 0, 1, 2, \ldots \tag{3}$$

Let M be the mathematical expectation of the distribution (3):

$$M = \frac{1}{m} \sum_{k=2}^{\infty} k(k-1) p_k \tag{4}$$

and let g be the extinction probability of the process $Z(t)$.

One of the important numerical characteristics of networks is modularity. It is a recently introduced quality measure for graph clustering when vertices are divided into groups (clusters). Graphs with high modularity have dense connections (edges) between the vertices within clusters but sparse connections between vertices in different clusters. Let H be a set of all possible divisions of our graph vertices into clusters and $A \in H$ is a particular division. By [3], [4] we can express the modularity for the division A as

$$Q_A = \frac{1}{\zeta_N} \sum_{i,j=1}^{\infty} \left(\alpha_{ij} - \frac{\xi_i \xi_j}{\zeta_N} \right) \delta_{i,j},$$

where α_{ij} are random elements of adjacency matrix, $\delta_{ij} = 1$ if i and j are in the same cluster and $\delta_{ij} = 0$ otherwise. It is known that $|Q_A| \leqslant 1$ for any $A \in H$.

We denote Q_H^* maximum modularity:

$$Q_H^* = \max_{A \in H} Q_A.$$

The maximum modularity of a graph is used to describe the level of graph clustering and to find the best division of vertices. Many random graph models have high modularity, see [5] for Erdos - Renyi random graphs and [6] for random regular graphs and for preferential attachment models. But we don't know results about modularity of configuration graphs and we proved the next theorem for maximum modularity in such models.

Theorem *Let $N \to \infty$. Then the following assertions hold a.a.s:*

1. *If $M \leqslant 1$, then $Q_H^* \to 1$.*
2. *If $M > 1$, then $Q_H^* \geqslant 1 - (1 - F(g))^2 + o(1)$.*

The authors of [7] show that for modeling of many complex networks there can be used configuration graphs where

$$p_k = \frac{1}{k^\tau} - \frac{1}{(k+1)^\tau}, \tag{5}$$

$k = 1, 2, \ldots$, $\tau > 1$. It is a well known fact (see e.g. [2]) that for a majority of networks $\tau \in (1, 2)$, however in some models, as it was shown in our previous research [8], models with $\tau > 2$ have to be a matter of interest too. From (1) and (2) follows that the vertex degree distribution (5) has a mathematical expectation $m = \zeta(\tau)$, where $\zeta(\tau)$ is Riemann zeta function in τ. From (3) – (5) we find that $M = \infty$ if $\tau \leqslant 2$, and in the case when $\tau > 2$

$$M = 2\left(\frac{\zeta(\tau-1)}{\zeta(\tau)} - 1\right).$$

It is not difficult to show that $M = 1$ when $\tau = \tau^* = 2.8106\ldots$, therefore when $\tau \geqslant \tau^*$ the first assertion of the theorem holds, and when $\tau < \tau^*$ – the second one.

We have made a series of simulations aiming to find the dependencies of the variations of Q_H^* on N. In these experiments we used our previous simulation model of power-law configuration graph described in [8]. To find an optimal division of graph into clusters which ensures maximum of modularity we used an algorithm given in [9]. Let us note that these experiments are computationally demanding for large N, thus for now we considered graphs of 100 to 3000 vertices with different values of the parameter τ. For each pair (τ, N) 100 graph realizations were generated. Some of the obtained results are given in the Table 1, where the columns 2–8 contain average empirical values of maximum modularity corresponding to the pairs (τ, N). The last two columns contain the values of the extinction probability g and the value $1-(1-F(g))^2$. It is easy to see that the obtained results are in accord with the assertions of the theorem. But the rate of maximum modularity changes is apparently low with the growth of N, so we plan to continue our experiments for graphs with $N > 3000$.

Table 1: Simulation results (in the last column $W = 1 - (1 - F(g))^2$)

	N								
τ	100	500	1000	1500	2000	2500	3000	g	W
1.1	0.311	0.276	0.262	0.262	0.243	0.248	0.235	0.052	0.056
1.5	0.516	0.517	0.514	0.515	0.505	0.519	0.514	0.292	0.367
2.0	0.700	0.726	0.720	0.723	0.724	0.719	0.720	0.617	0.781
3.0	0.871	0.896	0.898	0.899	0.903	0.900	0.902	1	1

Furthermore, regression dependencies of maximum modularity on N were found for different values of τ. In particular, the following dependencies were derived for some values of τ (where R^2 is the determination coefficient):

$$\begin{aligned}
\tau = 1.1: &\quad Q_{max} = 0.408 - 0.021 \ln N, &\quad R^2 = 0.91;\\
\tau = 1.5: &\quad Q_{max} = 0.521 - 0.001 \ln N, &\quad R^2 = 0.98;\\
\tau = 2.0: &\quad Q_{max} = 0.677 + 0.006 \ln N, &\quad R^2 = 0.98;\\
\tau = 3.0: &\quad Q_{max} = 0.835 + 0.009 \ln N, &\quad R^2 = 0.98.
\end{aligned}$$

The study was carried out under state order to the Karelian Research Centre of the Russian Academy of Sciences (Institute of Applied Mathematical Research KarRC RAS). The research was carried out using the equipment of the Core Facility of the Karelian Research Centre of the Russian Academy of Sciences.

References

[1] Bollobas B. A probabilistic proof of an asymptotic formulae for the number of labelled regular graphs. *Eur.J.Comb.* Vol. 2, 1980, 311–316.

[2] Hofstad R. Random graphs and complex networks. Vol. 1, 2017. Cambridge Univ.Press, Cambridge.

[3] Newman M.E.J., Girvan M. Finding and evaluating community structure in networks. *Physical Review E.* Vol. 69, 2004, 026113.

[4] Newman M.E.J. Modularity and community structure in networks. *PNAS.* Vol. 103, iss. 23, 2006, 8577-8582.

[5] McDiamid C., Sherman F. Modularity of Erdos-Renyi random graphs. arXiv: 1808.02243[math.CO], 2018.

[6] Prokhorenkova L.O., Pralat P., Raigorodskii A. Modularity in several random graph models. *Electronic Notes in Discrete Mathematics.* Vol. 61, 2017, 947-953.

[7] Reittu H., Norros I. On the power-law random graph model of massive data networks. *Performance Evaluation*, Vol. 55, iss. 1-2, 2004, 3-23.

[8] Leri M., Pavlov Yu. Power-law random graphs' robustness: link saving and forest fire model. *Austrian Journal of Statistics.* Vol. 43, iss. 4, 2014, 229-236.

[9] Newman M.E.J. Fast algorithm for detecting community structure in networks. *Physical Review E.* Vol. 69, 2004, 066133.

Game-Theoretic method for analysis of communication networks

Vladimir Mazalov
Institute of Applied Mathematical Research
Karelian Research Center of RAS
Petrozavodsk, Russia
vmazalov@krc.karelia.ru

We propose a new concept of the betweenness centrality for weighted graphs using the methods of cooperative game theory. The characteristic function is determined by special way for different coalitions (subsets of the graph). We use the approach in which the characteristic function is determined via the number of direct and indirect weighted connecting paths in the coalition. After that the betweenness centrality is determined as the Myerson value. The results of computer simulations for some examples of networks, in particular, for the popular social network "VKontakte", as well as the comparing with the PageRank method are presented. Then we apply game-theoretic methods for community detection in networks. The traditional methods for detecting community structure are based on selecting dense subgraphs inside the network. Here we propose to use the methods of cooperative game theory that highlight not only the link density but also the mechanisms of cluster formation. Specifically, we suggest two approaches from cooperative game theory: the first approach is based on the Myerson value, whereas the second approach is based on hedonic games. Both approaches allow to detect clusters with various resolution. However, the tuning of the resolution parameter in the hedonic games approach is particularly intuitive. Furthermore, the modularity based approach and its generalizations can be viewed as particular cases of the hedonic games. Finally, for approaches based on potential hedonic games we suggest a very efficient computational scheme using Gibbs sampling.

Stable Coalitions in Dynamic Multicriteria Games

Anna Rettieva*
Institute of Applied Mathematical Research
Karelian Research Center of RAS

Abstract

We consider a dynamic, discrete-time, game model where the players use a common resource and have different criteria to optimize. The coalition formation process in dynamic multicriteria games is considered. The characteristic function is constructed in two unusual forms: the model without information and the model with informed players. Coalition stability concepts are adopted for dynamic multicriteria games to obtain new weak and strong stability conditions. To illustrate presented approaches a multicriteria bioresource management problem with finite horizon is investigated.

1 Introduction

Mathematical models involving more than one objective seem more adherent to real problems. Often players have more than one goal which are often not comparable. These situations are typical for game-theoretic models in economic and ecology.

In this paper we consider a dynamic, discrete-time, game model where the players use a common resource and have different criteria to optimize. First, we construct a multicriteria Nash equilibrium using the approach presented in [4]. Then, we find a multicriteria cooperative equilibrium as a solution of a Nash bargaining scheme with the multicriteria Nash equilibrium payoffs playing the role of status quo points [5].

The coalition formation process in multicriteria dynamic games is considered. The characteristic function is constructed in two unusual forms. Under the first approach [2] players outside coalition S or singletons switch to their

*This work was supported by the Russian Science Foundation, project no. 17-11-01079.

Nash strategies, which were determined for the initial noncooperative game. This case can be interpreted as the situation when players have no information about the fact that the coalition was formed. Under the second approach singletons determine new Nash strategies in the game with $N\backslash S$ players. This case corresponds to the situation when players know that coalition S was formed.

We extend the internal and external stability concepts [1] to multicriteria dynamic games. The conditions for weak and strong stability of coalitions are presented.

To illustrate presented approaches a multicriteria bioresource management problem with finite horizon is investigated.

2 Dynamic Multicriteria Game with Finite Horizon

Consider a multicriteria dynamic game with finite horizon in discrete time. Let $N = \{1, \dots, n\}$ players exploit a common resource and each of them wishes to optimize k different criteria. The state dynamics is in the form

$$x_{t+1} = f(x_t, u_{1t}, \dots, u_{nt}) , \;\; x_0 = x , \tag{1}$$

where $x_t \geq 0$ is the population size at time $t \geq 0$, $f(x_t, u_{1t}, \dots, u_{nt})$ denotes the natural growth function, and $u_{it} \geq 0$ gives the catch of player i at time t, $i \in N$.

Denote $u_t = (u_{1t}, \dots, u_{nt})$. Each player has k goals to optimize. The players' payoffs on finite planning horizon $[0, m]$ are defined as

$$J_i = \begin{pmatrix} J_i^1 = \sum\limits_{t=0}^{m} \delta^t g_i^1(u_t) \\ \dots \\ J_i^k = \sum\limits_{t=0}^{m} \delta^t g_i^k(u_t) \end{pmatrix} , \, i \in N \tag{2}$$

where $g_i^j(u_t) \geq 0$ gives the instantaneous utility, $j = 1, \dots, k$, $i \in N$, $\delta \in (0, 1)$ denotes the discount factor.

First, we construct a multicriteria Nash equilibrium strategies and payoffs $J_i^{jN}(u_t^N)$, $i \in N$, $j = 1, \dots, k$ applying the approach presented in [4]. For that we determine the guaranteed payoffs points G_i^j, $i \in N$, $j = 1, \dots, k$ applying one of the variants of their construction.

Then, we find a multicriteria cooperative equilibrium as a solution of a Nash bargaining scheme with the multicriteria Nash equilibrium payoffs playing the role of status quo points [5], so we solve the next problem:

$$(\sum_{i=1}^{n} J_i^{1c}(u_t^c) - \sum_{i=1}^{n} J_i^{1N}(u_t^N)) \cdot \ldots \cdot (\sum_{i=1}^{n} J_i^{kc}(u_t^c) - \sum_{i=1}^{n} J_i^{kN}(u_t^N)) =$$
$$= (\sum_{t=0}^{m} \delta^t \sum_{i=1}^{n} g_i^1(u_t^c) - \sum_{i=1}^{n} J_i^{1N}(u_t^N)) \cdot \ldots \cdot$$
$$\cdot(\sum_{t=0}^{m} \sum_{i=1}^{n} g_i^k(u_t^c) - \sum_{i=1}^{n} J_i^{kN}(u_t^N)) \to \max_{u_t^c} . \qquad (3)$$

3 Coalition Formation Process

We consider a coalition formation process in dynamic multicriteria games. Let assume that a coalition S is formed. The characteristic function is constructed in two unusual forms. Under the first approach [2] singletons switch to their Nash strategies, which were determined for the initial noncooperative multicriteria game. This case can be interpreted as the situation when players have no information about the fact that the coalition was formed. Under the second approach singletons determine new Nash strategies in the game with $N\backslash S$ players. This case corresponds to the situation when players know that coalition S was formed. The sizes of stable coalitions are the subjects of investigation.

For the model without information, to determine the cooperative payoff of coalition S it is required to solve the next problem:

$$(\sum_{i\in S} J_i^{1S}(\tilde{u}_t) - \sum_{i\in S} J_i^{1N}(\tilde{u}_t)) \cdot \ldots \cdot (\sum_{i\in S} J_i^{kc}(\tilde{u}_t) - \sum_{i\in S} J_i^{kN}(\tilde{u}_t)) =$$
$$= (\sum_{t=0}^{m} \delta^t \sum_{i\in S} g_i^1(\tilde{u}_t) - \sum_{i\in S} J_i^{1N}(\tilde{u}_t)) \cdot \ldots \cdot$$
$$\cdot(\sum_{t=0}^{m} \delta^t \sum_{i\in S} g_i^k(\tilde{u}_t) - \sum_{i\in S} J_i^{kN}(\tilde{u}_t)) \to \max_{u_{it},\, i\in S} , \qquad (4)$$

where

$$\tilde{u}_t = \begin{cases} u_{it}, \ i \in S \,, \\ u_{it}^N, \ i \in N\backslash S \,. \end{cases}$$

For the model with informed players, to determine the cooperative payoff of coalition S it is required to solve the next problem:

$$(\sum_{i\in S} J_i^{1S}(\tilde{u}_t) - \sum_{i\in S} J_i^{1N}(\tilde{u}_t)) \cdot \ldots \cdot (\sum_{i\in S} J_i^{kS}(\tilde{u}_t) - \sum_{i\in S} J_i^{kN}(\tilde{u}_t)) =$$
$$= (\sum_{t=0}^{m} \delta^t \sum_{i\in S} g_i^1(\tilde{u}_t) - \sum_{i\in S} J_i^{1N}(\tilde{u}_t)) \cdot \ldots \cdot$$
$$\cdot (\sum_{t=0}^{m} \delta^t \sum_{i\in S} g_i^k(\tilde{u}_t) - \sum_{i\in S} J_i^{kN}(\tilde{u}_t)) \to \max_{u_{it},\, i\in S}\,, \tag{5}$$

where

$$\tilde{u}_t = \begin{cases} u_{it},\ i \in S\,, \\ \tilde{u}_{it}^N,\ i \in N\backslash S\,, \end{cases}$$

and the individual players' strategies $\tilde{u}_{it}^N$, $i \in N\backslash S$ are defined from the maximization problems:

$$H_i = (J_i^1(\tilde{u}_t) - G_i^1) \cdot \ldots \cdot (J_i^k(\tilde{u}_t) - G_i^k) \longrightarrow \max_{u_{it},\, i\in N\backslash S}, i \in N\backslash S\,.$$

Denote the cooperative strategies of the coalition S's members as $u_t^S = (u_{it}^S)_{i\in S}$ and the strategies of singletons as $u_t^{NS} = (u_{it}^N)_{i\in N\backslash S}$ (model without information) or $u_t^{NS} = (\tilde{u}_{it}^N)_{i\in N\backslash S}$ (model with informed players).

Note that under presented concepts there is no need to distribute cooperative payoff of coalition S among it's members as the vector payoff of coalition member $i \in S$ $J_i^S(\cdot) = (J_i^{1S}(\cdot), \ldots, J_i^{kS}(\cdot))$ is obtained from the schemes of characteristic function construction.

4 Coalition Stability

The classical coalition stability concept (internal and external stability) was presented by [1]. Here we adopt these concepts for multicriteria dynamic games to define weak and strong stable coalitions.

Definition 1. *Coalition S is weak internally stable if* $\neg\exists i \in S$:

$$J_i^S(u_t^S, u_t^{NS}) < J_i^N(u_t^{S\backslash\{i\}}, u_t^{NS\backslash\{i\}})\,. \tag{6}$$

Coalition S is weak externally stable if $\neg\exists i \in N\backslash S$:

$$J_i^N(u_t^S, u_t^{NS}) < J_i^{S\cup\{i\}}(u_t^{S\cup\{i\}}, u_t^{NS\cup\{i\}})\,. \tag{7}$$

Definition 2. *Coalition S is strong internally stable if $\neg\exists i \in S$:*

$$J_i^S(u_t^S, u_t^{NS}) \leqq J_i^N(u_t^{S\backslash\{i\}}, u_t^{NS\backslash\{i\}})\,. \tag{8}$$

Coalition S is strong externally stable if $\neg\exists i \in N\backslash S$:

$$J_i^N(u_t^S, u_t^{NS}) \leqq J_i^{S\cup\{i\}}(u_t^{S\cup\{i\}}, u_t^{NS\cup\{i\}})\,. \tag{9}$$

Here $a < b \Leftrightarrow a_j < b_j$, $a \leqq b \Leftrightarrow a_j \leq b_j$, $\forall j = 1, \ldots, k$.

Internal stability means that no coalition member wishes to leave the coalition and become a singleton. External stability means that no singleton wishes to join the coalition. And we have strong and weak conditions to guarantee the coalition stability.

Definition 3. *Coalition S is weak (strong) stable if conditions (6),(7) ((8),(9)) are fulfilled.*

We consider a dynamic multicriteria model related with the bioresource management problem (harvesting) to show how the suggested concepts work. We conclude that for ecological system and for coalition's members it is better when coalition is formed insensibly, but for singletons the second variant of characteristic function's construction is more profitable. As for coalition stability, we show that only small-size coalitions are internally stable.

References

[1] D'Aspremont, C. et al.: On the stability of collusive price leadership. Can. J. Econ. 16(1), 17–25 (1983)

[2] Petrosjan, L.A., Zaccour, G. Time-consistent Shapley value allocation of pollution cost reduction. J. of Econ. Dyn and Contr. 27(3), 381–398 (2003)

[3] Pieri, G., Pusillo, L.: Multicriteria Partial Cooperative Games. App. Math. 6(12), 2125–2131 (2015)

[4] Rettieva, A.N.: Equilibria in dynamic multicriteria games. Int. Game Theory Rev. 19(1), 1750002 (2017)

[5] Rettieva, A.N.: Dynamic multicriteria games with finite horizon. Mathematics. 6(9), 156, (2018)

[6] Shapley, L.S.: Equilibrium points in games with vector payoffs. Naval Res. Log. Quart. 6, 57–61 (1959)

n-person Optimal Stopping Game with Full Information

Anna Ivashko, Vladimir Mazalov
Institute of Applied Mathematical Research
Karelian Research Center of RAS
Petrozavodsk, Russia
aivashko@krc.karelia.ru, vmazalov@krc.karelia.ru

Tatiana Seregina
Ecole Nationale de l'Aviation Civile
and Toulouse Business School
Toulouse, France
ts.tseregina@gmail.com

We consider the following non-cooperative n-person optimal stopping game related with the popular TV game "The Price is Right". A player receives scores by observing sums of independent and identically distributed random variables from a uniform distribution on [0, 1]. At each step, each player has to decide whether to stop on the current observation or to proceed further and receive the next value of independent random variable, which is added to the scores obtained previously. The winner is the player whose total scores is the closest to, but not exceeding 1. If the score sums of each player exceeds the level 1, then the winner is the player with the lowest number of scores. Each player seeks to maximize his own winning probability.

According to the information type, the two versions of the game can be considered: a version with no information, where no player is revealed any information about other players' game, and, a full-information version, where each subsequent player is aware of actions and outcomes of previous players.

The game without information was considered in [1, 2]. The problem with full information and two steps was analyzed in [3] within the framework of probability theory.

In this paper, the solution for the multi-step full-information optimal stopping game and optimal stopping threshold strategies are provided.

Theorem *In the game of n players with full information and infinite number of steps, the optimal threshold of the first player* $u_1^{(inf,n,F)} = x$ *can be found from* *the equation*

$$(1 - e^x(1 - x))^{n-1} = \int_x^1 (1 - e^y(1 - y))^{n-1} dy.$$

We compare the optimal strategies in the games with full information and with no information. The properties of optimal strategies are proved and numerical results are given.

This work was supported by the Institute of Applied Mathematical Research KRC of RAS.

References

1. *Kaynar B.* Optimal stopping in a stochastic game. Probability in the Engineering and Information Sciences. 2009. N. 23. P. 51–60.

2. *Mazalov V.V., Ivashko A.A.* Equilibrium in n-person game of Showcase-Showdown. Probability in the Engineering and Informational Sciences, Cambridge Univ. Press. 2010. N. 24. P. 397–403.

3. *Tijms H.C.* Understanding probability, 2nd ed. Cambridge: Cambridge Univ. Press. 2007.

Learning Automata with Growing Memory

Alexander Kolnogorov

Yaroslav-the-Wise Novgorod State University, Velikiy Novgorod, Russia

E-mail: Alexander.Kolnogorov@novsu.ru

We consider learning automata which were proposed by M. L. Tsetlin and V. I. Krinsky (see, e.g., [1]). These automata provide expedient behavior in a random environment. Formally, random environment is a controlled random process ξ_n, $n = 1, 2, \dots$, which values ($\xi_n \in \{0, 1\}$) are interpreted as incomes, depend only on currently chosen actions y_n ($y_n \in \{1, 2\}$) and are described by probability distributions $\Pr(\xi_n = 1 | y_n = \ell) = p_\ell$, $\Pr(\xi_n = 0 | y_n = \ell) = q_\ell$; $p_\ell + q_\ell = 1$, $\ell = 1, 2$.

Expedient behavior implies that automaton chooses the best action, corresponding to the larger expected one-step income, more often then another, i.e.

$$\liminf_{N\to\infty} N^{-1}\mathbf{E}\left(\sum_{n=1}^{N}\xi_n\right) > 0.5(p_1 + p_2), \tag{1}$$

where $\mathbf{E}$ denotes mathematical expectation. The problem is also well-known as the two-armed bandit problem with time-invariant finite memory [2]. Although it was proved that the left-hand side of (1) enlarges with growing memory and tends to $\max(p_1, p_2)$, the asymptotically optimum analogs of these automata with time invariant memory can not be constructed. We propose asymptotically optimum analogs of learning automata which memory grows dynamically meanwhile the functioning of automata.

Consider automaton $< X, Y, S, s_0, \phi, \psi >$, where $X = \{1, 0\}$, $Y = \{1, 2\}$ are input and output alphabets, $S = \{(k, \ell, h) : k = 1, 2, \dots ; \ell = 1, 2; h = 1, 2, \dots\}$ is a set of states with initial state $s_0 = (1, 1, 1)$, $\phi : S \times X \to S$ and $\psi : S \to Y$ are transition and output functions. The state $s = (k, \ell, h)$ is described by the number of stage k, currently chosen action ℓ and current depth of the state h. In what follows we say that states $\{(\_, \ell, \_)\}$ belong to the ℓ-th branch of automaton. Transition and output functions are as follows

$$\phi((k,\ell,h),1) = \begin{cases} (k,\ell,h+1), \text{ if } \ h < m(k), \\ (k,\ell,m(k)), \text{ if } \ h = m(k), \end{cases}$$
$$\phi((k,\ell,h),0) = \begin{cases} (k,\ell,h-1), \text{ if } \ h > 1, \\ (k,2,1), \text{ if } \ h = 1, \ell = 1, \\ (k+1,1,1), \text{ if } \ h = 1, \ell = 2, \end{cases}$$
$$\psi((k,\ell,h)) = \ell.$$

Let automaton operate in a random environment. In this case, the values of the process $\{\xi_n\}$ are input signals of automaton and output signals $\{y_n\}$ are currently chosen actions. If $m(k) = m$ does not depend on k, one obtains automaton with linear tactic and time invariant finite memory (see [1]) which depth is equal to m. If $m(k)$ is not constant, this automaton starts with the 1-st stage and at the k-th stage operates like the automaton with linear tactic and current depth of memory $m(k)$. At each stage automaton firstly visits states of the first and secondly of the second branches. The k-th stage finishes and passes to the $(k+1)$-st one when the automaton leaves its second branch and passes to the first branch.

Note that automata with linear tactic must be considered in random environments satisfying requirements $\lambda_\ell = p_\ell / q_\ell > 1$, $\ell = 1, 2$. The following results can be proved (see [3, 4]).

Theorem 1. *Let $m(k)$ be nondecreasing integer-valued function, i.e. $m(k_2) \geq m(k_1)$ if $k_2 > k_1$. Denote $G(j) = [j^{2+\delta}]$. If equalities*

$$\lim_{j \to \infty} m(G(j) = \infty, \tag{2}$$

$$\lim_{j \to \infty} \frac{m(G(j+2)-1)}{m(G(j))} = 1 \tag{3}$$

hold for some $\delta > 0$ then considered automaton is asymptotically optimum, i.e.

$$\liminf_{N \to \infty} N^{-1} \left(\sum_{n=1}^{N} \xi_n \right) = \max(p_1, p_2). \qquad (a.s.) \tag{4}$$

Note that the following $m(k)$ satisfy conditions (2), (3):

$$m(k) = [\log(k)] + 1,$$
$$m(k) = [k^\alpha], \quad \alpha > 0,$$
$$m(k) = [k^{\log(k)}],$$

$k = 1, 2, \ldots$. Function $m(k) = 2^k$ does not satisfy conditions (2), (3) and one can prove that it does not provide asymptotic optimality (4).

Theorem 2. *Among all functions* $m(k) = [m^\alpha]$, $\alpha > 0$, *the linear function* $m(k) = k$ *provides the optimum rate of convergency of the current average expected income*

$$N^{-1}\mathbf{E}\left(\sum_{n=1}^{N} \xi_n\right)$$

to its limiting value $\max(p_1, p_2)$. *If* $p_1 > p_2$ *then this rate of convergency is of the order* $N^{-\mu}$ *with* $\mu = 1 - \log_{\lambda_1}(\lambda_2)$.

We present simulation results for different functions $m(k)$.

This research was supported in part by Russian Foundation for Basic Research (project no 18-29-16223-mk).

References

[1] Tsetlin, M. L. Automaton Theory and Modeling of Biological Systems, New York: Academic, 1973.

[2] Hellman, M. E. and Cover T. M. Learning with Finite Memory // Ann. Math. Statist., 41(3), P. 765–782, 1970.

[3] Kolnogorov, A. V. Asymptotically optimal automata with growing memory // Sov. Phys. Dokl., 28, P. 365–366, 1983.

[4] Kolnogorov, A. V. Asymptotically optimum automata with growing memory in a steady-state environment // Autom. Remote Control, 45, P. 1213–1220, 1984.

The linear complexity of new generalized cyclotomic binary sequences over finite field

Nikita Sokolovskii
Novgorod State University, Russia [*]
sokolovskiy.nikita@gmail.com

1 Introduction

Binary sequences are related to the one of the most widely used type of sequences. For example, binary sequences are used in stream ciphers. The linear complexity of a sequence is an important parameter in its evaluation as a key stream cipher for cryptographic applications. A high linear complexity is necessary for a good cryptographic sequence. One of the method to construct sequences with high linear complexity is using cyclotomic and generalized cyclotomic classes, and such sequences are calling cyclotomic and generalized cyclotomic sequences, respectively. There are many works devoted to the study of linear complexity of generalized cyclotomic binary sequences. New generalized cyclotomic classes were presented in [4]. The linear complexity of new family of cyclotomic binary sequences of period p^2 over the field of order two was studied in [3]. The results from [3] was generalized in [2] for cyclotomic binary sequences of period p^n. In this paper, we derive the linear complexity of these sequences over the field of odd characteristics. First, we recall the definition of new sequences from [3].

2 The definition of sequences

Let p be an odd prime and $p{=}ef{+}1$, where e, f are positive integers and f is an even number. Let g be a primitive root modulo p^n . Denote d_j =

[*] The reported study was funded by RFBR and NSFC according to the research project No 19-51-53003

$p^{j-1}(p-1)/e=\ p^{j-1}f$, where $j=1,2,\dots,\ n$. Put, by definition

$D_0^{(p^j)}{=}\left\{g^{t\cdot d_j}(\text{mod } p^j)\ |0\leq t{<}e\right\}$, and $D_i^{(p^j)}{=}g^iD_0^{(p^j)}{=}\left\{g^ix(\text{mod } p^j)\ {:}x\in D_0^{(p^j)}\right\}$,

here $i=1,2,\dots,\ d_j{-}1$. Then $D_i^{(p^j)}$ are called *generalized cyclotomic classes* of order d_j with respect to p^j [4].

As it was shown in [4] we have the partitions

$$\mathbb{Z}_{p^m}{=}\bigcup_{j=1}^{m}\bigcup_{i=0}^{d_j-1}p^{m-j}D_i^{(p^j)}\cup\{0\}$$

for each integer $j\geq 1$ and for an integer $m\geq 1$.

Let b be an integer with $0\leq b\leq p^n-1$. Define two sets

$$\mathcal{C}_0^{(p^n)}{=}\bigcup_{j=1}^{n}\bigcup_{i=d_j/2}^{d_j-1}p^{n-j}D_{(i+b)(\text{mod}d_j)}^{(p^j)}\ \text{ and }\mathcal{C}_1^{(p^n)}{=}\bigcup_{j=1}^{n}\bigcup_{i=0}^{d_j/2-1}p^{n-j}D_{(i+b)(\text{mod}d_j)}^{(p^j)}\cup\{0\}.$$

It is obvious that $\mathbb{Z}_{p^n}{=}\mathcal{C}_0^{(p^n)}\cup\mathcal{C}_1^{(p^n)}$ and $|\mathcal{C}_1^{(p^n)}|=(p^n{+}1)/2$. A new family of almost balanced binary sequences $s^\infty{=}\ (s_0,s_1,s_2,\dots)$ of period p^n was defined in [3] as

$$s_i{=}\begin{cases}0, & \text{if } i\,(\text{mod } p^n)\in\mathcal{C}_0^{(p^n)},\\ 1, & \text{if }\ i\,(\text{mod } p^n)\in\mathcal{C}_1^{(p^n)}.\end{cases}\tag{1}$$

The linear complexity of these sequences over the finite field $\mathbb{F}_2$ was considered in [2,3,5]. Here we consider these sequences over $\mathbb{F}_q$, where q is odd prime and $\mathbb{F}_\text{q}$ is the finite field of q elements.

It is well known that the linear complexity of s^∞ is given by

$$L{=}p^n{-}\deg(\gcd(x^{p^n}{-}1{,}S(x))),$$

where $S(x)\ {=}s_0{+}s_1x{+}\cdots{+}s_{p^n-1}x^{p^n-1}$. [1]. Thus, the linear complexity of s^∞ can be given by

$$L{=}p^n{-}|\ \{i\ |\ S\left(\alpha_n^i\right),i{=}\ 0,1{,}\ldots{,}p^n{-}1\}|,$$

where α_n is a primitive p^n-th root of unity in an extension field of $\mathbb{F}_q$. So it's enough to find roots of $S(x)$ in the set $\left\{\alpha_n^i,\ i{=}\ 0,1{,}\ldots{,}p^n{-}1\right\}$, in other words, we need to investigate discrete Fourier transform of the sequence.

3 The linear complexity of sequences

Studying the linear complexity we will use the same method as in [2] considering changing field characteristic. By [2] the analysis of values $S\left(\alpha_n^i\right)$ differs for $i \in \mathbb{Z}_{p^n} \backslash p^{n-1}\mathbb{Z}_p$ and $i \in p^{n-1}\mathbb{Z}_p$. The last option is eqivalent to studying $S\left(\alpha_1^i\right)$ for $n=1$. In [2] it was shown that $S\left(\alpha_1^i\right)$ depends on $v=\gcd(\frac{p-1}{\mathrm{ord}_p(q)}, f)$, where $\mathrm{ord}_p(q)$ denotes the order of q modulo p. By [2] , if $v=f$, that is $2 \in D_0^{(p)}$, then $S\left(\alpha_1^i\right) \in \{0,1\}$, $i=1,\ldots,\ p-1$ and always exists $i:\ S\left(\alpha_1^i\right)=0$. But if $q>2$ then from the condition $q \in D_0^{(p)}$ we can not conclude $S\left(\alpha_1^i\right) \in \{0,1\}$, $v=1,\ldots,\ p-1$ as it is for $q=2$. Indeed, here $\left(S\left(\alpha_1^i\right)\right)^q = S\left(\alpha_1^{iq}\right) = S\left(\alpha_1^i\right)$ over $\mathbb{F}_q$. The results of the calculation of the linear complexity using the Berlekamp-Massey algorithm for $b=0$, $v=f$ $\left(q \in D_0^{(p)}\right)$ show that for $q \geq 2$ the order of $|\{i \mid S\left(\alpha_1^i\right), i=0,1,\ldots,p-1\}|$ not necessary equals $(p-1)/2$, unlike to [2]. So, for $q \geq 2$ the first part of Proposition 3 from [2] for $v=f$ is not true, and the order estimate of $|\{i \mid S\left(\alpha_1^i\right), i=0,1,\ldots,p-1\}|$, obtained in [2] for other cases also needs correction.

Lemma 1. *Let $p=ef+1$ be an odd prime with f being an even positive integer and let s^∞ be a generalized cyclotomic binary sequence of period p defined in (1). Then,* $|\{i \mid S\left(\alpha_1^i\right), i=0,1,\ldots,p-1\}| = r \cdot \mathrm{ord}_p(q)$, *where* $0 \leq r \leq \frac{p-1}{2\mathrm{ord}_p(q)}$ *and* $r=0$ *if* $v \mid \frac{f}{2}$, *or* $v=2$ *and* $f \neq v$.

Proof. The properties of polynomial of classical cyclotomic sequences are well known [1]. Suppose $S\left(\alpha_1^i\right)=0$ for some integer k. Then

$$0=\left(S\left(\alpha_1^i\right)\right)^q=S\left(\alpha_1^{iq}\right)=S\left(\alpha_1^{ig^u}\right),$$

and so on , where $q \in D_u^{(p)}$ for some integer u. Since

$$S\left(\alpha_1^i\right)+S\left(\alpha_1^{ig^{f/2}}\right)=-1$$

for $i=0,1,\ldots,p-1$, it follows that

$$L=p^n-r\mathrm{ord}_p(q),$$

where r is an integer with $0 \leq r \leq \frac{p-1}{2\mathrm{ord}_p(q)}$.

The statement of Lemma 1 for $v \mid \frac{f}{2}$, or $v=2$ and $f \neq v$ is proved in exactly the same way as in [2]. □

Remark 2. *We cannot replace the r estimate $0 \le r \le \frac{p-1}{2\mathrm{ord}_p(q)}$ with $0 \le r \le \frac{p-1}{q\mathrm{ord}_p(q)}$ as it was done in [2] for $q = 2$. For example, if q= 3, d= 8, then L= 216 for p= 433 and L= 384 for p= 769.*

Calculating of the linear complexity using the Berlekamp-Massey algorithm confirm the validity of Lemma 1.

Lemma 1 shows that the series of statements of Theorem 1 from [2] does not hold for $q \ge 2$. Moreover, to use the method from [2] in this case we need to introduce the new constraint on p : $p \equiv 1(\mathrm{mod}\ q)$. Under the above assumption the statement that $S\left(\alpha_n^i\right) \ne 0$ for $i \in \mathbb{Z}_{p^n} \backslash p^{n-1}\mathbb{Z}_p$ is obtained in the same way as in [2] for $q = 2$. And so we come to the following Theorem, which is our main result.

Theorem 3. *Let p=ef+1 be an odd prime, $p \equiv 1(\mathrm{mod}\ q)$ and $q^{p-1} \not\equiv 1(\mathrm{mod}\ p^2)$ and f being an even positive integer. Let s^∞ be a generalized cyclotomic binary sequence of period p^n defined in (1). Let $\mathrm{ord}_p(q)$ denote the order of q modulo p and v= $\gcd(\frac{p-1}{\mathrm{ord}_p(q)}, f)$. Then the linear complexity of s^∞ is given by*

$$L = p^n - r \cdot \mathrm{ord}_p(q), \qquad 0 \le r \le \tfrac{p-1}{2\mathrm{ord}_p(q)},$$

Furthermore,

$$L = p^n, \quad \text{if } v \text{ divides } \ f/2 \text{ or } v = 2\ , \ \ f \ne 2.$$

References

[1] Cusick T.W., Ding C., Renvall A. Stream Ciphers and Number Theory// North-Holland Mathematical Library. Elsevier, North-Holland. 2003.

[2] Edemskiy V., Li C., Zeng X., Helleseth T. The linear complexity of generalized cyclotomic binary sequences of period p^n. Designs, Codes and Cryptography. PP., 1-15. //DOI: 10.1007/s10623-018-0513-2

[3] Xiao Z., Zeng X., Li C., Helleseth T. New generalized cyclotomic binary sequences of period p^2. Des. Codes Cryptography 86(7) (2018) 1483-1497.

[4] Zeng X., Cai H., Tang X., Yang Y. Optimal frequency hopping sequences of odd length. IEEE Transactions on Information Theory 59 (5) (2013) 3237-3248.

[5] Ye Z., Ke P., Wu C. A further study of the linear complexity of new binary cyclotomic sequence of length p^n. AAECC (2018). https://doi.org/10.1007/s00200-018-0368-9

Post-optimal analysis for multicriteria integer linear programming problem of finding extremum solutions

Vladimir A. Emelichev
Belarusian State University, Faculty of Mechanics and Mathematics,
BLR-220030 Minsk, Belarus
vemelichev@gmail.com
Yury V. Nikulin
University of Turku, Department of Mathematics and Statistics,
FIN-20014 Turku, Finland
yurnik@utu.fi

Abstract

We consider a multicriteria problem of integer linear programming with a targeting set of optimal solutions given by the set of all individual criterion minimizers (extrema). In this work, the lower and upper attainable bounds on the stability radius of the set of extremum solutions are obtained in the situation where solution and criterion spaces are endowed with various Hölder's norms. In addition, a case of Boolean problem is analyzed. Some computational challenges are also discussed.

Keywords: sensitivity analysis; multiple criteria; combinatorial optimization; Pareto set; stability radius.

1 Introduction

Multiobjective discrete models have been widely applied in decision making, design, management, economics, and many other applied fields. Therefore, the interest of mathematicians to multicriteria (vector) discrete optimization problems is far from being lost, which is confirmed by numerous recent publications. One of the directions in investigating these problems is the analysis of stability of solutions to perturbations of the initial data (problem parameters). Various statements of the stability problem generate numerous investigation lines.

The terms sensitivity, stability or post-optimal analysis are generally used for the phase of an algorithm at which a solution (or solutions) of the problem has been already found, and additional calculations are performed in order to investigate how this solution depends on changes in the problem data. Recognition of the stability problem as one of the central in mathematical research goes back to Jacques Hadamard. In 1923, he postulated that in order to be well-posed a problem should have three properties: existence of a solution; uniqueness of the solution; continuous dependence of the solution on the data [1]. Correspondingly, ill-posed multicriteria discrete optimization problem refers to this situation that it may have multiple solutions or the feasible solution set and/or criteria functions depend on uncertain parameters.

Despite existence of numerous approaches to stability analysis of optimization problems, two major directions can be pointed out: quantitative and qualitative.

A qualitative sensitivity analysis is usually conducted for multicriteria optimization problems with various (linear and nonlinear) partial criteria. The main typical results in there are necessary and sufficient condition formulations for different types of stability of one or a set of optimal solutions in the problems considered (see e.g. [2–12]).

Within the framework of quantitative direction various measures of solution stability are investigated. Analytical expressions, or (attainable) lower and upper bounds, on a quantitative characteristic, called stability radius, usually constitute typical results of the area. The results are usually formulated for the some generalized optimality situation invariant to changes of problem parameters in the case where parameter space is equipped with various metrics (see e.g. [13–21]). In addition to stability radius, some papers are focusing on more general characteristics of stability, for example stability and accuracy functions are analyzed in [22, 23]. Sensitivity analysis is also done for some problem of scheduling theory, see e.g. [24, 25].

This paper belongs to the family of quantitative approaches. It continues a series of publications [10, 15–17, 26–29] seeking for analytical bounds on stability radius (different types of stability) for multicriteria problem of Integer Linear Programming (ILP) with various optimality principles.

In multicriteria optimization and decision making, we deal sometimes with choice functions distinct from the well-known Pareto optimality principle. Such functions have a specific merit in many real life applications (see e.g. [30–34]). In this paper, we consider the multicriteria problem of ILP with extremum optimality principle, i.e. with the set of all extremum solutions. We study the type of stability to independent perturbations of linear function coefficients that is a discrete analogue of Hausdorff upper semi-continuity mapping transforming any set of problem parameters into a set of extremum solutions. In other words, this type of stability guarantees the existence of a neighborhood in problem parameter space such that no new extremum solutions appear within. Following terminology used in [15–18], the property as described above is called stability. As a result of parametric analysis performed in this paper, the lower and upper bounds on the stability radius are obtained for multicriteria ILP problem with extremum solutions for the case where criterion space is endowed with various Hölder's norms. Attainability of the estimates (both lower and uppers bounds) is shown.

2 Problem formulation and basic definitions

We consider an m-criteria problem of ILP problem in the following formulation. Let $C = [c_{ij}] \in \mathbf{R}^{m\times n}$ be a real valued $m \times n$ - matrix with corresponding rows $C_i \in \mathbf{R}^n,\ i \in N_m = \{1, 2, \dots, m\},\ m \geq 1$. Let also $X \subset \mathbf{Z}^n,\ 1 < |X| < \infty$, be a set of feasible solutions (integer vectors) $x = (x_1, x_2, \dots, x_n)^T$, $n \geq 2$. We define a vector criterion

$$Cx = \big(C_1x, C_2x, \dots, C_mx\big)^T \to \min_{x\in X},$$

with partial criteria being linear functions.

In this paper, $Z^m(C)$, $C \in \mathbf{R}^{m\times n}$, is a problem of finding the set of extremum solutions defined in traditional way (see e.g. [31–33]):

$$E^m(C) = \Big\{x \in X :\ \exists k \in N_m\ \ \forall x' \in X\ \ \big(C_k(x) \leq C_k(x')\big)\Big\}.$$

The set of extremum solutions $E^m(C)$ can equivalently be written as follows:

$$E^m(C) = \{x \in X :\ \exists k \in N_m\ \ (E^m_k(x, C_k) = \emptyset)\},$$

where

$$E^m_i(x, C_i) = \Big\{x' \in X :\ C_i(x - x') > 0\Big\},\ i \in N_m,\ x \in X.$$

Thus, the choice of extremum solutions can be interpreted as finding best solutions for each of m criteria, and then combining them into one set. In other words, the set of extremum solutions contains all the individual minimizers of each objective. Obviously, $E^1(C),\ C \in \mathbf{R}^n$ is the set of optimal solutions for scalar problem $Z^1(C)$.

We will perturb the elements of matrix $C \in \mathbf{R}^{m\times n}$ by adding elements of the perturbing matrix $C' \in \mathbf{R}^{m\times n}$. Thus the perturbed problem $Z^m(C + C')$ of finding extremum solutions has the following form

$$(C + C')x \to \min_{x\in X}.$$

The set of extremum solutions of the perturbed problem is denoted by $E^m(C + C')$. In the solution space $\mathbf{R}^n$, we define an arbitrary Hölder's norm $l_p,\ p \in$

$[1,\infty]$, i.e. the norm of vector $a=(a_1,a_2,\ldots,a_n)^T\in\mathbf{R}^n$ is defined by the number

$$\|a\|_p=\begin{cases}\Big(\sum\limits_{j\in N_n}|a_j|^p\Big)^{1/p} & \text{if } 1\le p<\infty,\\[2ex] \max\{|a_j|:\ j\in N_n\} & \text{if } p=\infty.\end{cases}$$

In the criterion space $\mathbf{R}^m$, we define another Hölder's norm $l_q,\ q\in[1,\infty]$, The norm of matrix $C\in\mathbf{R}^{m\times n}$ is defined by the number

$$\|C\|_{pq}=\|(\|C_1\|_p,\|C_2\|_p,\ldots,\|C_m\|_p)\|_q.$$

It is also easy to see that

$$\|C_i\|_p\le\|C\|_{pq},\ i\in N_m. \tag{1}$$

It is well-known that l_p norm, defined in $\mathbf{R}^n$, induces conjugated l_{p^*} norm in $(\mathbf{R}^n)^*$. For p and p^*, the following relations hold

$$\frac{1}{p}+\frac{1}{p^*}=1,\qquad 1<p<\infty. \tag{2}$$

In addition, if $p=1$ then $p^*=\infty$. Obviously, if $p^*=1$ then $p=\infty$. Also notice that p and p^* belong to the same range $[1,\infty]$. We also set $\frac{1}{p}=0$ if $p=\infty$.

It is easy to see that for any vector $a=(a_1,a_2,...,a_n)^T\in\mathbf{R}^n$ with $|a_j|=\sigma$, $j\in N_n$ it holds

$$\|a\|_p=n^{\frac{1}{p}}\sigma \tag{3}$$

for any $p\in[1,\infty]$. For any two vectors a and b of the same dimension, the following Hölder's inequalities are well-known

$$|a^Tb|\le\|a\|_p\|b\|_{p^*}. \tag{4}$$

Using the well-known condition (see [35]) that transforms (4) into equality, the validity of the following statement becomes transparent

$$\forall b\in\mathbf{R}^n\quad\forall\sigma>0\quad\exists a\in\mathbf{R}^n\quad\Big(|a^Tb|=\sigma\|b\|_{p^*}\ \&\ \|a\|_p=\sigma\Big). \tag{5}$$

Given $\varepsilon>0$, let

$$\Omega_{pq}(\varepsilon)=\Big\{C'\in\mathbf{R}^{m\times n}:\ \ \|C'\|_{pq}<\varepsilon\Big\}$$

be the set of perturbing matrices C' with rows $C'_k\in\mathbf{R}^n,\ k\in N_m$, and $\|C'\|_{pq}$ is the norm of $C'=[c'_{ij}]\in\mathbf{R}^{m\times n}$.

Denote

$$\Xi_{pq} = \Big\{\varepsilon > 0 : \quad \forall C' \in \Omega_{pq}(\varepsilon) \quad \Big(E^m(C + C') \subseteq E^m(C)\Big)\Big\}.$$

Following [15–17, 26], the number

$$\rho^m(p,q) = \begin{cases} \sup\ \Xi_{pq} & \text{if } \ \Xi_{pq} \neq \emptyset, \\ 0 & \text{if } \ \Xi_{pq} = \emptyset \end{cases}$$

is called stability radius (T_3-stability radius in terminology [2, 4–7, 10]) of problem $Z^m(C)$, $m \in \mathbf{N}$, with Hölder's norms l_p and l_q in the spaces $\mathbf{R}^n$ and $\mathbf{R}^m$ respectively. Thus, the stability radius of problem $Z^m(C)$ defines the extreme level of independent perturbations of the elements of matrix C in the metric space $\mathbf{R}^{m\times n}$ such that no new extremum solutions appear in the perturbed problem. The problem $Z^m(C)$ is called stable if and only if the stability radius is strictly positive ($\rho^m(p,q) > 0$).

Obviously, if $E^m(C) = X$, the inclusion $E^m(C+C') \subseteq E^m(C)$ holds for any perturbing matrix $C' \in \Omega_{pq}(\varepsilon)$ for any number $\varepsilon > 0$. Therefore, the stability radius of such a problem is not bounded from the above. The problem $Z^m(C)$ with $E^m(C) \neq X$ is called *non-trivial.*

3 Bounds on stability radius

Given the multicriteria ILP problem $Z^m(C)$, $m \in \mathbf{N}$, for any $p \in [1,\infty]$ we set

$$\phi^m(p) = \min_{i\in N_m} \ \min_{x\notin E^m(C)} \ \max_{x'\in X\backslash\{x\}} \frac{C_i(x-x')}{\|x-x'\|_{p^*}},$$

$$\eta^m(p) = \min\{\|C_i\|_p : \ i \in N_m\}.$$

The notation $Z^m_B(C)$ is used to denote a problem $Z^m(C)$ with all Boolean variables, i.e. $X \subseteq \{0,1\}^n$.

Theorem 1. *Given $p, q \in [1,\infty]$ and $m \in \mathbf{N}$, for the stability radius $\rho^m(p,q)$ of non-trivial multicriteria ILP problem $Z^m(C)$, the following lower and upper bounds are valid*

$$0 < \phi^m(p) \leq \rho^m(p,q) \leq \eta^m(p).$$

Moreover,

$$0 < \phi^m(p) \leq \rho^m(p,q) \leq \min\left\{n^{\frac{1}{p}}\phi^m(\infty), \eta^m(p)\right\}$$

if $Z^m(C) = Z^m_B(C)$.

Proof. According to the definition of $E^m(C)$, we have

$$\forall x \notin E^m(C) \ \ \forall i \in N_m \ \ \exists x^0 \in X \ \ \Big(C_i x > C_i x^0 \Big),$$

and hence $\phi^m(p) > 0$. Now we prove that

$$\rho^m(p,q) \geq \phi^m(p). \tag{6}$$

Let $C' \in \mathbf{R}^{m\times n}$ be an arbitrary perturbing matrix with rows $C'_i \in \mathbf{R}^n$, $i \in N_m$, and norm

$$\|C'\|_{pq} = \|(\|C'_1\|_p, \|C'_2\|_p, \ldots, \|C'_m\|_p)\|_q < \phi^m(p),$$

i.e. $C' \in \Omega_{pq}(\phi^m(p))$. Then, according to the definition of number $\phi^m(p)$ and due to (1), the following statement holds

$$\forall i \in N_m \ \ \forall x \notin E^m(C) \ \ \exists x^0 \in X\backslash\{x\}$$

$$\Big(\frac{C_i(x-x^0)}{\|x-x^0\|_{p^*}} \geq \phi^m(p) > \|C'\|_{pq} \geq \|C'_i\|_p \Big).$$

Taking into account Hölder's inequalities (4), we deduce that for any index $i \in N_m$ there exists $x^0 \neq x$ such that

$$(C_i + C'_i)(x - x^0) = C_i(x-x^0) + C'_i(x-x^0) \geq$$

$$C_i(x-x^0) - \|C'_i\|_p \|x-x^0\|_{p^*} > 0,$$

i.e. $x \notin E^m(C + C')$ for $x \notin E^m(C)$.

Thus, any non-extremum solution of $Z^m(C)$ remains being non-extremum in the perturbed problem $Z^m(C + C')$, and hence the inclusion $E^m(C + C') \subseteq E^m(C)$ holds for any perturbed matrix $C' \in \Omega_{pq}(\phi^m(p))$. So, equation (6), is true.

Further we prove that $\rho^m(p,q) \leq \eta^m(p)$. In order to do that it suffices to show $\rho^m(p,q) \leq \|C_k\|_p$ for any $k \in N_m$. Let fix $k \in N_m$ and let matrix $C^0 = [c_{ij}] \in \mathbf{R}^{m\times n}$ with rows $C^0_i \in \mathbf{R}^n$, $i \in N_m$ be constructed as follows

$$C^0_i = \begin{cases} -C_i & \text{if } i = k, \\ \mathbf{0}^T & \text{if } i \in N_m\backslash\{k\}, \end{cases}$$

where $\mathbf{0}$ is a vector column in $\mathbf{R}^n$ containing all zeroes. Then we get

$$\|C^0\|_{pq} = \|C^0_k\|_p = \|C_k\|_p,$$

$$E^m(C + C^0) = X.$$

Taking into account $X \not\subseteq E^m(C)$ we conclude $\rho^m(p,q) \leq \|C_k\|_p$. Hence $\rho^m(p,q) \leq \eta^m(p) = \min\{\|C_i\|_p : \ i \in N_m\}$.

Further we consider non-trivial m-criteria linear Boolean problem $Z_B^m(C)$, $C \in \mathbf{R}^{m\times n}$, $m \geq 1$, $X \subseteq \mathbf{E}^n = \{0,1\}^n$. All the bounds proven earlier remain valid. All we need is to show that an extra upper bound holds

$$\rho^m(p,q) \leq n^{\frac{1}{p}} \phi^m(\infty). \tag{7}$$

Indeed, according to the definition of $\phi = \phi^m(\infty)$, there exist a solution $x^0 = (x_1^0, x_2^0, ..., x_n^0)^T \notin E^m(C)$ and an index $k \in N_m$ such that for any solution $x \neq x^0$ the following inequality holds

$$\phi\|x - x^0\|_1 \geq C_k(x^0 - x). \tag{8}$$

Setting $\varepsilon > n^{\frac{1}{p}}\phi$ and choosing (fixing) δ such that

$$\phi < \delta < \frac{\varepsilon}{n^{\frac{1}{p}}},$$

we consider a row vector $\xi = (\xi_1, \xi_2, ..., \xi_n)$ with coordinates

$$\xi_j = \begin{cases} -\delta & \text{if } x_j^0 = 1, \\ \delta & \text{if } x_j^0 = 0. \end{cases}$$

Then according to (3), we get

$$\|\xi\|_p = n^{\frac{1}{p}}\delta$$

Further we define a perturbing matrix $C^0 = [c_{ij}] \in \mathbf{R}^{m\times n}$ with rows $C_i^0 \in \mathbf{R}^n$, $i \in N_m$ constructed as follows

$$C_i^0 = \begin{cases} \xi & \text{if } i = k, \\ \mathbf{0}^T & \text{if } i \in N_m \backslash \{k\}, \end{cases}$$

where $\mathbf{0}$ is a vector column in $\mathbf{R}^n$ containing all zeroes. Then we have

$$\|C^0\|_{pq} = n^{\frac{1}{p}}\phi,$$

$$C^0 \in \Omega_{pq}(\varepsilon).$$

In addition, for any $x \neq x^0$ we have

$$C_k^0(x^0 - x) = -\delta\|x^0 - x\|_1$$

From the above using inequality (8) we deduce for any $x \in X\backslash\{x^0\}$

$$(C_k + C_k^0)(x^0 - x) = C_k(x^0 - x) + C_k^0(x^0 - x) \leq (\phi - \delta)\|x^0 - x\|_1 < 0.$$

This implies that $x^0 \in E^m(C + C^0)$ for $x^0 \notin E^m(C)$. Summarizing, we have

$$\forall \varepsilon > n^{\frac{1}{p}}\phi^m(\infty) \ \ \exists C^0 \in \Omega_{pq}(\varepsilon) \ \ \Big(E^m(C + C^0) \nsubseteq E^m(C)\Big),$$

i.e. $\rho^m(p,q) < \varepsilon$ for any number $\varepsilon > n^{\frac{1}{p}}\phi^m(\infty)$. Therefore, therefore for the stability radius of $Z_B^m(C)$ we get that inequality (7) is true, i.e. Theorem 1 is now proven. □

4 Bounds attainability

The following corollaries indicate the lower bound attainability $\phi^m(p)$ for the stability radius $\rho^m(p,q)$ of non-trivial ILP problem $Z^m(C)$.

Corollary 1. *Let $m \in \mathbf{N}$. Given a non-trivial multicriteria ILP problem $Z^m(C)$ has a unique extremum solution $x^0 \in E^m(C)$, the stability radius $\rho^m(p,q)$ is expressed by the following formula*

$$\rho^m(p,q) = \min_{i \in N_m} \max_{x \in X\backslash\{x^0\}} \frac{C_i(x - x^0)}{\|x - x^0\|_{p^*}}. \tag{9}$$

Proof. Let Θ denote the right-hand side of (9). Assume $E^m(C) = \{x^0\}$. According to the definition of Θ, there exist $\hat{x} \in X\backslash\{x^0\}$ and $k \in N_m$ such that the following equality holds

$$C_k(\hat{x} - x^0) = \Theta\|\hat{x} - x^0\|_{p^*}. \tag{10}$$

Notice that here $\Theta > 0$.Setting $\varepsilon > \Theta$, we fix a number γ satisfying

$$\Theta < \gamma < \varepsilon.$$

According to formula (5), there exists a vector $a \in \mathbf{R}^n$ such that

$$a^T(\hat{x} - x^0) = -\gamma\|\hat{x} - x^0\|_{p^*},$$

$$\|a\|_p = \gamma.$$

Further we define a perturbing matrix $C^0 = [c_{ij}] \in \mathbf{R}^{m \times n}$ with rows $C_i^0 \in \mathbf{R}^n$, $i \in N_m$ constructed as follows

$$C_i^0 = \begin{cases} a^T & \text{if } i = k, \\ \mathbf{0}^T & \text{if } i \in N_m\backslash\{k\}, \end{cases}$$

where $\mathbf{0}$ is a vector column in $\mathbf{R}^n$ containing all zeroes. Then we have

$$\|C^0\|_{pq} = \gamma,$$

$$C^0 \in \Omega_{pq}(\varepsilon),$$

$$C^0_k(\hat{x} - x^0) = -\gamma\|\hat{x} - x^0\|_{p^*}$$

From the above using inequality (10) we deduce

$$(C_k + C^0_k)(\hat{x} - x^0) = C_k(\hat{x} - x^0) - \gamma\|\hat{x} - x^0)\|_{p^*} = (\Theta - \gamma)\|\hat{x} - x^0\|_{p^*} < 0.$$

This implies that $x^0 \notin E^m_k(\hat{x}, C_k + C^0_k)$. If $E^m_k(\hat{x}, C_k + C^0_k) = \emptyset$, then $\hat{x} \in E^m(C + C^0)$. If $E^m_k(\hat{x}, C_k + C^0_k) \neq \emptyset$, then there exists $\tilde{x} \in E^m_k(\hat{x}, C_k + C^0_k)$ such that $\tilde{x} \in E^m(C + C^0)$ and $\tilde{x} \neq x^0$.

Summarizing, we have that for any $\varepsilon > \Theta$ the exists a perturbing matrix $C^0 \in \Omega_{pq}(\varepsilon)$ such that we can specify $x' \in X\backslash\{x^0\}$ with the condition $x' \in E^m(C + C^0)$. This implies that $E^m(C + C^0) \not\subseteq E^m(C)$. Hence $\rho^m(p, q) < \varepsilon$ for any number $\varepsilon > \Theta$, i.e. $\rho^m(p, q) \leq \Theta$.

Therefore, taking into account the lower bound $\rho^m(p, q) \geq \Theta$ (earlier proven in Theorem 1) for the stability radius of $Z^m(C)$ we get formula (9), i.e. Corollary 1 is now proven. □

In the case of Boolean non-trivial problem $Z^m_B(C)$, the next corollary follows from Theorem 1 and indicates the lower bound attainability for the stability radius $\rho^m(\infty, q)$.

Corollary 2. *Given $m \in \mathbf{N}$ and $q \in [1, \infty)$, the stability radius $\rho^m(\infty, q)$ of a non-trivial multicriteria Boolean problem $Z^m_B(C)$ is expressed by the following formula*

$$\rho^m(\infty, q) = \phi^m(\infty) = \min_{i \in N_m} \min_{x \notin E^m(C)} \max_{x' \in X\backslash\{x\}} \frac{C_i(x - x')}{\|x - x'\|_1} \tag{11}$$

Further we show that for any number $p \in [1, \infty]$, the upper bound $n^{\frac{1}{p}}\phi^m(\infty)$ for the stability radius of Boolean problem $Z^m_B(C)$ is attainable for $m = 1$.

Theorem 2. *Given $p, q \in [1, \infty]$, there exists a class of scalar Boolean problems $Z^m_B(C)$, $C \in \mathbf{R}^n$ such that the stability radius $\rho^m(p, q)$ (of any such problem belonging to the class) is expressed by the following formula*

$$\rho^1(p, q) = n^{\frac{1}{p}}\phi^1(\infty). \tag{12}$$

Proof. Due to Theorem 1, in order to prove (12) it suffices to find a class of problems satisfying $\rho^1(p,q) \geq n^{\frac{1}{p}}\phi^1(\infty)$. Let $X = \{x^*, x^1, ..., x^n\} \in \mathbf{E}^n$, where $x^* = (0,0,...,0)^T \in \mathbf{R}^n$, $x^i = e^j$, $j \in N_n$. Here e^j is the j-th column of the $n \times n$ basis matrix (basic column vector). We set $C = (-a, -a, ..., -a) \in \mathbf{R}^n$, $a > 0$. Then

$$E^1(C) = X \backslash \{x^*\},$$

$$\phi^1(\infty) = a.$$

Let $C' = (c'_1, c'_2, ..., c'_n)$ be an arbitrary perturbing row vector belonging to $\Omega_{pq}(n^{\frac{1}{p}}a)$, i.e. $\|C'\|_{pq} < n^{\frac{1}{p}}a$. Proving by contradiction, it is easy to see that there exists at least on index $k \in N_m$ such that $|c'_k| < a$. Therefore, we get

$$(C + C')(x^* - x^k) = a - c'_k > 0,$$

i.e. $x^* \notin E^1(C + C')$ for any perturbing row $C' \in \Omega_{pq}(n^{\frac{1}{p}}\phi^1(\infty))$. Hence, due to $x^* \notin E^1(C)$, we get $\rho^1(p,q) \geq n^{\frac{1}{p}}\phi^1(\infty)$. Theorem 2 is now proven. □

The next numerical example shows that the upper bound for the stability radius of non-trivial Boolean problem $Z^m_B(C)$ can also be attainable in single criterion situation (when $m = 1$).

Example 1. *Let* $X = \{x^0, x^1\} \subset \mathbf{E}^n$ *where* $x^0 = (0,0,...,0)^T$, $x^1 = (1,1,...,1)^T$, *and* $C = (1,1,...,1)$. *Then we have*

$$Cx^0 = 0, \ Cx^1 = n,$$

$$E^1(C) = \{x^0\}, \ X \backslash E^1(C) = \{x^1\},$$

$$\rho^1(p,q) \leq \|C\|_p.$$

Moreover, taking into account (2) and (3), we obtain the equalities

$$\phi^1(p) = n^{\frac{1}{p}} = \|C\|_p.$$

Then according to Theorem 1,

$$\rho^1(p,q) = \|C\|_p, \ p,q \in [1,\infty].$$

In addition, we notice that

$$\phi^1(p) = \|C\|_p = n^{\frac{1}{p}}\phi^1(\infty),$$

i.e. all the three bounds are attainable in scalar case $m = 1$.

In order to emphasize the specific of stability radius $\rho^m(p.q)$ for the set of extremum solutions $E^m(C)$, we compare the results formulated in Theorem 1 with some earlier published results regarding the stability radius for the well-known Pareto set $P^m(C)$. We define the Pareto set as follows (see e.g. [36–40]):

$$P^m(C) = \Big\{ x \in X : \ P^m(x, C) = \emptyset \Big\},$$

where

$$P^m(x, C) = \Big\{ x' \in X : \ Cx \geq Cx' \ \& \ Cx \neq Cx' \Big\}.$$

Theorem 3. *[19] Given $p, q \in [1, \infty]$ and $m \in \mathbf{N}$, for the stability radius $\rho^m(p, q)$ of non-trivial multicriteria ILP problem $Z^m(C)$ of finding the Pareto set $P^m(C)$, the following lower and upper bounds are valid*

$$\min_{x \notin P^m(C)} \ \max_{x' \in P^m(x,C)} \ \min_{i \in N_m} \frac{C_i(x - x')}{\|x - x'\|_{p^*}} \leq \rho^m(p, q) \leq \min\{\|C_i\|_p : \ i \in N_m\}.$$

We also define the Slater set $Sl^m(C)$, $P^m(C) \subseteq Sl^m(C)$, as follows [41]:

$$Sl^m(C) = \Big\{ x \in X : \ \nexists \ x^0 \in X \ \ \forall k \in N_m \ \ \Big(C_k x > C_k x^0 \Big) \Big\}.$$

In addition to Theorem 3 the following result holds.

Theorem 4. *[2], [4] The non-trivial problem $Z^m(C)$ of finding the Pareto set $P^m(C)$ is stable, i.e. $\rho^m(p.q) > 0$, if and only if*

$$P^m(C) = Sl^m(C).$$

Finally, we give here one more result regarding lower and upper bounds of the stability radius $\rho^m(p, q)$ for Boolean problem $Z^m_B(C)$ of finding the Pareto set $P^m(C)$.

Theorem 5. *[42] Given $p, q \in [1, \infty]$ and $m \in \mathbf{N}$, for the stability radius $\rho^m(p, q)$ of non-trivial multicriteria Boolean problem $Z^m_B(C)$ of finding the Pareto set $P^m(C)$, the following lower and upper bounds are valid*

$$\xi^m(p) \leq \rho^m(p, q) \leq n^{\frac{1}{p}} m^{\frac{1}{q}} \xi^m(\infty),$$

where

$$\xi^m(p) = \min_{x \notin P^m(C)} \ \max_{x' \in P^m(x,C)} \ \min_{i \in N_m} \frac{C_i(x - x')}{\|x - x'\|_{p^*}}.$$

5 Conclusion

In this paper, the lower and upper attainable bounds on the stability radius of the set of extremum solutions were obtained in the situation where solution and criterion spaces are endowed with various Hölder's norms. As corollaries, analytical formulae for the stability radius are specified in the case of models with Boolean set of feasible solutions.

One of the biggest challenges in this area is to construct efficient algorithms to calculate the analytical expressions. To the best of our knowledge there are not so many results known in that area, and moreover some of those results which have been already known, put more questions than answers. As it was pointed out in [43], calculating exact values is an extremely difficult task in general, so one could concentrates either on finding easy computable classes of problems or developing general metaheuristic approaches.

Estimations of stability radius obtained in this paper is based on enumeration the set of feasible solutions whose cardinality may grow exponentially with n. In the case of a single objective function, an approach to calculating the stability radius of an ε-optimal solution to the linear problem of $0-1$ programming in polynomial time was given in [44]. They assumed that the objective function is minimized, the feasible solution set is fixed and a given subset of the objective function coefficients is perturbed. The approach requires that the original single objective optimization problem is polynomially solvable e, for example it can be one of the well-known graph theory problems, such as minimum spanning tree or shortest path problems. Another approach, based on k-best solutions, was proposed in [45] for NP-hard problems such as traveling salesman problem. In [18], it was shown how analytical formulae similar to (9) can be transformed into polynomial type calculation procedure in the case of Boolean variables, Chebyshev norm and polynomial solvability of $Z^1_P(C)$. However, for multicriteria case the question of existing polynomial time procedures remains to be open. As it is well-known that the presence of multiple criteria increases the level of complexity, for example, polynomially solvable single objective problems become intractable even in bicriteria case, see e.g. [40], the finding of polynomial methods seems to be unlikely in general. For some particular challenging combinatorial problems, it was proven that the problem of finding the radii of every type of stability is intractable unless $P = NP$ [46]. An application of inverse optimization results in logarithmic number of mixed integer programs for multi-objective combinatorial problems, where each objective function is a maximum sum and the coefficients are restricted to natural numbers [47].

References

[1] HADAMARD, J. (1923) *Lectures on Cauchys problem in linear partial differential equations*, Yale University Press, Yale.

[2] SERGIENKO, I. and SHILO, I. (2003) *Discrete Optimization Problems. Problems, Methods, Research*, Naukova dumka, Kiev.

[3] BELOUSOV, E. and ANDRONOV, V. (1993) *Solvability and Stability for Problems of Polynomial Programming*, Moscow University Publisher, Moscow.

[4] SERGIENKO, I., KOZERATSKAYA, L. and LEBEDEVA, T. (1995) *Stability and Parametric Analysis of Discrete Optimization Problems*, Naukova dumka, Kiev.

[5] LEBEDEVA, T., SEMENOVA, N. and SERGIENKO, T. (2005) Stability of vector problems of integer optimization: relationship with the stability of sets of optimal and nonoptimal solutions. *Cybernetics and Systems Analysis*, **41** (4), 551–558.

[6] LEBEDEVA, T. and SERGIENKO, T. (2006) Stability of a vector integer quadratic programming problem with respect to vector criterion and constraints. *Cybernetics and Systems Analysis*, **42** (5), 667–674.

[7] LEBEDEVA, T. and SERGIENKO, T. (2008) Different types of stability of vector integer optimization problem: general approach. *Cybernetics and Systems Analysis*, **44** (3), 429–433.

[8] LEBEDEVA, T, SEMENOVA, N. and SERGIENKO, T. (2014) Qualitative characteristics of the stability of vector discrete optimization problems with different optimality principles. *Cybernetics and Systems Analysis*, **50** (2), 228–233.

[9] LEBEDEVA, T., SEMENOVA, N. and SERGIENKO, T. (2014) Properties of perturbed cones ordering the set of feasible solutions of vector optimization problem. *Cybernetics and Systems Analysis*, **50** (5), 712–717.

[10] EMELICHEV, V., KOTOV, V., KUZMIN, K., LEBEDEVA, T., SEMENOVA, N. and SERGIENKO, T. (2014) Stability and effective algorithms for solving multiobjective discrete optimization problems with incomplete information. *Journal of Automation and Information Sciences*, **46** (2), 27–41.

[11] KUZMIN, K., NIKULIN, Y. and MÄKELÄ, M. (2017) On necessary and sufficient conditions of stability and quasistability in combinatorial multicriteria optimization. *Control and Cybernetics*, **46** (4), 361–382.

[12] EMELICHEV, V, KARELKINA, O. and KUZMIN, K. (2012) Qualitative stability analysis of combinatorial minmin problems *Control and Cybernetics*, **41** (1), 57–79.

[13] LEONTEV, V. (2007) Discrete Optimization. *Journal of Computatonal Physics and Mathematics*, **47** (2), 328–340.

[14] GORDEEV, E. (2015) Comparison of three approaches to studying stability of solutions to problems of discrete optimization and computational geometry. *Journal of Applied and Industrial Mathematics*, **9** (3), 358–366.

[15] EMELICHEV, V. and PODKOPAEV, D. (1998) On a quantitative measure of stability for a vector problem in integer programming. *Journal of Computatonal Physics and Mathematics*, **38** (11), 1727–1731.

[16] EMELICHEV, V. and PODKOPAEV, D. (2001) Stability and regularization of vector problems of integer linear programming. *Diskretnyi Analiz i Issledovanie Operatsii. Ser. 2*, **8** (1), 47–69.

[17] EMELICHEV, V., GIRLICH, E., NIKULIN, Y. and PODKOPAEV, D. (2002) Stability and regularization of vector problems of integer linear programming. *Optimization*, **51** (4), 645–676.

[18] EMELICHEV, V. and PODKOPAEV, D. (2010) Quantitative stability analysis for vector problems of 0-1 programming. *Discrete Optimization*, **7** (1-2), 48–63.

[19] EMELICHEV, V. and KUZMIN, K. (2010) Stability radius of a vector integer linear programming problem: case of a regular norm in the space of criteria. *Cybernetics and Systems Analysis*, **46** (1), 72–79.

[20] BUKHTOYAROV, S. and EMELICHEV, V. (2015) On the stability measure of solutions to a vector version of an investment problem. *Journal of Applied and Industrial Mathematics*, **9** (3), 328–334.

[21] EMELICHEV, V. a nd NIKULIN, Y. (2018) Aspects of stability for multicriteria quadratic problems of Boolean programming, *Bul. Acad. Stiinte Repub. Mold. Mat.*, **87** (2), 30 – 40.

[22] LIBURA, M. and NIKULIN, Y. (2006) Stability and accuracy functions in multicriteria linear combinatorial optimization problem. *Annals of Operations Research*, **147** (1), 255–267.

[23] NIKULIN, Y. (2009) Stability and accuracy functions in a coalition game with bans, linear payoffs and antagonistic strategies. *Annals of Operations Research*, **172**, 25–35, 2009.

[24] SOTSKOV, Y., SOTSKOVA, N., LAI, T. and WERNER, F. (2010) *Scheduling under Uncertainty, Theory and Algorithms*, Belaruskaya nauka, Minsk.

[25] NIKULIN, Y. (2014) Accuracy and stability functions for a problem of minimization a linear form on a set of substitutions, Chapter in Sequencing and Scheduling with Inaccurate Data, Editors Yuri Sotskov and Frank Werner. Nova Science Pub Inc.

[26] EMELICHEV, V. and PLATONOV, A. (2008) Measure of quasistability of a vector integer linear programming with generalized principle of optimality in the Hölder metric. *Buletine of Academy of Sciences of Moldova. Mathematics*, **57** (2), 58–67.

[27] EMELICHEV, V. and KUZMIN, K. (2013) A general approach to studying the stability of a Pareto optimal solution of a vector integer linear programming problem. *Discrete Mathematics and Applications*, **17** (4): 349–354.

[28] EMELICHEV, V. and KUZMIN, K. (2007) On a type of stability of a multicriteria integer linear programming problem in the case of monotonic norm. *Journal of Computers and Systems Sciences International*, **46** (5), 714–720.

[29] EMELICHEV, V, KRICHKO, V. and NIKULIN, Y. (2004) The stability radius of an efficient solution in minimax Boolean programming problem *Control and Cybernetics*, **33** (1), 127–132.

[30] PODINOVSKII, V. and NOGHIN, V. (1982) *Pareto-Optimal Solutions of Multicriteria Problems*, Fizmatlit, Moscow.

[31] SHOLOMOV, L. (1989) *Logical Methods for Investigation of the Discrete Choice Models*, Nauka, Moscow.

[32] YUDIN, D. (1989) *Computational Methods in Decision Making*, Nauka, Moscow.

[33] AIZERMAN, M. and ALEKSEROV, F. (1990) *Choice of Alternatives: Theoretical Foundations*, Nauka, Moscow.

[34] LOTOV, A. and POSPELOV, I. (2008) *Multicriteria Decision Making Problems*, Fizmatlit, Moscow.

[35] HARDY, G., LITTLEWOOD, J. and POLYA, G. (1988) *Inequalities.* Cambridge University Press, Cambridge.

[36] PARETO, V. (1909) *Manuel D'ecoonomie Politique*, Qiard, Paris.

[37] STEUER, R. (1986) *Multiple Criteria Optimization: Theory, Computation and Application*, John Wiley&Sons, New York.

[38] MIETTINEN, K. (1999) *Nonlinear Multiobjective Optimization.* Kluwer Academic Publishers, Boston.

[39] NOGHIN, V. (2018) *Reduction of the Pareto Set: An Axiomatic Approach* (Studies in Systems, Decision and Control), Springer, Cham.

[40] EHRGOTT, M. (2005) *Multicriteria Optimization.* Springer, Birkhäuser.

[41] SLATER, M. (1950) Lagrange Multipliers Revisited. *Cowles Commission Discussion Paper 80. Mathematics*; Reprinted in Giorgi, G. & Kjeldsen, T., eds. *Traces and Emergence of Nonlinear Programming.* Basel, Birkhäuser, 293–306, 2014.

[42] EMELICHEV, V., KUZMIN, K. and MYCHKOV, V. (2015) Estimates of stability radius of multicriteria Boolean problem with Holder metrics in parameter spaces *Bul. Acad. Stiinte Repub. Mold. Mat*, **78** (2), 74–81.

[43] NIKULIN, Y., KARELKINA, O. and MÄKELÄ, M. (2013) On accuracy, robustness and tolerances in vector Boolean optimization. *European Journal of Operational Research*, **224**, 449–457.

[44] CHAKAVARTI, N. and WAGELMANS, A. (1999) Calculation of stability radius for combinatorial optimization problems. *Oper. Res. Lett.*, **23**, 1–7.

[45] LIBURA M, VAN DER POORT ES, SIERKSMA G, VAN DER VEEN JAA. Stability aspects of the traveling salesman problem based on k-best solutions. Discrete Applied Mathematics 1998; 87:159–185.

[46] KUZMIN, K. (2015) A general approach to the calculation of stability radii for the max-cut problem with multiple criteria. *Journal of Applied and Industrial Mathematics*, **9** (4), 527–539.

[47] ROLAND, J., SMET, Y. and FIGUEIRA, J. (2012) On the calculation of stability radius for multi-objective combinatorial optimization problems by inverse optimization. *4OR-Q. J. Oper. Res.*, **10**, 379–389.

The Conjugacy Problem is Undecidable for Two-Dimensional Reversible Cellular Automata

Joonatan Jalonen[1], **Jarkko Kari**[2]

University of Turku

The *conjugacy problem* for a group G with a given presentation asks whether it is decidable if for given $g_1, g_2 \in G$ there exists $h \in G$ such that $g_1 h = h g_2$, i.e. whether g_1 and g_2 are conjugate. In this talk we will show that the conjugacy problem is undecidable for two-dimensional reversible cellular automata. This talk is based on [1] which is an extended version of [2].

Let A be a finite set and denote $A^{\mathbb{Z}^2}$ the set of maps $\mathbb{Z}^2 \to A$, which can be considered as colorings of the two-dimensional integer lattice. For $c \in A^{\mathbb{Z}^2}$ we denote $c(\vec{n}) = c_{\vec{n}}$ for any $\vec{n} \in \mathbb{Z}^2$. For a subset $D \subseteq \mathbb{Z}^2$ we denote c_D the restriction of c to D. For every $\vec{n} \in \mathbb{Z}^2$ we define an *$\vec{n}$-shift map* $\sigma_{\vec{n}} : A^{\mathbb{Z}^2} \to A^{\mathbb{Z}^2}$ by $\sigma_{\vec{n}}(c)_{\vec{i}} = c_{\vec{i}+\vec{n}}$ for every $\vec{i} \in \mathbb{Z}^2$. We can now give the definition of cellular automata.

Definition. Let $D \subset \mathbb{Z}^2$ be a finite subset. A map $F_{loc} : A^D \to A$ defines a *cellular automaton* $F : A^{\mathbb{Z}^2} \to A^{\mathbb{Z}^2}$ by $F(c)_{\vec{n}} = F_{loc}(\sigma_{\vec{n}}(c)_D)$.

The above definition is natural from an algorithmic perspective, but since our proof is partially topological we also give the topological definition: Define a metric $d : A^{\mathbb{Z}^2} \to \mathbb{R}$ by $d(c, e) = 2^{-\min\{\|\vec{n}\| | c_{\vec{n}} \neq e_{\vec{n}}\}}$ (where for $\vec{n} = (n_1, n_2)$, $\|\vec{n}\| = |n_1| + |n_2|$) for all $c, e \in A^{\mathbb{Z}^2}$ which are different, and of course $d(c, c) = 0$. This turns $A^{\mathbb{Z}^2}$ into a compact metric space. Due to the Curtis-Hedlund-Lyndon Theorem the following definition is equivalent to the one given above.

Definition. A map $F : A^{\mathbb{Z}^2} \to A^{\mathbb{Z}^2}$ is a *cellular automaton* if 1) it is continuous (w.r.t. the metric d defined above) and 2) it commutes with the shift maps, i.e. for all $\vec{n} \in \mathbb{Z}^2$ it we have that $F\sigma_{\vec{n}} = \sigma_{\vec{n}} F$.

A cellular automaton F is *reversible* if there exists another cellular automaton F' such that $FF' = F'F = \text{id}$, where $\text{id} : A^{\mathbb{Z}^2} \to A^{\mathbb{Z}^2}$ is defined by $\text{id}(c) = c$ (which is clearly a cellular automaton). The set of reversible cellular automata over $A^{\mathbb{Z}^2}$ forms a group (function composition as the product) and we can ask if the conjugacy problem is decidable for it. It turns out not to be:

Theorem. *There is an alphabet A such that the conjugacy problem for reversible cellular automata over $A^{\mathbb{Z}^2}$ is undecidable.*

[1] Author's research supported by the Finnish Cultural Foundation

[2] Author's research supported by the Academy of Finland Grant 296018

We will next outline the proof which relies on [3] and [4].

Let $D \subset \mathbb{Z}^2$ be a finite subset and let $V \subset A^D$ be some set of *patterns*; we will consider the patterns in V to be *valid* and the patterns in $A^D \setminus V$ to be *invalid*. Next we modify the letters of A so that we have a *directed alphabet*, this means nothing more than that to every letter we attach a unique direction vector from $\{(0, \pm 1), (\pm 1, 0)\}$. Now every configuration $c \in A^{\mathbb{Z}^2}$ has paths defined by following these direction vectors. These paths are either forward infinite or eventually periodic. A path $\vec{p}_1, \vec{p}_2, \ldots, \vec{p}_k \in \mathbb{Z}^2$ in $c \in A^{\mathbb{Z}^2}$ is called a *valid path* if the pattern in every position along the path is valid, i.e. if for all $i \in \{1, 2, \ldots, k\}$ it holds that $\sigma_{\vec{p}_i}(c)_D \in V$. In what follows we always assume that A and V are chosen so that valid paths have no cycles and are deterministic also backwards.

Let $I(V, A, c) \in \mathbb{N} \cup \{\infty\}$ denote the number of disjoint forward infinite valid paths in c and denote $I(V, A) = \sup_{c \in A^{\mathbb{Z}^2}} I(V, A, c)$. Combining results from [3] and [4] yields the following.

Theorem. *The following decision problem is undecidable:*

Instance: *A directed alphabet A and a set of valid patterns V such that $I(V, A) < \infty$.*

Question: *Is $I(V, A) = 0$?*

Now the idea of the proof is to reduce the above problem to the conjugacy problem.

Suppose A and V are such that $I(V, A) < \infty$. We will construct two cellular automata F_1 and F_2 which will be conjugate if $I(V, A) = 0$ and not conjugate if $I(V, A) > 0$. We will add a new layer on top of $A^{\mathbb{Z}^2}$ and both F_1 and F_2 will leave $A^{\mathbb{Z}^2}$-layer untouched. On the new layer we will simulate one-dimensional cellular automata on the valid paths. Essentially we want F_1 to simulate the one-dimensional shift map σ which is defined by $\sigma(c)_i = c_{i+1}$ on the two-way infinite valid paths and F_2 to simulate σ^2. In order for these to be reversible also over one-way infinite and finite valid paths, we add another tape on which we move the letters to the opposite direction. Overall the layer we add on top of $A^{\mathbb{Z}^2}$ is $(\{0,1\}^4)^{\mathbb{Z}^2}$, but this should be considered as a two-track tape going back and forth.

On the invalid paths F_1 does nothing. On the two-way infinite valid paths F_1 is defined by the cellular automaton $\sigma \times \sigma^{-1} : (\{0,1\}^2 \times \{0,1\}^2)^{\mathbb{Z}} \to (\{0,1\}^2 \times \{0,1\}^2)^{\mathbb{Z}}$, $(\sigma \times \sigma^{-1})(d, e)_i = (d_{i+1}, e_{i-1})$ for all $d, e \in (\{0,1\}^2)^{\mathbb{Z}}$. If the path is not two-way infinite, in other words it has an end or a beginning (or both, in which case it is finite), F_1 is defined as for the two-way infinite paths but in the end and/or the beginning of the path the two tapes are glued together. In other words, in the beginning of a valid path F_1 transfers the content of the first tape to the second tape and in the end of a valid path F_1 transfers the content from the second tape to the first one.

The cellular automaton F_2 is very similar to F_1 but instead of shifting the tape contents one step at a time, it shifts them two steps. So it is simulating the cellular automaton $\sigma^2 \times \sigma^{-2}$ on two-way infinite paths. The second difference is how F_2 handles the ends of valid paths (the beginnings of valid paths are handled exactly as for F_1, i.e. we just glue the tapes together). For F_2 we do not just glue the tapes together in the end of a valid path, but we also flip the tape. In other words when a letter (a, b) (which is a tuple as our tapes have two tracks) moves in the end of a valid path from second tape to the first one it is simultaneously flipped and becomes the letter (b, a).

Consider the case that $I(V, A) = 0$. Then by compactness there is a global bound on the length of valid paths. Now all tapes have finite even length (finite since the paths are finite and even since when the ends are glued together we get a tape which goes twice the length of the valid path) we can define a permutation ϕ of even length words over $\{0, 1\}^2$ such that "$\phi F_1 = F_2\phi$". Further on, this ϕ can be defined by a local rule, as we just noticed that there is a global bound on the lengths of the valid paths, so we can take large enough neighborhood to see the entire valid path that a given cell is part of. This shows that F_1 and F_2 are conjugate.

Next suppose that $0 < I(V, A) < \infty$. Now according to [4] both F_1 and F_2 have finite entropies and these entropies are directly tied to the cellular automata which they define on infinite paths. Since F_1 defines the shift and F_2 defines the double-shift, it follows that F_2 has larger entropy. In particular we have that F_1 and F_2 cannot be conjugate as entropy is a conjugacy invariant.

We are not quite done: In order to have the result we went after, the underlying alphabet of the cellular automata constructed should be fixed, yet here our alphabet is not fixed as it is not fixed in the decision problem we used in our reduction. We can avoid this probelm as follows: Let all our cellular automata be defined over the alphabet $B = \{0, 1, -, |, +\}$. The symbols $\{-, |, +\}$ should be considered as horizontal lines, vertical lines, and intersecting lines, respectively. Now by choosing n large enough we can inject A into $\{0, 1\}$-squares of size $n \times n$. The configurations in $A^{\mathbb{Z}^2}$ can be represented as configurations of $B^{\mathbb{Z}^2}$ by dividing the lattice into $n \times n$-squares using the symbols in $\{-, |, +\}$ and then writing the encodings of A into these squares. When defining F_1 and F_2 we need to take larger neighborhoods to evaluate whether the configuration is locally an encoding of some configuration of $A^{\mathbb{Z}^2}$ and further whether this is an encoding of a valid pattern or not, but this is fine since even though we need a larger neighborhood a finite one still suffices.

Following the steps described above proves the claim, and in fact gives the following stronger result.

Theorem. *There is an alphabet B such that the following sets of pairs of reversible two-dimensional cellular automata over $B^{\mathbb{Z}^2}$ are recursively inseparable:*

1. *Pairs where the first cellular automaton has higher entropy than the second one.*
2. *Pairs which are conjugate and both have zero entropy.*

References

[1] J. Kari J. Jalonen. On the conjugacy problem of cellular automata. *submitted.*

[2] J. Kari J. Jalonen. Conjugacy of one-dimensional one-sided cellular automata is undecidable. In *SOFSEM 2018: Theory and Practice of Computer Science*, volume 10706 of *Lecture Notes in Computer Science*, pages 227–238. Edizioni della Normale, Cham, 2018.

[3] J. Kari. Reversibility and surjectivity problems of cellular automata. *Journal of Computer and System Sciences*, 48:149–182, 1994.

[4] T. Meyerovitch. Finite entropy for multidimensional cellular automata. *Ergodic Theory and Dynamical Systems*, 28(4):1243–1260, 2008.

Arnoux-Rauzy interval exchange transformations

extended abstract

Pierre Arnoux, Julien Cassaigne,
Sébastien Ferenczi, Pascal Hubert
Aix Marseille Université, CNRS, Centrale Marseille,
Institut de Mathématiques de Marseille,
I2M - UMR 7373, 13453 Marseille, France
pierre@pierrearnoux.fr,
julien.cassaigne@math.cnrs.fr,
ssferenczi@gmail.com hubert.pascal@gmail.com

Acknowledgement: a part of this research was carried out when the second and third authors participated in the meeting organized by S. Brlek in Murter (Croatia) in april 2018, and another part in july 2018 while the first author was in Unité Mixte IMPA-CNRS (Institut Jean-Christophe Yoccoz) in Rio de Janeiro and the third author was a temporary visitor of IMPA through the Réseau Franco-Brésilien en Mathématiques.

Arnoux-Rauzy dynamical systems were introduced in [5] in order to generalize the very fruitful triple interaction between Sturmian sequences and rotation of the 1-torus through the Euclid continued fraction approximation. Arnoux-Rauzy sequences are defined through word-combinatorial conditions, see Section 2.1 below, and what everybody would like to get is a geometric representation of the associated symbolic dynamical system, the preferred one being as a natural coding of a rotation of the 2-torus. The set of possible angles of this rotation is known as the Rauzy gasket, and defined in Section 2.3 below. A very famous particular case, the Tribonacci sequence, was shown in [17] to be a natural coding of a rotation of the 2-torus, and thus the corresponding system is measure-theoretically isomorphic to that rotation. This was generalized to a larger class of Arnoux-Rauzy systems in [4], and recently to almost all Arnoux-Rauzy systems [9], in the same sense as in Theorem 4.11 below. On the other hand, [11] provides counter-examples where this isomorphism cannot hold, see Section 5 below. For a general Arnoux-Rauzy system, one has to be content with what looks like a second-best geometric representation built in [5], a coding of a six-interval exchange on the circle, see Section 2.3 below.

However, these six-interval exchanges have been recently understood to represent by themselves a very interesting family of systems, as, though the number of intervals is six, they are interval exchanges of rank three (not to be confused with the rank defined by Rokhlin towers which will be used in Section 4.4 below), meaning that the set of lengths of the intervals has dimension three over the rationals. This kind of interval exchanges was pointed out (in a very different context and language) by S. P. Novikov [16], which prompted several authors to make deep studies of the Rauzy gasket in [6] [7] [8], solving partially a conjecture in [16], and to look at everything we can find about this particular family. But indeed, a priori not much is known, as these six-interval exchanges (called AR6 in the present paper) are only semi-conjugate to the original Arnoux-Rauzy systems (called AR3 in the present paper): namely, an AR6 interval exchange admits a coding by a partition into three sets which is an AR3 symbolic system, but this partition is not known to be a generating partition, while, as far as we know, the coding by the natural partition into six intervals cannot be built by substitutions, contrarily to its AR3 coding. Hence no property of an AR6 interval exchange can be directly carried out from the underlying AR3 symbolic system. Moreover, deep geometric methods have allowed I. Dynnikov and A. Skripchenko [12] to prove, again in a completely different language, the existence of minimal non-uniquely ergodic AR6 interval exchanges, in stark contrast with always minimal and uniquely ergodic AR3.

The relation between AR6 interval exchanges and underlying AR3 symbolic systems was partially tackled in [3], though only in the particular case of Tribonacci, and with a certain lack of details: that paper defines yet another Arnoux-Rauzy interval exchange, this time on nine intervals (called AR9 in the present paper), where an AR3 appears again as a coding by a partition into three sets, and where the coding by the natural partition into nine intervals can be explicitly generated by a substitution. This is the key for studying ergodic properties of AR9 interval exchanges, and extending them to the AR6 interval exchanges which appear as factors of AR9. The only one stated in [3] is the measure-theoretical isomorphism between the three corresponding systems (AR3, AR6, AR9) in the Tribonacci case, though no proof is offered.

In the present paper, we generalize the construction of AR9 systems to every set of parameters in the Rauzy gasket, and use them to derive dynamical properties of AR6 and AR9 systems. Our main result is an explicit sufficient condition for measure-theoretical isomorphism between the corresponding AR9, AR6 and AR3 systems, which implies unique ergodicity for the AR6 and AR9. This condition is satisfied by almost all Arnoux-Rauzy systems in the sense of [9], and many explicit examples including Tribonacci; proving at last the isomorphism in that case provides the backbone of the answer to Question 9 (asked by G. Forni) in [14] where the Tribonacci AR6 (or AR9) provide nontrivial examples of rigid self-induced interval exchanges, and this was another motivation for the present paper. Then we give a class of examples of non-uniquely ergodic AR9 (or AR6) which may be somewhat more explicit than those in [12], and give both examples and counter-examples to the isomorphism problem: these AR9 are measure-theoretically isomorphic to their AR3 coding if we equip them with an ergodic invariant measure, but of course this cannot hold if we take one of the many non-ergodic measures. Then we show that weak mixing is also present in the class of AR9 (or AR6) systems.

1 Basic definitions

We look at finite *words* on a finite alphabet $\mathcal{A} = \{1, ...k\}$. A word $w_1...w_t$ has *length* $|w| = t$. The *concatenation* of two words w and w' is denoted by ww'.

Definition 1.1. *A word $w = w_1...w_t$* occurs at place *i in a word $v = v_1...v_s$ or an infinite sequence $v = v_1v_2...$ if $w_1 = v_i$, $...w_t = v_{i+t-1}$. We say that w is a* subword *of v.*

Definition 1.2. *A* language *L over $\mathcal{A}$ is a set of words such if w is in L, all its subwords are in L, aw is in L for at least one letter a of $\mathcal{A}$, and wb is in L for at least one letter b of $\mathcal{A}$.*
A language L is minimal *if for each w in L there exists n such that w occurs in each word of L of length n.*
The language $L(u)$ of an infinite sequence u is the set of its finite subwords.

Definition 1.3. *A* substitution *ψ is an application from an alphabet $\mathcal{A}$ into the set $\mathcal{A}^\star$ of finite words on $\mathcal{A}$; it extends naturally to a morphism of $\mathcal{A}^\star$ for the operation of concatenation.*

Definition 1.4. *The* symbolic dynamical system *associated to a language L is the one-sided shift $S(x_0x_1x_2...) = x_1x_2...$ on the subset Y_L of $\mathcal{A}^{\mathbb{N}}$ made with the infinite sequences such that for every $t < s$, $x_t...x_s$ is in L.*

Note that the symbolic dynamical system (X_L, S) is minimal (in the usual sense, every orbit is dense) if and only if the language L is mimimal.

Definition 1.5. *For a dynamical system (X', U) and a finite partition $\{P_1, \dots P_l\}$ of X', the* trajectory *of a point x in X' is the infinite sequence $(x_n)_{n\in\mathbb{N}}$ defined by $x_n = i$ if $U^n x$ falls into P_i, $1 \leq i \leq l$.*
Then if L is the language made of all the finite subwords of all the trajectories, (Y_L, S) is called the coding *of (X', U) by the partition $\{P_1, \dots P_l\}$.*

2 Classical Arnoux-Rauzy systems

2.1 AR3 symbolic systems

These systems are the "genuine" Arnoux-Rauzy systems; we take here as a definition their constructive characterization, derived in [5] from the original definition, and modified in the present paper by a renaming of letters and words. We choose to name a, b, c, the letters of the alphabet, in such a way that the words of length 2 are aa, ab, ac, ba, ca; then the following definition is equivalent to the original one.

Definition 2.1. *An* AR3 symbolic system *is the symbolic system on $\{a, b, c\}$ generated by the three substitutions*

- *σ_I: $a \to ab$, $b \to ac$, $c \to a$,*
- *σ_{II}: $a \to ab$, $b \to a$, $c \to ac$,*
- *σ_{III}: $a \to a$, $b \to ab$, $c \to ac$,*

and a directing sequence r_n, $n \in GN^\star$, $i_n \in \{I, II, III\}$, taking the value I infinitely many times.

Namely, it is the symbolic system (Y_3, S) whose language is generated by the words $A_k = \sigma_{r_1}...\sigma_{r_k}a$, $B_k = \sigma_{r_1}...\sigma_{r_k}b$,, $C_k = \sigma_{r_1}...\sigma_{r_k}c$, $k \geq 1$. The respective lengths of the words A_k, B_k, C_k will always be denoted by $h_{a,k}$, $h_{b,k}$, $h_{c,k}$.

(Y_3, S) is minimal [5] and uniquely ergodic (by Boshernitzan's result [10] using the fact that the language complexity is $2n + 1$) with a unique invariant probability measure μ.

Note that our modification of the rules changes the usual condition of [5], that each substitution is used infinitely often, to the present condition that σ_I is used infinitely often. The most famous particular case is the *Tribonacci system*, where $r_n = I$ for all n.

2.2 Partial quotients and multiplicative rules

These quantities are defined in [11], but we redefine them here as the notations are different.

Definition 2.2. *We write the directing sequence* (r_n) *in a unique way as* $k_1 - 1 \geq 0$ *times the symbol* III *followed by one symbol* I *or* II*, then* $k_2 - 1 \geq 0$ *times* III *followed by one* I *or* II *etc.... the* $k_n \geq 1$ *are then called the* partial quotients *of the system.*
The multiplicative times *are* $m_0 = 0$*,* $m_n = k_1 + ...k_n$*,* $n \geq 1$.

Then the words $A_{m_n}, B_{m_n}, C_{m_n}$ can be built by the following *multiplicative rules*, which could also be expressed by substitutions but would need a countable set of them:

- if $r_{m_{n+1}} = I$, we say that *the* $n+1$*-th multiplicative rule is a rule* I_m, and we have
  - $A_{m_{n+1}} = A_{m_n}^{k_{n+1}} B_{m_n}$,
  - $B_{m_{n+1}} = A_{m_n}^{k_{n+1}} C_{m_n}$,
  - $C_{m_{n+1}} = A_{m_n}$;
- if $r_{m_{n+1}} = II$, we say that *the* $n+1$*-th multiplicative rule is a rule* II_m, and
  - $A_{m_{n+1}} = A_{m_n}^{k_{n+1}} B_{m_n}$,
  - $B_{m_{n+1}} = A_{m_n}$,
  - $C_{m_{n+1}} = A_{m_n}^{k_{n+1}} C_{m_n}$.

For Tribonacci, we have $k_n = 1$ for all n, and all multiplicative rules are of type Im.

We shall use the inequalities proved in Lemma 7 of [11] at the multiplicative times: namely $h_{b,m_n} \leq 2h_{a,m_n}$ and $h_{c,m_n} \leq 2h_{a,m_n}$. These are not true in general at other (additive) times $p \neq m_n$.

2.3 AR6 interval exchanges

These exchanges of six intervals on a circle are defined in [5].

Definition 2.3. *The* Rauzy gasket Γ *is the set of triples of positive real numbers* (a_0, b_0, c_0)*, such that, if we define recursively the numbers* a_n*,* b_n*,* c_n *by taking the triple* $(a_{n-1} - b_{n-1} - c_{n-1}, b_{n-1}, c_{n-1})$ *and reordering it, then for each* $n \geq 0$ *we have* $a_n > b_n > c_n > 0$.

Definition 2.4. *An* AR6 nterval exchange (X_6, T) *is defined in the following way from any triple* (a_0, b_0, c_0) *in* Γ*:* X_6 *is a circle of length* $2a_0 + 2b_0 + 2c_0$*. The circle is partitioned into three intervals of respective lengths* $2a_0$*,* $2b_0$*,* $2c_0$*, then each one is cut into two halves; the action of* T *first exchanges by translations respectively the two intervals of length* a_0*, the two intervals of length* b_0*, the two intervals of length* c_0*, then translates everything by* $a_0 + b_0 + c._0$*, i.e. a half-circle.*

Note that the order between the intervals of lengths $2a_0$, $2b_0$, $2c_0$ is not mentioned in Definition 2.4 (the fact that it is not always the same is somewhat understated in [5]); but it follows from this definition that two AR6 interval exchanges defined with the same (a_0, b_0, c_0) but different orders of these intervals are conjugate by a map which is continuous except on a finite number of points, and hence *measure-theoretically isomorphic for any invariant measure*, in the sense that any invariant measure on one of them can be carried to the other one, and the two measure-theoretic systems are isomorphic. Similarly, the location of the origin on the circle does not change the system up to topological conjugacy and measure-theoretically isomorphism for any invariant measure.

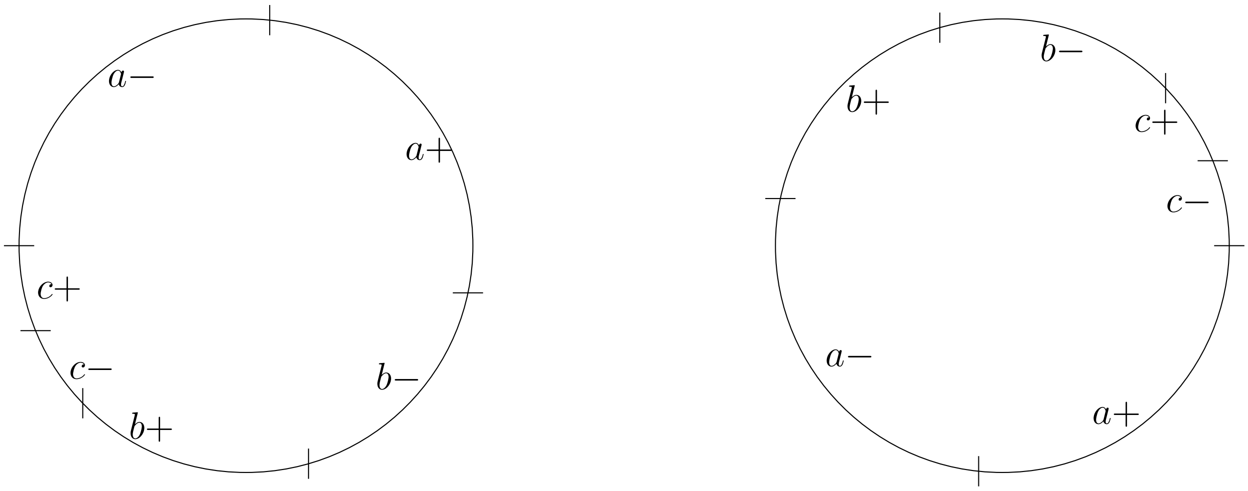

Figure 1: AR6 interval exchange

For example, when the intervals of lengths $2a_0$, $2b_0$, $2c_0$ are successive intervals of the circle in that order, T is shown in Figure 1, where on the left circle $a-$, $a+$, $b-$, ... denote the intervals of length a_0, a_0, b_0 ... while on the right circle the letters correspond to the images of these intervals by the transformation. If in Figure 1 we choose to put the origin at the left end of the interval denoted by $a-$, $[0, a_0)$ is sent to $[a_0 + a_0 + b_0 + c_0, 2a_0 + a_0 + b_0 + c_0)$ modulo $2a_0 + 2b_0 + 2c_0$, $[a_0, 2a_0)$ is sent to $[a_0 + b_0 + c_0, a_0 + a_0 + b_0 + c_0)$ modulo $2a_0 + 2b_0 + 2c_0$, etc...

2.4 Note on endpoints

One recurring problem when dealing with interval exchanges is what to do with interval endpoints? A satisfying answer to this question is given by M. Keane in Section 5 of [15]: by carefully doubling the endpoints and their orbits, he defines a Cantor set on which the transformation becomes an homeomorphism, and show this is equivalent to taking the natural coding by the partition into defining intervals. In the present paper, to make definitions easier, we do not use Keane's construction, and all intervals are closed on the left, open on the right; but that will introduce technical difficulties, see Remark 3.1 below.

3 The new systems: Arnoux-Rauzy on nine symbols

3.1 AR9 interval exchanges

These are defined for the particular case of Tribonacci in [3].

An AR9 interval exchange is defined by a point (a_0, b_0, c_0) in Γ and three auxiliary parameters, real numbers d_0, e_0, f_0, satisfying the *compatibilty rules*.

- either (first order) $d_0 + a_0 + b_0 \leq e_0 < e_0 + b_0 + c_0 \leq f_0$,
- or (second order) $e_0 + b_0 + c_0 \leq f_0 < f_0 + a_0 + c_0 \leq d_0$,
- or (third order) $f_0 + a_0 + c_0 \leq d_0 < d_0 + a_0 + b_0 \leq e_0$,
- or (reversed first order) $f_0 + a_0 + c_0 \leq e_0 < e_0 + b_0 + c_0 \leq d_0$,
- or (reversed second order) $d_0 + a_0 + b_0 \leq f_0 < f_0 + a_0 + c_0 \leq e_0$,
- or (reversed third order) $e_0 + a - c_0 + b_0 \leq d_0 < d_0 + b_0 + a_0 \leq f_0$.

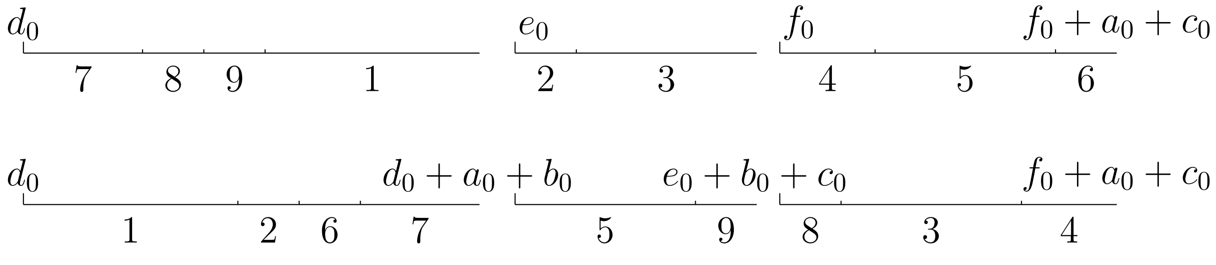

Figure 2: AR9 interval exchange

Definition 3.1. *For a point (a_0, b_0, c_0) in Γ and auxiliary parameters d_0, e_0, f_0, an AR9 interval exchange (X_9, T) is defined on the union of the intervals $[d_0, d_0 + a_0 + b_0)$, $[e_0, e_0 + b_0 + c_0)$ and $[f_0, f_0 + a_0 + c_0)$ by piecewise translations, in the following way when d_0, e_0, f_0 are in the first, second or third order:*

- *we partition the interval $[d_0, d_0 + a_0 + b_0)$, from left to right, into four intervals of successive lengths $b_0 - c_0$, c_0, c_0, $a_0 - c_0$, denoted respectively by $I_{7,0}$, $I_{8,0}$, $I_{9,0}$, $I_{1,0}$, and into four intervals of successive lengths $a_0 - c_0$, c_0, c_0, $b_0 - c_0$, which we define respectively to be $TI_{1,0}$, $TI_{2,0}$, $TI_{6,0}$, $TI_{7,0}$,*
- *we partition the interval $[e_0, e_0 + b_0 + c_0)$, from left to right, into two intervals of successive lengths c_0, b_0, denoted respectively by $I_{2,0}$, $I_{3,0}$, and into two intervals of successive lengths b_0, c_0, which we define respectively to be $TI_{5,0}$, $TI_{9,0}$,*
- *we partition the interval $[f_0, f_0 + a_0 + c_0)$, from left to right, into three intervals of successive lengths $a_0 - b_0$, b_0, c_0, denoted respectively by $I_{4,0}$, $I_{5,0}$, $I_{6,0}$, and into three intervals of successive lengths c_0, b_0, $a_0 - b_0$, which we define respectively to be $TI_{8,0}$, $TI_{3,0}$, $TI_{4,0}$.*

If d_0, e_0, f_0 are in the reversed first, second or third order, we do as in the previous case, except that everywhere "from left to right" is replaced by "from right to left" (note that all intervals are still closed on the left, open on the right).

It is clear from the definition that two AR9 interval exchanges defined with the same (a_0, b_0, c_0) but different d_0, e_0, f_0 are conjugate by a map which is continuous except on a finite number of points (it will be continuous everywhere if we suppose no two of the three intervals $[d_0, d_0 + a_0 + b_0)$, $[f_0, f_0 + a_0 + c_0)$, $[e_0, e_0 + b_0 + c_0)$ are adjacent), and measure-theoretically isomorphic for any invariant measure, in the sense of Section 2.3 above. We could choose d_0, e_0, f_0 to start from one interval, but as we shall see below this will not be conserved by induction, so we keep the auxiliary parameters, and shall check that all our results, in particular Lemma 4.4 below, which states the adjacency of certain intervals, is true for any choice of d_0, e_0, f_0.

For example, if d_0, e_0, f_0 are in the first order, we get

- $I_{7,0} = [d_0, d_0 + b_0 - c_0)$, $TI_{7,0} = [d_0 + a_0 + c_0, d_0 + b_0 + a_0)$,
- $I_{8,0} = [d_0 + b_0 - c_0, d_0 + b_0)$, $TI_{8,0} = [f_0, f_0 + c_0)$,
- $I_{9,0} = [d_0 + b_0, d_0 + b_0 + c_0)$, $TI_{9,0} = [e_0 + b_0, e_0 + b_0 + c_0)$,
- $I_{1,0} = [d_0 + b_0 + c_0, d_0 + b_0 + a_0)$, $TI_{1,0} = [d_0, d_0 + a_0 - c_0)$,

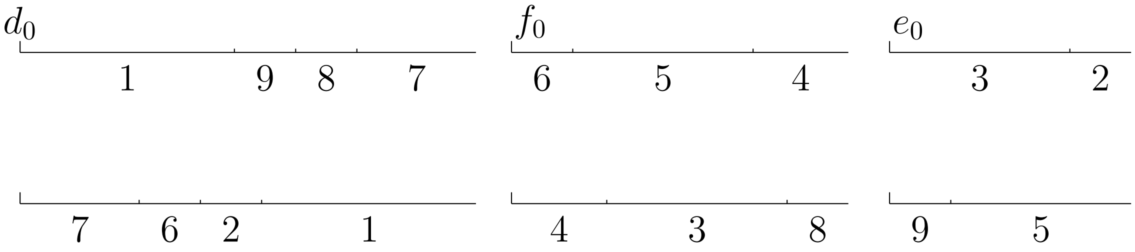

Figure 3: AR9 interval exchange in reversed order

- $I_{2,0} = [e_0, e_0 + c_0)$, $TI_{2,0} = [d_0 + a_0 - c_0, d_0 + a_0)$,
- $I_{3,0} = [e_0 + c_0, e_0 + b_0 + c_0)$, $TI_{3,0} = [f_0 + c_0, f_0 + b_0 + c_0)$,
- $I_{4,0} = [f_0, f_0 + a_0 - b_0)$, $TI_{4,0} = [f_0 + b_0 + c_0, f_0 + a_0 + c_0)$,
- $I_{5,0} = [f_0 + a_0 - b_0, f_0 + a_0)$, $TI_{5,0} = [e_0, e_0 + b_0)$,
- $I_{6,0} = [f_0 + a_0, f_0 + a_0 + c_0)$, $TI_{6,0} = [d_0 + a_0, d_0 + a_0 + c_0)$,

and T is shown in Figure 2, where i in the upper part corresponds to $I_{i,0}$ and i in the lower part corresponds to $TI_{i,0}$. An example in the reversed second order is shown in Figure 3.

3.2 Induction

Now, we take an AR9 system; to fix ideas, we suppose d_0, e_0, f_0 *are in the first order*. Let T_1 be the induced map of T on $I_{1,0} \cup I_{2,0} \cup I_{3,0} \cup I_{4,0}$. We define $a_1 > b_1 > c_1$ as the triple $(a_0 - b_0 - c_0, b_0, c_0)$ after reordering. Then there are three cases, which we tackle by growing difficulty.

3.2.1 Induction step case III: $a_1 = a_0 - b_0 - c_0$.

Then $b_1 = b_0$, $c_1 = c_0$.

The situation is essentially described in Figure 4. The induction set $I_{1,0} \cup I_{2,0} \cup I_{3,0} \cup I_{4,0}$ is cut into nine new intervals $I_{i,1}$, whose respective lengths are, from left to right, $b_1 - c_1$, c_1, c_1, $a_1 - c_1$, c_1, b_1, $a_1 - b_1$, b_1, c_1. Then T acts on the picture as a move upwards, until we reach again the induction set, which is marked by dashed lines. Each interval of the picture is labelled by j above if it is in $I_{j,0}$; the labels are between parentheses for the dashed intervals, as they will not be used further (note that $T_1 I_{5,1} = T^2 I_{5,1}$ is the union of a (full) subinterval of $I_{2,0}$ with a (left) subinterval of $I_{3,0}$, hence the ambiguous label). Thus for example $I_{7,1}$ is sent by T onto $I_{7,0}$, then by another application of T into $I_{1,0}$, hence $T_1 = T^2$ on $I_{7,1}$. And we check that

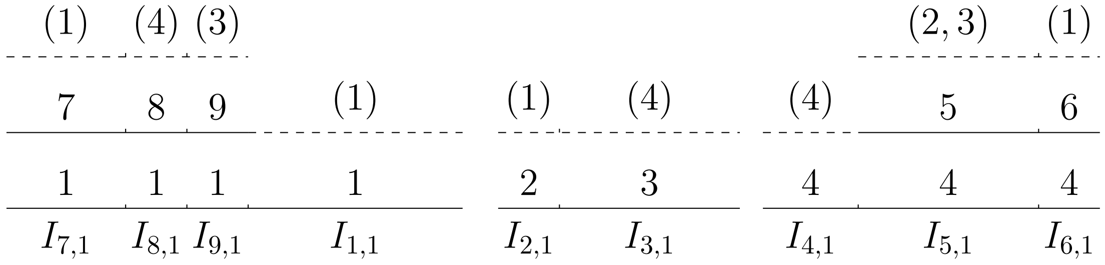
(1) (4) (3)
(2, 3) (1)
7 8 9
(1)
(1) (4)
(4)
5 6
1 1 1 1 2 3 4 4 4
$I_{7,1}$ $I_{8,1}$ $I_{9,1}$ $I_{1,1}$ $I_{2,1}$ $I_{3,1}$ $I_{4,1}$ $I_{5,1}$ $I_{6,1}$

Figure 4: Induction Case III

T_1 is indeed an AR9 interval exchange defined by (a_1, b_1, c_1). We can also compute $d_1 = d_0 + b_0 + c_0$, $e_1 = e_0$, $f_1 = f_0$; the order is still the first one.

3.2.2 Induction step case I: $c_1 = a_0 - b_0 - c_0$.

Then $a_1 = b_0$, $b_1 = c_0$.

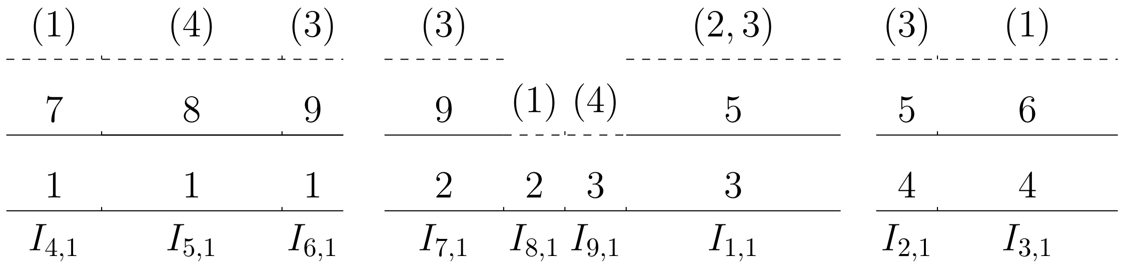
(1) (4) (3)
(3)
(2, 3)
(3) (1)
7 8 9
9 (1) (4) 5
5 6
1 1 1 2 2 3 3 4 4
$I_{4,1}$ $I_{5,1}$ $I_{6,1}$ $I_{7,1}$ $I_{8,1}$ $I_{9,1}$ $I_{1,1}$ $I_{2,1}$ $I_{3,1}$

Figure 5: Induction Case I

The length of each $I_{i,1}$ is the same as in case III. T_1 is an AR9 interval exchange defined by (a_1, b_1, c_1); $d_1 = e_0$, $e_1 = f_0$, $f_1 = d_0 + b_0 + c_0$ are in the third order.

3.2.3 Induction step case II: $b_1 = a_0 - b_0 - c_0$.

Then $a_1 = b_0$, $c_1 = c_0$.

The length of each $I_{i,1}$ is the same as in case III. T_1 is an AR9 interval exchange, defined by (a_1, b_1, c_1), and where $d_1 = d_0 + b_0 + c_0$, $e_1 = f_0$, $f_1 = e_0$ are in the reversed second order.

The same computations work if we start from an AR9 when d_0, e_0, f_0 are in the second order: we get the same pictures except that d_1, e_1, f_1 are in the second order in Case III, the first order in Case I, the reversed first order in Case II. When d_0, e_0, f_0 are in the third order, we get the same pictures except that d_1, e_1, f_1 are in the third order in Case III, the reversed third order in Case II, and the second order in Case I. If we start form a reversed order, just reverse the orientation of the pictures.

3.3 AR9 symbolic systems

Definition 3.2. *An AR9 symbolic system (Y_9, S) is the* natural coding *of an AR9 interval exchange (X_9, T), that is its coding by the partition into $I_{i,0}$, $1 \leq i \leq 9$; we denote by ψ the map associating to each point $x \in X_9$ its trajectory in Y_9.*

Remark 3.1. *Because of the way we deal with the endpoints, see Section 2.4 above, ψ is injective but not surjective; we have $Y_9 = \psi(X_9) \cup D_9$, where D_9 is a countable set made with the* improper trajectories *of the right endpoints of the intervals $I_{i,0}$ and their negative orbits: these are the limits, in the product topology of $\{1, ...9\}^{\mathbb{N}}$, in which Y_9 is closed, of trajectories of points approaching these endpoints from the left, and similarly for their pre-images.*

Proposition 3.1. *For each (a_0, b_0, c_0) in Γ, the AR9 symbolic system associated to any AR9 interval exchange defined by (a_0, b_0, c_0) is the symbolic system on $\{1, ...9\}$ generated by the three substitutions*

- σ'_I: 1 → 35, 2 → 45, 3 → 46, 4 → 17, 5 → 18, 6 → 19, 7 → 29, 8 → 2, 9 → 3,
- σ'_{II}: 1 → 17, 2 → 46, 3 → 45, 4 → 35, 5 → 3, 6 → 2, 7 → 1, 8 → 19, 9 → 18,
- σ'_{III}: 1 → 1, 2 → 2, 3 → 3, 4 → 4, 5 → 45, 6 → 46, 7 → 17, 8 → 18, 9 → 19.

and a directing sequence r_n, $n \in GN^\star$, $i_n \in \{I, II, III\}$, defined by $r_n = I$ if $a_n = a_{n-1} - b_{n-1} - c_{n-1}$, $r_n = II$ if $b_n = a_{n-1} - b_{n-1} - c_{n-1}$, $r_n = III$ if $c_n = a_{n-1} - b_{n-1} - c_{n-1}$; r_n takes the value I infinitely many times.

Any system defined in this way is an AR9 symbolic system.

Thus the AR9 symbolic system does not depend on d_0, e_0, f_0. The common length of the words 1_k, 2_k, 3_k, 4_k, is $h_{a,k}$ defined in Section 2.1, $h_{b,k}$ is the common length of the words 5_k, 6_k, 7_k, $h_{c,k}$ the common length of the words 8_k, 9_k.

The multiplicative rules of Section 2.2 above extend immediately to AR9 systems, in the following way

- if the $n+1$-th multiplicative rule is a rule I_m,

- $1_{m_{n+1}} = 3_{m_n} 4_{m_n}^{k_{n+1}-1} 5_{m_n}$,
- $2_{m_{n+1}} = 4_{m_n}^{k_{n+1}} 5_{m_n}$,
- $3_{m_{n+1}} = 4_{m_n}^{k_{n+1}} 6_{m_n}$,
- $4_{m_{n+1}} = 1_{m_n}^{k_{n+1}} 7_{m_n}$,
- $5_{m_{n+1}} = 1_{m_n}^{k_{n+1}} 8_{m_n}$,
- $6_{m_{n+1}} = 1_{m_n}^{k_{n+1}} 9_{m_n}$,
- $7_{m_{n+1}} = 2_{m_n} 1_{m_n}^{k_{n+1}-1} 9_{m_n}$,
- $8_{m_{n+1}} = 2_{m_n}$,
- $9_{m_{n+1}} = 3_{m_n}$;

- if the t $n+1$-th multiplicative rule is a rule II_m,
  - $1_{m_{n+1}} = 1_{m_n}^{k_{n+1}} 7_{m_n}$,
  - $2_{m_{n+1}} = 4_{m_n}^{k_{n+1}} 6_{m_n}$,
  - $3_{m_{n+1}} = 4_{m_n}^{k_{n+1}} 5_{m_n}$,
  - $4_{m_{n+1}} = 3_{m_n} 4_{m_n}^{k_{n+1}-1} 5_{m_n}$,
  - $5_{m_{n+1}} = 3_{m_n}$,
  - $6_{m_{n+1}} = 2_{m_n}$,
  - $7_{m_{n+1}} = 1_{m_n}$,
  - $8_{m_{n+1}} = 1_{m_n}^{k_{n+1}} 9_{m_n}$,
  - $9_{m_{n+1}} = 1_{m_n}^{k_{n+1}} 8_{m_n}$.

3.4 Relations between Arnoux-Rauzy systems

Starting from a point (a_0, b_0, c_0) in Γ, and some auxiliary parameters, we have defined two geometric systems, (X_9, T) and (X_6, T).

Proposition 3.2. *An AR9 interval exchange defined by (a_0, b_0, c_0) is conjugate to an AR6 interval exchange defined by (a_0, b_0, c_0) by a map which is continuous except on a finite number of points, and thus gives a measure-theoretic isomorphism for each invariant measure, and any AR6 interval exchange is conjugate to an AR9 in this way.*

As in Proposition 3.1, any point in Γ defines a directing sequence (r_n). Each directing sequence defines two symbolic systems, (Y_9, S) and (Y_3, S).

Proposition 3.3. *The coding of an AR9 symbolic system defined by (a_0, b_0, c_0), by the partition into three sets $J_{a,0} = I_{1,0} \cup I_{2,0} \cup I_{3,0} \cup I_{4,0}$, $J_{b,0} = I_{5,0} \cup I_{6,0} \cup I_{7,0}$, $J_{c,0} = I_{8,0} \cup I_{9,0}$, is the AR3 symbolic system defined by the directing sequence in Proposition 3.1, and all AR3 symbolic systems can be built in this way.*

$$\begin{tikzcd}
(Y_9, S) \arrow[r, dashed, "\phi_6"] \arrow[rr, dashed, bend left, "\phi"] & (Y_6, S) \arrow[r, dashed, "\phi_3"] & (Y_3, S) \\
(X_9, T) \arrow[u, "\psi"] \arrow[r, dashed, "\phi'_6"] & (X_6, T) \arrow[u, "\psi'"] &
\end{tikzcd}$$

Figure 6: The five AR systems

Corollary 3.4. *An AR9 symbolic system has an AR3 symbolic system defined by the same directing sequence as a factor, and all AR3 symbolic systems can be built in this way.*

We define the letter-to-letter map ϕ by $\phi(1) = \phi(2) = \phi(3) = \phi(4) = a$, $\phi(5) = \phi(6) = \phi(7) = b$, $\phi(8) = \phi(9) = c$. The map associating to a point in (X_9, S) its coding in (Y_3, S) is just $\phi\psi$, where ψ is defined in Definition 3.2. As in Remark 3.1, we have $\phi\psi(X_9) = Y_3 \backslash D'_3$ for the countable set D'_3 made with improper trajectories; note that $D'_3 \subset D_3$ where $D_3 = \phi(D_9)$. $\phi\psi$ conjugates the map T on X_9 with the shift S on X_3: to use the vocabulary of [5], $\phi\psi$ is called a *semi-conjugacy*; as is pointed out in the introduction above, this does not give a one-to-one correspondence between points. Similarly, ϕ conjugates the shifts on Y_9 on Y_3 and $\phi(Y_9) = Y_3$; it is also a semi-conjugacy, and not injective, see Proposition 4.6 below.

We now place the AR6 in the picture: we can also define the *AR6 symbolic system* (Y_6, S) on $\{a-, a+, b-, b+, c-, c+\}$, by the natural coding ψ_6, of (X_6, S) by its defining six intervals; we have $Y_6 = \psi_6(X_6) \cup D_6$ for a countable set D_6. We can write $\phi = \phi_3 \circ \phi_6$, with $\phi_6(1) = \phi_6(2) = a-$, $\phi_6(3) = \phi_6(4) = a+$, $\phi_6(5) = b-$,

$\phi_6(6) = \phi_6(7) = b+$, $\phi_6(8) = c-$, $\phi_6(9) = c+$, and $\phi_3(j-) = \phi_3(j+) = j$ for $j = a, b, c$.

In the same way as Proposition 3.3, we could reprove the main result of [5]: the coding of an AR6 interval exchange defined by (a_0, b_0, c_0), by the partition into three sets $\phi_6'(J_{a-,0} \cup J_{a+,0})$, $\phi_6'(J_{b-,0} \cup J_{b+,0})$, $\phi_6'(J_{c-,0} \cup J_{c+,0})$, is the AR3 symbolic system defined by the directing sequence of Proposition 3.1, and all AR3 symbolic systems can be built in this way. Thus (Y_6, S) appears as an intermediate coding between the AR3 and AR9 symbolic systems; because of Proposition 3.2, ϕ_6, applied letter to letter, is invertible except on a countable set (included in $\phi_6(D_9)$), and conjugates (Y_9, S) and (Y_6, S), which are thus measure-theoretically isomorphic for each invariant measure.

As was already mentioned, we do not know any way to build the trajectories in Y_6 as in Definition 2.1 or Proposition 3.1; but they can be deduced from the trajectories in Y_9 by applying ϕ_6 letter to letter, and that was the main objective of the theory of AR9 systems; however, in general it will be easier to work directly on AR9 systems and then derive the properties of AR6 systems.

At this stage, it may be useful to recall the various notations we use, for which we had to make choices because of the number of systems we have defined and some long pre-existing notations: a, b, c are always the three symbols on which AR3 systems are built. But a_k, b_k, c_k, for any k, are real numbers, describing lengths of intervals. A_k, B_k, C_k are the words used to build AR3 systems, of lengths (i.e. number of letters) $h_{a,k}$, $h_{b,k}$, $h_{c,k}$. 1 to 9 are the symbols on which AR9 symbolic systems are built, 1_k to 9_k are the words used to build them, their lengths are among $h_{a,k}$, $h_{b,k}$, $h_{c,k}$. Interval lengths for AR9 systems, when needed, are defined in terms of a_k, b_k, c_k. Roman numerals are used for the substitutions and rules to build words.

4 Dynamical properties

4.1 Minimality

By using the condition that $r_n = I$ for infinitely many n, the minimality of AR3 symbolic systems and AR6 interval exchanges is shown in [5]. The minimality of AR6 symbolic systems follows, as the minimality of an interval exchange is equivalent to the minimality of its natural coding, small intervals corresponding to small cylinders.

Proposition 4.1. *Any AR9 system is minimal.*

4.2 Rokhlin towers

Definition 4.1. *In a system (X', U), a* Rokhlin tower *is a collection of disjoint measurable sets F, UF, ..., $U^{h-1}F$ (U^jF is called* level j *of the tower, F is called the* base, *h the* height *of the tower). A* slice *of τ is a union of consecutive levels U^pF ... U^qF, and a* column *of τ is made with levels G, ... $U^{h-1}G$ for a subset G of F. We shall usually write "the tower τ" as a shortened form of "the tower for which the union of the levels is the set τ".*

Proposition 4.2. *In an AR9 interval exchange (X_9, T), there are nine sequences of towers $\tau_{i,k}$, respectively of base $I_{i,k}$, and height equal to the length of the word i_k, $1 \leq i \leq 9$, $k \geq 0$: every point x in X_9 is determined by the sequence $\iota(x, k)$, $\eta(x, k)$ such that x is in $T^{\eta(x,k)}I_{\iota(x,k),k}$, $k \geq 0$. This remains true if we restrict k to a subsequence, for example the m_n. All levels of these towers are intervals.*

Corollary 4.3. *In (Y_9, S), the $\tau'_{i,k} = \psi(\tau_{i,k})$, $i = 1, ...9$, form nine sequences of Rokhlin towers. If D_9 is the countable set defined in Remark 3.1, every point y in $Y_9 \setminus D_9$ is determined by the sequences $\iota(y, k)$, $\eta(y, k)$ such that y is in $S^{\eta(x,k)}\psi(I_{\iota(x,k),k})$, $k \geq 0$.*

In (X_9, T), there exist three sequences of Rokhlin towers $\tau_{a,k}$, $\tau_{b,k}$, $\tau_{c,k}$, respectively of bases $J_{a,k}$, $J_{b,k}$, $J_{c,k}$, and heights equal to $h_{a,k}$, $h_{b,k}$, $h_{c,k}$, $k \geq 0$, where $J_{a,k} = I_{1,k} \cup I_{2,k} \cup I_{3,k} \cup I_{4,k}$, $J_{b,k} = I_{5,k} \cup I_{6,k} \cup I_{7,k}$, $J_{c,k} = I_{8,k} \cup I_{9,k}$. The union of all their levels for fixed k is X_9.

In the AR3 system (Y_3, S), the $\tau'_{j,k} = \phi\psi(\tau_{j,k})$, $j = a, b, c$, form three sequences of Rokhlin towers; if $D_3 = \phi(D_9)$, every point x in $Y_3 \setminus D_3$ is determined by the sequences $\iota'(y, k)$, $\eta(y, k)$ such that y is in $S^{\eta(y,k)}\phi\psi(J_{\iota'(y,k),k})$, $k \geq 0$.

Remark 4.1. *We can also build directly (slightly) enlarged versions of the various towers τ' in the symbolic systems: this is done in [11] for the $\tau'_{j,k}$, $j = a, b, c$, by induction on cylinders which are the closure of $\phi\psi(J_{a,k})$ in the topology of the symbolic systems, and can be done in the same way for the $\tau'_{i,k}$, $i = 1, ...9$, by induction on unions of cylinders which are the closure of $\psi(J_{a,k})$. These enlarged towers are closed and include also improper trajectories; but we do not need that for our results, for which countable sets can be neglected, and in any case points of D_3 must be taken into account, see Remark 4.2 below.*

Lemma 4.4. *For every k, the sets $T^jI_{2,k}$ and $T^jI_{3,k}$, $0 \leq j \leq h_{a,k} - 1$, resp. $T^jI_{5,k}$ and $T^ji_{6,k}$, $0 \leq j \leq h_{b,k} - 1$, resp. $T^jI_{8,k}$ and $T^ji_{9,k}$, $0 \leq j \leq h_{c,k} - 1$, are adjacent intervals.*

An immediate consequence is best seen on Figure 6:

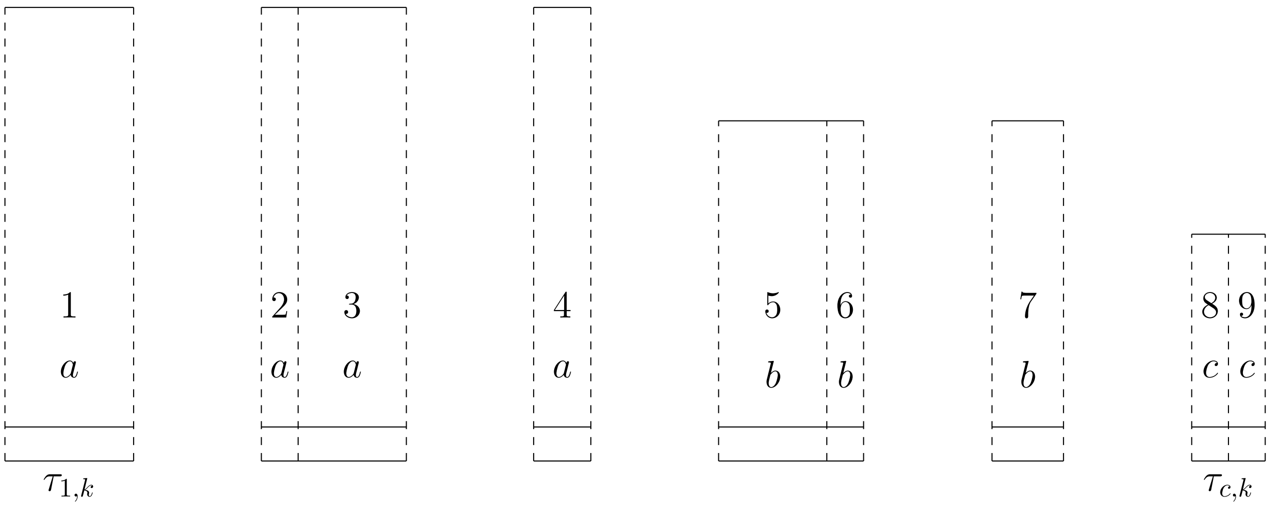

Figure 7: Rokhlin towers in X_9

Corollary 4.5. *Each level of the towers $\tau_{c,k}$ is an interval, each level of the towers $\tau_{b,k}$ is a union of at most two intervals, each level of the towers $\tau_{a,k}$ is a union of at most three intervals.*

Note that the $J_{j,k}$ and their images are not intervals for $j = a, b$, except maybe for the first values of k, with a suitable choice of d_0, e_0, f_0, but even in that case, for example if they are in the first order, $J_{b,0}$ is not an interval. Similarly, except maybe for the first values of k, the levels of the towers $\tau_{b,k}$ are not intervals, the levels of the towers $\tau_{a,k}$ are not unions of less than three intervals.

4.3 Isomorphism

Definition 4.2. *For $i = 1, 2, 3$, let $E_i \subset Y_3$ be the set of points which have i pre-images under ϕ.*

Proposition 4.6. *$Y_3 \setminus D_3 \subset E_1 \cup E_2 \cup E_3$. E_3 is countable. If $\mu(E_1) < 1$, then for any invariant probability μ' the system (Y_9, S, μ') is a two-point extension of (Y_3, S, μ)*

Lemma 4.7. *Let y be in $Y_3 \setminus D_3$. If y is in $\tau'_{c,k}$ for infinitely many k, then y is in E_1.*

Remark 4.2. *If we enlarge the towers to cover all Y_3 as in [11] and Remark 4.1 above, the generalization of Lemma 4.7 does not hold for $y \in D_3$: indeed, the point x_0 separating $I_{8,0}$ from $I_{9,0}$ defines one trajectory in $\psi(X_9)$ and one improper trajectory (as in Remark 3.1), and both these trajectories have the same image y_0 by ϕ, though we can check that, for example in the Tribonacci case, y_0 is in the enlarged $\tau'_{c,k}$ for infinitely many k. However, it is true that every point in Y_3 has at most three pre-images by ϕ, as the only candidates to have more are the points which are in* *the enlarged $\tau'_{a,k}$ for all $k \geq k_0$, and their pre-images do not give rise to improper trajectories.*

At this stage, one can ask whether the condition to be in $\tau'_{c,k}$ for infinitely many k is necessary for y to be in E_1. Hopefully, a necessary and sufficient condition will be given in a further paper, but the following lemma gives already a negative answer for many systems including Tribonacci.

Lemma 4.8. *Suppose that,*

- *(i) either for an infinite sequence s_j, the $s_j + 2$-th multiplicative rule is Im with $k_{s_j+2} = 1$,*
- *(ii) or for an infinite sequence s_j the $s_j + 2$-th multiplicative rules is Im and the $s_j + 1$-th multiplicative rule is IIm with $k_{s_j+1} = 1$.*

Let y be in $Y_3 \setminus D_3$. If we are in case (i) and for infinitely many j y is in $\tau'_{b,m_{s_j+1}} \cap \tau'_{b,m_{s_j+3}}$, or if we are in case (ii) and for infinitely many j y is in $\tau'_{b,m_{s_j}} \cap \tau'_{b,m_{s_j+3}}$, then y is in E_1.

Note that Lemma 4.8 gives only sufficient conditions, the same reasoning can produce many others. It will not be used further, as Lemma 4.7 is enough to prove

Proposition 4.9. *Let*

- *$\xi_n = \frac{1}{k_{n+2}}$ if the $n + 1$-th multiplicative rule is of type Im and $k_{n+1} \geq 2$,*
- *$\xi_n = \frac{1}{3^l k_{n+2} \ldots k_{n+l+1}}$ if the $n+1$-th multiplicative rule is of type Im with $k_{n+1} = 1$ or of type IIm, and the next multiplicative rule of type Im is the $n+l$-th, $l \geq 2$.*

Suppose $\sum \xi_n = +\infty$. Let Z be the set of y in Y_3, such that y is not in $\tau'_{c,k}$ for all k large enough. Then $\mu(Z) = 0$ for the unique invariant measure μ.

Note that Proposition 4.9 is intended as a sufficient condition; the first set of values of ξ_n takes care of almost all the Arnoux-Rauzy systems, see Theorem 4.11 below; the second set takes care of the Tribonacci case, for which the resulting Theorem 4.10 is claimed, though not proved, in [3], and completes taking care of all Arnoux-Rauzy systems where the k_n are bounded, (in [9] these are said to have bounded weak partial quotients), which include the *substitutive* AR9 or AR3 symbolic systems.

We turn now to the isomorphism problem: as E_3 is nonempty, the best we can hope is to replace the semi-conjugacies in Section 3.4 by measure-theoretic isomorphisms.

Theorem 4.10. *Under the hypothesis of Proposition 4.9, an AR9 or AR6 symbolic system or interval exchange is uniquely ergodic and measure-theoretically isomorphic to its AR3 coding.*

Definition 4.3. *As in [9], we consider measures on all infinite sequences of symbols I, II, III and take any shift invariant ergodic probability measure ν which assigns positive measure to each cylinder; by identifying an AR3, AR6, or AR9 system with its defining sequence (r_n), we can define ν on the set of all AR3, AR6, or AR9 systems.*

In particular, one of these possible measures ν coincides with the measure of maximal entropy for the suspension flow of the Rauzy gasket built in [7], see also [8].

Theorem 4.11. *The hypothesis of Proposition 4.9 is satisfied by ν-almost every AR3, AR6, or AR9 system.*

4.4 Non unique ergodicity

Theorem 4.12. *If $\sum_{n=1}^{+\infty} \frac{1}{k_n} < +\infty$, each corresponding AR9 or AR6 symbolic system or interval exchange is not uniquely ergodic; it has two ergodic invariant measures; it is measure-theoretically isomorphic to its AR3 coding if and only if it is equipped with an ergodic measure,*

Note that in the only family of counter-examples we have, the two-point extension of Proposition 4.6 is rather degenerate, being ergodic only when the measure is concentrated on one copy of the factor.

5 Weak mixing

Definition 5.1. *If (X', U, μ_0) is a finite measure-preserving dynamical system, a real number $0 \leq \theta < 1$ is a* measurable eigenvalue *(denoted additively) if there exists a non-constant f in $\mathcal{L}^1(X', \mathbb{R}/\mathbb{Z})$ such that $f \circ U = f + \theta$ (in $\mathcal{L}^1(X', \mathbb{R}/\mathbb{Z})$); f is then an* eigenfunction *for the eigenvalue θ.*

As constants are not eigenfunctions, $\theta = 0$ is not an eigenvalue if U is ergodic.

(X', U, μ_0) is weakly mixing *if it has no measurable eigenvalue.*

The existence of weak mixing for AR3 systems, proved in [11], came as a surprise; this existence persists for AR9 (and AR6) systems, because under the hypothesis $\sum_{n=1}^{+\infty} \frac{1}{k_n} < +\infty$, by Theorem 4.12 above the AR9 or AR6 system equipped with one of its ergodic measures is isomorphic to its AR3 coding, while by Theorem 2 of [11] this AR3 system is weakly mixing. The sufficient condition given in [11] for weak mixing of AR3 systems is weaker than the condition $\sum_{n=1}^{+\infty}\frac{1}{k_n} < +\infty$: we shall show now that under this sufficient conditions the AR9 systems are also weakly mixing, for any ergodic invariant measure. But indeed this raises more questions than gives answers, as we shall see in the discussion below.

Proposition 5.1. *An ergodic AR9 or AR6 system is weakly mixing if*

- k_{n_i+2} *is unbounded,*
- $$\sum_{i=1}^{+\infty}\frac{1}{k_{n_i+1}} < +\infty,$$
- $$\sum_{i=1}^{+\infty}\frac{1}{k_{n_i}} < +\infty,$$

where the n_i are the $n \geq 1$ for which the n-th multiplicative rule is of type Im.

We do not know whether this sufficient condition gives interesting new examples; it might help to find a weakly mixing AR9 system for which $\mu(E_1) = 1$ in the AR3 coding, but this we were not able to achieve. Indeed, starting from Lemma 4.7 as in Section 4.3, we are able to build such AR9 systems under the condition $\sum_{i=1}^{+\infty}\frac{1}{k_{n_i+1}} = +\infty$. while $\sum_{i=1}^{+\infty}\frac{1}{k_{n_i}}$ may be finite; we could also get these conditions by starting from Lemma 4.8 and imitating the proof of Proposition 4.9; this falls short of being compatible with the conditions of Proposition 5.1. Indeed, we conjecture that these conditions are not compatible with $\mu(E_1) = 1$, and not even with unique ergodicity; whether these conditions are necessary for weak mixing is not known either. It would be also very interesting to find a uniquely ergodic weakly mixing AR9, or a weakly mixing AR9 which is not isomorphic to its AR3 coding.

References

[1] T. ADAMS, S. FERENCZI, K. PETERSEN: Constructive symbolic presentations of rank one measure-preserving systems, *Colloq. Math.* 150 (2017), p. 243–255.

[2] P. ARNOUX: Un exemple de semi-conjugaison entre un échange d'intervalles et une translation sur le tore, *Bull. Soc. Math. France* 116 (1988), p. 489–500.

[3] P. ARNOUX, J. BERNAT, X. BRESSAUD: Geometrical models for substitutions, Exp. Math. 20 (2011), no. 1, p. 97–127.

[4] P. ARNOUX, Sh. ITO: Pisot substitutions and Rauzy fractals. Journées Montoises d'Informatique Théorique (Marne-la-Vallée, 2000), *Bull. Belg. Math. Soc. Simon Stevin* 8 (2001), no. 2, p. 181–207.

[5] P. ARNOUX, G. RAUZY: Représentation géométrique de suites de complexité $2n+1$, *Bull. Soc. Math. France* 119 (1991), p. 199–215.

[6] P. ARNOUX, S. STAROSTA: The Rauzy gasket, in Further developments in fractals and related fields, *Trends Math.*, Birkhaűser (2013), p. 1–23.

[7] A. AVILA, P. HUBERT, A. SKRIPCHENKO: Diffusion for chaotic plane Sections of 3-periodic plane surfaces, *Invent. Math.* 206 (2016), p. 109–146.

[8] A. AVILA, P. HUBERT, A. SKRIPCHENKO: On the Hausdorff dimension of the Rauzy gasket, *Bull. Soc. Math. France* 144 (2016), no. 3, p. 539–568.

[9] V. BERTHÉ, W. STEINER, J. THUSWALDNER: Geometry, dynamics and arithmetic of S-adic shifts; arXiv:1410.0331v4.

[10] M. BOSHERNITZAN: A unique ergodicity of minimal symbolic flows with linear block growth, *J. Analyse Math.* 44 (1984/85), p. 77–96.

[11] J. CASSAIGNE, S. FERENCZI, A. MESSAOUDI: Weak mixing and eigenvalues of Arnoux-Rauzy systems, *Ann. Inst. Fourier (Grenoble)* 56 (2006), p. 2315–2343.

[12] I. DYNNIKOV, A. SKRIPCHENKO: Symmetric band complexes of thin type and chaotic Sections which are not quite chaotic. (English summary) *Trans. Moscow Math. Soc.* 2015, p. 251–269.

[13] S. FERENCZI: Systems of finite rank, *Colloq. Math.* 73 (1997), p. 35–65.

[14] S. FERENCZI, P. HUBERT: Rigidity of interval exchanges, *J. Mod. Dyn.* 14 (2019), p. 153–177.

[15] M.S. KEANE: Interval exchange transformations, *Math. Zeitsch.* 141 (1975), p. 25–31.

[16] S. P. NOVIKOV: The Hamiltonian formalism and a multivalued analogue of Morse theory, *Uspekhi Mat. Nauk* 37 (1982), p. 3–49; translated in *Russian Math. Surveys* 37 (1982), p. 1–56.

[17] G. RAUZY: Nombres algébriques et substitutions, *Bull. Soc. Math. France* 110 (1982), p. 147–178.

Quantum Streaming Algorithm with Logarithmic Memory and Advice for Online Disjointness Problem

Kamil Khadiev[*] Aliya Khadieva[†] Yassine Hamoudi[‡]

Abstract

We consider quantum and classical (deterministic or randomize) streaming online algorithms with respect to competitive ratio. We consider online version of the well-known Disjointness problem (Checking is two sets are disjoint or not). We suggest a quantum online streaming algorithm (quantum automata) with single advice bit that is better than any classical online streaming algorithm even if it gets non constant numeber of advice bits.

Keywords: quantum computation, online algorithms, logarithmic space, streaming algorithms, online minimization problems, OBDD, computational complexity

Online algorithms are a well-known computational model for solving optimization problems. An online algorithm reads an input piece by piece and should return output variables after some of the input variables immediately, even if the answer depends on the whole input. An online algorithm should return the answer for minimizing an objective function. The most standard is the competitive ratio [27]. It is the ratio of the cost of the online algorithm's solution and the cost of a solution of an optimal offline algorithm. Typically, online algorithms have unlimited computational power. The main restriction is a lack of knowledge on future input variables. At the same time, it is quite interesting to solve online minimization problems in the case of a big input stream such that it cannot be stored in a memory. In that case, we can discuss online algorithms with restricted memory. As the algorithms, we can consider streaming algorithms. Especially, we want to restrict memory of quantum algorithms, because current and near-feature devices cannot manipulate many

[*] Smart Quantum Technologies Ltd., Kazan, Russia; Kazan Federal University, Kazan, Russia; e-mail: kamilhadi@gmail.com

[†] Faculty of Computing, University of Latvia, Riga, Latvia; Kazan Federal University, Kazan, Russia; e-mail: aliya.khadi@gmail.com

[‡] IRIF, Universit Paris Diderot, France; e-mail: hamoudi@irif.fr

qubits. Streaming algorithms (automata, branching programs) as online classical and quantum algorithms were considered in [11, 23, 14, 32, 31, 33, 28, 1, 30]. In a case of one-way streaming algorithms, it is known that quantum online streaming algorithms can be better than classical ones. This result was proven for sublogarithmic memory [32, 33] and polylogarithmic memory [31]. Another model that was considered by researchers is quantum online streaming algorithms with repeated test [40]. We are also interested in an *advice complexity* measure [34, 13, 10, 17, 16, 15]. In this case, an online algorithm gets some bits of advice about an input. A trusted *Adviser* sending these bits knows the whole input and has unlimited computational power. deterministic and randomized online algorithms with advice are considered in [25, 34, 12]. We compare the power of quantum online algorithms and classical ones in the case of using streaming algorithms with logarithmic memory. This question was not investigated before. Typically, the term “Adviser” is used in online algorithms theory; and the term “Oracle” in the case of other models. The question of comparing quantum and classical models was explored for streaming algorithms (OBDDs and automata) [35, 22, 3, 5, 4, 18, 39, 29, 8, 9, 35, 2, 20, 21, 19, 26].

There is one restriction of the previous example of a problem that can be solved quantumly better than classically in a case of logarithmic memory. It is not defined for any input and requires a pre-validation for checking that input is permissible. Such problems are called “promise problems” or ”partial functions”. In this work we consider the “total function” or problem that does not require a pre-validation for an input. As the problem we consider the `onlineDISJ` problem that is an online version of $DISJ(x, y)$ (the Disjointness Boolean function). The $DISJ$ function is defined on two binary strings $x = (x_1, \ldots, x_m)$ and $y = (y_1, \ldots, y_m)$, and $DISJ(x, y) = \neg \bigvee\limits_{i=1}^{m} x_i \wedge y_i$. We can interpret x and y as characteristic vectors of two sets $A, B \subset \{1, \ldots, m\}$. The result is 1 iff $A \cap B = \emptyset$.

We show that there is a quantum algorithm for `onlineDISJ` that is c-competitive with a single advice bit. At the same time, any classical algorithm with $o(\log n)$ advice bits is c'-competitive and $c' > c$, where n is a length of an input.

The paper is organized in the following way. We give definitions in Section 1. In Section 2 we present our results.

1 Preliminaries

An online minimization problem consists of a set $\mathcal{I}$ of inputs and a cost function. Each input $I \in \mathcal{I}$ is a sequence of requests $I = (x_1, \ldots, x_n)$. Furthermore, a set of feasible outputs $\mathcal{O}(I)$ (or solutions) is associated with each I; an output is a sequence of answers $O = (y_1, \ldots, y_n) \in \mathcal{O}(I)$. The cost function assigns a positive real value $cost(I, O)$ to $I \in \mathcal{I}$ and $O \in \mathcal{O}(I)$. An optimal solution for I is $O_{opt}(I) = argmin_{O \in \mathcal{O}(I)} cost(I, O)$.

Let us define an online algorithm for this problem as an algorithm which gets requests x_i from $I = (x_1, \ldots, x_n)$ one by one and should return answers y_i from $O = (y_1, \ldots, y_n)$ immediately, even if an optimal solution can depend on future requests. **A deterministic online algorithm** A computes the output sequence $A(I) = (y_1, \ldots, y_n)$ such that y_i is computed from $x_1, \ldots, x_i$. We say that a deterministic online algorithm A is *c-competitive* if there exists a non-negative constant α such that, for every n and for any input I, we have: $cost(I, A(I)) \leq c \cdot cost(I, Opt(I)) + \alpha$, where Opt is an optimal offline algorithm for the problem; $|I| \leq n$ and $|I|$ is a length of I. Also we call c the **competitive ratio** of A. An algorithm A is optimal if $c = 1, \alpha = 0$. **An online algorithm** A **with advice** computes an output sequence $A^{\phi}(I) = (y_1, \ldots, y_n)$ such that y_i is computed from $\phi, x_1, \ldots, x_i$, where ϕ is the message from the adviser, who knows the whole input. A is c-competitive with advice complexity $b = b(n)$ if there exists a constant $\alpha \geq 0$ such that, for every n and for any input I of size n, there exists some ϕ such that $cost(I, A^{\phi}(I)) \leq c \cdot cost(I, Opt(I)) + \alpha$ and $|\phi| \leq b$.

Next, let us define a randomized online algorithm. **A randomized online algorithm** R computes an output sequence $R^{\zeta} := R^{\zeta}(I) = (y_1, \cdots, y_n)$ such that y_i is computed from $\zeta, x_1, \cdots, x_i$, where ζ is a content of a random tape, i. e., an infinite binary sequence, where every bit is chosen uniformly at random and independently of all the others. By $cost(I, R^{\zeta}(I))$ we denote the random variable expressing the cost of the solution computed by R on I. R is c-competitive in expectation if there exists a non-negative constant α such that, for every I, we have $\mathbb{E}[cost(I, R^{\zeta}(I))] \leq c \cdot cost(I, Opt(I)) + \alpha$.

We use streaming algorithms for online minimization problems as online algorithms with restricted memory. You can read more about streaming algorithms in literature [37, 7]. Shortly, these are algorithms that use small size of memory and read input variables one by one. Suppose A is a **deterministic online streaming algorithm** with $s = s(n)$ bits of memory that processes an input $I = (x_1, \ldots, x_n)$. Then we can describe a state of memory for A by a vector $d^i = (d^i_1, \ldots, d^i_s) \in \{0, 1\}^s$ before reading an input variable x_{i+1}. The algorithm computes an output $A(I) = (y_1, \ldots, y_n)$ such that y_i depends on d^{i-1} and x_i; d^i depends on d^{i-1} and x_i. A **randomized online streaming algorithm** has a similar definition, but with respect to the definition of randomized online algorithm.

Let us consider a **quantum online streaming algorithm**. For some integers $n > n' > 0$, a quantum online algorithm Q with q qubits is defined on input $I = (x_1, \ldots, x_n) \in \{0, \ldots, \gamma - 1\}^n$ and outputs $(y_1, \ldots, y_{n'}) \in \{0, \ldots, \beta - 1\}^{n'}$. Here γ and β are given integers that are sizes of input and output alphabets, respectively. A memory of the quantum algorithm is a state of a quantum register of q qubits. In other words, the computation of Q on an input I can be traced by a 2^q-dimensional vector from Hilbert space over the field of complex numbers. The initial state is the given 2^q-vector $|\psi\rangle_0$. In each step $j \in \{1, \ldots, n\}$ the input variable x_j is tested and then a unitary operator G^{x_j} is applied: $|\psi\rangle_j = G^{x_j}(|\psi\rangle_{j-1})$, where $|\psi\rangle_j$ represents the state of the system after the j-th step. If the algorithm reads some specific symbol, then it can measure one or more quantum bits. If the outcome of the measurement is u, then the algorithm continues computing from a state $|\psi(u)\rangle$ and it can output $Result(u)$ on this step, where $Result : \{0, \ldots, 2^q - 1\} \to \{0, \ldots, \beta - 1\}$ is a function that converts the result of a measurement to an output variable. The algorithm Q is c-competitive in expectation if there exists a non-negative constant α such that, for every I, $\mathbb{E}[cost(I, Q(I))] \leq c \cdot cost(I, Opt(I)) + \alpha$.

Let us describe the measurement process. Suppose that Q is in a state $|\psi\rangle = (v_1, \ldots, v_{2^q})$ before a measurement and the algorithm measures the i-th qubit. Suppose states with numbers $a^0_1, \ldots, a^0_{2^{q-1}}$ correspond to 0 value of the i-th qubit, and states with numbers $a^1_1, \ldots, a^1_{2^{q-1}}$ correspond to 1 value of the qubit. Then the result of the qubit's measurement is 1 with probability $pr_1 = \sum_{j=1}^{2^{q-1}} |v_{a^1_j}|^2$ and 0 with probability $pr_0 = 1 - pr_1$. If the algorithm measures v qubits on the j-th step, then $u \in \{0, \ldots, 2^v - 1\}$ is an outcome of the measurement.

An randomized online algorithm with advise, an randomized online streaming algorithm with advise, an deterministic online streaming algorithm with advise and an quantum online streaming algorithm with advise can be defined as deterministic online algorithm with advice with respect to corresponding definitions.

2 Main Results

Let us define $\texttt{onlineDISJ}_\texttt{t}$ problem that is based on the Disjointness Boolean function. The $DISJ : \{0,1\}^m \times \{0,1\}^m \to \{0,1\}$ function is such that $DISJ(x,y) = \neg \bigvee_{i=1}^m x_i \wedge y_i$. The problem $\texttt{onlineDISJ}_{t,k,r,w}$ is the following, for some integers k, t, r and w such that $k \bmod t = 0$, $r < w$. An input $I = (x_1, \ldots, x_n) \in \{0, \ldots, 6\}^n$ has the following structure: $I = 6\ Z^1\ 6\ Z^2\ 6 \ldots 5\ Z^k$, where $Z^i \in \{0, \ldots, 5\}^*$ for $i \in \{1, \ldots, k\}$. Let the length of I be $|I| = n$ for some integer n. Let $MDISJ(Z^i) = 1$ iff the following properties are right for some constant

$\varepsilon'' > 0$:

1. $Z^i = M^i\ 5\ x^{i,1}\ 2\ y^{i,1}\ 3\ z^{i,1}\ 4 \dots 4\ x^{i,m_i}\ 2\ y^{i,m_i}\ 3\ z^{i,m_i}\ 4$, for $M^i, x^{i,j}, y^{i,j}, z^{i,j} \in \{0,1\}^*$ and some integer m_i;
2. $x^{i,1} = x^{i,2} = \dots = x^{i,m_i}$, d $y^{i,1} = y^{i,2} = \dots = y^{i,m_i}$ and $z^{i,1} = z^{i,2} = \dots = z^{i,m_i}$;
3. $x^{i,1} = z^{i,1}$;
4. $|x^{i,1}| = |y^{i,1}|$, where $|v|$ is a length of a vector v;
5. $val(M^i) = m_i = 2 + 2^{-\log \varepsilon''} \cdot \frac{\pi}{4} \cdot \lceil \sqrt{|x^{i,1}|} \rceil$, where $val(M^i)$ is a number which binary representation is M^i.
6. $DISJ(x^{i,1}, y^{i,1}) = 1$.

The similar idea of the problem was used in [35, 36].

Let $g_i = \bigoplus_{j=i}^{k} MDISJ(Z^j)$. We consider only output variables that correspond to $x_j = 6$. Let these variables be $O' = (y_1, \dots, y_k)$. The cost function is $cost(I, O') = kw + (r - w) \cdot \sum_{r=0}^{k/t} \prod_{j=r\cdot(t-1)}^{r\cdot t-1} \delta(g_j, y_j)$, where $\delta(a,b) = 1$ if $a = b$ and $\delta(a,b) = 0$ otherwise. Note that k and t are parameters of the problem such that $k \bmod t = 0$; and r and w are parameters of the problem such that $r < w$. The cost function means the following. We split the output to k/t blocks of size t. Then, we say that if all output variables y_j of a block are right, i.e. $y_j = g_j$, then the block is "right" and the cost of the block is r. Otherwise, the block is wrong and it costs w. A cost of the whole input is the sum of costs of all blocks. We want to construct an algorithm that minimizes a cost of an input.

Our results are based on result for comparing two Boolean strings:

Lemma 1 ([6, 29]) *There is a bounded error quantum streaming algorithm for checking equality of two binary strings of length d. The algorithm uses $O(\log d)$ qubits and has ε' error for some constant $\varepsilon' > 0$.*

Additionally, we use a property of the Disjointness Boolean function:

Lemma 2 ([35, 38]) *Suppose we have a promise that the first four properties of $MDISJ(Z^i)$ are right. If $b = |x^{i,1}|$ and $m_i < b$, then there is no bounded error randomized (probabilistic) streaming algorithm for $MDISJ(Z^i)$ that uses $o(b/m_i)$ bits of memory.*

Let us discuss a quantum streaming algorithm for $MDISJ$ function.

Lemma 3 *There is a bounded error quantum streaming algorithm for $MDISJ(Z^i)$ that uses $O(\log d)$ qubits of memory and has ε error probability for some $\varepsilon > \varepsilon'' > 0$ and $d = |Z^i|$.*

Proof. (Sketch) Let us present a quantum streaming algorithm for $MDISJ(Z^i)$. We run five procedures in a parallel way. The procedures check the following properties:

1. $Z^i = \{0,1\}^*5(\{0,1\}^b2\{0,1\}^b3\{0,1\}^b4)^*$ for some integer b, where * means repeating the string several times;
2. $val(M^i) = m_i = 2 + 2^{-\log \varepsilon''} \cdot \frac{\pi}{4} \cdot \lceil \sqrt{|x^{i,1}|} \rceil$
3. $x^{i,1} = \ldots = x^{i,m_i}$, $y^{i,1} = \ldots = y^{i,m_i}$ and $z^{i,1} = \ldots = z^{i,m_i}$;
4. $x^{i,1} = z^{i,1}$;
5. $DISJ(x^{i,1}, y^{i,1}) = 1$.

Let $d = \log_2 |Z^i|$, where $|Z^i|$ is a length of Z^i.

The first procedure is a simple deterministic procedure that uses only $O(d)$ bits of memory that checks the first property. The second algorithm is a deterministic procedure that stores M^i and computes m_i that is a number of 4s and 5s. Then, it checks the equality $val(M^i) = m_i = 2 + 2^{-\log \varepsilon''} \cdot \frac{\pi}{4} \cdot \lceil \sqrt{b} \rceil$, where $b = |x^{i,1}|$.

The third procedure is a quantum procedure that is based on quantum fingerprinting technique. We construct two strings: $s^1 = x^{i,1} \circ y^{i,1} \circ z^{i,1} \circ x^{i,2} \circ y^{i,2} \circ z^{i,2} \circ \ldots \circ x^{i,m_i-1} \circ y^{i,m_i-1} \circ z^{i,m_i-1}$, $s^2 = x^{i,2} \circ y^{i,2} \circ z^{i,2} \circ x^{i,3} \circ y^{i,3} \circ z^{i,3} \circ \ldots \circ x^{i,m_i} \circ y^{i,m_i} \circ z^{i,m_i}$, where "$\circ$" operation is concatenation. If $s^1 = s^2$, then $x^{i,1} = x^{i,2}, x^{i,2} = x^{i,3}, \ldots, x^{i,m_i-1} = x^{i,m_i}$, $y^{i,1} = y^{i,2}, y^{i,2} = y^{i,3}, \ldots, y^{i,m_i-1} = y^{i,m_i}$ and $z^{i,1} = z^{i,2}, z^{i,2} = z^{i,3}, \ldots, z^{i,m_i-1} = z^{i,m_i}$. Using the algorithm from Lemma 1, we can construct a quantum algorithm that checks the equality of these strings with bounded error ε' and uses $O(d)$ qubits for some constant $\varepsilon' > 0$.

The forth procedure is quantum. It is similar to the procedure that checks the third property. We want to check equality of $x^{i,1}$ and $z^{i,1}$.

The fifth procedure is modification of the algorithm from [35, 36]. The algorithm is based on Grover's Search Algorithm [24]. It uses $O(\log d)$ qubits and has $O(\varepsilon'')$ error probability, where $d = |Z^i|$. □

Additionally, let us discuss properties of `onlineDISJ` construction with respect to the function $MDISJ$. Assume, that we have online minimization problem P_f that is defined similar to `onlineDISJ`, but function $MDISJ$ is replaced by f. For example, P_{MDISJ} is exactly `onlineDISJ`. The problem P_f has two following properties:

Lemma 4 ([31]) *Let a Boolean function f be such that there is a quantum streaming algorithm R that computes f with bounded error ε using s qubits of memory, where $0 \leq \varepsilon < 0.5$. Then there is a quantum online streaming algorithm A using at most $s+1$ qubits of memory, single advice bit and solving P_f such that the expected competitive ratio is $c \leq \left(0.5(1-\varepsilon)^{z-1} \cdot \left(t+1+\frac{v^t-v}{v-1}\right)(r-w)+\right.$ for $v = (1-2\varepsilon)^z, z = k/t$. If $\varepsilon = 0$, then $c = 1$.*

Lemma 5 ([31]) *Let a Boolean function f be such that there are no randomized streaming algorithms that compute f using space less than s bits. Then any randomized online streaming algorithm A using space less than $s-b$ bits, b advice bits and solving P_f, has the expected competitive ratio $c \geq (hr+\delta_u\cdot(2^{u-z}r+(1-2^{u-z})w)+(t-h-\delta_u)(2^{-z}r+(1-2^{-z})w))/(tr)$, for $h = \lfloor v/z \rfloor, z = k/t, u = v-hz$, v is such that $b = (1+(1-v/k)\log_2(1-v/k)+(v/k)\log_2(v/k))\,k$, $0.5k \leq v < k$.*

The next two theorems show a competitive ratio of algorithms for `onlineDISJ` problem:

Theorem 1 *There is the c-competitive in expectation quantum online streaming algorithm Q with $O(\log n)$ qubits of memory for* `onlineDISJ` *that uses single advice bit, where*
$c \leq \left(0.5(1-\varepsilon)^{z-1} \cdot \left(t+1+\frac{v^t-v}{v-1}\right)(r-w)+tw\right)/(tr) = \mathcal{C}_Q$, for $v = (1-2\varepsilon)^z, z = k/t$ and some constant $\varepsilon > 0$.

Proof. The idea of the online algorithm is the following. The algorithm gets g_1 as an advice bit. The result will be y_1. Then, we can compute $MDISJ(Z^1)$ and $y_2 = y_1 \oplus MDISJ(Z^1)$, and so on. $y_i = y_{i-1} \oplus MDISJ(Z^{i-1})$. By Lemma 4 and Lemma 3, we can show that $c \leq \mathcal{C}_Q$. □

Theorem 2 *Any randomized online streaming algorithm Q with $o(\log n)$ advice bits and $O(\log n)$ bits of memory for* `onlineDISJ` *is c'-competitive in expectation, where $c' > (hr+\delta_u\cdot(2^{u-z}r+(1-2^{u-z})w)+(t-h-\delta_u)(2^{-z}r+(1-2^{-z})w))/(tr) = \mathcal{C}_R > \mathcal{C}_Q$, for $h = \lfloor v/z \rfloor, z = k/t, u = v-hz$, v is such that $b = (1+(1-v/k)\log_2(1-v/k)+(v/k)\log_2(v/k))\,k$, $0.5k \leq v < k$.*

Proof. According to Lemma 2, we cannot construct a bounded error randomized streaming algorithm for $MDISJ$. By Lemma 5, we can show that $c' > \mathcal{C}_R > \mathcal{C}_Q$. □

So, two previous theorems show that the provided quantum online streaming algorithm with single advice bit has better competitive ratio than classical online algorithms in a case of logarithmic memory and sublogarithmic number of advice bits.

Acknowledgments The work is supported by Russian Scientific Found, project No. 17–71–10152.

References

[1] F. Ablayev, M. Ablayev, K. Khadiev, and A. Vasiliev. Classical and quantum computations with restricted memory. *LNCS*, 11011:129–155, 2018.

[2] F. Ablayev, A. Ambainis, K. Khadiev, and A. Khadieva. Lower bounds and hierarchies for quantum memoryless communication protocols and quantum ordered binary decision diagrams with repeated test. *In SOFSEM, LNCS*, 10706:197–211, 2018.

[3] F. Ablayev, A. Gainutdinova, M. Karpinski, C. Moore, and C. Pollett. On the computational power of probabilistic and quantum branching program. *Information and Computation*, 203(2):145–162, 2005.

[4] F. Ablayev, A. Gainutdinova, K. Khadiev, and A. Yakaryılmaz. Very narrow quantum OBDDs and width hierarchies for classical OBDDs. *Lobachevskii Journal of Mathematics*, 37(6):670–682, 2016.

[5] F. Ablayev, A. Gainutdinova, K. Khadiev, and A. Yakarylmaz. Very narrow quantum OBDDs and width hierarchies for classical OBDDs. In *DCFS*, volume 8614 of *LNCS*, pages 53–64. Springer, 2014.

[6] F. Ablayev and A. Vasilyev. On quantum realisation of boolean functions by the fingerprinting technique. *Discrete Mathematics and Applications*, 19(6):555–572, 2009.

[7] C. C. Aggarwal and C. K. Reddy. *Data Clustering: Algorithms and Applications.* CRC press, 2013.

[8] A. Ambainis and A. Yakaryılmaz. Superiority of exact quantum automata for promise problems. *Information Processing Letters*, 112(7):289–291, 2012.

[9] A. Ambainis and A. Yakaryılmaz. Automata and quantum computing. Technical Report 1507.01988, arXiv, 2015.

[10] H.-J. Bckenhauer, D. Komm, R. Krlovi, R. Krlovi, and . Mmke. On the advice complexity of online problems. *In ISAAC 2009, LNCS*, 5878:331–340, 2009.

[11] L. Becchetti and E. Koutsoupias. Competitive analysis of aggregate max in windowed streaming. In *ICALP*, volume 5555 of *LNCS*, pages 156–170, 2009.

[12] H.-J. Böckenhauer, J. Hromkovič, D. Komm, R. Královič, and P. Rossmanith. On the power of randomness versus advice in online computation. In *Languages Alive*, pages 30–43. Springer, 2012.

[13] J. Boyar, L.M Favrholdt, C. Kudahl, K.S. Larsen, and J.W. Mikkelsen. Online algorithms with advice: A survey. *ACM Computing Surveys*, 50(2):19, 2017.

[14] J. Boyar, K. S. Larsen, and A. Maiti. The frequent items problem in online streaming under various performance measures. *International Journal of Foundations of Computer Science*, 26(4):413–439, 2015.

[15] S. Dobrev, R. Královič, and D. Pardubská. How much information about the future is needed? In *SOFSEM*, pages 247–258. Springer, 2008.

[16] Y. Emek, P. Fraigniaud, A. Korman, and A. Rosén. Online computation with advice. In *ICALP*, pages 427–438. Springer, 2009.

[17] Y. Emek, P. Fraigniaud, A. Korman, and A. Rosén. Online computation with advice. *Theoretical Computer Science*, 412(24):2642–2656, 2011.

[18] A. Gainutdinova. Comparative complexity of quantum and classical OBDDs for total and partial functions. *Russian Mathematics*, 59(11):26–35, 2015.

[19] A. Gainutdinova and A. Yakaryılmaz. Unary probabilistic and quantum automata on promise problems. In *Developments in Language Theory*, pages 252–263. Springer, 2015.

[20] A. Gainutdinova and A. Yakaryılmaz. Nondeterministic unitary OBDDs. In *CSR 2017*, pages 126–140. Springer, 2017.

[21] A. Gainutdinova and A. Yakaryılmaz. Unary probabilistic and quantum automata on promise problems. *Quantum Information Processing*, 17(2):28, 2018.

[22] D. Gavinsky, J. Kempe, I. Kerenidis, R. Raz, and R. de Wolf. Exponential separations for one-way quantum communication complexity, with applications to cryptography. In *STOC '07*, pages 516–525, 2007.

[23] Y. Giannakopoulos and E. Koutsoupias. Competitive analysis of maintaining frequent items of a stream. *Theoretical Computer Science*, 562:23–32, 2015.

[24] Lov K Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pages 212–219. ACM, 1996.

[25] J. Hromkovic. Design and analysis of randomized algorithms: Introduction to design paradigms, 2005.

[26] R. Ibrahimov, K. Khadiev, K. Prūsis, and A. Yakarylmaz. Error-free affine, unitary, and probabilistic OBDDs. *Lecture Notes in Computer Science*, 10952 LNCS:175–187, 2018.

[27] A. R Karlin, M. S Manasse, L. Rudolph, and D. D Sleator. Competitive snoopy caching. In *FOCS, 1986., 27th Annual Symposium on*, pages 244–254. IEEE, 1986.

[28] K. Khadiev and A. Khadieva. Quantum automata for online minimization problems. In *Ninth Workshop on NCMA 2017 Short Papaers*, pages 25–33. Institute fur Computersprachen TU Wien, 2017.

[29] K. Khadiev and A. Khadieva. Reordering method and hierarchies for quantum and classical ordered binary decision diagrams. In *CSR 2017*, volume 10304 of *LNCS*, pages 162–175. Springer, 2017.

[30] K. Khadiev and A. Khadieva. Two-way quantum and classical machines with small memory for online minimization problems. In *International Conference on Micro- and Nano-Electronics 2018*, volume 11022 of *Proc. SPIE*, page 110222T, 2019.

[31] K. Khadiev, A. Khadieva, D. Kravchenko, A. Rivosh, and I. Yamilov, R.and Mannapov. Quantum versus classical online algorithms with advice and logarithmic space. *arXiv:1710.09595*, 2017.

[32] K. Khadiev, A. Khadieva, and I. Mannapov. Quantum online algorithms with respect to space and advice complexity. *Lobachevskii Journal of Mathematics*, 39(9):1210–1220, 2018.

[33] K. Khadiev, M. Ziatdinov, I. Mannapov, A. Khadieva, and R. Yamilov. Quantum online streaming algorithms with constant number of advice bits. *arXiv:1802.05134*, 2018.

[34] Dennis Komm. *An Introduction to Online Computation: Determinism, Randomization, Advice.* Springer, 2016.

[35] François Le Gall. Exponential separation of quantum and classical online space complexity. SPAA '06, pages 67–73. ACM, 2006.

[36] François Le Gall. Exponential separation of quantum and classical online space complexity. *Theory of Computing Systems*, 45(2):188–202, 2009.

[37] S. Muthukrishnan. Data streams: Algorithms and applications. *Foundations and Trends® in Theoretical Computer Science*, 1(2):117–236, 2005.

[38] Alexander A Razborov. On the distributional complexity of disjointness. In *International Colloquium on Automata, Languages, and Programming*, pages 249–253. Springer, 1990.

[39] M. Sauerhoff and D. Sieling. Quantum branching programs and space-bounded nonuniform quantum complexity. *Theoretical Computer Science*, 334(1):177–225, 2005.

[40] Q. Yuan. *Quantum online algorithms.* UC Santa Barbara, 2009. PhD thesis.

LL(1) linear grammars are as powerful as LL(k) linear grammars*

Alexander Okhotin
Ilya Olkhovsky
St. Petersburg State University, , Saint Petersburg 199034, Russia
alexander.okhotin@spbu.ru, ilianolhin@gmail.com

April 17, 2019

Abstract

It is proved that every LL(k) linear grammar has an equivalent LL(1) linear grammar, that is, for linear grammars there is no hierarchy with respect to the length of the look-ahead.

1 Introduction

The LL(k) parsing is one of the most well-known linear-time parsing techniques. In this method, a parse tree of an input string is reconstructed top-down, along with reading the string from left to right. A parser selects each rule by looking ahead by at most k symbol. The family of *LL(k) grammars*, to which this algorithm is applicable, was introduced and systematically studied in the papers by Knuth [3], Lewis and Stearns [5] and Rozenkrantz and Stearns [6]. In particular, Kurki-Suonio [4] and, independently, Rozenkrantz and Stearns [6], proved that $LL(k+1)$ grammars are more powerful than $LL(k)$ grammars, and thus there is a strict hierarchy of languages defined by LL(k) grammars, with different k.

An important subclass of $LL(k)$ grammars, the *LL(k)-linear grammars*, was first studied by Ibarra et al. [2] and by Holzer and Lange [1], who proved that the languages defined by these grammars are in the complexity class NC^1. However,

*Research supported by RFBR grant 18-31-00118.

the natural question of whether LL(k)-linear grammars also form a hierarchy with respect to the length of the look-ahead k, remains uninvestigated.

This paper demonstrates that in the case of LL(k)-linear grammars, the hierarchy with respect to k collapses, that is, all languages defined by LL(k)-linear grammars, for some k, are defined by LL(1)-linear grammars. The proof is constructive: it is shown how to transform any given LL(k)-linear grammar to a LL(1)-linear grammar that defines the same language.

2 Definitions

Definition 1 *A (formal) grammar is a quadruple $G = (\Sigma, N, R, S)$, where Σ is the* alphabet *of the language being defined, N is the set of syntactic categories defined in the grammar, known as* nonterminal symbols*; R is a finite set of rules, each of the form $A \to \alpha$, with $A \in N$ and $\alpha \in (\Sigma \cup N)^*$, and $S \in N$ is a nonterminal symbol representing all well-formed sentences in the language, known as the* initial symbol.

Each rule $A \to X_1 \ldots X_\ell$ in R states that each string representable as a concatenation of ℓ substrings of the form $X_1, \ldots, X_\ell$, therefore has the property A.

A grammar is called linear*, if each rule in R is of the form $A \to uBv$, with $u, v \in \Sigma^*$ and $B \in N$, or of the form $A \to w$, with $w \in \Sigma^*$.*

A top-down parser attempts to construct a parse tree of an input string, while reading it from left to right. At every point of its computation, the parser's memory configuration is a pair (α, v), where v is the unread portion of the input string uv. The parser tries to parse v as a concatenation $\alpha = X_1 \ldots X_\ell$, where $\ell \geqslant 0$ and $X_1, \ldots, X_\ell \in \Sigma \cup N$. This sequence of symbols is stored in a stack, with X_1 as the top of the stack.

At each point of the computation, the parser sees the top symbol of the stack and the first k symbols of the unread input (the *look-ahead string*), where $k \geqslant 1$ is a constant. If there is a nonterminal symbol $A \in N$ at the top of the stack, the parser determines a rule $A \to \alpha$ for this symbol, pops this symbol, and pushes the right-hand side of the rule onto the stack.

$$(A\beta, v) \xrightarrow{A \to \alpha} (\alpha\beta, v)$$

The rule is chosen by accessing a look-up table $T_k \colon N \times \Sigma^{\leqslant k} \to R \cup \{-\}$, which contains either a rule to apply, or a marker indicating a syntax error.

If the top symbol of the stack is a symbol $a \in \Sigma$, the parser checks that the unread portion of the input begins with the same symbol, and then pops this symbol from the stack and reads it from the input.

$$(a\beta, av) \xrightarrow{\text{READ } a} (\beta, v)$$

For a string $w \in \Sigma^*$, denote its first k symbols, with $k \geqslant 0$, by

$$\mathrm{First}_k(w) = \begin{cases} w, & \text{if } |w| \leqslant k \\ \text{first } k \text{ symbols of } w, & \text{if } |w| > k \end{cases}$$

This definition is extended to languages as $\mathrm{First}_k(L) = \{\, \mathrm{First}_k(w) \mid w \in L \,\}$.

Definition 2 *Let $k \geqslant 1$ and let $G = (\Sigma, N, R, S)$ be a grammar. An LL(k) table for G is a partial function $T_k \colon N \times \Sigma^{\leqslant k} \to R$ that satisfies the following condition: for all $A \in N$, $u, v \in \Sigma^*$ if, for every parse tree and for every subtree in that tree, if $A \in N$ is the label of its root, $A \to \alpha$ is the rule applied to A, and $v \in \Sigma^*$ is the suffix to the right of this subtree, then $T_k(A, \mathrm{First}_k(v)) = A \to \alpha$.*

If such a table exists, then the grammar is said to be LL(k).

3 General plan of the transformation

The goal of this paper is to transform an arbitrary linear LL(k) grammar G to a linear LL(1) grammar G' that defines the same language. If there is a nonterminal symbol A in the original grammar, then choosing a rule for A requires knowing the next k symbols of the input. The general plan is to use a *buffer* for up to $k-1$ next input symbols, so that the parser reads them before having to choose a rule for A. In the new grammar, this buffer shall be attached to every nonterminal symbol, so that they are of the form ${}_uA$, with $A \in N$ and $u \in \Sigma^{\leqslant k-1}$. The goal is to have $L_{G'}({}_uA) = \{\, w \mid uw \in L_G(A) \,\}$.

Upon a closer inspection, there is a certain problem with this plan. If there is a rule $A \to s$ in the original grammar, with $s \in \Sigma^*$ and $|s| < k-1$, then, in order to choose a rule for A, an LL(1) parser needs to know *more symbols than there are in s and in its own 1-symbol lookahead.* If there are $k-1$ symbols in the buffer attached to A as a subscript, and this "short" rule $A \to s$ is to be applied, then what is this nonterminal symbol supposed to do with the surplus symbols in the buffer?

Example 3 *The following grammar is linear LL(3).*

$$S \to aabSa \mid a$$

In order to distinguish between these two rules, a hypothetical LL(1) parser buffers up to two first symbols using the following rules.

$$
\begin{aligned}
{}_{\varepsilon}S &\to a_{a}S \\
{}_{a}S &\to a_{aa}S
\end{aligned}
$$

Once the parser has aa in the buffer and sees that the next symbol is b, it continues as planned.

$$ {}_{aa}S \to b_{\varepsilon}Sa $$

However, if aa is in the buffer and the next symbol is a, then the parser realizes that the first symbol in its buffer should have been used in the rule $A \to a$, whereas the second a in its buffer should have been matched by the last symbol in some earlier rule $S \to aabSa$, and there seems to be no natural way to apply that rule retroactively.

The cause of this problem is a *short rule* that defines a substring of length less than $k-1$ in the middle of the input. Accordingly, the first step of the proposed transformation is to eliminate such rules.

4 Elimination of "short" rules

The first step in the transformation of a linear LL(k) grammar to a linear LL(1) grammar is the elimination of so-called *short rules*, that is, rules of the form $A \to s$, with $s \in \Sigma^{<k-1}$ and $\text{Follow}(A) \neq \{\varepsilon\}$.

Lemma 4 *For every linear LL(k) grammar $G = (\Sigma, N, R, S)$ there exists a linear LL(k) grammar G' and without short rules that defines the same language. The number of nonterminal symbols in the grammar G' is $|\Sigma^{\leqslant k-1}| \cdot |N|$.*

In the new grammar $G' = (\Sigma, N', R', S')$, nonterminals are of the form A_u, with $A \in N$ and $u \in \text{Follow}_{k-1}(A)$. The goal is that every nonterminal A_u defines all strings defined by A in G, with a suffix u appended: $L_{G'}(A_u) = \{\, xu \mid x \in L_G(A) \,\}$.

For every nonterminal symbol A_u and for every rule for A in G, the new grammar has a rule defined as follows. For a rule $A \to w_1 B w_2 \in R$, let s denote the first $k-1$ symbols of $w_2 u$, so that $st = w_2 u$ with $|s| = \min(|w_2 u|, k-1)$. The corresponding rule in G' defers the string s to the nonterminal B, and appends the rest of the symbols in the end; these include all the remaining symbols of u.

$$A_u \to w_1 B_s t$$

Once a rule $A \to s$ is reached, the corresponding rule in the new grammar appends the suffix to s.

$$A_u \to su$$

The correctness proof consists of the following claims.

Claim. If a string w is defined by A_u in the new grammar, then $w = xu$ and A defines x in the original grammar.

Claim. If a string x is defined by A in the original grammar, then A_u defines xu in the new grammar.

Claim. The new grammar has no short rules.

Claim. If the original grammar is LL(k), then so is the constructed grammar.

5 Reduction to one-symbol lookahead

Lemma 5 *For every LL(k) linear grammar $G = (\Sigma, N, R, S)$ without short rules, there exists and can be effectively constructed an LL(1) linear grammar $G' = (\Sigma, N', R', {}_\varepsilon S)$, with $N' = \{\, {}_u A \mid A \in N,\ u \in \Sigma^{\leqslant k-1} \,\}$, that describes the same language.*

Proof In the new grammar G', nonterminal symbols are of the form ${}_uA$, with $A \in N$ and $u \in \Sigma^*$. The left substript u of a nonterminal ${}_uA$ is a buffer storing up to $k-1$ last symbols read by a parser. The goal is to have $L_{G'}({}_uA) = \{\, w \mid uw \in L_G(A) \,\}$.

When the buffer is underfull, the parser reads extra symbols and appends them to the buffer. As soon as the buffer is filled, the parser sees a nonterminal symbol ${}_uA$ with $u \in \Sigma^{k-1}$, as well as a one-symbol look-ahead. Therefore, the parser has all k symbols needed to determine a rule to apply to A, which is given in the entry $T(A, u)$ in the LL(k) table for G. The buffer is updated along with simulating this rule: the first symbols of the rule for A are removed from the buffer, and all symbols remaining in the buffer are attached to the next nonterminal symbol, which is of the form ${}_vB$.

The initial symbol of the new grammar, ${}_\varepsilon S$, is S with an empty buffer. The buffer is filled by the following rules.

$${}_uA \to a\,{}_{ua}A \qquad\qquad (A \in N,\ |u| < k-1)$$

For each $A \in N$, $u \in \Sigma^{k-1}$ and $a \in \Sigma$ with $T(A, ua)$ defined, the new grammar contains at most one rule defined as follows. If $T(A, ua) = A \to sBt$, then one of u, s is a prefix of the other; there are two cases, depending on which string is longer.

$$\begin{aligned} {}_uA &\to s'{}_\varepsilon Bt \qquad && (s = us', \text{ for } s' \in \Sigma^*) \\ {}_uA &\to {}_vBt && (u = sv, \text{ for } v \in \Sigma^+) \end{aligned}$$

If $T(A, ua) = A \to s$, then it can be proved that $s = ux$, and a is the first symbol of x if $x \neq \varepsilon$. Then the following rule is included in the new grammar.

$${}_uA \to x$$

If the end of the string is visible: for $A \in N$ and $u \in \Sigma^{\leqslant k-1}$, with $T(A, u)$ defined.

$${}_uA \to \varepsilon$$

The resulting grammar is linear, and for each rule ${}_uA \to \alpha \in R'$ obtained from one of the rules in R, that rule can be uniquely reconstructed by processing $u\alpha$ as follows: $us'{}_\varepsilon Bt$ becomes sBt; $u_vBt = sv_vB$ becomes sBt by cancelling v and the buffer of B; ux remains as it is.

Claim. If $x \in L_{G'}({}_uA)$, then $ux \in L_G(A)$.

Induction on the length of the derivation of x in G'.

Claim. If $ux \in L_G(A)$, then $x \in L_{G'}({}_uA)$.

Induction on the length of the derivation of ux in G.

Claim. The grammar G' is LL(1).

Theorem 6 *For every linear LL(k) grammar there exists a linear LL(1) grammar that describes the same language.*

The construction incurs a blow-up by a factor of $|\Sigma|^{2k}$. Understanding whether this blow-up is necessary, or whether the construction could be improved, is left for future investigation.

References

[1] M. Holzer, K.-J. Lange, "On the complexities of linear LL(1) and LR(1) grammars", *Fundamentals of Computation Theory* (FCT 1993, Hungary, August 23–27, 1993), LNCS 710, 299–308.

[2] O. H. Ibarra, T. Jiang, B. Ravikumar, “Some subclasses of context-free languages in NC^1”, *Information Processing Letters*, 29:3 (1988), 111–117.

[3] D. E. Knuth, “Top-down syntax analysis”, *Acta Informatica*, 1 (1971), 79–110.

[4] R. Kurki-Suonio, “Notes on top-down languages”, *BIT Numerical Mathematics*, 9:3 (1969), 225–238.

[5] P. M. Lewis II, R. E. Stearns, “Syntax-directed transduction”, *Journal of the ACM*, 15:3 (1968), 465–488.

[6] D. J. Rosenkrantz, R. E. Stearns, “Properties of deterministic top-down grammars”, *Information and Control*, 17 (1970), 226–256.

Colorings of pseudoregular graphs

Svetlana N. Selezneva, Marina V. Melnik

Lomonosov Moscow State University,
Faculty of Computational Mathematics and Cybernetics,
e-mail: selezn@cs.msu.ru, melnikmv@cs.msu.ru

Graph coloring is to label the vertices of some given graph by integers, called colors, such that adjacent vertices receive different colors. For a positive integer k, the k-coloring problem is the problem to decide whether a graph can be colored with at most k colores. For each fixed $k \geqslant 3$, the k-coloring problem is NP-complete [1, 2]. Currently, the complexity of k-coloring is widely studied for graph classes with structure restrictions, in particular, for classes that can be characterized by forbidden induced subgraphs. The complexity classification of 3-coloring is obtained in [3, 4] for H-free graphs, where H is a fixed graph on at most six vertices. The complexity classification of 4-coloring is established in [4] for the case when H is a fixed graph on at most five vertices. The complexity of k-coloring is considered in [5–7] for P_m-free graphs, where P_m denotes the path on m vertices, $m \geqslant 1$. Some other results can be found in [8, 9]. In the paper, we restrict the degrees of vertices in graphs. It is well known that an n-subregular graph, i.e., a graph, in which the degree of each vertex is at most n, $n \geqslant 3$, is n-colorable if and only if it is K_{n+1}-free, where K_{n+1} denotes the complete graph on $(n+1)$ vertices [10]. We consider so called n-pseudoregular graphs, i.e., graphs, in which the degree of a single vertex is at most $(n+1)$, and the degrees of the rest vertices are at most n, $n \geqslant 3$.

We only consider finite undirected graphs without loops and multiple edges. We refer to [11] for any undefined graph terminology. A graph $H = (V', E')$ is called a subgraph of a graph $G = (V, E)$ if $V' \subseteq V$, $E' \subseteq E$, and it is called an induced subgraph if, in addition, $E' = \{(v, w) \in E \mid v, w \in V'\}$. Let $\{H_1, \ldots, H_m\}$ be a set of graphs, $m \geqslant 1$. A graph G is called $\{H_1, \ldots, H_m\}$-free if G has no induced subgraphs isomorphic to a graph in $\{H_1, \ldots, H_m\}$. The degree of a vertex v in a graph G, denoted by $d_G(v)$, is the number of edges incident with v in G. For a positive integer n, a graph $G = (V, E)$ is called n-subregular if $d_G(v) \leqslant n$ for each vertex $v \in V$, and it is called n-pseudoregular if there exists a vertex $v_0 \in V$ such that $d_G(v_0) \leqslant n + 1$, and $d_G(v) \leqslant n$ for each vertex $v \in V$, $v \neq v_0$. A (vertex) k-coloring of a graph $G = (V, E)$ is a mapping $\rho : V \to K$, where K is a set of k colors, i.e., $|K| = k$, such that $\rho(v) \neq \rho(w)$ whenever $(v, w) \in E$. We say that a graph G is k-colorable if there exists a k-coloring of G. The smallest positive integer k, for which a graph G is k-colorable, is called the chromatic number, $\chi(G)$, of G.

The graph K_n denotes the complete graph on n vertices, and the graph K_n^- denotes the graph that is K_n without an edge. Two vertices of K_n^- that is not adjacent are called special. Let G be an n-pseudoregular graph, $n \geqslant 3$, and $H = (V', E')$ be its induced subgraph isomorphic to K_n^- with special vertices w_1, w_2. Then the graph $G' = G : -H$ is constructed from G by deleting the all vertices in $V' \setminus \{w_1, w_2\}$ and then by identifing w_1 with w_2.

For a fixed positive integer k, the k-coloring problem is to decide whether a given graph is k-colorable.

In the paper, the following results are established.

Proposition 1. *Let G be an n-pseudoregular graph, H be its induced subgraph isomorphic to K_{n+1}^-, $n \geqslant 3$, and $G' = G : -H$. Then G is n-colorable if and only if G' is n-colorable.*

Theorem 1. *If $n \geqslant 3$, G is a $\{K_{n+1}, K_{n+1}^-\}$-free n-pseudoregular graph then $\chi(G) \leqslant n$.*

To prove Theorem 1 we introduce palettes which are a special type of graph list colorings [12]. If K is a set of colors then a palette on K for a graph $G = (V, E)$ is a mapping $\pi : V \to 2^K$ (where 2^K denotes the set of all subsets of K) such that $\pi(v) \neq \emptyset$ for each $v \in V$. If $|K| = k$ then the set of all palettes on K for G is denoted by $\pi_k(G)$. A coloring of a graph $G = (V, E)$ by a palette $\pi \in \pi_k(G)$ is a mapping $\rho : V \to K$ such that

1) $\rho(v) \in \pi(v)$ for each $v \in V$;

2) $\rho(v) \neq \rho(w)$ for each $(v, w) \in E$.

We prove the following Proposition 2 and Proposition 3.

Proposition 2. *Let $G = (V, E)$ be a graph, and $\pi \in \pi_k(G)$, $k \geqslant 3$, be a palette such that $|\pi(v)| = 2$ for each $v \in V$. Then,*

1) *for the case when G is an even simple cycle, there exists a coloring of G by π;*

2) *for the case when G is an odd simple cycle, there exists a coloring of G by π if and only if there exists a pair $v, w \in V$ such that $\pi(v) \neq \pi(w)$.*

Proposition 3. *Let $G = (V, E)$ be a graph, and $\pi \in \pi_k(G)$, $k \geqslant 3$, be a palette such that $|\pi(v)| = k - 1$ for each $v \in V$. Then, for the case when G is K_k, there exists a coloring of G by π if and only if there exists a pair $v, w \in V$ such that $\pi(v) \neq \pi(w)$.*

Proposition 2 and Proposition 3 are used to prove Theorem 1.

Proof of Theorem 1 (sketch). Let $G = (V, E)$ be a $\{K_{n+1}, K_{n+1}^-\}$-free n-pseudoregular graph, and $v_0 \in V$ where $d_G(v_0) \leqslant n + 1$. We consider the cases $n = 3$ and $n \geqslant 4$ separately.

1. Case $n = 3$. If G contains an induced even simple cycle $C = v_1, \ldots, v_m$, where $v_i \neq v_0$ for $i = 1, \ldots, m$, then we put $G' = G - \{v_1, \ldots, v_m\}$. We show that there exists a 3-coloring ρ' of G'. Then, based on the coloring ρ', we construct a palette $\pi \in \pi_3(C)$ such that $\pi(v_i) = 2$ for $i = 1, \ldots, m$. By Proposition 2, there exists a coloring ρ'' of C by π. Finally, the union of ρ' and ρ'' is a 3-coloring ρ of G. If G contains an induced odd simple cycle $C = v_1, \ldots, v_m$, where $v_i \neq v_0$ for $i = 1, \ldots, m$, then we put $G' = G - \{v_1, \ldots, v_m\} + (v_i, v_j)$ for some choice of the pair v_i, v_j. Then we continue similarly to an even cycle. If any cycle in G contains v_0 then we put $G' = G - v_0$. Then G' is a forest, therefore, G' is 2-colorable. To obtain a 3-coloring of G we label v_0 by the third color.

2. Case $n \geqslant 4$. If G contains a subgraph H on vertices $v_1, \ldots, v_n$, where $v_i \neq v_0$ for $i = 1, \ldots, n$, such that H is K_n, then we put $G' = G - \{v_1, \ldots, v_n\} + (v_i, v_j)$ for some choice of the pair v_i, v_j. We show that there exists an n-coloring ρ' of G'. Then, based on the coloring ρ', we construct a palette $\pi \in \pi_n(H)$ such that $\pi(v_i) = n - 1$ for $i = 1, \ldots, n$. By Proposition 3, there exists a coloring ρ'' of H by π. Finally, the union of ρ' and ρ'' is an n-coloring ρ of G. If G has no v_0-free subgraphs isomorphic to K_n then we construct G' by the following way. We find a set $W \subseteq V$ with the following properties: $v_0 \in W$; $(w', w'') \notin E$ for each $w', w'' \in W$; and, for each $v \in V \setminus W$, there exists $w \in W$ such that $(v, w) \in E$. If we put $G' = G - W$ then G' is an $(n-1)$-colorable. To obtain an n-coloring of G we label each vertex w from W by the n-th color.

The following Theorem 2 arises from Proposition 1 and Theorem 1.

Theorem 2. *For each fixed positive integer $n \geqslant 3$, the n-coloring problem for n-pseudoregular graphs is solvable in polynomial time.*

References

1. Stockmeyer L.J. Planar 3-colorability is NP-complete // SIGACT News. 1973. V. 5, N 3. P. 19–25.

2. Garey M. R., Johnson D. S., Stockmeyer L. Some simplified NP-complete graph problems // Theoretical Computer Science. 1976. V. 1. P. 237–267.

3. Broersma H., Golovach P. A., Paulusma D., Song J. Updating the complexity status of coloring graphs without a fixed induced linear forest // Theoretical Computer Science. 2012. V. 414, N 1. P. 9–19.

4. Golovach P., Paulusma D., Song J. 4-coloring H-free graphs when H is small // Discrete Applied Mathematics. 2013. V. 161, N 1–2. P. 140–150.

5. Hoang C. T., Kaminski M., Lozin V. V., Sawada J., Shu X. Deciding k-colorability of P_5-free graphs in polymomial time // Algorithmica. 2010. V. 57. P. 74–81.

6. Bonomo F., Chudnovsky M., Maceli P., Schaudt O., Stein M., Zhong M. Three-coloring and list three-coloring of graphs without induced paths on seven vertices // Combinatorica. 2017. P. 1–23.

7. Huang S. Improved complexity results on k-coloring P_t-free graphs // European Journal of Combinatorics. 2016. V. 51. P. 336–346.

8. Malyshev D. The complexity of the 3-colorability problem in the absence of a pair of small forbidden induced subgraphs // Discrete Mathematics. 2015. V. 338, N 11. P. 1860–1865.

9. Malyshev D. The complexity of the vertex 3-colorability problem for some hereditary classes defined by 5-vertex forbidden induced subgraphs // Graphs and Combinatorics. 2017. V. 33, N 4. P. 1009–1022.

10. Brooks R. L. On colouring the nodes of a network // Proc. Cambridge Philos. Soc. 1941. V. 37. P. 194–197.

11. Bondy J. A., Murty U. S. R. Graph Theory. Springer, 2008.

12. Vizing V. G. Vertex coloring of a graph in preassigned colors // Discrete Analysis Methods in the Theory of Codes and Schemes. V. 29. Novosibirsk, 1976. P. 3–10 (in Russian).

New Results on Codes for Location in Graphs

Ville Junnila, Tero Laihonen and Tuomo Lehtilä*
Department of Mathematics and Statistics
University of Turku, FI-20014 Turku, Finland
viljun@utu.fi, terolai@utu.fi and tualeh@utu.fi

1 Introduction

Sensor networks consist of sensors monitoring various places and connections between these places. We model a sensor network as a simple and undirected graph $G = (V(G), E(G)) = (V, E)$. In this context, a sensor can be placed on a vertex v and its closed neighbourhood $N[v]$ represents the set of locations that the sensor monitors. Besides assuming that graphs are simple and undirected, we also assume that they are connected and have cardinality at least two. In the following, we present some terminology and notation. The *closed neighbourhood* of v is defined $N[v] = N(v) \cup \{v\}$, where $N(v)$ is the *open neighbourhood* of v, that is, the set of vertices adjacent to v. A *code* C is a nonempty subset of V and its elements are *codewords*. The codeword $c \in C$ *covers* a vertex $v \in V$ if $v \in N[c]$. We denote the set of codewords covering v in G by

$$I(G, C; v) = I(G; v) = I(C; v) = I(v) = N[v] \cap C.$$

The set $I(v)$ is called an *identifying set* or an *I-set*. We say that a code $C \subseteq V$ is *dominating* in G if $I(C; u) \neq \emptyset$ for all $u \in V$. If the sensors are placed at the locations corresponding to the codewords, then each vertex is monitored by the sensors located in $I(v)$. More explanation regarding location detection in the sensor networks can be found in [1, 8, 12].

*Research supported by the University of Turku Graduate School (UTUGS) and the Vilho, Yrjö and Kalle Väisälä Foundation.

Let us now define *identifying codes*, which were first introduced by Karpovsky *et al.* in [7]. For numerous papers regarding identifying codes and related topics, the interested reader is referred to the online bibliography [9].

Definition 1. A code $C \subseteq V$ is *identifying* in G if for all distinct $u, v \in V$ we have $I(C; u) \neq \emptyset$ and

$$I(C; u) \neq I(C; v).$$

An identifying code C in a finite graph G with the smallest cardinality is called *optimal* and the number of codewords in an optimal identifying code is denoted by $\gamma^{ID}(G)$.

Identifying codes require unique I-sets for codewords as well as for non-codewords. However, if we omit the requirement of unique I-sets for codewords, then we obtain the following definition of *locating-dominating codes*, which were first introduced by Slater in [10, 13, 14].

Definition 2. A code $C \subseteq V$ is *locating-dominating* in G if for all distinct $u, v \in V \setminus C$ we have $I(C; u) \neq \emptyset$ and

$$I(C; u) \neq I(C; v).$$

Notice that an identifying code in G is also locating-dominating (by the definitions). In [4], self-locating-dominating and solid-locating-dominating codes have been introduced and, in [5, 6], they have been further studied. The definitions of these codes are given as follows.

Definition 3. Let $C \subseteq V$ be a code in G.

(i) We say that $C \subseteq V$ is *self-locating-dominating code* in G if for all $u \in V \setminus C$ we have $I(C; u) \neq \emptyset$ and

$$\bigcap_{c \in I(C;u)} N[c] = \{u\}.$$

(ii) We say that $C \subseteq V$ is *solid-locating-dominating code* in G if for all distinct $u, v \in V \setminus C$ we have

$$I(C; u) \setminus I(C; v) \neq \emptyset.$$

Observe that since G is a connected graph on at least two vertices, a self-locating-dominating and solid-locating-dominating code is always dominating. Analogously to identifying codes, in a finite graph G, we say that dominating, locating-dominating, self-locating-dominating and solid-locating-dominating codes with the smallest cardinalities are *optimal* and we denote the cardinality of an optimal code by $\gamma(G)$, $\gamma^{LD}(G), \gamma^{SLD}(G)$ and $\gamma^{DLD}(G)$, respectively.

In the following theorem, we offer characterizations of self-locating-dominating and solid-dominating codes for easier comparison of them.

Theorem 4 ([4]). *Let $G = (V, E)$ be a connected graph on at least two vertices:*

(i) A code $C \subseteq V$ is self-locating-dominating if and only if for all distinct $u \in V \setminus C$ and $v \in V$ we have

$$I(C; u) \setminus I(C; v) \neq \emptyset.$$

(ii) A code $C \subseteq V$ is solid-locating-dominating if and only if for all $u \in V \setminus C$ we have $I(C; u) \neq \emptyset$ and

$$\left(\bigcap_{c \in I(C;u)} N[c] \right) \setminus C = \{u\}.$$

Based on the previous theorem, we obtain the following corollary.

Corollary 5. *If C is a self-locating-dominating or solid-locating-dominating code in G, then C is also solid-locating-dominating or locating-dominating in G, respectively. Furthermore, for a finite graph G, we have*

$$\gamma^{LD}(G) \leq \gamma^{DLD}(G) \leq \gamma^{SLD}(G).$$

The structure of the paper is described as follows. First, in Section 2, we give optimal locating-dominating, self-locating-dominating and solid-locating-dominating codes in the direct product $K_n \times K_m$ of complete graphs, where $2 \leq n \leq m$ as well as optimal solid-locating-dominating codes for graphs $K_q \square K_q \square K_q$ with $q \geq 2$. Then, in Section 3, we obtain optimal self-locating-dominating and solid-locating-dominating codes in infinite king and triangular grids, i.e., the smallest possible codes regarding their density.

2 Products of complete graphs

A graph is called a *complete graph* on q vertices, denoted by K_q, if each pair of vertices of the graph is adjacent. The vertex set $V(K_q)$ is denoted by $\{1, 2, \ldots, q\}$. The *Cartesian product* of two graphs $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ is defined as $G_1 \square G_2 = (V_1 \times V_2, E)$, where E is a set of edges such that $(u_1, u_2)(v_1, v_2) \in E$ if and only if $u_1 = v_1$ and $u_2v_2 \in E_2$, or $u_2 = v_2$ and $u_1v_1 \in E_1$. The *direct product* of two graphs G_1 and G_2 is defined as $G_1 \times G_2 = (V_1 \times V_2, E)$, where $E = \{(u_1, u_2)(v_v, v_2) \mid u_1v_1 \in E_1 \text{ and } u_2v_2 \in E_2\}$. A *complement* of a graph $G = (V, E)$ is the graph $\overline{G} = (V, E')$ with the edge set E' being such that $uv \in E'$ if and only if $uv \notin E$.

In this section, we first give optimal locating-dominating, self-locating-dominating and solid-locating-dominating codes in the direct product $K_n \times K_m$, where $2 \leq n \leq m$. For location-domination and solid-location-domination, the results heavily depend on the exact values of $\gamma^{LD}(K_n \square K_m)$ and $\gamma^{DLD}(K_n \square K_m)$, which have been determined in [4]. In the graphs $K_n \times K_m$ and $K_n \square K_m$, the jth *row* (of $V(K_n) \times V(K_m)$) is denoted by R_j and it consists of the vertices $(1, j), (2, j), \ldots, (n, j)$. Analogously, the ith *column* is denoted by P_i and it consists of the vertices $(i, 1), (i, 2), \ldots, (i, m)$. Now we are ready to present the following observations:

- In the Cartesian product $K_n \square K_m$, the closed neighbourhood $N[(i, j)] = N[i, j]$ consists of the row R_j and the column P_i. Therefore, as the closed neighbourhood of a vertex resembles the movements of a rook in a chessboard, $K_n \square K_m$ is also sometimes called the *rook's graph*.

- In the direct product $K_n \times K_m$, we have $N((i, j)) = N(i, j) = V(K_n \square K_m) \setminus (R_j \cup P_i)$.

Due to the previous observations, we know that $\overline{K_n \square K_m} = K_n \times K_m$.

Recall that identification is a topic closely related to the various location-domination type problems. Previously, in [11], the identifying codes have been studied in the direct product $K_n \times K_m$ of complete graphs by Goddard and Wash. More precisely, they determined the exact values of $\gamma^{ID}(K_n \times K_m)$ for all m and n.

In what follows, we determine the exact values of $\gamma^{LD}(K_n \times K_m)$ for all m and n. For this purpose, we first present the following result concerning location-domination in the Cartesian product $K_n \square K_m$ of complete graphs given in [4].

Theorem 6 ([4], Theorem 14). *Let m and n be integers such that $2 \leq n \leq m$. Now we have*

$$\gamma^{LD}(K_n \square K_m) = \begin{cases} m - 1, & 2n \leq m, \\ \left\lceil \frac{2n+2m}{3} \right\rceil - 1, & n \leq m \leq 2n - 1. \end{cases}$$

There is a strong connection between the values of $\gamma^{LD}(K_n\square K_m)$ and $\gamma^{LD}(K_n\times K_m)$ as explained in the following. In [3], it has been shown that $|\gamma^{LD}(G)-\gamma^{LD}(\overline{G})|\leq 1$. Therefore, as $\overline{K_n\times K_m}=K_n\square K_m$, we obtain that $\gamma^{LD}(K_n\square K_m)-1\leq\gamma^{LD}(K_n\times K_m)\leq\gamma^{LD}(K_n\square K_m)+1$. This result is further sharpened in the following lemma.

Lemma 7. *For $2\leq n\leq m$ and $(n,m)\neq(2,4)$, we have*

$$\gamma^{LD}(K_n\square K_m)-1\leq\gamma^{LD}(K_n\times K_m)\leq\gamma^{LD}(K_n\square K_m).$$

If $\gamma^{LD}(K_n\times K_m)=\gamma^{LD}(K_n\square K_m)-1$, then the optimal locating-dominating code C in $K_n\times K_m$ has a non-codeword v such that $I(v)=C$.

Proof. First denote $G=K_n\square K_m$ and $H=K_n\times K_m$. The lower bound of the claim is immediate by the result preceding the lemma. For the upper bound, let C be an optimal locating-dominating code in G. The code C can also be viewed as a code in H. If we have $I(H;u)=I(H;v)$ for some non-codewords u and v, then a contradiction follows since $I(G;u)=C\setminus I(H;u)=C\setminus I(H;v)=I(G;v)$. Hence, we have $I(H;u)\neq I(H;v)$ for all distinct non-codewords u and v. Moreover, if $I(G;v)\neq C$ for each non-codeword v, then we also have $I(H;v)\neq\emptyset$, and the upper bound follows since C is a locating-dominating code in H.

Hence, we may assume that $I(G;v)=C$ for some non-codeword v. This implies that $C\subseteq P_i\cup R_j$ for some i,j. There exists at most one non-codeword in $P_i\setminus\{v\}$ since otherwise there are at least two non-codewords with the same I-set. Similarly, there exists at most one non-codeword in $R_j\setminus\{v\}$. Furthermore, if both $P_i\setminus\{v\}$ and $R_j\setminus\{v\}$ contain a non-codeword, then there exists a vertex with an empty I-set. Thus, in conclusion, there exists at most two non-codewords in $P_i\cup R_j$ and, hence, we have $|C|\geq n+m-3$. Dividing into the following cases depending on n and m, we next show that $|C|\geq n+m-3>\gamma^{LD}(G)$ in majority of the cases of the lemma:

- If $n\geq 3$ and $m\geq 2n$, then we have $\gamma^{LD}(G)=m-1<n+m-3\leq|C|$ (by Theorem 6).
- If $n\geq 4$, $n\leq m\leq 2n-1$ and $(n,m)\neq(4,4)$, then $\gamma^{LD}(G)=\lceil 2(n+m)/3\rceil-1<n+m-3\leq|C|$ (by Theorem 6).

Thus, if $n\geq 3$ and $m\geq 2n$, or $n\geq 4$, $n\leq m\leq 2n-1$ and $(n,m)\neq(4,4)$, then a contradiction with the optimality of C follows. Hence, in these cases, we have $\gamma^{LD}(H)\leq\gamma^{LD}(G)$. The rest of the cases are mostly small special cases which can be verified one by one (the details are omitted).

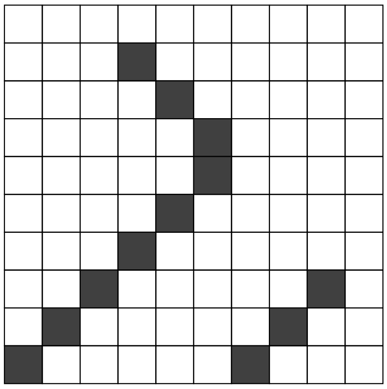

Figure 1: Optimal locating-dominating code for $K_{10} \times K_{10}$. Dark boxes are codewords.

Let then C' be a locating-dominating code in H. Similarly as above, we get that if $I(H; v) \neq C'$ for each non-codeword v, then C' is also a locating-dominating code in G. Therefore, if $\gamma^{LD}(H) = \gamma^{LD}(G) - 1$, then there exist a non-codeword v such that $I(H; v) = C'$. Thus, the last claim of the lemma follows. □

Now with the help of the previous lemma and Theorem 6, we determine the exact values of $\gamma^{LD}(K_m \times K_n)$ in the following theorem. The rather long and technical proof is omitted.

Theorem 8. *For $2 \leq n \leq m$ we have*

$$\gamma^{LD}(K_n \times K_m) = \begin{cases} m-1, & 2n \leq m \text{ and } (n,m) \neq (2,4), \\ \left\lceil \frac{2n+2m-1}{3} \right\rceil - 1, & 2 < n \leq m < 2n \text{ and } (m,n) \neq (4,4), \\ m, & n = 2, m \leq 4, \\ 5, & n = 4, m = 4. \end{cases}$$

Let us next briefly consider solid-location-domination. The following result has been shown in [4].

Theorem 9 ([4]). *For all integers m and n such that $m \geq n \geq 1$, we have*

$$\gamma^{DLD}(K_n \Box K_m) = \begin{cases} m, & 4 \leq 2n \leq m \text{ or } n = 2, \\ 2n, & 2 < n < m < 2n, \\ 2n-1, & 2 < m = n. \end{cases}$$

In the following theorem, we show that the cardinalities of optimal solid-locating-dominating codes are same for $K_n \times K_m$ and $K_n \Box K_m$.

Theorem 10. *For all integers m and n such that $m \geq n \geq 2$, we have*

$$\gamma^{DLD}(K_n \times K_m) = \gamma^{DLD}(K_n \square K_m).$$

Proof. By [6, Theorem 21], we have $\gamma^{DLD}(G) = \gamma^{DLD}(\overline{G})$ if G is not a discrete or a complete graph. Therefore, as this is the case for $G = K_n \times K_m$, we have $\gamma^{DLD}(K_n \times K_m) = \gamma^{DLD}(\overline{K_n \times K_m}) = \gamma^{DLD}(K_n \square K_m)$. □

Let us then consider self-location-domination. Unlike location-domination [3, Theorem 7] and solid-location-domination [6, Theorem 21], the optimal cardinality of a self-locating-dominating code in G does not depend on the one of the complement graph $\overline{G}$. In the following theorem, we first give the result presented in [4] regarding $\gamma^{SLD}(K_n \square K_m)$.

Theorem 11 ([4])**.** *For all integers m and n such that $m \geq n \geq 2$, we have*

$$\gamma^{SLD}(K_n \square K_m) = \begin{cases} m, & 2n \leq m, \\ 2n, & 2 \leq n < m < 2n, \\ 2n-1, & 2 < m = n, \\ 4, & n = m = 2. \end{cases}$$

In the following theorem, we determine the exact values of $\gamma^{SLD}(K_n \times K_m)$ for all values of m and n. Notice that $\gamma^{SLD}(K_n \square K_m) = \gamma^{SLD}(K_n \times K_m)$ if and only if $n = m$, $m = n + 1 > 3$, or $n = 2$ and $m \geq 4$ (the proof is omitted).

Theorem 12. *For all integers m and n such that $m \geq n \geq 2$, we have*

$$\gamma^{SLD}(K_n \times K_m) = \begin{cases} m+n-1, & n > 2, \\ m, & n = 2, m > 2, \\ 4, & n = m = 2. \end{cases}$$

Previously, in [5], an optimal self-locating-dominating code in $K_q \square K_q \square K_q$ has been presented as well as some upper and lower bounds for $\gamma^{ID}(K_q \square K_q \square K_q)$. In the following theorem, we present the optimal value for $\gamma^{DLD}(K_q \square K_q \square K_q)$, the proof is omitted.

Theorem 13. *We have for $q \geq 2$*

$$\gamma^{DLD}(K_q \square K_q \square K_q) = q^2.$$

3 Grids

In this section, we consider solid-location-domination and self-location-domination in the so called infinite king and triangular grids. Previously, for finite graphs, the optimality of a code has been defined using the minimum cardinality. However, this method is not valid for the infinite graphs of this section. Hence, we need to define the concept of *density* of a code. Let us first consider the *infinite king grid.*

Definition 14. Let $G = (V, E)$ be a graph with $V = \mathbb{Z}^2$ and for the vertices $v = (v_1, v_2) \in V$ and $u = (u_1, u_2) \in V$ we have $vu \in E$ if and only if $|v_1 - u_1| \leq 1$ and $|v_2 - u_2| \leq 1$. The obtained graph G is called the *infinite king grid.* Further let V_n be a subset of V such that $V_n = \{(x, y) \mid |x| \leq n, |y| \leq n\}$. The *density* of a code $C \subseteq V = \mathbb{Z}^2$ is now defined as

$$D(C) = \limsup_{n \to \infty} \frac{|C \cap V_n|}{|V_n|}.$$

We say that a code is *optimal* if there exists no other code with smaller density.

In what follows, we first consider solid-location-domination in the king grid. In the following theorem, we present a solid-locating-dominating code in the king grid with density 1/3. The code is illustrated in Figure 2. Later, in Theorem 17, it is shown that the code is optimal.

Theorem 15. *Let $G = (V, E)$ be the king grid. The code*

$$C = \big\{(x, y) \in \mathbb{Z}^2 \mid |x| + |y| \equiv 0 \pmod 3\big\}$$

is solid-locating-dominating in G and its density is $1/3$.

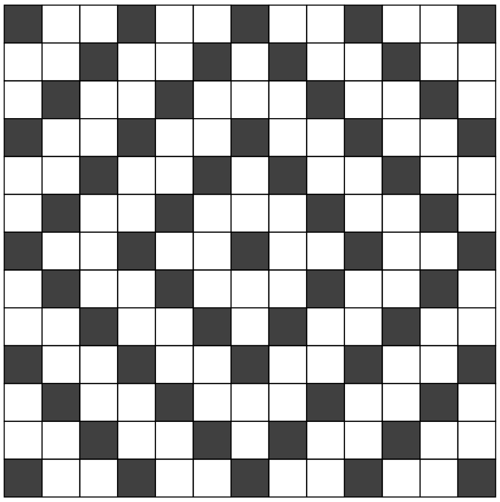

Figure 2: Solid-locating-dominating code of density $\frac{1}{3}$ in the king grid. The darkened squares are codewords.

In order to prove that the solid-locating-dominating code of the previous theorem is optimal, we first present the following lemma on forbidden patterns of non-codewords.

Lemma 16. *Let $G = (V, E)$ be the king grid and $C \subseteq V$ be a solid-locating-dominating code in G. Then $T = \{(i, j), (i, j + 1), (i, j + 2), (i + 1, j + 2), (i - 1, j + 2)\}$ and any formation obtained from T by a rotation of $\pi/2$, π or $3\pi/2$ radians around the origo contains a codeword of C.*

In the following theorem, we prove that the solid-locating-dominating code of Theorem 15 is optimal, i.e., there is no code with density smaller than 1/3.

Theorem 17. *If $G = (V, E)$ is the king grid and $C \subseteq V$ is a solid-locating-dominating code in G, then the density $D(C) \geq \frac{1}{3}$.*

Proof. Let S^j be a subgraph of G induced by the vertex set $V_j' = \{(x, y) \mid 1 \leq x \leq 3, 1 \leq$ Recall first the definition $V_n = \{(x, y) \mid |x| \leq n, |y| \leq n\}$. Observe now that we may fit into the first quadrant $\{(x, y) \mid 1 \leq x \leq n, 1 \leq y \leq n\}$ of V_n $\lfloor n/3 \rfloor$ graphs isomorphic to S^n. Similarly, the other three quadrants of V_n can each contain $\lfloor n/3 \rfloor$ graphs isomorphic to S^n. Thus, in total, $4\lfloor n/3 \rfloor$ graphs isomorphic to S_n can be fitted into V_n.

Let C be a solid-locating-dominating code in G. In the final part of the proof, which is omitted, we show that any subgraph of G isomorphic to S^n contains at least $n - 3$ codewords. Assuming this is the case, the density of C can be estimated as follows:

$$D(C) = \limsup_{n\to\infty} \frac{|C \cap V_n|}{|V_n|} \geq \limsup_{n\to\infty} \frac{4\lfloor \frac{n}{3} \rfloor \cdot (n-3)}{(2n+1)^2} \geq \limsup_{n\to\infty} \frac{4(n-3)^2}{3(2n+1)^2} = \frac{1}{3}.$$

It remains to be shown that any subgraph of G isomorphic to S^n contains at least $n-3$ codewords. By symmetry, it is enough to show that $|C \cap V_n'| \geq n-3$. □

Above, we have shown that the density of an optimal solid-locating-dominating code in the king grid is $1/3$. Recall that a self-locating-dominating code is always solid-locating-dominating. Hence, by the previous lower bound, we also know that there exists no self-locating-dominating code in the king grid with density smaller than $1/3$. However, the construction given for the solid-location-domination does not work for self-location-domination. For example, we have $I(2,0) = \{(2,-1),(2,1),(3,0)\}$ and $N[(2,-1)] \cap N[(2,1)] \cap N[(3,0)] = \{(2,0),(3,0)\}$ contradicting with the definition of self-locating-dominating codes (see Figure 2). In the following theorem, we present a self-locating-dominating code in the king grid with the density $1/3$. Notice that this code is also solid-locating-dominating.

Theorem 18. *Let $G=(V,E)$ be the king grid. The code*

$$C = \left\{(x,y) \in \mathbb{Z}^2 \mid x-y \equiv 0 \pmod 3\right\}$$

is self-locating-dominating in G and its density is $1/3$.

Proof. The density $D(C) = 1/3$ since in each row every third vertex is a codeword. Furthermore, C is a self-locating-dominating code since each non-codeword v is covered either by the set of three codewords $\{v+(1,0), v+(0,-1), v+(-1,1)\}$ or $\{v+(-1,0), v+(0,1), v+(1,-1)\}$, and in both cases the closed neighbourhoods of the codewords intersect uniquely in the vertex v. □

In conclusion, we have shown that the density of an optimal self-locating-dominating code in the king grid is $1/3$. Next we consider self-locating-dominating and solid-locating-dominating codes in the infinite triangular grid.

Definition 19. Let $G=(V,E)$ be a graph with the vertex set

$$V = \left\{ i(1,0) + j\left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right) \mid i,j \in \mathbb{Z} \right\}$$

and two vertices are defined to be adjacent if their Euclidean distance is equal to one. The obtained graph G is called the *infinite triangular grid* and it is illustrated in Figure 3. We further denote $v(i,j) = i(1,0) + j\left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right)$. Let R_n

be the subgraph of G induced by the vertex set $V_n = \{v(i,j) \mid |i|, |j| \leq n\}$. The density of a code in G is now defined as follows:

$$D(C) = \limsup_{n\to\infty} \frac{|C \cap V_n|}{|V_n|}$$

We say that a code is *optimal* if there exists no other code with smaller density.

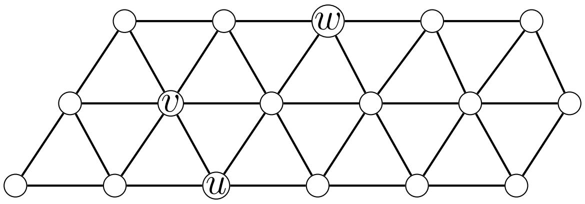

Figure 3: Triangular grid with the vertices $v = v(0,0)$, $u = v(1,-1)$ and $w = v(1,1)$.

In the following theorem, optimal self-locating-dominating and solid-locating-dominating codes are given in the triangular grid. We omit the proof.

Theorem 20. *Let $G = (V,E)$ be the triangular grid. The code*

$$C = \{v(i,j) \mid i,j \equiv 0 \pmod 2\}$$

is self-locating-dominating in G and, therefore, also solid-locating-dominating. The density of the code C is equal to $1/4$ and there exists no self-locating-dominating or solid-locating-dominating code with smaller density, i.e., the code is optimal in both cases.

4 Acknowledgement

The authors would like to thank María Luz Puertas for fruitful discussions on the topic.

References

[1] N. Fazlollahi, D. Starobinski, and A. Trachtenberg. Connected identifying codes. *IEEE Trans. Inform. Theory*, 58(7):4814–4824, 2012.

[2] W. Goddard and K. Wash. ID codes in Cartesian products of cliques. *J. Combin. Math. Combin. Comput.*, 85:97–106, 2013.

[3] C. Hernando, M. Mora, and I. M. Pelayo. Nordhaus-Gaddum bounds for locating domination. *European J. Combin.*, 36:1–6, 2014.

[4] V. Junnila, T. Laihonen, and T. Lehtilä. On regular and new types of codes for location-domination. *Discrete Appl. Math.*, 247:225–241, 2018.

[5] V. Junnila, T. Laihonen, and T. Lehtilä. Solving a conjecture on identification in Hamming graphs. arXiv:1805.01693, 2018.

[6] V. Junnila, T. Laihonen, T. Lehtilä, and M. L. Puertas. On stronger types of locating-dominating codes. arXiv:1808.06891, 2018. To appear, *Discrete Math. Theor. Comput. Sci.*.

[7] M. G. Karpovsky, K. Chakrabarty, and L. B. Levitin. On a new class of codes for identifying vertices in graphs. *IEEE Trans. Inform. Theory*, 44(2):599–611, 1998.

[8] M. Laifenfeld and A. Trachtenberg. Disjoint identifying-codes for arbitrary graphs. In *Proceedings of International Symposium on Information Theory, 2005. ISIT 2005*, pages 244–248, 2005.

[9] A. Lobstein. Watching systems, identifying, locating-dominating and discriminating codes in graphs, a bibliography. Published electronically at `https://www.lri.fr/∼lobstein/debutBIBidetlocdom.pdf`.

[10] D. F. Rall and P. J. Slater. On location-domination numbers for certain classes of graphs. *Congr. Numer.*, 45:97–106, 1984.

[11] D. Rall and K. Wash. Identifying codes of the direct product of two cliques *European J. Combin.*, 36:159–171, 2014.

[12] S. Ray, D. Starobinski, A. Trachtenberg, and R. Ungrangsi. Robust location detection with sensor networks. *IEEE J. Sel. Areas Commun.*, 22(6):1016–1025, August 2004.

[13] P. J. Slater. Domination and location in acyclic graphs. *Networks*, 17(1):55–64, 1987.

[14] P. J. Slater. Dominating and reference sets in a graph. *J. Math. Phys. Sci.*, 22:445–455, 1988.

On the Reconstruction of Graphs of Connectivity 2

Dmtri V. Karpov

E-mail: dvk0@yandex.ru

We consider graphs without loops and multiple edges and use the standard notation. For a graph G, let $V(G)$ denote its vertex set and $v(G) = |V(G)|$. For a vertex $x \in V(G)$, we denote by $d_G(x)$ its degree. As usual, we denote the minimal vertex degree by $\delta(G)$. Let $G - x$ be the graph obtained from G upon deleting the vertex x and all edges incident to it.

Definition 1. For a graph G with $V(G) = \{v_1, \dots, v_n\}$, let $G_i = G - v_i$ and $D(G)$ be the collection of graphs $G_1, \dots, G_n$.

The well known *Graph Reconstruction Conjecture*, formulated by Kelly [1] and Ulam [2] states the following.

Conjecture 1. *Let G and H be graphs with $v(G) = v(H) \geq 3$, such that $D(G) = D(H)$. Then these graphs are isomorphic.*

Note, that several graph parameters can be easily extracted from $D(G)$: the number of vertices, the number of edges (for graphs on at least 3 vertices), the vertex connectivity of a graph, and others.

The conjecture is rather easy for disconnected graphs. In 1957, Kelly [1] has proved it for trees. In 1969, Bondy [3] has proved the Conjecture for graphs of connectivity 1 without pendant vertices. Finally, in 1988 Yongzhi [4] proved the Conjecture for all graphs of connectivity at most 1.

We suggest the following result on semi-reconstruction for graphs of connectivity 2.

Theorem 1. *Let G be a graph of connectivity 2 with $\delta(G) \geq 3$. Having $\mathcal{D}(G)$, we can find a pair of graphs G_1, G_2 such that $G \in \{G_1, G_2\}$.*

The following theorem describes the possible nonuniqueness in the reconstruction of graphs of connectivity 2.

Theorem 2. *Let G_1 and G_2 be two graphs of connectivity 2 on the vertex set V such that $\mathcal{D}(G_1) = \mathcal{D}(G_2)$. Then there exist two graphs H and H' such that $V(H) \cup V(H') = V$, $V(H) \cap V(H') = \{a, b\}$ and both graphs G_1 and G_2 are obtained by gluing together H and H' by the set $\{a, b\}$.*

And one more result on the full reconstruction for some graphs of connectivity 2.

Theorem 3. *Let G be a 2-connected graph with $\delta(G) \geq 3$ and $T \subset V(G)$ be such that $|T| = 2$ and the graph $G - T$ has at least 3 connected components. Then G can be reconstructed from $D(G)$ (i.e., any graph H with $D(H) = D(G)$ is isomorphic to G).*

Proofs of all these Theorems contain polynomial algorithms of the corresponding reconstruction.

References

[1] P. J. Kelly. *A congruence theorem for trees*, Pacific J. Math. 7 (1957), 961-968.

[2] S. M. Ulam. *A collection of mathematical problems,* Wiley, New York, 1960.

[3] J. A. Bondy. *On Ulam's conjecture for separable graphs.* Toronto, Univ. Toronto Press, 1966.

[4] Y. Yongzhi. *The reconstruction conjecture is true if all 2-connected graphs are reconstructible.* Journal of graph theory 12, p.237-243 (1988).

On solid-resolving sets in graphs

Anni Hakanen *† Ville Junnila † Tero Laihonen †
María Luz Puertas‡

Let G be a finite, connected, simple and undirected graph with vertices V and edges E. Consider a vertex set $S = (s_1, s_2, \dots, s_k)$. We define the *distance array* of $v \in V$ with respect to S as $\mathcal{D}_S(v) = (d(s_1, v), d(s_2, v), \dots, d(s_k, v))$. If each vertex of G has a unique distance array with respect to S, then S is a *resolving set* of G. The smallest cardinality of a resolving set of G is called the *metric dimension* of G. Resolving sets were first introduced by Slater [5] and Harary and Melter [3], independently. This concept is now widely studied and many variants have been introduced.

One quite recent concept is the $\{\ell\}$-resolving set of a graph, which was introduced in [4]. Instead of individual vertices, we now consider sets of vertices with at most ℓ elements. To that end, we define the distance array of a vertex set X with respect to S as $\mathcal{D}_S(X) = (d(s_1, X), \dots, d(s_k, X))$, where $d(s_i, X) = \min\{d(s_i, x) \mid x \in X\}$. If each non-empty vertex set X with at most ℓ elements has a unique distance array with respect to S, then S is an *$\{\ell\}$-resolving set* of G. When $\ell = 1$, this definition is equivalent with the definition of the ordinary resolving set. When $\ell \geq 2$, $\{\ell\}$-resolving sets have properties that $\{1\}$-resolving sets do not have. For example, in [2], it was shown that when $\ell \geq 2$ certain types of vertices are included in every $\{\ell\}$-resolving set. These vertices are called *forced vertices*. On the other hand, $\{1\}$-resolving sets do not have any forced vertices, since $V \setminus \{v\}$ is a $\{1\}$-resolving set of G for any $v \in V$.

Consider a network where we locate faulty processors with an ordinary resolving set. If there are two or more faulty processors simultaneously, the distance array given by the resolving set might correspond to some vertex which

*Corresponding author, email: anehak@utu.fi

†Department of Mathematics and Statistics, University of Turku, Turku, Finland

‡Department of Mathematics, Universidad de Almería, Almería, Spain

does not represent a faulty processor. Now we end up trying to repair a processor which is functioning correctly. To avoid this type of situation, *solid-resolving sets* were introduced in [1]. A vertex set is a solid-resolving set, if each vertex has a unique distance array and no vertex set with two or more vertices has the same distance array as any one vertex.

In this talk, we generalise the concept of solid-resolving sets. Let X and Y be non-empty vertex sets such that $X \neq Y$ and $|X| \leq \ell$. If S is a vertex set such that $\mathcal{D}_S(X) \neq \mathcal{D}_S(Y)$ for all X and Y, then S is called an *ℓ-solid-resolving set*. Notice that for $\{\ell\}$-resolving sets we would have the restriction $|Y| \leq \ell$.

In what follows, we will state without proofs some of our new results regarding $\{\ell\}$-resolving sets and ℓ-solid-resolving sets.

Theorem 1. *Let $S \subseteq V$ and $\ell \geq 1$. The set S is an ℓ-solid-resolving set of G if and only if for all $x \in V$ and nonempty $Y \subseteq V$ such that $x \notin Y$ and $|Y| \leq \ell$ there exists an element $s \in S$ such that*

$$d(s,x) < d(s,Y). \tag{1}$$

Theorem 2. *Let $S \subseteq V$ and $\ell \geq 1$.*

(i) If S is an ℓ-solid-resolving set, then it is also an $\{\ell\}$-resolving set of G.

(ii) If S is an $\{\ell+1\}$-resolving set, then it is also an ℓ-solid-resolving set of G.

Theorem 1 gives us a way to consider ℓ-solid-resolving sets in graphs via the structure of the graph and not the distance arrays. Theorem 2 shows the connection between $\{\ell\}$-resolving sets and ℓ-solid-resolving sets. By means of these two theorems we can search for an $\{\ell\}$-resolving set of G by considering first $(\ell-1)$-solid-resolving sets of G with the characterisation (1). The following two theorems provide characterisations for forced vertices of ℓ-solid-resolving sets and $\{\ell\}$-resolving sets. As it turns out, the forced vertices of an $\{\ell\}$-resolving set are exactly the same as those of an $(\ell-1)$-solid-resolving set. For $U \subseteq V$, let us denote

$$N[U] = \bigcup_{u \in U} N[u].$$

Theorem 3. *Let $\ell \geq 1$. A vertex $v \in V$ is a forced vertex of an ℓ-solid-resolving set if and only if there exists a set $U \subseteq V$ such that $v \notin U$, $|U| \leq \ell$ and $N(v) \subseteq N[U]$.*

Theorem 4. *Let $\ell \geq 2$. A vertex $v \in V$ is a forced vertex of an $\{\ell\}$-resolving set if and only if there exists a set $U \subseteq V$ such that $v \notin U$, $|U| \leq \ell - 1$ and $N(v) \subseteq N[U]$.*

References

[1] A. Hakanen, V. Junnila, and T. Laihonen. The solid-metric dimension. *Theoret. Comput. Sci.*, 2019. In press.

[2] A. Hakanen and T. Laihonen. On $\{\ell\}$-metric dimensions in graphs. *Fundam. Inform.*, 162(2-3):143–160, 2018.

[3] F. Harary and R. Melter. On the metric dimension of a graph. *Ars Comb.*, 2:191–195, 1976.

[4] T. Laihonen. The metric dimension for resolving several objects. *Inform. Process. Lett.*, 116(11):694–700, 2016.

[5] P. J. Slater. Leaves of trees. In *Proceedings of the Sixth Southeastern Conference on Combinatorics, Graph Theory, and Computing (Florida Atlantic Univ., Boca Raton, Fla., 1975)*, pages 549–559. Congressus Numerantium, No. XIV, Winnipeg, Man., 1975. Utilitas Math.

Lower bound for the size of 1-perfect bitrades of Hamming graphs

Alexandr Valyuzhenich

Sobolev Institute of Mathematics, pr. Akademika Koptyuga 4,
Novosibirsk 630090, Russia
graphkiper@mail.ru

Trades of different types are used to study, construct, and classify different kinds of combinatorial objects (see, e.g., [1, 2]). Trades are also studied independently, as some natural generalization of objects of the corresponding type. In this paper we study 1-perfect bitrades in the Hamming graphs.

Let $\Sigma_q = \{0, 1, \ldots, q-1\}$. The vertex set of the Hamming graph $H(n, q)$ is Σ_q^n, and two vertices are adjacent if and only if they differ in exactly one position. A 1-perfect code is a set C of vertices of $H(n, q)$ such that $|C \cap B| = 1$ for every ball B of radius 1. A 1-perfect bitrade is a pair (T_0, T_1) of disjoint vertex sets of $H(n, q)$ such that $|T_0 \cap B| = |T_1 \cap B| \in \{0, 1\}$ for every ball B of radius 1.

In this work we consider the problem of finding the minimum size of 1-perfect bitrades of $H(n, q)$. In [4] Potapov solved this problem for $q = 2$. In [5] Vorob'ev and Krotov obtained the lower bound on the size of 1-perfect bitrades of $H(n, q)$ for $q > 3$. In this paper we solve the problem for $q = 3$ and find the minimum size of 1-perfect bitrades of $H(n, 3)$.

Theorem 1 *Let $n = 3m + 1$. Then the minimum size of 1-perfect bitrades of $H(n, 3)$ is $2^{m+1} \cdot 3^m$.*

This work was funded by the Russian Science Foundation under grant 18-11-00136.

References

[1] A. S. Hedayat, G. B. Khosrovshahi. Trades, in: C. J. Colbourn, J. H. Dinitz (Eds.), Handbook of Combinatorial Designs, 2nd Edition, Discrete Mathematics and Its Applications, Chapman Hall/CRC, Boca Raton, London, New York, 2006, pp. 644-648.

[2] D. Krotov, I. Mogilnykh, V. Potapov. To the theory of q-ary Steiner and other-type trade. Discrete Mathematics. 2016. V. 339, N 3. P. 1150-1157.

[3] D. S. Krotov. The extended 1-perfect trades in small hypercubes. Discrete Mathematics. 2017. V. 340, N. 10, P. 2559-2572.

[4] V. N. Potapov. On perfect 2-colorings of the q-ary n-cube. Discrete Mathematics. 2012. V. 312, N. 8, 1269-1272.

[5] K. V. Vorobev, D. S. Krotov. Bounds for the size of a minimal 1-perfect bitrade in a Hamming graph. Journal of Applied and Industrial Mathematics. 2015. V. 9, N. 1, P. 141-146.

For which graphs the sages can guess a color of at least one hat

A. Latyshev, K. Kokhas

This talk based on Kokhas, K. & Latyshev, A. J Math Sci (2019) 236: 503.

Several sages wearing colored hats are situated at the vertices of a graph. Each sage tries to guess his own hat color merely on the basis of observing the hats worn by their neighbours without exchanging the information. Each hat can have one of *three* colors. A predetermined guessing strategy is winning if it guarantees at least one correct individual guess for every assignment of colors.

For fast check whether a strategy is winning we introduce a «*9-vertex model*» that describes the strategy by means of special tensors and reduce the question to calculations of tensor convolutions. This model allows also to reduce a problem of the winning strategy search to the boolean satisfiability problem. Thus we can use SAT-solver to find the winning strategies on small graphs. After that we consider *hints*, i.e. some restrictions for the hat assignments which help the sages to win. We develop the *hints theory* and apply it for constructing strategies and for logical explanations of strategies that were found by computer. For the most of graphs it allows us to give «logical» proofs which do not rely on the results of a computer search. Nonetheless in the small number of cases we prove the absence of a winning strategy or give a technical proofs (using 9-vertex model) by computer only. In this way we completely solve the question and prove the following theorem.

The sages lose on a connected graph G if and only if graph G is a tree or G contains the unique cycle C_n, where n is not divisible by 3, $n \geq 5$.

Periodicity in Algebraic Subshifts*

Jarkko Kari[1] and Etienne Moutot[1,2]

[1]Department of Mathematics and Statistics, University of Turku
[2]LIP, ENS de Lyon – CNRS – UCBL – Université de Lyon

In his keynote talk celebrating the 25th anniversary of the European Association for Theoretical Computer Science, EATCS, at ICALP 1997 in Bologna, Maurice Nivat formulated the following problem now know as "Nivat's conjecture": If an infinite two-dimensional grid has been colored in such a way that, for some $n, m \in \mathbb{N}$, the number of distinct $n \times m$ patterns is at most nm (this case is called to be a low complexity coloring), is the coloring necessarily periodic in some direction? The conjecture has attracted wide interest, but it has turned out to be a very difficult problem and remains still unsolved today.

In this talk, based on the manuscript [1], we continue to investigate the algebraic approach initiated in [2]. We prove that Nivat's conjecture holds for colorings coming from certain algebraically defined sets, including the Ledrappier subshift [3]. We even prove a stronger claim, very similar, but with a more general definition of low complexity.

For a finite alphabet A, colorings $c \in A^{\mathbb{Z}^2}$ of the two-dimensional grid by elements of A are called (two-dimensional) *configurations*. Typically we use notation $c_{\mathbf{n}}$ for the color $c(\mathbf{n}) \in A$ of cell $\mathbf{n} \in \mathbb{Z}^2$. Basic operations on $A^{\mathbb{Z}^2}$ are *translations*: for any $\mathbf{t} \in \mathbb{Z}^2$ the translation $\tau_{\mathbf{t}} : A^{\mathbb{Z}^2} \longrightarrow A^{\mathbb{Z}^2}$ by $\mathbf{t}$ is defined by $\tau_{\mathbf{t}}(c)_{\mathbf{n}} = c_{\mathbf{n}-\mathbf{t}}$, for all $c \in A^{\mathbb{Z}^2}$ and all $\mathbf{n} \in \mathbb{Z}^2$. We call a configuration c *periodic* if $\tau_{\mathbf{t}}(c) = c$ for some non-zero $\mathbf{t} \in \mathbb{Z}^2$, and we call $\mathbf{t}$ a *vector of periodicity*. If there are two linearly independent vectors of periodicity then c is *two-periodic*. In this case it is easy to see that there are horizontal and vertical vectors of periodicity $(k, 0)$ and $(0, k)$ for some $k \neq 0$, and consequently a vector of periodicity in every rational direction. We call c *one-periodic* if it is periodic but not two-periodic.

*Research supported by the Academy of Finland grant 296018.

Colorings $p \in A^D$ of a finite shape $D \subset \mathbb{Z}^d$ are called *D-patterns*, or simply patterns. The set of D-patterns that appear in a configuration c is denoted by $P(c, D)$, that is,

$$P(c, D) = \{\tau_{\mathbf{t}}(c)|_D \mid \mathbf{t} \in \mathbb{Z}^2 \}.$$

We say that c has *low complexity* with respect to shape D if $|P(c, D)| \leq |D|$, and we call c a *low complexity configuration* if it has low complexity with respect to some finite D.

To study the conjecture algebraically we replace the colors by integers, or elements of some other integral domain R, and express the configuration c as a formal power series $c(X, Y)$ over two variables X and Y in which the coefficient of monomial X^iY^j is $c_{i,j}$, for all $i, j \in \mathbb{Z}$. Note that the exponents of the variables range from $-\infty$ to $+\infty$. In the following also polynomials may have negative powers of variables so all polynomials considered are actually Laurent polynomials. Let us denote by $R[X^{\pm1}, Y^{\pm1}]$ and $R[[X^{\pm1}, Y^{\pm1}]]$ the sets of such polynomials and power series, respectively, with coefficients in domain R. We call a power series $c \in R[[X^{\pm1}, Y^{\pm1}]]$ *finitary* if its coefficients take only finitely many different values. Since we color the grid using finitely many colors, configurations are identified with finitary power series.

Multiplying configuration $c \in R[[X^{\pm1}, Y^{\pm1}]]$ by a monomial corresponds to translating it, and the periodicity of the configuration by vector $\mathbf{t} = (n, m)$ is then equivalent to $(X^nY^m - 1)c = 0$, the zero power series. More generally, we say that polynomial $f \in R[X^{\pm1}, Y^{\pm1}]$ *annihilates* power series c if the formal product fc is the zero power series.

One of the main results of [2] states that, in the case $R = \mathbb{Z}$, if a configuration c is annihilated by a non-zero polynomial then it has annihilators of particularly nice form:

Theorem 1 ([2])**.** *Let $c \in \mathbb{Z}[[X^{\pm1}, Y^{\pm1}]]$ be a configuration (a finitary power series) annihilated by some non-zero polynomial. Then there exists non-zero $(i_1, j_1), \ldots, (i_m, j_m) \in \mathbb{Z}^2$ such that*

$$(X^{i_1}Y^{j_1} - 1) \cdots (X^{i_m}Y^{j_m} - 1)$$

annihilates c.

For a polynomial $f = \sum a_{i,j}X^iY^j$, we call $\text{supp}(f) = \{(i, j) \mid a_{i,j} \neq 0\}$ its *support*. A *line polynomial* is a polynomial with its terms aligned all on the same line: f is a line polynomial in direction $\mathbf{u} \in \mathbb{Z}^2 \setminus \{\mathbf{0}\}$ if and only if $\text{supp}(f)$ contains at least two elements and for some $\mathbf{n} \in \mathbb{Z}^2$ we have $\text{supp}(f) \subseteq \{\mathbf{n} + r\mathbf{u} \mid r \in \mathbb{Q}\}$. Note that the annihilator provided by Theorem 1 is a product of line polynomials. A central feature of line polynomials is that any configuration that is annihilated by a line polynomial is periodic in the direction of that line polynomial [2].

Here our main subject of interest is a specific type of configurations, that lies in what is called algebraic subshift. If R is a finite field and if $f \in R[X^{\pm1}, Y^{\pm1}]$ is a non-zero polynomial then we define the set

$$X_f = \{c \in R[[X^{\pm1}, Y^{\pm1}]] \mid fc = 0\}$$

of all configurations that f annihilates and call it the *algebraic subshift* defined by f. It is a subshift of finite type (SFT, see [4] for the symbolic dynamics terminology). We have that $c \in X_f \iff fc = 0$.

The first example we are interested in is the *Ledrappier subshift* [3], which is the algebraic subshift X_{f_L} defined by the annihilator $f_L = 1 + X + Y$. For this specific subshift, we are able to prove that Nivat's conjecture holds for our more general definition of low complexity.

Theorem 2. *Any low complexity $c \in X_{f_L}$ is two-periodic.*

Naturally, the next step is to tackle more general polynomials. A determining factor in the complexity of the Nivat's conjecture on algebraic subshifts seems to be the the number of line polynomials factors. In fact for an algebraic subshift defined by a polynomial with zero or one line polynomials factors, we are able to characterize the periodicity of its low complexity configurations. This is our main result in [1].

Theorem 3. *Let $c \in X_f$ for a polynomial $f \in \mathbb{F}_p[X^{\pm1}, Y^{\pm1}]$, and suppose that c is annihilated by some non-zero polynomial over $\mathbb{Z}$.*

- *If f has no line polynomial factors then c is two-periodic.*
- *If all line polynomial factors of f are in the same direction then c is periodic in this direction.*

Corollary 4. *Let $c \in X_f$ for a polynomial $f \in \mathbb{F}_p[X^{\pm1}, Y^{\pm1}]$ whose line polynomial factors are all in the same direction. If c has low complexity then it is periodic.*

For more than one line polynomial factor however, the problem becomes much more complicated. For the *4-dot system S*, the algebraic subshift X_{f_S} over $\mathbb{F}_2$ defined by the annihilator $f_S = (1 + X)(1 + Y)$, the low complexity assumption still ensures the periodicity of the configuration (Theorem 5). However, with a very similar polynomial $f_T = (1 + X^2)(1 + Y^2)$ this is not the case: some low complexity configurations are non-periodic (Example 6).

Theorem 5. *Every low complexity $c \in X_{f_S}$ is periodic.*

Example 6. *There exists a configuration c over $\mathbb{F}_2$ annihilated by $f_T = (1 + X^2)(1 + Y^2)$ which is not periodic but has low complexity.*

References

[1] J. Kari and E. Moutot. An Algebraic Geometric Approach to Nivat's Conjecture. *Submitted to a journal.*

[2] J. Kari and M. Szabados. An Algebraic Geometric Approach to Nivat's Conjecture. In *Automata, Languages, and Programming - 42nd International Colloquium, ICALP 2015, Kyoto, Japan, July 6-10, 2015, Proceedings, Part II*, pages 273–285, 2015.

[3] F. Ledrappier. Un champ markovien peut e dentropie nulle et mngeant. *C. R. Acad. Sci. Paris S A-B*, 287(7):A561–A563, 1978.

[4] D. Lind and B. Marcus. *An Introduction to Symbolic Dynamics and Coding.* Cambridge University Press, 1995.

Roots and Powers in Regular Languages: Recognizing Nonregular Properties by Finite Automata [Brief Announcement]

Fabian Frei

Department of Computer Science, ETH Zrich, Switzerland

fabian.frei@inf.ethz.ch

Juraj Hromkovič

Department of Computer Science, ETH Zrich, Switzerland

juraj.hromkovic@inf.ethz.ch

Juhani Karhum

Department of Mathematics and Statistics, University of Turku, Finland*

karhumak@utu.fi

Abstract

It is well known that the set of powers of any given order, for example squares, in a regular language need not be regular. We show that, nevertheless, finite automata can identify them via their roots. More precisely, we show the set of square roots of a regular language L, that is $\{u \in \Sigma^* \mid u^2 \in L\}$, to be regular. More generally, this holds true for the nth roots for all $n \geq 2$ and also for the union of these sets.

The above results yield decision algorithms for many natural problems on powers. For example, it is decidable, given two regular languages, whether they contain the same number of squares at each length. Finally, we give an exponential lower bound on the size of deterministic finite automata identifying powers in regular languages via their roots.

*Research done in part during a stay at ETH Zurich.

1 Introduction

Most natural properties of regular languages are algorithmically decidable, as is well known. Typically, the set of words satisfying such a property is a regular language, and thus all the machinery for regular languages becomes available.

We provide an example of a very natural property that exhibits a surprisingly different behavior. Namely, we introduce a problem that is nonregular and yet, at the same time, identifiable by finite automata. More precisely, the instances of the problem are mapped by a one-to-one function in such a way that the set of images of the words satisfying the property is regular. This allows us to present algorithms for many problems that do not seem to be—at least at first glance—of the "finite state type."

We will introduce a multidimensional product automaton construction in order to show that, given a regular language, the set of its square roots is regular. This allows us to give clear and simple answers to a number of intriguing algorithmic questions. For example, we show that it is decidable whether or not two regular languages contain the same number of squares at each length.

Our result can easily be extended to nth roots, for any natural n. Moreover, it is possible to compute all proper roots (i.e., roots of order at least 2) of a given regular language. To obtain the latter result, we prove a special version of the pumping lemma for regular languages.

The above results deserve a word of warning. Although we can compute all proper roots of a regular language and prove the resulting set to be a regular language, we do not claim that a finite automaton can recognize the primitive roots of a regular language. Indeed, this is in general a nonregular language.

Finally, we prove that the set of roots of a regular language, while always regular, has an exponentially increased state complexity in the worst case. In other words, we give an exponential lower bound on the minimal number of states of an automaton recognizing the roots of L in terms of the minimal number of states of an automaton for L.

2 Results

We present a few automata constructions computing different type of roots of words in a regular language. We recall that the set of squares in a regular language, for instance in Σ^*, need not be regular. Our first result shows that, surprisingly, the set of square roots of a regular language is always regular.

Theorem 1. *For each regular set L, the set $\{u \in \Sigma^* \mid u^2 \in L\}$ of its square roots is a regular.*

We then extend this theorem to fixed order roots, that is, $\{u \in \Sigma^* \mid u^n \in L\}$ for any $n \in \mathbb{N}$. A more complicated question is whether the union of these sets (i.e, all proper roots of L) is again regular. Surprisingly, it is. We show this using a variant of the pumping argument of regular languages.

Theorem 2. *For each regular set L, the set $\{u \in \Sigma^* \mid \exists k \geq 2\colon u^k \in L\}$ of its proper roots is regular.*

A nonempty word w is called *primitive* if is not a proper power of any other word. We analyze the three sets

- $\mathrm{Q}(L)$, the primitive roots of L,
- $\mathrm{QR}(L)$, the primitive roots of proper powers in L, and
- $\mathrm{R}(L)$, the set of all roots of L.

and show the general relations among them can be outlined as in Figure 1.

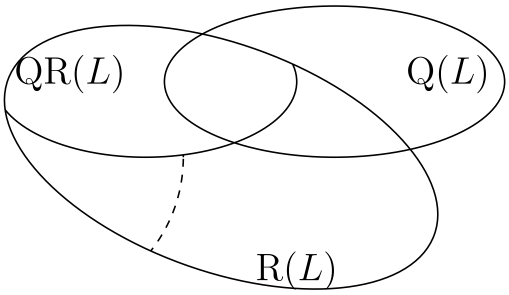

Figure 1. The general relations between $\mathrm{Q}(L)$, $\mathrm{QR}(L)$, and $\mathrm{R}(L)$. The dashed line divides the roots of L into primitive ones and nonprimitive ones.

From the above, we are able to derive a number of interesting decidability results, the last being the most sophisticated one.

Theorem 3. *The following problems are decidable:*

1. *Given a regular language L, does it contain a square?*
2. *Given a regular language L, does it contain infinitely many squares?*
3. *Given an integer $n \geq 2$ and a regular language L, does L contain an nth power?*
4. *Given an integer $n \geq 2$ and a regular language L, does L contain infinitely many nth powers?*
5. *Given regular languages L and L', do they contain exactly the same squares?*

6. *Given two regular languages L and L' and an integer $n \geq 2$, do L and L' contain exactly the same nth powers?*

7. *Given two regular languages L and L', do they contain exactly the same proper roots?*

8. *Given two regular languages L and L', do they contain the same number of squares of each length?*

Finally, we complement our main automaton construction that proves Theorem 1 with an exponential lower bound on the state complexity of taking the square roots of regular languages.

Theorem 4. *There is a family $\{L_k \mid k \geq 2\}$ of languages such that the minimal number of states of a deterministic finite automaton recognizing $\mathrm{SQR}(L_k)$ is exponentially larger than the minimal number of states of a deterministic finite automaton recognizing L_k.*

References

[1] Samuel Eilenberg. *Automata, Languages, and Machines, Volume A.* Academic Press, 1974.

[2] John E. Hopcroft and Jeffrey D. Ullman. *Introduction to Automata Theory, Languages, and Computation.* Addison-Wesley, 1979.

[3] Sor Horv, Masami Ito, and Gerhard Lischke. Roots and Powers of Regular Languages. In *Proceedings of DLT, LNCS.* Springer, 2002.

[4] M. Lothaire. *Combinatorics on Words, Second Edition.* Cambridge University Press, 1997.

[5] Arto Salomaa and Matti Soitola. *Automata-Theoretic Aspects of Formal Power Series.* Springer 1978.

On Equations over Monoids Defined by Generalizations of Abelian Equivalence (Extended Abstract)

Markus A. Whiteland
Department of Mathematics and Statistics, University of Turku,
FI-20014 University of Turku, Finland
mawhit@utu.fi

1 Abstract

The notion of *k-abelian equivalence* has attracted a lot of interest in the recent literature [2, 3, 7–9, 12]. The k-abelian equivalence is defined as follows. Let $k \geq 1$ be in integer and let u, v be words. Then u and v are k-abelian equivalent, in symbols $u \sim_k v$ if, for each word x of length at most k, x occurs equally many in times in u and v as a factor. For $k = 1$, the 1-abelian equivalence coincides with the usual abelian equivalence, an extremely popular subject of research in the recent times. By defining ∞-abelian equivalence as the equality relation, we see that letting k vary, we obtain an infinite hierarchy of equivalence relations

$$u \sim_1 v \supseteq u \sim_2 v \supseteq \cdots \supseteq u \sim_k v \supseteq u \sim_{k+1} v \supseteq \cdots \supseteq u = v.$$

More precisely, as can be seen from the definition of k-abelian equivalence, $u \sim_k v$ implies $u \sim_{k'} v$ for all $k' \leq k$.

Another interesting equivalence relation is the *k-binomial equivalence* introduced in [14] by M. Rigo and P. Salimov. Let $k \geq 1$ be an integer. Two words u and v are k-binomial equivalent, in symbols $u \equiv_k v$, if, for each word x of length at most k, x occurs equally many times in u and v as a subword. Notice that this equivalence relation is incomparable to k-abelin equivalence, as was already noted in [14]. Again, the 1-binomial equivalence is the usual abelian equivalence, and $u \equiv_k v$ implies that $u \equiv_{k'} v$ for each $k' \leq k$. The k-binomial eqivalence is also a congruence. Once again, letting $\equiv_\infty$ be the equality relation, we obtain an infinite hierarchy of equivalence relations between abelian equivalence and the equality relation.

Since the relations $\sim_k$ and $\equiv_k$ are congruences, the quotients $\Sigma^*/{\sim_k}$ and $\Sigma^*/{\equiv_k}$ are monoids. We may thus naturally define equations over these monoids. Let Ξ be a finite non-empty set of *variables* and S a monoid (we assume that $\Xi^+ \cap S = \emptyset$). An element $(u, v) \in (\Xi \cup S)^+ \times (\Xi \cup S)^+$ is called an *equation* over S with variables Ξ. A *solution* to an equation (u, v) over S with variables Ξ is a morphism $\alpha : \Xi \to S$ such that $\alpha(u) = \alpha(v)$ (α is the identity morphism on S). In this note we consider some particular equations and their solutions in the k-abelian and k-binomial monoids. The equations are the commutation (xy, yx) and conjugacy (xz, zy). The k-abelian equations are quite straightforward to analyze, but the case of k-binomial equations turns out to be quite hard. We are able to give characterizations to these equations in the k-abelian monoid, but this far from the case when studying the k-binomial monoid.

We also consider systems of equations over the monoids $\Sigma^*/{\sim_k}$ and $\Sigma^*/{\equiv_k}$. The basic notion studied here is the so-called *compactness property* of semigroups, defined as follows.

Definition 1.1. A semigroup S is said to have the *compactness property* if any system of equations E over a finite number of variables has a finite equivalent subsystem E' (i.e., the sets of solutions are equal).

Famously, the free monoid Σ^* has the compactness property, as was proved in [1] and [4] independently. The latter also shows that free groups have the compactness property. In [5] it is shown, employing Redei's Theorem [13] among other arguments, that all commutative semigroups have the compactness property. Thus, for example, for each $x, y \in \Sigma^{k-1}$, the subsemigroup $(x\Sigma^* \cap \Sigma^* y)/{\sim_k}$ of $\Sigma^*/{\sim_k}$ has the compactness property, since it is commutative as follows from our considerations of k-abelian commutativity.

Not all semigroups have the compactness property. For example, neither the monoid of finite languages, nor the so-called *bicyclic monoid*, nor the *Baumslag–Solitar group* have the compactness property. For the first result, see [10], the latter two are shown in [5].

In this note we show that the monoids $\sim_k$ and $\equiv_k$ have the compactness property. This follows almost immediately by showing that these monoids are isomorphic to some (distinct) subsemigroups of $n \times n$ matrices for some n depending on k (for the k-binomial monoid this isomorphism was already proved in [14]). We then consider the cardinalities of independent systems of equations (which are automatically finite by the compactness property). The aspect of considering sizes of independent systems of equations in semigroups has been treated, e.g., in the paper [6]. See also [11], and references therein, concerning the free semigroup.

We show that, for the monoids $\Sigma^*/\sim_k$ and $\Sigma^*/\equiv_k$, there exists a uniform upper bound on the number of equations of an independent system of equations. For k fixed, the the size of an independent system of equations has a polynomial upper bound with respect to the number of unknowns. On the other hand, the upper bound is exponential when the number of unknowns is fixed and k is allowed to vary. We remark that these bounds do not depend on the size of the alphabet Σ, when the equations have no constants, that is, the system of equations is a subset of $\Xi^+ \times \Xi^+$.

The results presented here are to be part of the Doctoral Thesis of the author.

References

[1] M. Albert and J. Lawrence. A proof of Ehrenfeucht's conjecture. *Theoretical Computer Science*, 41:121–123, 1985.
DOI: 10.1016/0304-3975(85)90066-0.

[2] J. Cassaigne, J. Karhumäki, and A. Saarela. On growth and fluctuation of k-abelian complexity. *European Journal of Combinatorics*, 65:92–105, 2017.
DOI: 10.1016/j.ejc.2017.05.006.

[3] T. Ehlers, F. Manea, R. Mercas, and D. Nowotka. k-Abelian pattern matching. *Journal of Discrete Algorithms*, 34:37–48, 2015.
DOI: 10.1016/j.jda.2015.05.004.

[4] V. S. Guba. Equivalence of infinite systems of equations in free groups and semigroups to finite subsystems. *Matematicheskie Zametki*, 40(3):321–324, 428, 1986. In Russian.

[5] T. Harju, J. Karhumäki, and W. Plandowski. Compactness of systems of equations in semigroups. *International Journal of Algebra and Computation*, 7(4):457–470, 1997.
DOI: 10.1142/S0218196797000204.

[6] J. Karhumäki and W. Plandowski. On the size of independent systems of equations in semigroups. *Theoretical Computer Science*, 168(1):105 – 119,

1996.
DOI: 10.1016/S0304-3975(96)00064-3.

[7] J. Karhumäki and S. Puzynina. On k-Abelian Palindromic Rich and Poor Words. In *Developments in Language Theory - 18th International Conference, DLT 2014, Ekaterinburg, Russia, August 26-29, 2014. Proceedings*, pages 191–202, 2014.
DOI: 10.1007/978-3-319-09698-8_17.

[8] J. Karhumäki, S. Puzynina, and A. Saarela. Fine and Wilf's Theorem for k-Abelian Periods. *International Journal of Foundations of Computer Science*, 24(7):1135–1152, 2013.
DOI: 10.1142/S0129054113400352.

[9] J. Karhumäki, A. Saarela, and L. Q. Zamboni. Variations of the Morse–Hedlund theorem for k-abelian equivalence. *Acta Cybernetica*, 23(1):175–189, 2017.
DOI: 10.14232/actacyb.23.1.2017.11.

[10] J. Lawrence. The non-existence of finite test sets for set-equivalence of finite substitions. *Bulletin of the EATCS*, 28:34–36, 1986.

[11] D. Nowotka and A. Saarela. One-variable word equations and three-variable constant-free word equations. *International Journal of Foundations of Computer Science*, 29(5), 2018.
DOI: 10.1142/S0129054118420121.

[12] M. Rao and M. Rosenfeld. Avoidability of long k-abelian repetitions. *Mathematics of Computation*, 85(302):3051–3060, 2016.
DOI: 10.1090/mcom/3085.

[13] L. Rédei. *The theory of finitely generated commutative semigroups*. International series of monographs in pure and applied mathematics. Pergamon Press, 1965.
DOI: 10.1016/C2013-0-01797-5.

[14] M. Rigo and P. Salimov. Another Generalization of Abelian Equivalence: Binomial Complexity of Infinite Words. *Theoretical Computer Science*, 601:47–57, 2015.
DOI: 10.1016/j.tcs.2015.07.025.

Representations of permutation groups and semigroups on combinatorial structures

Tatiana B. Jajcayová[*]
Comenius University, Bratislava, Slovakia
tatiana.jajcayova@fmph.uniba.sk

April 17, 2019

Abstract

Every finite group is known to be isomorphic to the automorphism group of some finite graph. We review results for various combinatorial structures whose full automorphism groups act regularly on their sets of vertices. Such structures can be thought of as combinatorial representations of the corresponding groups. Previous results on this topic include the classification of graphical regular representations (graphs with regular automorphism groups), classification of digraphical regular representations (directed graphs with regular automorphism groups), as well as the classification of general combinatorial structures (incidence structures) with regular automorphism groups. We generalize these results to the class of k-hypergraphs which are incidence structures with all blocks of size k, and consider the spectrum of all k's for which such representation is possible.

The inverse monoid of partial automorphisms of a combinatorial structure is a richer and more complex object that contains more information about the structure than its automorphism group. We review the results we obtained in the study of analogous questions to those concerning automorphism groups for the inverse monoids of partial automorphisms.

1 Introduction

Knowledge of the automorphism group of a specific combinatorial structure allows one to make various claims about the structure. The fact that every

[*] Author supported in part by VEGA 1/0719/18 and VEGA 1/0039/17.

finite group is isomorphic to a group of automorphisms of a finite graph has been established by Frucht in his 1938 paper [2]

Theorem 1.1 (Frucht 1938)**.** *For any finite group G there exists a graph Γ such that $Aut(\Gamma) \cong G$.*

However, in this result, the type of the actions of these groups on the vertices of the corresponding graphs is not specified. They can be very far from being regular. To address regularity specifically, the *Graphical Regular Representation Problem* (the GRR problem) asks for the classification of finite groups G that admit the existence of an edge set E with the property that the full automorphism group of the graph (G, E) acts *regularly* on G. Such groups are said to *admit a GRR* and include almost all finite groups with the exception of abelian groups of exponent at least 3, generalized dicyclic groups, and thirteen sporadic groups of order not exceeding 32.

Theorem 1.2 ([3,5,12,13,15])**.** *Let G be a finite group that does not have a GRR, i.e., a finite group that does not admit a regular representation as the full automorphism group of a graph. Then G is an abelian group of exponent greater than 2 or G is a generalized dicyclic group or G is isomorphic to one of the 13 groups :* $\mathbf{Z}_2^2$, $\mathbf{Z}_2^3$, $\mathbf{Z}_2^4$, $\mathcal{D}_3$, $\mathcal{D}_4$, $\mathcal{D}_5$, $\mathcal{A}_4$, $\mathcal{Q} \times \mathbf{Z}_3$, $\mathcal{Q} \times \mathbf{Z}_4$, $\langle a, b, c \mid a^2 = b^2 = c^2 = 1,\ abc = bca = cab \rangle$, $\langle a, b \mid a^8 = b^2 = 1,\ b^{-1}ab = a^5 \rangle$,
$\langle a, b, c \mid a^3 = b^3 = c^2 = 1,\ ab = ba,\ (ac)^2 = (bc)^2 = 1 \rangle$,
$\langle a, b, c \mid a^3 = b^3 = c^3 = 1,\ ac = ca,\ bc = cb,\ b^{-1}ab = ac \rangle$.

In a variation of this problem, the *Digraphical Regular Representation Problem* (DRR), Babai addresses the same question for digraphs. The classification shows that finite groups admitting DRR's include all finite groups but $\mathcal{Z}_2^2$, $\mathcal{Z}_2^3$, $\mathcal{Z}_2^4$, $\mathcal{Z}_3^2$ and the quaternion group $\mathcal{Q}_8$ admits a DRR [1].

These are examples of classification questions related to automorpism groups one can ask about various combinatorial structures. In the last section of this paper, Section 4, we review results for hypergraps and our results for regular k-hypergraphs.

The usefulness of knowing the automorphism group of a combinatorial structure decreases with an increasing number of orbits of its action on the vertices. As an extreme case, note that knowing that the automorphism group of a graph is trivial yields almost no information about the structure of the graph since almost all finite graphs have a trivial automorphism group, [4, Corollary 2.3.3]). To generalize the concept of automorphism, we propose to study partial automorphisms, and use Inverse Semigroup Theory, that is often viewed as a generalization of Group Theory thanks to the Wagner-Preston theorem, which is an analogue of Cauley's theorem for groups:

Theorem 1.3 (Wagner-Preston)**.** *Every finite inverse semigroup is isomorphic to an inverse subsemigroup of the symmetric inverse semigroup of all partial bijections of some finite set V.*

We study *the partial automorphism monoid* $PAut(\mathcal{B})$ *of a finite combinatorial structure* $\mathcal{B}$ instead of automorphism group $Aut(\mathcal{B})$. As the partial automorphism monoid $PAut(\mathcal{B})$ is a more complex algebraic structure, it may reveal some information about $\mathcal{B}$ even in cases when use of group theory is rather limited. Earlier attempts in this direction, as well as our results for graphs, directed graphs and edge-colored graphs are reviewed in Section 3.

2 Preliminaries

All the groups, inverse semigroups and monoids considered in our paper are finite, and so are the sets upon which they act.

2.1 Combinatorial structures

A *combinatorial structure* $\mathcal{C} = (V, \mathcal{F})$ consists of a (finite) non-empty set V and a family $\mathcal{F}$ of subsets of V, $\mathcal{F} \subseteq \mathcal{P}(V)$. Examples include graphs, directed graphs, hypergraphs, geometries, designs, etc. An *automorphism* of a combinatorial structure $(V, \mathcal{F})$ is a permutation $\varphi \in \mathcal{S}ym(V)$ satisfying the property $\varphi(B) \in \mathcal{F}$, for all $B \in \mathcal{F}$. The group of all automorphisms of $\mathcal{C}$ will be denoted by $Aut(\mathcal{C})$. It is clear that $Aut(\mathcal{C}) \leq Sym(V)$, the symmetric group on set V.

In particular, a *graph* is an ordered pair $\Gamma = (V, E)$, where V is the set of vertices, and E is the set of (undirected) edges, which is a set of 2-element subsets of V. Similarly, a *digraph* is an ordered pair $\Gamma = (V, E)$, with V being the set of vertices, and E the set of (directed) edges, consisting of ordered pairs of vertices. Graphs can naturally be regarded as special digraphs where each edge $\{e_1, e_2\}$ of the graph is replaced by two directed edges of opposite directions, (e_1, e_2) and (e_2, e_1). In both cases, we use the notation $V(\Gamma)$ and $E(\Gamma)$ for V and E, respectively. Furthermore, we also consider *edge-colored digraphs*, that is, structures $\Gamma = (V, E_1, \ldots, E_l)$, where $\{1, \ldots, l\}$ is the set of colors, and $E_c \subseteq V \times V$ $(c \in \{1, 2, \ldots, l\})$ are the pairwise disjoint sets of (directed) edges of color c. In this case, $V(\Gamma)$ and $E(\Gamma)$ stands for V and $\bigcup_{c=1}^{l} E_c$, respectively. The way edge-colored digraphs arise naturally is as Cayley color graphs.

2.2 Inverse Monoids

A non-empty set together with an associative multiplication is called a semigroup, and a semigroup admitting an identity (neutral) element is called a monoid. A monoid $\mathcal{S}$ is said to be an *inverse monoid* if for every $s \in \mathcal{S}$, there exists a unique element $s^{-1} \in \mathcal{S}$, called the inverse of s, such that $ss^{-1}s = s$ and $s^{-1}ss^{-1} = s^{-1}$ hold. Note that the operation of taking inverse has the properties that $(s^{-1})^{-1} = s$ and $(st)^{-1} = t^{-1}s^{-1}$ for any $s, t \in \mathcal{S}$.

A typical example of an inverse monoid is the the *symmetric inverse monoid* on a set X, denoted $PSym(X)$, and defined as follows: The underlying set of $PSym(X)$ is the set of all bijections between subsets of X, including the empty set. The elements of $PSym(X)$ are called *partial permutations* of X. If $\varphi\colon Y \to Z \in PSym(X)$ then Y and Z are the *domain* and *range* of φ denoted $dom\varphi$ and $ran\varphi$, respectively. The common size $|dom\varphi| = |ran\varphi|$ of the sets $dom\varphi$ and $ran\varphi$ is called the *rank* of φ. The multiplication on $PSym(X)$ is the usual composition of partial maps defined for a pair of partial permutations $\varphi_1\colon Y_1 \to Z_1$ and $\varphi_2\colon Y_2 \to Z_2$ to be the partial permutation $\varphi_2\varphi_1\colon \varphi_1^{-1}(Z_1 \cap Y_2) \to \varphi_2(Z_1 \cap Y_2)$ where $(\varphi_2\varphi_1)(x) = \varphi_2(\varphi_1(x))$ for any $x \in \varphi_1^{-1}(Z_1 \cap Y_2)$. For every $\varphi \in PSym(X)$, the inverse of φ in $PSym(X)$ is just the usual inverse φ^{-1} of the bijection $\varphi\colon dom\varphi \to ran\varphi$. The identity element of $PSym(X)$ is the identity map id_X on X, and $PSym(X)$ also has a zero element, the empty map $id_\emptyset$. It is clear that if Γ is a graph, a digraph, or an edge-colored digraph then $PAut(\Gamma)$ is an inverse submonoid of $PSym(V(\Gamma))$. For further details on Inverse Monoids see [10].

3 Partial Automorphism Monoid

In this section we review the results for Partial Automorphism Monoids of combinatorial structures. Let $(V, \mathcal{F})$ be a combinatorial structure and $U \subseteq V$. The block system $\mathcal{F}'$ of the *substructure induced* by U, $(U, \mathcal{F}')$, is the system of all blocks $F \in \mathcal{F}$ that are subsets of U. A *partial automorphism* of a combinatorial structure $(V, \mathcal{F})$ is an isomorphism between two *induced* substructures of $(V, \mathcal{F})$. The set of *all partial automorphisms* of $\mathcal{C} = (V, \mathcal{F})$ is denoted $\mathrm{PAut}(\mathcal{C})$ and $\mathrm{PAut}(\mathcal{C}) \leq PSym(V)$. In particular for graphs, a *partial automorphism* of a graph is an isomorphism between its two induced subgraphs.

One source of motivation to study partial automorphisms comes from the graph theory. As an example, we mention the long-standing open problem called *Graph Reconstruction Conjecture*, first introduced in [8]:
Given a finite graph $\Gamma = (\{v_1, \ldots, v_n\}, E)$ of order n, let the *deck of* Γ, $\mathrm{Deck}(\Gamma)$, be the multiset consisting of the subgraphs $\Gamma - v_i$ $(1 \leq i \leq n)$ induced by $n-1$ vertices of Γ. The Graph Reconstruction Conjecture predicts the unique 'reconstructability' of any graph Γ of order at least 3 from its $\mathrm{Deck}(\Gamma)$. In other words, the multisets $\mathrm{Deck}(\Gamma_1)$ and $\mathrm{Deck}(\Gamma_2)$ coincide if and only if $\Gamma_1 \cong \Gamma_2$ for any pair of graphs Γ_1, Γ_2 of order at least 3. This problem is closely related to partial automorphisms. Namely, any two induced subgraphs $\Gamma - v_i$ and $\Gamma - v_j$ $(i \neq j)$ admit at least one partial isomorphism φ with domain of size $n-2$, the 'identity' isomorphism, between $(\Gamma - v_i) - v_j$ and $(\Gamma - v_j) - v_i$. Clearly, if $\Gamma - v_i$ and $\Gamma - v_j$ admit exactly one partial isomorphism φ with domain of size $n-2$, Γ is reconstructable from $\Gamma - v_i$ and $\Gamma - v_j$ alone, by identifuing v and $\varphi(v)$, for each v in the domain of φ. Furthermore, two induced subgraphs $\Gamma - v_i$ and $\Gamma - v_j$ of Γ (or sometimes the vertices v_i, v_j) are said to be *pseudo-similar* if $\Gamma - v_i \cong \Gamma - v_j$, but no automorphism of Γ maps v_i to v_j and $\Gamma - v_i$ to $\Gamma - v_j$. Using the language of partial automorphisms: $\Gamma - v_i$ and $\Gamma - v_j$ are

pseudo-similar, if PAut(Γ) contains a partial automorphism mapping $\Gamma - v_i$ to $\Gamma - v_j$ that cannot be extended to a full automorphism of Γ. It has been claimed in [9] that the Graph Reconstruction Conjecture holds for graphs containing no pseudo-similar vertices.

In the rest of this section, we address two closely related classification problems concerning the partial automorphism monoids of graphs, digraphs and edge-colored digraphs. For related concepts and details of proofs see [7].

In Theorems 3.1 and 3.2, we characterize those inverse submonoids $\mathcal{S}$ of the inverse monoid $PSym(X)$ which admit the existence of a graph, digraph or edge-colored digraph Γ with set of vertices X, such that the partial automorphism monoid PAut(Γ) is *equal* to $\mathcal{S}$.

Theorem 3.1. [Partial automorphism monoids of graphs] *Given an inverse submonoid $S \leq PSym(X)$, where X is a finite set, there exists a graph with vertex set X whose partial automorphism monoid is S if and only if the following conditions hold:*

1. *S is a full inverse submonoid of $PSym(X)$,*
2. *for any compatible subset $A \subseteq S$ of rank 1 partial permutations, if S contains the join of any two elements of A, then S contains the join of the set A,*
3. *the rank 2 elements of S form at most two -classes,*
4. *the -classes of rank 2 elements are nontrivial.*

Theorem 3.2. [Partial automorphism monoids of edge-colored digraphs] *Given an inverse submonoid $\mathcal{S}$ of X, where X is a finite set, there exists an edge-colored digraph $\Gamma = (X, E_1, \dots, E_l)$ whose partial automorphism monoid* PAut(Γ) *is equal to $\mathcal{S}$ if and only if the following conditions hold:*

1. *$\mathcal{S}$ is a full inverse submonoid of X,*
2. *for any compatible subset $A \subseteq \mathcal{S}$ of rank 1 partial permutations, if $\mathcal{S}$ contains the join of any two elements of A, then $\mathcal{S}$ contains the join of the set A.*

These results are reminiscent of the more specialized problem from the group theory of the classification of the finite groups that admit a Graphical Regular Representation (GRR) - see Section 1.

Building on Theorems 3.1 and 3.2, we give a similar description in Theorems 3.3 and 3.4 for the finite inverse monoids which are *isomorphic* to partial automorphism monoids of finite graphs, digraphs or edge-colored digraphs. The transition between the partial permutation case and the abstract case is provided by a slightly altered version of the Munn representation.

Theorem 3.3. [Partial automorphism monoids of graphs, up to isomorphism] *Given a finite inverse monoid S, there exists a finite graph whose partial automorphism monoid is isomorphic to S if and only if the following conditions hold:*

1. *S is Boolean,*
2. *S is fundamental,*
3. *for any subset $A \subseteq S$ of compatible 0-minimal elements, if all 2-element subsets of A have a join in S, then the set A has a join in S,*
4. *S has at most two $\mathcal{D}$-classes of height 2,*
5. *the $\mathcal{H}$-classes of the height 2 $\mathcal{D}$-classes of S are nontrivial.*

Theorem 3.4. [Partial automorphism monoids of edge-colored digraphs, up to isomorphism] *Given a finite inverse monoid $\mathcal{S}$, there exists a finite edge-colored digraph whose partial automorphism monoid is isomorphic to $\mathcal{S}$ if and only if the following conditions hold:*

1. *$\mathcal{S}$ is Boolean,*
2. *$\mathcal{S}$ is fundamental,*
3. *for any subset $A \subseteq \mathcal{S}$ of compatible 0-minimal elements, if all 2-element subsets of A have joins in $\mathcal{S}$, then the set A has a join in $\mathcal{S}$.*

It turns out that the class of finite inverse monoids arising as partial automorphism monoids of (edge-colored di)graphs is very restrictive. This is in contrast to the result of Frucht (Section 1, Theorem1.1).

There were several attempts to establish Frucht type of results in the setting of inverse semigroups. One has been obtained in [11].

Theorem 3.5 (Nemirovskaya 1997). *If S is a finite inverse semigroup, then there exists a weighted graph Γ such that $S \cong PAut_\omega(\Gamma)$.*

In [11], it is proved that every finite inverse semigroup is isomorphic to the partial weighted automorphism monoid of a finite weighted graph, where a weighted graph is a graph whose vertices are assigned values from a lower semilattice, and a partial weighted automorphism is a partial graph automorphism, which preserves the weights of the vertices, and whose domain and range are required to be maximal sets of vertices with the property that their weights form a principal order ideal in the semilattice of weights. Given an inverse monoid S, the first step of the proof in constructing the appropriate weighted graph is to consider the Cayley color graph Γ of S, and to show that the Wagner–Preston representation of S consists of partial automorphisms of the edge-colored digraph Γ.

The latter result [14] states that the partial automorphisms of the Cayley color graph of an inverse semigroup, whose domains and ranges are maximal sets of vertices where each element can be reached from a unique vertex, form an inverse monoid isomorphic to the original inverse monoid.

Theorem 3.6 (Sieben 2008)**.** *The inverse semigroup of partial automorphisms of the* **Cayley color graph** *of an inverse semigroup is isomorphic to the original inverse semigroup.*

4 Hypergraphs

In this section, we consider *k-uniform hypergraphs*, called k-hypergraphs, and briefly review our results for Regular Representations on Hypergraphs problem.

Problem 4.1. *Classify finite groups G that admit a regular representation as the full automorphism group of some k-hypergraph.*

We ask which finite groups G admit a k, $0 \leq k \leq |G|$, such that there exists a set of k-hyperedges $\mathcal{H} \subseteq \mathcal{P}_k(G)$ with the property that the full automorphism group of the k-hypergraph $(G, \mathcal{H})$ acts regularly on G.

A *hypergraph* $\Gamma = (V, \mathcal{H})$ consists of a set V and a collection $\mathcal{H}$ of subsets of V. A hypergraph is said to be *k-uniform* if all the subsets in $\mathcal{H}$ are of the size k, i.e., $\mathcal{H} \subseteq \mathcal{P}_k(V)$. We will call the elements from $\mathcal{H}$ *hyperedges*, or more specifically, *k-hyperedges* of Γ. The *automorphism group* of a k-hypergraph $\Gamma = (V, \mathcal{H})$, denoted $\mathrm{Aut}(\Gamma)$, is the group of permutations of V that preserve the k-hyperedges, i.e., permutations $\varphi \in Sym_V$ with the property $\varphi(H) \in \mathcal{H}$, for all $H \in \mathcal{H}$. A finite group G admits a *regular representation as the full automorphism group of a k-uniform hypergraph* if there exists a set of k-hyperedges $\mathcal{H} \subseteq G$ for which $Aut(G, \mathcal{H}) = G_L$.

Our results mostly concern the case $k = 3$. The case $k = 2$ is the original GRR problem (Section 1, Theorem 1.2).

The more general case of this question concerning hypergraphs with hyperedges of varying sizes has already been settled in [6], where it has been shown that a hypergraph (but not necessarily a k-uniform hypergraph) whose full automorphism group is equal to the left regular representation G_L of G exists for all finite groups but $\mathbb{Z}_3$, $\mathbb{Z}_4$, $\mathbb{Z}_5$, and $\mathbb{Z}_2^2$. The results in [6] rely heavily on the hyperedges being of varying sizes, and thus mimic the situation in DRR (Section 1).

For the case of cyclic groups, we have the following theorem.

Theorem 4.2. *A cyclic group $\mathbb{Z}_n$, $n \geq 6$, admits a regular representation on a k-uniform hypergraph $(\mathbb{Z}_n, \mathcal{H})$ if and only if* $3 \leq k \leq n - 3$.

We now introduce the following generalization of Cayley graphs.

Let G be a group, and let $X_1, X_2, \dots, X_{k-1}$ be subsets of G that do not contain the identity 1_G. The *Cayley k-hypergraph* $C_k(G; X_1, X_2, \dots, X_{k-1})$ is the incidence structure $(G, \mathcal{H})$ with $\mathcal{H}$ being the set of all k-subsets of the form

$$\{g, gx_1, gx_1x_2, \ \dots, \ gx_1x_2 \dots x_{k-1}\},$$

$g \in G$, and $x_i \in X_i$, for $1 \leq i \leq k-1$. Note that we require that the blocks have exactly k vertices, i.e., all the group elements $g, gx_1, gx_1x_2, \ \dots, \ gx_1x_2 \dots x_{k-1}$ must be different.

The automorphism group of a k-hypergraph $C_k(G; X_1, X_2, \dots, X_{k-1})$ is related to the groups $Aut(C(G, X_i))$. Since graph automorphisms preserve k-arcs,

$$Aut(C(G, X)) \leq Aut(C_k(G; X, X, \dots, X)).$$

The next lemma presents sufficient conditions for this inclusion to be an identity. The *girth* of a graph $\Gamma = (V, \mathcal{E})$ is the number of edges in a smallest cycle in Γ.

Lemma 4.3. *Let $k \geq 2$ be an integer, and $C(G, X)$ be a Cayley graph of girth $g > 2k-2$ and valency $|X| > k-1$. Then*

$$Aut(C(G, X)) = Aut(C_k(G; X, X, \dots, X)).$$

The proof of this lemma uses the fact that graphs of large girth are locally isomorphic to trees.

Corollary 4.4. *If a finite group G admits a GRR of girth $g > 2m-2$ and valency r, then G can be regularly represented as the full automorphism group of some k-hypergraph for all $2 \leq k \leq \min\{m, r-1\}$.*

In particular, any finite group G that admits a GRR of degree at least 4 and not containing 3- or 4-cycles, admits a 3-uniform regular representation.

References

[1] L. Babai, *Finite digraphs with given regular automorphism groups*, Period. Math. Hungar. Vol 11 (4) (1980), 257-271.

[2] R. Frucht, *Herstellung von Graphen mit vorgegebener abstrakter Gruppe*, J. Compos. Math. 6 (1938), 239-250.

[3] C.D.Godsil, *GRR's for non-solvable groups*, Algebraic methods in graph theory, Vol. I., II. (Szeged, 1978), 221-239.

[4] C. Godsil and G. Royle, *Algebraic Graph Theory*, Springer-Verlag, New York (2001).

[5] W. Imrich, *On graphical regular representations of groups*, Colloq. Math. Soc. Janos Bolyai, Vol. 10 (1975), 905-925.

[6] R. Jajcay, *Representing finite groups as regular automorphism groups of combinatorial structures*, Ars Combinatoria 62 (2002), 51-64.

[7] R. Jajcay, T.B. Jajcayová, N. Szakács, and M. B. Szendrei, *Inverse monoids of partial graph automorphisms*, submitted for publication (2018)

[8] P.J. Kelly, A congruence theorem for trees, *Pacific J. Math.* 7 (1957), 961–968.

[9] J. Lauri, Pseudosimilarity in graphs – a survey, *Ars. Comb.* 46 (1997) 77–95.

[10] M.V. Lawson, *Inverse Semigroups: The Theory of Partial Symmetries*, World Scientific, Singapore (1998).

[11] M. Nemirovskaya, Frucht theorem for inverse semigroups, *Math. Notes* 61 (2) (1997) 246–251.

[12] L.A. Nowitz and M.E. Watkins, *Graphical regular representations of non-abelian groups, I*, Canadian J. Math., 24 (1972), 993-1008.

[13] L.A. Nowitz and M.E. Watkins, *Graphical regular representations of non-abelian groups, II*, Canadian J. Math., 24 (1972), 1009-1018.

[14] N. Sieben, Cayley color graphs of inverse semigroups and groupoids, *Czech. Math. J.* 58 (3) (2008) 683–692.

[15] M.E. Watkins, *The state of the GRR problem*, Proc. Second Czechoslovak Sympos., Prague (1974), 517-522.

An extended abstract on Fibonacci words and Fibonacci numbers

Giuseppe Pirillo
Dipartimento di Matematica ed Informatica U. Dini
Università di Firenze
viale Morgagni 67/A
50134 Firenze Italia
pirillo@math.unifi.it

Abstract

In this extended abstract we briefly recall some of our previous results on the Fibonacci words then we expose our hypothesis on the origin of the Fibonacci numbers. In this way we present a personal survey on these very important precious mathematical objects given us as a gift by Fibonacci, by Knuth and, perhaps, even by the Pythagorean School active in Crotone in the south of Italy from the 6th to the 4th century BC.

Keyword: Common measure, Golden Ratio, Fibonacci Numbers.

Introduction. Let be $\varphi : \{a,b\}^* \to \{a,b\}^*$ the morphism (see [5] and [6]) defined as follows $\{a,b\}$:

$$\varphi(a) = ab, \varphi(b) = a.$$

Put $f_0 = b$ and, for each $n \geq 0$,

$$f_{n+1} = \varphi(f_n).$$

In particular, we have: $f_1 = a$, $f_2 = ab$, $f_3 = aba$, $f_4 = abaab$, $f_5 = abaababa$, $f_6 = abaababaabaab$, $f_7 = abaababaabaababaababa\ldots$. It is clear that, for each $n \geq 2$, f_n is the product (concatenation) $f_{n-1}f_{n-2}$ of f_{n-1} and f_{n-2}. Also, for each $n \geq 0$, $|f_n|$ is the n-th element F_n of the sequence of Fibonacci numbers $F_0 = 1$, $F_1 = 1$, $F_2 = 2$, $F_3 = 3$, $F_4 = 5$, $F_5 = 8$, $F_6 = 13$, $F_7 = 21\ldots$ Note that, for each $n \geq 1$, f_n is a prefix of f_{n+1}.

There exist a unique infinite word, the Fibonacci infinite word f, such that, for each $n \geq 1$, f_n is a prefix of f and we have

$$f = abaababaabaababaababaabaababaabaababaababa\ldots.$$

In order to underline the importance of the Fibonacci word, we recall that in the first book on combinatorics on words [7] (of which we are responsible for the chapter "Repetitive mappings and morphisms") the Fibonacci word appears in the first chapter.

Now, for each $n \geq 2$, denote g_n the product $f_{n-2}f_{n-1}$ and denote h_n the longest common prefixe of f_n and g_n. In particular, we have: $g_2 = ba$, $g_3 = aab$, $g_4 = ababa$, $g_5 = abaabaab$, ... and $h_2 = 1$, $h_3 = a$, $h_4 = aba$, $h_5 = abaaba$ ....

In our "Doctorat d'État ès sciences" we pointed out the importance of the the following three properties of the factors of Fibonacci word:

1) For all $n \geq 2$, *h_nab is a conjugate of h_nba.*

2) It is clear that the first occurrence of palindrome a is in the central position in the palindromic a prefix of f! The first occurrence of the palindrome b is in the central position in the palindromic prefix $h_4 = aba$ of f, the first occurrence of aa is central in $h_5 = abaaba$, ...

3) The factors aa, aab, $aaba$ are respectively are the smallest ones in the lexicographic order among the factors of f of length 2, 3, 4 ...

Properties 1-3, indeed, are very useful for the study of Sturmian and episturmian words. Drawing inspiration from Property 1), we proved in [16]: *a word w is a palindromic prefix of a standard sturmian word if and only if $wab \sim wba$.* Property 2) leads to the definition of episturmian words on which many articles have been written. Property 3) is at the origin of several results on Sturmian and episturmians words.

Now here we quickly give some information about our results by choosing just a few examples and reserving a more detailed review of the works in the complete version of this paper.

For example, in [19] we consider the smallest and the greatest factors with respect to the lexicographic order and we associate to each infinite word r two other infinite words $min(r)$ and $max(r)$. We prove that the inequalities $as \leq min(s) \leq max(s) \leq bs$ characterize standard Sturmian words (proper ones and periodic ones) and that the condition for any $x \in A$ and lexicographic order $<$ satisfying $x = min(A)$ one has $xs \leq min(s)$ characterizes standard episturmian words.

With slight changes we recall here the summary of [11]: *Many papers are concerned with the existence of integer powers in "long enough" words or in infinite words; a classical combinatorial property is wether a given infinite word is k power-free or not, with k natural number. No word on a two letters alphabet can avoid a square but it is well known that the Thue infinite word t on a two letter alphabet does not contain cubes and that the Thue infinite word m on a three letter alphabet does not contain squares. The notion of overlap-free word and more generally the notion of fractional power are considered in many papers. In this paper we prove that the Fibonacci infinite word contains no fractional power with exponent greater than*

$$2 + \tfrac{1+\sqrt{5}}{2}$$

and that for any real number $\epsilon > 0$ the Fibonacci infinite word contains a fractional power with exponent greater than

$$2 + \frac{1+\sqrt{5}}{2} - \epsilon$$

To our knowledge this is the first time that this property for a non rational value is looked for in a given infinite word. The main result of [11] generalizes a result of Karhumäki, [4].

With slight change we also recall here the summary of [1]: *An infinite word is Sturmian if and only if, for any integer n, the number of distinct words of length n occurring in it is $n + 1$. A palindrome is a word that can be read indistinctly from left to right or from right to left. We prove that word s is Sturmian if and only if, for each n, the number of palindromes of length n occurring in s is 1 when n is even and 2 when n is odd.*

In [12], dedicated to Giovanni Prodi, we study the fractional powers of f with exponent greather than $(2 + \Phi)/2$ and we improve some previous results: the above recalled result of Karhumäki, a result of Séébold [26] and also the previous one of Mignosi and Pirillo [11]. In the complete paper we better explain that the fractional power with exponent greater than $(2 + \Phi)/2$ can always be extended at a least to a square.

In [20] we present a new characterization of circular code that is a notion studied in theoretical biology and also in several of our articles. The subject is intimately related with the notion of Fibonacci word and presented during an invited talk in *Workshop on Fibonacci Words* in Turku in 2006.

In [17], *in memoriam Gian-Carlo Rota*, we present several examples of properties of Fibonacci word. Using the words of Jean-Paul Allouche we try *to show that "reasonable" properties of the Fibonacci word extend to all Sturmian words.*

In [14], we prove that the factors of f of some factorizations are codes (in the sense of the variable length code theory). For example, let $f = u_0u_1u_2\dots$ a factorization of f as a product of finite and non-empty words: if the length of u_i is F_{2i+1} [resp. $F_{2(i+1)}$] then the u_i ($i \geq 0$) form a prefix code.

The Pythagorean origin of Fibonacci numbers. In this section we summarize our paper [24]. It is well known that, given three consecutive Fibonacci numbers $F_i \leq F_{i+1} < F_{i+2}$, the following *Cassini identity* $F_iF_{i+2} - F_{i+1}^2 = (-1)^i$ holds.

We point out that, in our opinion, this identity is, in a sense, a "translation" of the exact Pythagorean identity between the side b and the diagonal a of regular pentagon $b(b + a) = a^2$. (The details are in [24] and, will be repeted in the complete version of this paper.) More precisely, our opinion is that the discovery of incommensurability and of the previous equalities came "almost simultaneously", most likely first the Pythagorean identity and immediately after the Cassini identity.

We introduce a definition which will be crucial in the rest of the paper.

Definition 1. *Let β a positive integer. When there exists a positive integer α such that, for some non-negative integer γ, the equality*

$$\beta(\beta+\alpha)-\alpha^2=(-1)^\gamma$$

holds, then we say that β is a Hippasus number *and that α is a* Hippasus successor *of β.*

The following proposition holds

Proposition 1. *Any Hippasus number is a Fibonacci number.*

The following lemmas allow us to prove the following Proposition 2

Lemma 1. *The number* 1 *is a Hippasus number and* 1 *itself is one of its Hippasus successor.*

Lemma 2. *The number* 1 *has also* 2 *as a Hippasus successor.*

Lemma 3. *No positive integer different from* 1 *and* 2 *is a Hippasus successor of* 1*.*

Lemma 4. *A Hippasus number greater than* 1 *has a unique Hippasus successor.*

Lemma 5. *Let β be a Hippasus number and α be a Hippasus successor of β. Then $\alpha-\beta\leq\beta$.*

Lemma 6. Let β be a Hippasus number and α be a Hippasus successor of β with $\alpha>\beta$. Then $\alpha-\beta$ is a Hippasus number and β is a Hippasus successor of $\alpha-\beta$.

Lemma 7. *Let $\beta\geq 1$ be a Hippasus number and α a Hippasus successor of β. If $\alpha-\beta=\beta$ then $\alpha-\beta=1$, $\beta=1$ and $\alpha=2$.*

Proposition 2. *Any Hippasus number is a Fibonacci number.*

Hence we have

Proposition 3. *A positive integer is a Hippasus number if, and only if, it is a Fibonacci number.*

References

[1] X. Droubay, Pirillo. *Palindromes and Sturmian words*, *Theoret. Comput. Sci.*, 223(1-2):73–85, 1999.

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

[3] Fibonacci (Leonardo Pisano, Bigollo), *Liber abbaci* pubblicato secondo la lezione del Codice Magliabechiano C. 1, 2616, Badia Fiorentina, n. 73 da Baldassarre Boncompagni, socio ordinario dell'Accademia pontificia de' nuovi Lincei, Roma, Tipografia delle scienze matematiche e fisiche, 1857.

[4] J. Karhumäki, *On cube-free ω-words generated by binary morphism*, Discr. Appl Math., 1983, 5, pp. 279-297.

[5] D. E. Knuth, *The Art of Computer Programming*, volume 1: Fundamental Algorithms, Addison-Wesley, 1968.

[6] D. E. Knuth, J. H. Morris, Jr., V. R. Pratt, *Fast pattern matching in strings SIAM J. Comput.*, **6** (2) (1977) 323–350.

[7] M. Lothaire. *Combinatorics on words*, volume 17 of *Encyclopedia of Mathematics and its Applications.* Addison-Wesley Publishing Co., Reading, Mass., 1983.

[8] Yu. V.Matiyasevich *Enumerable sets are diophantine*, Soviet. Math. Doklai, vol. 11 (1970), N. 2.

[9] Yu. V.Matiyasevich, *Hilberts Tenth Problem: Diophantine Equations in the Twentieth Century*, Translated by R. Cooke, in Mathematical Events of the Twentieth Century Edited by A. A. Bolibruch, Yu. S. Osipov, and Ya. G. Sinai, Moscow, Russia, 2003.

[10] G. Pirillo, *On a combinatorial property of Fibonacci infinite word* Pure Math. Appl. Ser. A, 1(2):143–147, 1990).

[11] F. Mignosi, G, Pirillo. *Repetitions in the Fibonacci infinite word*, *RAIRO Inform. Théor. Appl.*, 26(3):199–204, 1992.

[12] G. Pirillo. *Fibonacci numbers and words*, *Discrete Math.*, 173(1-3):197–207, 1997. Dedicated to Giovanni Prodi.

[13] G. Pirillo. *From the Fibonacci word to Sturmian words*, *Publ. Math. Debrecen*, 54(suppl.):961–971, 1999. Automata and formal languages, VIII (Salgótarján, 1996).

[14] G. Pirillo. *Some factorizations of the Fibonacci word* *Algebra Colloq.*, 6(4):361–368, 1999.

[15] G. Pirillo. *From the Fibonacci word to Sturmian words II*, *Pure Math. Appl.*, 11(3):533–537, 2000.

[16] G. Pirillo. *A curious characteristic property of standard Sturmian words*, In *Algebraic combinatorics and computer science*, pages 541–546. Springer Italia, Milan, 2001.

[17] G. Pirillo. *Fibonacci word and Sturmian words*, in memoriam Gian-Carlo Rota, *Sci. Math. Jpn.*, 55(3):641–647, 2002.

[18] G. Pirillo, *A curious characteristic property of standard Sturmian words*, in "Algebraic combinatorics and computer science", Springer Italia, Milan, 2001, 541–546.

[19] G. Pirillo, *Inequalities characterizing standard Sturmian and episturmian words*, *Theoret. Comput. Sci.*, **341** (1-3) (2005), 276–292.

[20] G. Pirillo, *A hierarchy for circular codes*, Fibonacci, Turku, 2006. RAIRO-Theor. Inf. Appl. 42 (2008) 717728.

[21] G. Pirillo, *Some recent results of Fibonacci numbers, Fibonacci words and Sturmian words*, Southeast Asian Bull. of Math., to appear on vol 43

[22] G. Pirillo, *La scuola pitagorica ed i numeri di Fibonacci*, Archimede, 2, 2017.

[23] G. Pirillo, *Figure geometriche su un portale del Duomo di Prato*, *Prato Storia e Arte*, **121**, (2017).

[24] G. Pirillo, *A characterzation of Fibonacci numbers*, ArXiv, 2017.

[25] F. P. Ramsey, *On a problem of formal logic*, *Proc. London Math. Soc*, 30:264–286, 1930.

[26] P. Séébold. *Propriétés combinatoires des mots infinis engendrés par certains morphismes*, Thèse de doctorat, LITP, 85-15, Paris, 1985.

[27] K. von Fritz, *The Discovery of Incommensurability by Hippasus of Metapontum*, Annals of Mathematics, Second Series, **46**, 2 (1945), 242–264.

[28] J. Wasteels, *Quelques Propriétés des Nombres de Fibonacci*, troisième sèr., Mathesis, **3** (1902), 60–62.

Palindromic length of words and morphisms in class $\mathcal{P}$

Petr Ambrož, Ondřej Kadlec, Zuzana Masáková, Edita Pelantová
FNSPE, Czech Technical University in Prague
Trojanova 13, 120 00 Praha 2, Czech Republic

1 Introduction

In 2013, Frid, Puzynina and Zamboni [7] introduced the palindromic length of a finite word w, denoted by $|w|_{\mathrm{pal}}$, as the minimum number of palindromes whose concatenation is equal to w. They conjectured that if there is a constant K such that the palindromic length of every factor in an infinite word $\boldsymbol{u}$ is bounded by K, then $\boldsymbol{u}$ is eventually periodic. Formally, defining for a given infinite word $\boldsymbol{u}$ the function $\mathrm{pal}_{\boldsymbol{u}} : \mathbb{N} \to \mathbb{N}$ by

$$\mathrm{pal}_{\boldsymbol{u}}(n) := \max\{|w|_{\mathrm{pal}} : w \text{ is a factor of length } n \text{ in } \boldsymbol{u}\},$$

the conjecture is that if $\boldsymbol{u}$ is not eventually periodic, then $\limsup_{n\to\infty} \mathrm{pal}_{\boldsymbol{u}}(n) = +\infty$. The authors of [7] proved the conjecture for infinite words which do not contain an r-power for some positive integer r. In particular, the conjecture is true for any aperiodic fixed point of a primitive morphism, as such fixed points have bounded powers [11]. In fact, the general Theorem 8 in [7] ensures unbounded palindromic length for any infinite word satisfying the so-called (k,l)-condition. It is likely that with the results of [9] one can show that a fixed point $\boldsymbol{u}$ of any morphism (not necessarily primitive) satisfies $\limsup_{n\to\infty} \mathrm{pal}_{\boldsymbol{u}}(n) = +\infty$. Later, Frid [6] showed that Sturmian words have unbounded palindromic length even if they contain unbounded powers. Palindromic length of Sturmian words is studied also in [2]. It is shown that $\mathrm{pal}_{\boldsymbol{u}}$ can grow arbitrarily slowly. For other infinite words besides Sturmian words and bounded-repetition words the conjecture of $\limsup_{n\to\infty} \mathrm{pal}_{\boldsymbol{u}}(n) = +\infty$ remains open. A contribution to the question was given by Saarela [13] who showed that if the palindromic length is unbounded for factors, it is unbounded also for prefixes. Theorem 7 of [13] implies that the ratio of respective bounds is at most 2.

We study palindromic length of factors of fixed points of primitive morphisms. Here, as we have stated above, the palindromic length in unbounded, whenever the fixed point is not eventually periodic. The main results of this contribution are formulated as Proposition 7 and Theorem 8. We prove that for any primitive morphism φ from the class $\mathcal{P}$ there is a constant $K > 0$ such that the palindromic length of every factor w in the language of φ is less than or equal to $K \ln |w|$. We also provide a method of estimating the constant K.

2 Preliminaries

Let A be a finite set called *alphabet*, its elements are called *letters*. A *word* $w = w_1 \cdots w_n$ (over A) is a finite sequence of elements in A, its *length* (the number of its elements) is denoted by $|w| = n$. The notation $|w|_a$ is used for the number of occurrences of the letter a in w. The *empty word* – unique word of length zero – is denoted by ε. The *concatenation* of words $v = v_1 \cdots v_k$ and $w = w_1 \cdots w_l$ is $vw = v \cdot w = v_1 \cdots v_k w_1 \cdots w_l$. The set of all finite words over A equipped with the operation concatenation of words is a free monoid, denoted by A^*.

For a word $w = w_1 \cdots w_n$ we define its mirror image as $\overleftarrow{w} = w_n \cdots w_1$. A word w is called *palindrome* if $w = \overleftarrow{w}$. The *palindromic length* of a word w, denoted by $|w|_{\mathrm{pal}}$, is the smallest number K of palindromes $p_1, \ldots, p_K$ such that $w = p_1 \cdots p_K$, i.e., the minimal number of palindromes whose concatenation is equal to w. For convenience, we define $|\varepsilon|_{\mathrm{pal}} = 0$.

An infinite sequence of letters $\boldsymbol{u} = (u_i)_{i \geq 1}$ in A is called *infinite word*. The set of all infinite words over A is denoted $A^{\mathbb{N}}$. The word $\boldsymbol{u} \in A^{\mathbb{N}}$ is said to be *eventually periodic* if it is of the form $\boldsymbol{u} = vz^{\omega}$, where $v, z \in A^*$, $z \neq \varepsilon$ and $z^{\omega} = zzz \cdots$.

A *factor* of a (finite of infinite) word w is a finite word v such that $w = w_1 v w_2$ for some words w_1, w_2. If $w_1 = \varepsilon$ then v is called a *prefix* of w, if $w_2 = \varepsilon$ then v is called a *suffix* of w. The set of all factors of an infinite word $\boldsymbol{u}$, called the *language* of $\boldsymbol{u}$, is denoted by $\mathcal{L}(\boldsymbol{u})$.

A *morphism* of the free monoid A^* is a map $\varphi : A^* \to A^*$ such that $\varphi(vw) = \varphi(v)\varphi(w)$ for all $v, w \in A^*$. A morphism of A^*, where $A = \{a_1, \ldots, a_r\}$, is called *primitive* if there is a constant K such that $\varphi^K(a_i)$ contains a_j for every $i, j \in \{1, \ldots, r\}$. The action of the morphism φ is naturally extended to infinite words by concatenation, in particular, we have

$$\varphi(u_0 u_1 u_2 \cdots) = \varphi(u_0)\varphi(u_1)\varphi(u_2) \cdots$$

An infinite word $\boldsymbol{u}$ is called a *fixed point* of the morphism φ if $\boldsymbol{u} = \varphi(\boldsymbol{u})$.

Clearly, a morphism ψ can have several different fixed points, however, if ψ is primitive then all its fixed points have the same language, denoted $\mathcal{L}(\psi)$.

Let $A = \{a_1, \dots, a_r\}$ and let ψ be a morphism of A^*. The *incidence matrix* of ψ is the $r \times r$ matrix $\boldsymbol{M}_\psi$ given by $[\boldsymbol{M}_\psi]_{ij} = |\psi(a_j)|_{a_i}$.

3 Morphisms in class $\mathcal{P}$

Definition 1. A primitive morphism $\psi : A^* \to A^*$ belongs to class $\mathcal{P}$ if there is a palindrome $p \in A^*$ such that for each $a \in A$

$$\psi(a) = pq_a, \qquad \text{where } q_a \in A^* \text{ is a palindrome.} \tag{1}$$

Example 1. The Fibonacci morphism $\varphi_F : a \mapsto ab, b \mapsto a$ belongs to class $\mathcal{P}$; Equation (1) is fulfilled for $p = a, q_a = b, q_b = \varepsilon$.

Example 2. The Thue-Morse morphism $\varphi_{\mathrm{TM}} : a \mapsto ab, b \mapsto ba$ does not belong to class $\mathcal{P}$, however, its square $\varphi_{\mathrm{TM}}^2 : a \mapsto abba, b \mapsto baab$ does ($p = \varepsilon, q_a = abba, q_b = baab$).

The following simple observation is due to Hof, Knill and Simon [8].

Observation 2. *Let ψ be a primitive morphism in the form (1) and let $\boldsymbol{u}$ be a fixed point of ψ. Then*

i) if $w \in \mathcal{L}(\psi)$ then $\psi(w)p \in \mathcal{L}(\psi)$,

ii) if w is a palindrome then $\psi(w)p$ is a palindrome.

By repeated application of Observation 2, one obtains the following corollary, which was first shown in [8].

Corollary 3. *The language of a fixed point of a morphism in class $\mathcal{P}$ contains infinitely many palindromes.*

In fact, as was noticed in [1], the same statement as Corollary 3 is valid for fixed points of morphisms that are not in class $\mathcal{P}$ by themselves, but some of their conjugates is, see Definition 4 below. The reason for that is that languages of infinite words fixed by conjugated primitive morphisms coincide.

Definition 4. Morphisms $\psi_1, \psi_2 : A^* \to A^*$ are said to be *conjugated*, denoted by $\psi_1 \sim \psi_2$, if there is a word $w \in A^*$ such that either $\psi_1(a)w = w\psi_2(a)$ for every $a \in A$ or $w\psi_1(a) = \psi_2(a)w$ for every $a \in A$.

The proof of the following fact can be found for example in [1].

Proposition 5. *Let ψ_1 be a primitive morphism and let ψ_2 be conjugated with ψ_1. Then $\mathcal{L}(\psi_1) = \mathcal{L}(\psi_2)$.*

In [1] the authors also make the observation that any morphism of class $\mathcal{P}$ is conjugated to a morphism of the form (1) where the palindrome p is either the empty word or a single letter. From now on, in view of Proposition 5, we will only consider morphisms in class $\mathcal{P}$ of this form. The following lemma shows how palindromic length of a finite word changes under application of such a morphism.

Lemma 6. *Let $\psi : A^* \to A^*$ be a morphism in class $\mathcal{P}$ in the form* (1)*.*

i) If $p = \varepsilon$, then $|\psi(w)|_{\text{pal}} \leq |w|_{\text{pal}}$ for every $w \in A^*$.

ii) Suppose $|p| = 1$. If $|w|_{\text{pal}}$ is even then $|\psi(w)|_{\text{pal}} \leq |w|_{\text{pal}}$, otherwise $|\psi(w)|_{\text{pal}} \leq |w|_{\text{pal}} + 1$.

iii) If $|\psi(w)|_{\text{pal}} = |w|_{\text{pal}} + 1$ then $|\psi^2(w)|_{\text{pal}} \leq |\psi(w)|_{\text{pal}}$.

The above lemma states that by applying a morphism ψ of class $\mathcal{P}$ to a word, palindromic length can increase by at most one, and this happens only at alternating iterations of the morphism ψ. With this knowledge, we can find an estimate on the growth of the palindromic length $\text{pal}_{\boldsymbol{u}}(n)$.

Proposition 7. *Let $\psi : A^* \to A^*$ be a morphism in class $\mathcal{P}$ such that for each $a \in A$ it holds that $\psi(a) = pq_a$, where $p \in \{\varepsilon\} \cup A$ and q_a is a palindrome. Let us denote*

$$C := \max\{|x|_{\text{pal}} : \exists\, a \in A, x \textit{ is a proper prefix of } q_a\}.$$

Then for a fixed point $\boldsymbol{u}$ of ψ we have

$$\limsup_{n\to\infty} \frac{\text{pal}_{\boldsymbol{u}}(n)}{\ln n} \leq \frac{2C + \frac{3}{2}|p|}{\ln \Lambda},$$

where Λ is the dominant eigenvalue of the incidence matrix of ψ.

Proposition 7 provides an upper estimate on the palindromic length $\text{pal}_{\boldsymbol{u}}(n)$ for any fixed point $\boldsymbol{u}$ of any morphism of class $\mathcal{P}$. The result is valid independently of the size of the alphabet. Reducing our consideration to binary infinite words, we recall the result of Bo Tan [14]. He shows that any binary morphism φ producing a fixed point with infinitely many palindromes is either itself conjugated to a morphism in class $\mathcal{P}$, or this can be said about its second iterate φ^2. This allows us to formulate a summarizing corollary to our Proposition 7.

Theorem 8. *Let $\boldsymbol{u}$ be a fixed point of a primitive morphism over a binary alphabet. Then there is a constant $K > 0$ such that either*

$$\mathrm{pal}_{\boldsymbol{u}}(n) \leq K \ln n \qquad \textit{for all } n \in \mathbb{N},$$

or

$$\mathrm{pal}_{\boldsymbol{u}}(n) \geq Kn \qquad \textit{for all } n \in \mathbb{N}.$$

Note that on morphisms over an alphabet with more than two letters, one cannot prove a result as strong as that of Bo Tan [14]. A counterexample was given on a ternary morphism in [10].

4 Fibonacci and Thue-Morse words

Let us provide an upper bound on the constant K of Theorem 8 for the Fibonacci word $\boldsymbol{f}$ and for the Thue-Morse word $\boldsymbol{t}$.

The Fibonacci word. The Fibonacci morphism $\varphi_F : a \mapsto ab, b \mapsto a$ belongs to class $\mathcal{P}$ (cf. Example 1). Since its fixed point, the Fibonacci word $\boldsymbol{f}$, is a Sturmian word, it follows from the result by Frid [6] that $\limsup_{n\to\infty} \mathrm{pal}_{\boldsymbol{f}}(n) = +\infty$.

Let us apply Proposition 7 in this case. Obviously $p = a$ and $C = 0$ and the dominant eigenvalue of the incidence matrix $\left(\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ of φ_F is the golden mean $\tau = \frac{1+\sqrt{5}}{2}$. Therefore

$$\limsup_{n\to\infty} \frac{\mathrm{pal}_{\boldsymbol{f}}(n)}{\ln n} \leq \frac{3}{2\ln\tau}. \tag{2}$$

The Fibonacci word $\boldsymbol{f}$ is also the fixed point of $\varphi_F^3 : a \mapsto abaab, b \mapsto aba$. Consider morphism $\psi : a \mapsto ababa, b \mapsto aba$. Taking $w = aba$, we see that

$$\varphi_F^3(a)w = abaababa = w\psi(a), \qquad \varphi_F^3(b)w = abaaba = w\psi(b),$$

which by Definition 4 means that $\varphi_F^3 \sim \psi$. According to Proposition 5, we have $\mathcal{L}(\varphi_F^3) = \mathcal{L}(\psi)$. Let us apply Proposition 7 to ψ. Obviously $p = \varepsilon$ and $C = 2$. The dominant eigenvalue of $\boldsymbol{M}_\psi$ is τ^3. Therefore

$$\limsup_{n\to\infty} \frac{\mathrm{pal}_{\boldsymbol{f}}(n)}{\ln n} \leq \frac{4}{3\ln\tau}, \tag{3}$$

which gives a better estimate than (2).

If we use $\psi^2 : a \mapsto ababaabaababaabaababa, b \mapsto ababaabaababa$, which also fixes the Fibonacci word, we have $p = \varepsilon$, $C = 3$, and $\Lambda = \tau^6$. This improves the constant in estimate (3) to $\frac{1}{\ln\tau}$. Making similar considerations for ψ^k, $k \le 13$, we obtain that $K \le \frac{2(k+1)}{3k\ln\tau}$. This makes us conjecture that

$$\limsup_{n\to\infty} \frac{\mathrm{pal}_{\boldsymbol{f}}(n)}{\ln n} = \frac{2}{3\ln\tau}.$$

Let us remark that Frid [5] investigated the palindromic length only of prefixes of the Fibonacci word. Proposition 3 of [5] implies an upper bound $\ln(n)/3\ln(\tau)$ for the palindromic length of a prefix of length n. Together with Saarela's Theorem 7 of [13] it would prove our conjecture $\limsup_{n\to\infty}\mathrm{pal}_{\boldsymbol{u}}(n) \le 2\ln(n)/3\ln(\tau)$. The proof of Frid's Proposition 3 has however not been published yet.

Frid also conjectures that the prefix $w^{(k)}$ of the Fibonacci word whose length written in the Zeckendorf numeration system is $(|w^{(k)}|)_F = (100)^{2k-1}101$ has $|w^{(k)}|_{\mathrm{pal}} = 2k+1$. Should this conjecture be valid, it would imply that

$$\limsup_{n\to\infty} \frac{\mathrm{pal}_{\boldsymbol{f}}(n)}{\ln n} \ge \frac{1}{3\ln\tau}.$$

The Thue-Morse word. Let us consider the Thue-Morse word $\boldsymbol{t}$, i.e., the fixed point of the morphism $\varphi_{TM}^2 : a \mapsto abba, b \mapsto baab$ (cf. Example 2). Similarly to the case of the Fibonacci word we are interested in the constant K where $\limsup_{n\to\infty}\frac{\mathrm{pal}_{\boldsymbol{t}}(n)}{\ln n} \le K$.

Applying Proposition 7 to φ_{TM}^2, where $\Lambda = 4$, $C = 2$, $p = \varepsilon$, we get $K \le \frac{4}{\ln 4}$. Further iteration of the procedure in Proposition 7 with φ_{TM}^{2k} for $k \le 13$ show that $K \le (3 + \frac{1}{k})\frac{1}{\ln 4}$. This leads us to conjecture that

$$\limsup_{n\to\infty} \frac{\mathrm{pal}_{\boldsymbol{t}}(n)}{\ln n} = \frac{3}{\ln 4}.$$

5 Open problems

The palindromic length of finite and infinite words has been introduced in 2013 [7]. Since then, several groups of authors focused on the design of fast algorithms for computing the minimal palindromic factorization, see e.g. [4, 12, 3]. On the other hand, an analytic study of the palindromic length is still in its beginnings. Let us formulate several open questions which we consider of interest.

i) According to [1], any morphism from the class $\mathcal{P}$ can be conjugated to the form $a \mapsto pq_a$ for every $a \in A$ where p is a palindrome of length 1 or the empty word. When studying palindromic length of the Fibonacci and Thue-Morse word, we have conveniently considered a power of the morphism that could be conjugated to a morphism in which the image of every letter is a palindrome, i.e., $p = \varepsilon$. According to our knowledge, question on determining for which morphisms such a power exists, has not been considered yet. Both the the Fibonacci and the Thue-Morse morphism have this nice property, but we do not see why this would be true in general.

ii) In the study of the growth of $\mathrm{pal}_{\boldsymbol{u}}(n)$ we provide a method of finding an upper bound on the constant K, in the estimate $\mathrm{pal}_{\boldsymbol{u}}(n) \leq K \ln n$, which is valid for any fixed point $\boldsymbol{u}$ of any morphism in class $\mathcal{P}$. On the other hand, the proof of Theorem 1 in [7] implies a super-exponential upper bound to the minimum length of a prefix not decomposable to k palindromes, which gives a very rough lower bound on $\mathrm{pal}_{\boldsymbol{u}}(n)$. Frid [5] has focused on improving the lower bound on the palindromic length. Her study is specific for the Fibonacci word $\boldsymbol{f}$. She states a conjecture describing the prefixes w of $\boldsymbol{f}$ having palindromic length $|w|_{\mathrm{pal}}$ strictly bigger than all the shorter prefixes of $\boldsymbol{f}$.

iii) The validity of the conjectured lower bound of Frid [5] would imply that

$$\limsup_{n\to\infty} \frac{\mathrm{pal}_{\boldsymbol{f}}(n)}{\ln n} \geq \frac{1}{3\ln\tau}.$$

Our computations (cf. Section 4) suggest that lim sup should have a bigger value. This is probably caused by the fact that Frid only considers the palindromic length of prefixes of the Fibonacci word. It may be the case that bigger palindromic length is achieved on factors that are not prefixes of $\boldsymbol{f}$. We do not have candidates for such factors. It should be mentioned that Saarela [13] shows equivalence between the unboundedness of the palindromic length when taken over the factors and considering only the prefixes. This, however, does not mean that the growth of the function depending on n should be equal.

Acknowledgments

This work was supported by the project CZ.02.1.01/0.0/0.0/16_019/0000778 from European Regional Development Fund. We also acknowledge financial support of the Grant Agency of the Czech Technical University in Prague, grant No. SGS17/193/OHK4/3T/14.

References

[1] Jean-Paul Allouche, Michael Baake, Julien Cassaigne, and David Damanik. Palindrome complexity. *Theoret. Comput. Sci.*, 292(1):9–31, 2003.

[2] Petr Ambrož and Edita Pelantová. A note on palindromic length of sturmian sequences. Submitted to European J. Combin., 2018.

[3] Kirill Borozdin, Dmitry Kosolobov, Mikhail Rubinchik, and Arseny M. Shur. Palindromic length in linear time. In *28th Annual Symposium on Combinatorial Pattern Matching*, volume 78 of *LIPIcs. Leibniz Int. Proc. Inform.*, Art. No. 23. 2017.

[4] Gabriele Fici, Travis Gagie, Juha Kärkkäinen, and Dominik Kempa. A subquadratic algorithm for minimum palindromic factorization. *J. Discrete Algorithms*, 28:41–48, 2014.

[5] Anna E. Frid. Representations of palindromes in the Fibonacci word. In *Numeration 2018*, 9–12. 2018.

[6] Anna E. Frid. Sturmian numeration systems and decompositions to palindromes. *European J. Combin.*, 71:202–212, 2018.

[7] Anna E. Frid, Svetlana Puzynina, and Luca Q. Zamboni. On palindromic factorization of words. *Adv. in Appl. Math.*, 50(5):737–748, 2013.

[8] A. Hof, Oliver Knill, and Barry Simon. Singular continuous spectrum for palindromic Schrödinger operators. *Comm. Math. Phys.*, 174(1):149–159, 1995.

[9] Karel Klouda and Štěpán Starosta. An algorithm for enumerating all infinite repetitions in a D0L-system. *J. Discrete Algorithms*, 33:130–138, 2015.

[10] Sébastien Labbé. A counterexample to a question of Hof, Knill and Simon. *Electron. J. Combin.*, 21(3):Paper 3.11, 2014.

[11] Brigitte Mossé. Puissances de mots et reconnaissabilité des points fixes d'une substitution. *Theoret. Comput. Sci.*, 99(2):327–334, 1992.

[12] Mikhail Rubinchik and Arseny M. Shur. EERTREE: an efficient data structure for processing palindromes in strings. *European J. Combin.*, 68:249–265, 2018.

[13] Aleksi Saarela. Palindromic length in free monoids and free groups. In *Combinatorics on words*, volume 10432 of *Lecture Notes in Comput. Sci.*, pages 203–213. Springer, Cham, 2017.

[14] Bo Tan. Mirror substitutions and palindromic sequences. *Theoret. Comput. Sci.*, 389(1-2):118–124, 2007.

Undecidable word problem in subshift automorphism groups

Pierre Guillon Emmanuel Jeandel Jarkko Kari
Pascal Vanier

may 2019

Subshifts are sets of colorings of a group G avoiding some family of forbidden finite patterns. They have first been introduced, for $G = \mathbb{Z}$, as a way of discretizing dynamical systems on compact spaces. SFTs correspond to the particular case when only finitely many patterns are forbidden; they are used in information theory to model data streams with coding constraints. When $G = \mathbb{Z}^2$, SFTs turn out to be, up to recoding, the sets of colorings defined by some Wang tiles, and a tool to study decidability questions. When G is the free group, subshifts can be seen as sets of colorings of a tree; the case of the free monoid is known to correspond to the so-called tree languages, and SFTs to tree automata [1–3].

Subshifts are hence both a means to model complex systems, and to provide complete problems for a wide range of complexity and computability classes.

An automorphism of a subshift X is a shift-invariant continuous bijection from X onto X, or equivalently a reversible cellular automaton on X. Understanding the automorphism group of a subshift can be seen as a way to understand how constraints over the "physical space" (the possible configurations) restrict the interactions between the cellular automata that act on them.

Little is known about automorphism groups of subshifts in general, besides that they are countable. As an example of our ignorance, it is a long-standing open problem whether the automorphism groups of the 2-symbol full shift and of the 3-symbol full shift are isomorphic.

Many results have nevertheless been recently reached, for $G = \mathbb{Z}$, in two kinds:

- The automorphism group of some *large* subshifts (positive-entropy SFTs, ...) is rich [4]: it contains all finite groups, finitely generated abelian groups, countable free and free abelian groups, ... This means that when you pick some reversible cellular automata over these subshifts, they can have very complex interactions. In [5], it is proved that periodicity of cellular automata is undecidable, which can be interpreted as the torsion problem for the automorphism group of these subshifts.

- The automorphism group of some *small* subshifts (small complexity function, substitutive, ...) is poor [6–8]: in the most extreme case, it is proven to be virtually $\mathbb{Z}$, which means that every reversible cellular automaton is essentially the shift (up to finitely many local permutations).

With $G = \mathbb{Z}^d$ when $d \geq 2$, computability has played a central role in the study of SFTs. From a computability point of view, it is noted in [9] that their automorphism groups have a computably enumerable word problem (which is formalized in a general setting in Theorem 3). The word problem essentially corresponds to picking up a reversible cellular automaton rule over this subshift, and asking whether it is equal to the identity. We show that it can be arbitrarily complex: for any given computably enumerable degree, one can construct an SFT the automorphism group of which has a word problem with this degree (Corollary 6).

1 Preliminaries

1.1 Computability

Computability problems are naturally defined over $\mathbb{N}$, but can easily be extended through subsets of it, cartesian products or disjoint union (by canonically injecting $\mathbb{N}$ in sets of tuples). For example, if $\mathcal{G} \subset \mathbb{N}$, then the set $\mathcal{G}^*$ of tuples admits a simple injection into $\mathbb{N}$. Let us fix a (computable) countable set I, that we can identify to integers.

Let us define the following reducibility notions, for $X, Y \subset I$:

1. X is *enumeration-reducible* to Y, $X \leq_e Y$, if: from any x and any integer $i \in \mathbb{N}$, one can compute a finite set $Y_i(x)$ such that $x \in X$ if and only if $\exists i \in \mathbb{N}, Y_i(x) \subset Y$.

2. X is *positive-reducible* to Y, $X \leq_p Y$, if: from any x, one can compute finitely many finite sets $Y_0(x), \ldots, Y_{n-1}(x)$ such that $x \in X$ if and only if $\exists i < n, Y_i(x) \subset Y$.

3. X is *one-one-reducible* to Y, $X \leq_1 Y$, if, $X \leq_m Y$ and the corresponding ϕ is one-to-one.

See [10] for a reference on computability-theoretical reductions.

1.2 Monoids and groups

We will deal with countable monoids $\mathbb{M} = \mathcal{G}^*/R$, where $\mathcal{G} \subset \mathbb{N}$, $\mathcal{G}^*$ is the free monoid generated by symbols from $\mathcal{G}$ and R is a monoid congruence[1]. The monoid is always implicitly endowed with its generating set $\mathcal{G}$ (later, some problems may depend on the presentation). Each element of the monoid is represented by a word $u \in \mathcal{G}^*$, but the representation is not one-to-one (except for the free monoid itself). We note $i =_{\mathbb{M}} j$ if $\pi(i) = \pi(j)$ and $\pi : \mathcal{G}^* \to \mathbb{M}$ is the natural quotient map.

It is also clear that the concatenation map, which from any two words $i, j \in \mathcal{G}^*$ outputs $i \cdot j$, which is one representative of the corresponding product, is computable. We say that $\mathbb{M}$ is an *effective group* if, additionally, there is a computable map $\psi : \mathcal{G}^* \to \mathcal{G}^*$ such that $i \cdot \psi(i) =_{\mathbb{M}} \psi(i) \cdot i =_{\mathbb{M}} \lambda$.

The *equality problem* of $\mathbb{M}$, endowed with generating family $\mathcal{G}$, is the set of pairs $\left\{ (i,j) \in (\mathcal{G}^*)^2 \middle| i =_{\mathbb{M}} j \right\}$, endowed with a natural enumeration so that we can consider it as a computability problem.

1.3 Subshifts

Let $\mathcal{A}$ be a finite alphabet with at least two letters, and $\mathbb{M}$ a group (most of the following should be true if $\mathbb{M}$ is a cancellative monoid though). In a first reading, the reader is encouraged to think of $\mathbb{M}$ as being $\mathbb{Z}$: the results are not significantly simpler in that specific setting (except those that mention 1D SFT). A finite *pattern* w over $\mathcal{A}$ with *support* $W = \mathcal{S}(w) \Subset \mathcal{G}^*$ is a map $w = (w_i)_{i \in W} \in \mathcal{A}^W$. An element of $\mathcal{A}^{\mathbb{M}}$ is called a *configuration*. Configurations can be seen as colorings of the Cayley graph by the letters of $\mathcal{A}$ and patterns can be seen as finite configurations. Depending on the context, note that, for $g \in \mathcal{S}(w)$, w_g may either be an element of $\mathcal{A}$ or a subpattern with support $\{g\}$. If $g \in \mathcal{G}^*$ and w is a pattern, we will denote by $\sigma^g(w)$ the pattern with support $W \cdot g$ such that $\sigma^g(w)_{i \cdot g^{-1}} = w_i$ for all $i \in \mathcal{S}(w)$.

We are interested in $\mathcal{A}^{\mathbb{M}}$, which is a Cantor set, when endowed with the prodiscrete topology, on which $\mathbb{M}$ acts continuously by (left) shift: we note $\sigma^i(x)_j = x_{i.j}$ for $i, j \in \mathbb{M}$ and $x \in \mathcal{A}^{\mathbb{M}}$. $\mathcal{A}^{\mathbb{M}}$ is thus called the *full shift* on alphabet $\mathcal{A}$. A *subshift* is a closed σ-invariant subset $X \subset \mathcal{A}^{\mathbb{M}}$. Equivalently, X can be defined as the set $X_{\mathcal{F}} := \left\{ x \in \mathcal{A}^{\mathbb{M}} \middle| \forall i \in \mathbb{M}, \forall w \in \mathcal{F}, \exists j \in \mathcal{S}(w), x_{i \cdot j} \neq w_j \right\}$ avoiding a language $\mathcal{F} \subset \bigsqcup_{W \Subset \mathcal{G}^*} \mathcal{A}^W$, which is then called a (defining) *forbidden language*. If $\mathcal{F}$ can be chosen finite, the subshift is called *of finite type* (SFT); if it can be chosen computably enumerable, it is called *effective*.

The *language* with *support* $W \Subset \mathcal{G}^*$ of subshift X is the set $\mathcal{L}_W(X) :=$

[1] We could deal in the same way with semigroups, by prohibiting the empty word.

$\left\{ (x_{\pi(i)})_{i\in W} \middle| x \in X \right\}$; the *language* of X is $\mathcal{L}(X) = \bigsqcup_{W \Subset \mathcal{G}^*} \mathcal{L}_W(X)$, and its *colanguage* is the complement of it. The latter is a possible defining forbidden language. If $u \in \mathcal{L}_W(X)$, we define the corresponding *cylinder*

$$[u] = \left\{ x \in X \middle| \forall i \in W, x_{\pi(i)} = u_i \right\}.$$

1.4 Homomorphisms

Let $X \subset \mathcal{A}^{\mathbb{M}}$ and $Y \subset \mathcal{B}^{\mathbb{M}}$ be subshifts. Denote $\mathcal{E}nd(X,Y)$ the set of *homomorphisms* (continuous shift-commuting maps) from X to Y, and $\mathcal{A}ut(X,Y)$ the set of bijective ones (*conjugacies*). We also note $\mathcal{E}nd(X) = \mathcal{E}nd(X,X)$ the monoid of *endomorphisms* of X, and $\mathcal{A}ut(X) = \mathcal{A}ut(X,X)$ the group of its *automorphisms*.

If $\mathbb{M}$ is finitely generated, then homomorphisms correspond to block maps (and endomorphisms to cellular automata), thanks to a variant of the Curtis-Hedlund-Lyndon theorem [11].

Theorem 1. *Let $\mathbb{M}$ be finitely generated. A map Φ from subshift $X \subset \mathcal{A}^{\mathbb{M}}$ into subshift $Y \subset \mathcal{B}^{\mathbb{M}}$ is a homomorphism if and only if there exist a* radius *$r \in \mathbb{N}$ and a* block map *$\phi : \mathcal{A}^{\mathcal{G}^{\leq r}} \to \mathcal{B}$ such that for every $x \in \mathcal{A}^{\mathbb{M}}$ and $i \in \mathcal{G}^*$, $\Phi(x)_{\pi(i)} = \phi(x_{|\pi(i \cdot \mathcal{G}^{\leq r})})$ (where the latter has to be understood with the obvious reindexing of the argument).*

Let us order the block maps $\phi : \mathcal{A}^{\mathcal{G}^{\leq r}} \to \mathcal{B}$ by increasing radius $r \in \mathbb{N}$, and then by lexicographic order, so that we have a natural bijective enumeration $\mathbb{N} \to \bigsqcup_{r\in\mathbb{N}} \mathcal{B}^{\mathcal{A}^{\mathcal{G}^{\leq r}}}$ (because $\mathcal{A}$, $\mathcal{B}$ and $\mathcal{G}$ are finite). This gives in particular a surjective enumeration $\mathbb{N} \to \mathcal{E}nd(\mathcal{A}^{\mathcal{G}^*}, \mathcal{B}^{\mathcal{G}^*})$ and in general, a partial surjective enumeration $\mathbb{N}' \subset \mathbb{N} \to \mathcal{E}nd(X,Y)$.

For the rest of the paper, let us assume that $\mathbb{M}$ is an effective group.

2 Equality problem is not too hard

Remark 2. *Two distinct block maps $\phi, \psi : \mathcal{A}^{\mathcal{G}^{\leq r}} \to \mathcal{A}$ representing endomorphisms of X actually represent the same endomorphism if and only if for every pattern $u \in \mathcal{A}^{\mathcal{G}^{\leq r}}$, $\phi(u) \neq \psi(u) \Rightarrow u \in \mathcal{L}(X)^C$.*

This remark allows to establish that the equality problem is at most as complex as knowing whether a pattern is in the colanguage.

Theorem 3. *The equality problem in $\mathcal{E}nd(X)$ is positive-reducible to $\mathcal{L}(X)^C$.*

Corollary 4.

1. *The equality problem is decidable, in the endomorphism monoid of any subshift with computable language (for instance 1D sofic subshift, 1D substitutive subshift, minimal effective subshift, two-way space-time diagrams of a surjective cellular automaton...).*

2. *The equality problem is computably enumerable, in the endomorphism monoid of any effective subshift (for instance multidimensional sofic subshift, substitutive subshift, limit set of cellular automaton...).*

3 Automorphism groups with hard equality problem

The purpose of this section is to prove a partial converse to Theorem 3: we can build a subshift X for which the two problems involved are equivalent, however complex they are.

Let $X \subset \mathcal{A}^{\mathbb{M}}$ and $Y \subset \mathcal{B}^{\mathbb{M}}$ be subshifts. For $\alpha : \mathcal{B} \to \mathcal{B}$ and $u \in \mathcal{A}^{\mathbb{M}}$, let us define the *controlled map* $C_{u,\alpha}$ as the homomorphism over $X \times Y$ such that $C_{u,\alpha}(x,y)_0 = (x_0, \alpha(y_0))$ if $x \in [u]$; (x_0, y_0) otherwise. Informally, $C_{u,\alpha}(x,y)$ applies α somewhere in y iff it sees u at the corresponding position in x. Denote also π_1 the projection to the first component, and σ_1^g the shift of the first component with respect to element $g \in \mathbb{M}$: $\sigma_1^g(x,y)_0 = (x_g, y_0)$ for every $(x,y) \in X \times Y$.

If $a,b,c \in \mathcal{B}$, let us denote $\alpha_{abc} : \mathcal{B} \to \mathcal{B}$ the 3-*cycle* that maps a to b, b to c, c to b, and any other symbol to itself. The following lemma corresponds essentially to [12, Lemma 18] and shows that controlled permutations, no matter the size of the control pattern u, can be expressed with a finite number of generators.

Theorem 5. *Let $X \subset \mathcal{A}^{\mathbb{M}}$ be a subshift and $Y \subset \mathcal{B}^{\mathbb{M}}$ an α_{abc}-permutable subshift for every $a,b,c \in \mathcal{B}' \subset \mathcal{B}$, where $|\mathcal{B}'| \geq 5$. Then $\mathcal{L}(X)^C$ is one-one-reducible to the word problem in the subgroup of automorphisms of $X \times Y$ generated by σ_1^g and $C_{u_0,\alpha_{abc}}$ for $g \in \mathcal{G}$, $a,b,c \in \mathcal{B}'$ and $u_0 \in \mathcal{A}$.*

Consequently, subshifts can have finitely generated automorphism subgroups with equality problem as complex as their colanguage, as formalized by the following corollary. In that case, the equality problem of the whole automorphism group is as complex also.

Corollary 6.

1. *If X and Y are as in Theorem 5, then $\mathcal{L}(X)^C$ is one-one-equivalent to the word problem in (a finitely generated subgroup of) $\mathcal{A}ut(X \times Y)$.*

2. *For every subshift X over a finitely generated group $\mathbb{M}$, there exists a countable-to-one extension $X \times Y$ such that $\mathcal{L}(X)^C$ is one-one-equivalent to the word problem in (a finitely generated subgroup of) $\mathcal{A}ut(X \times Y)$.*

3. *For every subshift X over a finitely generated group $\mathbb{M}$, there exists a full extension $X \times \mathcal{B}^{\mathbb{M}}$ such that $\mathcal{L}(X)^C$ is one-one-equivalent to the word problem in (a finitely generated subgroup of) $\mathcal{A}ut(X \times \mathcal{B}^{\mathbb{M}})$.*

4. *Every Σ_1^0 Turing degree contains the word problem in (a finitely generated subgroup of) $\mathcal{A}ut(X)$, for some 2D SFT X.*

5. *There exists a 2D SFT X for which the word problem in (a finitely generated subgroup of) $\mathcal{A}ut(X)$ is undecidable.*

Point 5 answers [9, Problem 5].

References

[1] Nathalie Aubrun and Marie-Pierre Béal. Decidability of conjugacy of tree-shifts of finite type. In *Automata, Languages and Programming*, pages 132–143. Springer Berlin Heidelberg, 2009.

[2] H. Comon, M. Dauchet, R. Gilleron, C. Löding, F. Jacquemard, D. Lugiez, S. Tison, and M. Tommasi. Tree automata techniques and applications. Available on: `http://www.grappa.univ-lille3.fr/tata`, 2007. release October, 12th 2007.

[3] Wolfgang THOMAS. Chapter 4 - automata on infinite objects. In JAN VAN LEEUWEN, editor, *Formal Models and Semantics*, Handbook of Theoretical Computer Science, pages 133 – 191. Elsevier, Amsterdam, 1990.

[4] Mike Boyle, Douglas A. Lind, and Daniel J. Rudolph. The automorphism group of a shift of finite type. *Transactions of the American Mathematical Society*, 306(1):71–114, 1988.

[5] Jarkko Kari and Nicolas Ollinger. Periodicity and immortality in reversible computing. In *MFCS 2008*, LNCS 5162, pages 419–430, apr 2008.

[6] Ethan Coven and Reem Yassawi. Endomorphisms and automorphisms of minimal symbolic systems with sublinear complexity.

[7] Van Cyr and Bryna Kra. The automorphism group of a shift of linear growth: beyond transitivity.

[8] Sebastionoso, Fabien Durand, Alejandro Maass, and Samuel Petite. On automorphism groups of low complexity subshifts.

[9] Michael Hochman. Groups of automorphisms of SFTs. Open problems ; `http://math.huji.ac.il/~mhochman/problems/automorphisms.pdf`.

[10] Hartley Rogers, Jr. *Theory of Recursive Functions and Effective Computability.* MIT Press, Cambridge, MA, USA, 1987.

[11] Gustav Arnold Hedlund. Endomorphisms and automorphisms of the shift dynamical system. *Mathematical Systems Theory*, 3:320–375, 1969.

[12] Tim Boykett, Jarkko Kari, and Ville Salo. Finite generating sets for reversible gate sets under general conservation laws. *Theoretical Computer Science*, 701:27–39, November 2017.

On Kolmogorov quotients

Teemu Pirttimäki*

Department of Mathematics and Statistics
University of Turku

Abstract

Every topological space has a Kolmogorov quotient that is obtained by identifying points if they are contained in exactly the same open sets. In this survey, we look at the relationship between topological spaces and their Kolmogorov quotients. In most natural examples of spaces, the Kolmogorov quotient is homeomorphic to the original space. A non-trivial relationship occurs, for example, in the case of pseudometric spaces, where the Kolmogorov quotient is a metric space. The author's interest in the subject was sparked by study of abstract model theory, specifically the paper [1] by X. Caicedo, where Kolmogorov quotients are used in a topological proof of Lindström's theorem. We omit the proofs in this extended abstract; a full version [2] with detailed proofs is in preparation.

1 Introduction

Given a topological space X, we obtain its *Kolmogorov quotient* $X/\equiv$ by identifying points x and y if and only if they have exactly the same open neighbourhoods. Such points are topologically indistinguishable; there is no sequence of operations on open sets that would give a set A such that $x \in A$ and $y \notin A$. Nothing topologically important to the space X is lost in identifying these points.

The resulting space is a T_0-*space*: a space where all points are topologically distinguishable. Most topological spaces of interest are T_0. A T_0-space is, arguably, aesthetically more pleasing than a space that is not T_0. In a T_0-space, every point serves a purpose. When studying the topology of X, there seems to be no reason to keep useless, superfluous points around.

The construction of the Kolmogorov quotient is simple, intuitive, and can be carried out for any topological space. If a mathematician comes across a space

*tealpi@utu.fi

that is not naturally T_0, the unnecessary points can be left out from the space right at the beginning and the original space forgotten. Perhaps for this reason, the construction is not even mentioned in most textbooks on topology, and where it is mentioned, this is done very briefly, and proofs are generally omitted.

However, there are situations where it is inconvenient if a space is T_0. Such a situation occurs when one is interested in refinements of the topology: the more points there are in X, the more choices there are for refinements. The same is true for subspaces, though the loss here is not so dramatic: for each subspace $S \subseteq X$ that we lose, $X/\equiv$ retains a subspace homeomorphic to $S/\equiv$. Still, if one is interested in the specific points of the space, one might not wish to clump them together in equivalence classes.

Removing the T_0-property from a space can generate new properties for topological spaces. Given a property P (for example, the Hausdorff separation axiom T_2) of a T_0-space we obtain a new property P' by defining: a space X has the property P' if and only if $X/\equiv$ has the property P. Generally the arising property is interesting in itself and admits a more direct definition. In a similar vein, given a structure S (for example, a metric) on a T_0-space we can define: a space X has the structure S' if and only if $X/\equiv$ has the property S.

This survey is not about T_0-spaces, but focuses rather on the relationship between spaces and their Kolmogorov quotients. It appears that no comprehensive treatment on the matter has been published, and as stated before, standard textbooks often omit the construction entirely. As our sources don't usually give proofs, it seems unnecessary to cite each theorem individually. Various results presented here can be found without proofs in [1] and [3]. The notes in [4] contain some proofs. We present the results in a more general form when possible.

2 Kolmogorov quotients

Given a topological space X and a subset $A \subseteq X$, we write A^c for the complement $X \setminus A$ and $\overline{A}$ for the closure of A. We denote the Borel algebra of X by Σ_X and the collection of (not necessarily open) neighbourhoods of $x \in X$ by $\mathcal{N}(x)$.

Let X be a topological space. We define an equivalence relation $\equiv\, \subseteq X^2$ by letting $x \equiv y$ if and only if every open neighbourhood of x is an open neighbourhood of y and vice versa. If $x \equiv y$, we say that the points x and y are *topologically indistinguishable*. Otherwise they are *topologically distinguishable*, and we write $x \not\equiv y$. A space where all pairs of distinct points are topologically distinguishable is called a *T_0-space* or a *Kolmogorov space*. Most spaces studied by mathematicians are T_0.

Example 2.1. A space with the trivial topology is not T_0, unless it has less than two points.

Example 2.2. All Hausdorff spaces are T_0. This includes all discrete spaces and the space $\mathbb{R}$ with the euclidean topology.

Example 2.3. Let $X = \{0, 1\}$ and $\tau = \{\emptyset, \{1\}, \{0, 1\}\}$. The *Sierpiński space* (X, τ) is T_0 but not Hausdorff.

Example 2.4. The product of $\mathbb{R}$ with the euclidean topology and $\mathbb{R}$ with the trivial topology is not T_0: indeed, the points $(1, 0)$ and $(1, 1)$ are topologically indistinguishable.

We will see more examples later. In the meanwhile, the following lemma should provide intuition into topological indistinguishability.

Lemma 2.5. *Let X be a topological space and $x, y \in X$. The following statements are equivalent:*

(i) *$x \equiv y$;*
(ii) *$\mathcal{N}(x) = \mathcal{N}(y)$;*
(iii) *x and y are contained in the same basic open sets;*
(iv) *x and y are contained in the same subbasic open sets;*
(v) *x and y are contained in the same open sets;*
(vi) *x and y are contained in the same closed sets;*
(vii) *$\overline{\{x\}} = \overline{\{y\}}$;*
(viii) *x and y are contained in the same Borel sets;*
(ix) *a filter or net that converges to x, converges also to y, and vice versa;*
(x) *a filter or net that has x as a cluster point, has also y as a cluster point, and vice versa.*

Example 2.6. Let $U_m = \{n \in \mathbb{N} \mid m \text{ divides } n\}$ for all $m \in \mathbb{Z}_+$. Then $\mathcal{S} = \{\mathbb{N}\} \cup \{U_p \mid p \text{ is a prime}\}$ is a subbasis of a topology on $\mathbb{N}$. By lemma 2.5, $x \equiv y$ if and only if x and y have the same prime factors.

Given a topological space X, we denote by $\eta(x)$ the equivalence class of $x \in X$ with respect to $\equiv$, that is, $\eta(x) = \{y \in X \mid y \equiv x\}$. The following theorem gives a simple formula for the equivalence classes.

Theorem 2.7. *Let (X, τ) be a topological space. For all $x \in X$,*

$$\eta(x) = \overline{\{x\}} \cap \bigcap_{\substack{U \in \tau \\ x \in U}} U = \bigcap_{\substack{B \in \Sigma_X \\ x \in B}} B.$$

Corollary 2.8. *For all $x \in X$,*

$$\eta(x) \subseteq \bigcap_{U \in \mathcal{N}(x)} U.$$

Corollary 2.9. *For all $x \in X$, $\eta(x) \subseteq \overline{\{x\}}$.*

Given a topological space X, we define $X/{\equiv}$ as the topological space, where the space as a set is the set of equivalence classes under $\equiv$, and the topology is the finest such topology that the quotient map $\eta \colon X \to X/{\equiv}$ that maps each element $x \in X$ to its equivalence class $\eta(x)$ is continuous. In other words, the open sets of $X/{\equiv}$ are precisely those sets whose preimage under η is open in X. We call the space $X/{\equiv}$ the *Kolmogorov quotient* of X.

Clearly the Kolmogorov quotient is always a Kolmogorov space. A space is T_0 if and only if it is homeomorphic to the Kolmogorov quotient of itself.

The continuity of η already lets us know some things about the relationship between X and $X/{\equiv}$; for example, if $A \subseteq X$ is compact, then so is $\eta(A)$.

Example 2.10. Take the set $X = \{1, 2, 3, 4\}$ with the clopen basis $\{\{1, 2\}, \{3, 4\}\}$. The Kolmogorov quotient $X/{\equiv}$ is the two-element set $\{\eta(1), \eta(3)\} = \{\{1, 2\}, \{3, 4\}\}$ with the discrete topology.

Example 2.11. The Kolmogorov quotient of any nonempty set with the trivial topology is a space consisting of a single point.

Example 2.12. Let $p \geq 1$. Let L^p be the set of all measurable functions f from a measure space (S, Σ, μ) to $\mathbb{R}$ such that

$$\int_S |f|^p \,\mathrm{d}\mu < \infty.$$

Denote

$$\|f\|_p = \left(\int_S |f|^p \,\mathrm{d}\mu \right)^{\frac{1}{p}}.$$

The map $f \mapsto \|f\|_p$ is a *seminorm*: there are functions f other than the zero function for which $\|f\|_p = 0$, but all other properties of a norm are satisfied. In the Kolmogorov quotient $\mathcal{L}^p = L^p/{\equiv}$, this seminorm becomes a norm. The spaces $\mathcal{L}^p$ are important in analysis and measure theory ([5]).

Example 2.13. A discrete version of example 2.12 is obtained by taking the measure space $\mathbb{N}$ with the counting measure i.e. the measure of a subset of $\mathbb{N}$ is its cardinality. In this case, the space consists of sequences converging to 0, and

$$\|(x_n)\|_p = \left(\sum_{n=0}^{\infty} |x_n|^p \right)^{\frac{1}{p}}.$$

Based on the quotient map $\eta\colon X \to X/{\equiv}$, we define two maps $\eta^{\to}\colon \Sigma_X \to \Sigma_{X/\equiv}$ and $\eta^{\leftarrow}\colon \Sigma_{X/\equiv} \to \mathcal{P}(X)$ as follows:

$$\eta^{\to}(B) = \eta(B) = \{\eta(x) \mid x \in B\},$$

and

$$\eta^{\leftarrow}(B') = \eta^{-1}(B') = \{x \in X \mid \eta(x) \in B'\}$$

for all $B \in \Sigma_X$ and $B' \in \Sigma_{X/\equiv}$.

Theorem 2.14. *The map $\eta^{\to}$ is an isomorphism between the Boolean algebras Σ_X and $\Sigma_{X/\equiv}$.*

Corollary 2.15. *The quotient map η is open, i.e. if $A \subseteq X$ is open, then $\eta^{\to}(A)$ is open.*

Corollary 2.16. *The quotient map η is closed, i.e. if $A \subseteq X$ is closed, then $\eta^{\to}(A)$ is closed.*

Lemma 2.17. *Let X and Y be topological spaces and $f\colon X \to Y$ continuous. If $x_1 \equiv x_2$ for some $x_1, x_2 \in X$, then $f(x_1) \equiv f(x_2)$.*

Theorem 2.18. *Let $\eta_X\colon X \to X/{\equiv}$ and $\eta_Y\colon Y \to Y/{\equiv}$ be the quotient maps and $f\colon X \to Y$ an arbitrary continuous map. Then there exists a continuous map $f_{\equiv}\colon X/{\equiv} \to Y/{\equiv}$ such that the diagram below commutes.*

$$\begin{tikzcd}
X \arrow[r, "f"] \arrow[d, "\eta_X"'] & Y \arrow[d, "\eta_Y"] \\
X/{\equiv} \arrow[r, "f_{\equiv}"] & Y/{\equiv}
\end{tikzcd}$$

Choosing a representative from each equivalence class gives the following theorem, which states that all topological properties of the Kolmogorov quotient of X hold also in a dense subspace of X. If there are infinitely many equivalence classes, then the axiom of choice is required.

Theorem 2.19. *The space $X/{\equiv}$ is homeomorphic to a dense subspace of X.*

The Kolmogorov quotient may have fewer subspaces than the original space. The following theorem tells that the quotients of the lost subspaces are still subspaces of $X/{\equiv}$, up to homeomorphism.

Theorem 2.20. *Let X be a topological space and S a subspace of X. Then the space $S/{\equiv}$ is homeomorphic to some subspace of $X/{\equiv}$.*

Sketch of proof. Let $\eta\colon X \to X/{\equiv}$ and $\eta_S\colon S \to S/{\equiv}$ be the quotient maps. Let $f\colon S/{\equiv} \to \eta(S)$, $f(\eta_S(x)) = \eta(x)$ for all $\eta_S(x) \in S/{\equiv}$. The map f is a homeomorphism when $\eta(S)$ is considered as a subspace of $X/{\equiv}$. □

Theorem 2.21. *Let $\mathcal{I}$ be a set and $(X_i)_{i\in\mathcal{I}}$ a sequence of topological spaces. The spaces $\left(\prod_{i\in\mathcal{I}} X_i\right)/{\equiv}$ and $\prod_{i\in\mathcal{I}} X_i/{\equiv}$ are homeomorphic.*

$$\begin{tikzcd}
 & & X_i \arrow[drr, "\eta_i"] & & \\
\prod_{i\in\mathcal{I}} X_i \arrow[urr, "p_i"] \arrow[dr, "\eta"] & & & & X_i/{\equiv} \\
 & \left(\prod_{i\in\mathcal{I}} X_i\right)/{\equiv} \arrow[rr, "f"] & & \prod_{i\in\mathcal{I}} X_i/{\equiv} \arrow[ur, "\pi_i"] &
\end{tikzcd}$$

Sketch of proof. Let η be the quotient map from $\prod_{i\in\mathcal{I}} X_i$ to $\left(\prod_{i\in\mathcal{I}} X_i\right)/{\equiv}$, and let η_i be the quotient map from X_i to $X_i/{\equiv}$ for all $i \in \mathcal{I}$. Define a map $f\colon \left(\prod_{i\in\mathcal{I}} X_i\right)/{\equiv} \to \prod_{i\in\mathcal{I}} X_i/{\equiv}$ from the condition $f(\eta(z))(i) = \eta_i(z(i))$ for all $i \in \mathcal{I}$ and all $z \in \prod_{i\in\mathcal{I}} X_i$. The diagram above should commute. The maps p_i and π_i are the canonical projections. The map f is a homeomorphism. □

3 Properties of spaces compared to properties of their Kolmogorov quotients

The *separation axioms* are properties a topological space can have that guarantee the existence of disjoint neighbourhoods in various situations. The separation axioms are ordered so that T_i implies T_j whenever $i \geq j$. There is also another set of analogous properties called the *regularity axioms* such that $T_i = R_{i-1} \wedge T_0$. In other words, a space satisfies T_i if and only if it is a Kolmogorov quotient of a space that satisfies R_{i-1}. Table 1 shows the connection. Some authors require normal and regular spaces to be Hausdorff; we do not.

A topological space X is *symmetric* if for all pairs of topologically distinguishable points $x, y \in X$, there are open sets U and V such that $x \in U$, $y \notin U$ and $y \in V$, $x \notin V$.

Theorem 3.1. *If X is symmetric, then $\eta(x) = \overline{\{x\}}$ for all $x \in X$.*

A topological space X is *preregular* if for all pairs of topologically distinguishable points $x, y \in X$, there are open sets U and V such that $x \in U$, $y \in V$ and $U \cap V = \emptyset$.

Table 1: The connection between separation and regularity axioms

$X/\equiv$	X
Kolmogorov (T_0)	topological space
Fréchet (T_1)	symmetric (R_0)
Hausdorff (T_2)	preregular (R_1)
regular Hausdorff (T_3)	regular (R_2)
Tychonoff ($T_{3.5}$)	completely regular ($R_{2.5}$)
normal Hausdorff (T_4)	normal regular (R_3)
completely normal Hausdorff (T_5)	completely normal regular (R_4)
perfectly normal Hausdorff (T_6)	perfectly normal regular (R_5)

Theorem 3.2. *If K_1 and K_2 are disjoint compact subsets of a preregular topological space X and do not have disjoint open neighbourhoods, then there exist $x_1 \in K_1$ and $x_2 \in K_2$ such that $x_1 \equiv x_2$.*

A *pseudometric on X* is a function $d\colon X^2 \to \mathbb{R}$ that satisfies all the properties of a metric, except it is possible that $d(x, y) = 0$ even if $x \neq y$. A pseudometric determines a topology in the same way a metric does. The resulting topological space is called a *pseudometric space* and can be denoted by (X, d).

Example 3.3. Pseudometrics can be used in the context of cellular automata. Given a finite set A, let $A^{\mathbb{Z}}$ denote the set of functions from $\mathbb{Z}$ to A. For $x \in A^{\mathbb{Z}}$, we write x_j for $x(j)$. Also, for n, $k \in \mathbb{Z}$, let $[n, k]$ denote the set of integers m such that $n \leq m \leq k$. Finally, for sequences $(a_n)_{n=0}^{\infty}$ of natural numbers, denote

$$\limsup_{n\to\infty} a_n = \lim_{n\to\infty} \left(\sup_{m\geq n} a_m \right).$$

Then

$$d_B(x, y) = \limsup_{l\to\infty} \frac{|\{j \in [-l, l] \mid x_j \neq y_j\}|}{2l + 1}$$

is the *Besicovitch pseudometric* on $A^{\mathbb{Z}}$, and

$$d_W(x, y) = \limsup_{l\to\infty} \max_{k\in\mathbb{Z}} \frac{|\{j \in [k + 1, k + l] \mid x_j \neq y_j\}|}{2l + 1}$$

is the *Weyl pseudometric* on $A^{\mathbb{Z}}$. The topologies induced by these pseudometrics have some advantages to the standard approach, where A is given the discrete topology and $A^{\mathbb{Z}}$ the product topology; for example, the class of continuous functions from $A^{\mathbb{Z}}$ to itself is larger [6].

Theorem 3.4. *Let (X, d) be a pseudometric space. Then $d^*\colon (X/{\equiv})^2 \to \mathbb{R}$, $d^*(\eta(x), \eta(y)) = d(x, y)$ for all $x, y \in X$, is a metric on $X/{\equiv}$ that determines the same topology as the quotient map.*

The space $(X/{\equiv}, d^*)$ is called the *metric identification of* (X, d).

We mentioned seminorms in example 2.12. A (semi)norm on V induces a (pseudo)metric on V by defining $d(x, y) = \|x - y\|$ for all $x, y \in X$. The resulting topological space is called a *(semi)normed vector space* and can be denoted by $(V, \|\cdot\|)$.

Theorem 3.5. *Let $(V, \|\cdot\|)$ be a seminormed vector space. Then $(V/{\equiv}, \|\cdot\|^*)$ is a normed vector space, where*

$$\begin{aligned} \lambda\eta(x) &= \eta(\lambda x) && \text{for all } \lambda \in K, x \in V, \\ \eta(x) + \eta(y) &= \eta(x + y) && \text{for all } x, y \in V, \end{aligned}$$

and

$$\|\eta(x)\|^* = \|x\| \qquad \text{for all } x \in V.$$

Furthermore, $\|\cdot\|^*$ determines the same topology as the quotient map.

A space is *Alexandrov-discrete* if all intersections of open sets are open. All finite spaces are Alexandrov-discrete, as is the space of natural numbers with a basis consisting of the sets $V_n = \{m \in \mathbb{N} \mid m \geq n\}$.

Theorem 3.6 ([7]). *If X is an Alexandrov-discrete space, then η is a homotopy equivalence.*

The proof of theorem 3.6 uses the axiom of choice.

References

[1] X. Caicedo: *Lindström's theorem for positive logics, a topological view.* Logic Without Borders: Essays on Set Theory, Model Theory, Philosophical Logic and Philosophy of Mathematics (Å. Hirvonen, J. Kontinen, R. Kossak, A. Villaveces, eds.), Ontos Mathematical Logic, De Gruyter, 2015, pp. 73–90

[2] T. Pirttimäki: *A survey of Kolmogorov quotients*, in preparation

[3] E. Schechter: *Handbook of Analysis and its Foundations.* Academic Press, London, 1997

[4] P. L. Clark: *General Topology.* `http://math.uga.edu/~pete/pointset2018.pdf` (last visited 2018-12-12)

[5] Wolfram MathWorld: *L^p-Space.* `http://mathworld.wolfram.com/Lp-Space.html` (last visited 2018-12-12)

[6] F. Blanchard, E. Formenti, P. Kůrka: *Cellular Automata in the Cantor, Besicovitch, and Weyl Topological Spaces.* Complex Systems 11 (2), 107–123, 1997

[7] M. C. McCord: *Singular homology groups and homotopy groups of finite topological spaces.* Duke Mathematical Journal 33 (3): 465-–474, 1966

An Inventory of Ternary Square-free Morphisms

Nguyen Huong Lam
Email: nhlam@math.ac.vn
Hanoi Institute of Mathematics
18 Hoang Quoc Viet Road, Cau Giay, 10307 Hanoi

Abstract. We produce numerous infinite ternary square-free words relatively with ease, based on recasting the existing square-freeness tests in a more manageable form. Usually, square-free morphisms are a chief tool but sometimes, non-square-free ones come to the scene as well. This is the case with Istrail's morphism whose fixed point an infinite ternary square-free word. We explain how it works and how to map it into more infinite ternary square-free words. We also clarify why the very special Lallement's morphism is minimal (of length) in its class and how to come to the example of F. Dejean, based solely on which she formulated the conjecture — now theorem – on the repetitiveness threshold. Finally we exhibit an infinite ternary square-free word that avoids *aba* and *aca*. Note that Istrail's word avoids *aca* and *bcb*. The procedure we use shows that for one class, the square-free morphism has the shortest total length of 18 and it is very probable that it is also of minimum total length of all square-free morphisms save for the trivial endomorphism on the base alphabet.

1. Introduction

Square-free words, that is words covering no two identical adjacent blocs, stood at the origin of Combinatorics Words, over one hundred year ago. Although a binary word of length 4 or more contains a square, that there are infinitely many ternary words that do not contain two identical sequential blocs of letters is far from evident but very probable, and is exhibited by Axel Thue in the seminal work of 1906. Actually, he produced an infinite binary overlap-free (a power higher than square) word that gave rise to an infinite ternary square-free word, now called Thue-Morse word.

One just marvels at the way the intuition guided its discoverers: over thirty years later, in 1938, Morse and Hedlund rediscovered it by an identical method. However, according to Raoul Bott and Jean Berstel, Thue's word was already mentioned in Morse's thesis (1917) and was subsequently published in the paper on recurrent geodesics of 1921, where he proved that it is recurrent and nonperiodic; but that is not all. Since square-free words have applications in the Burnside problem, S. Adian in his book [1] on Word Problem (1975) informed of (and gave) a construction by a Russian researcher named Arshon of another infinite ternary square-free word in 1937 [3]. Actually, this "Morse trajectory" had recurred earlier in Novikov's disproof of Burnside conjecture in

1959 [12] and was there credited to Arshon. But a strange and striking tale did not commence just like that. According to Choffrut and Karhumäki [CK], Thue's sequence on two symbols was already described by Prouhet in a paper of 1851 [13] on a problem of arithmetics now known as Prouhet-Tarry-Escott problem, on two collections of numbers with equal sums of equal powers. So Prouhet is likely to be one of the originators of Combinatorics of Words. That is how the Thue word blazed its illustrious own trail leaving behind a crown jewel for those who rediscovered it.

How to construct an infinite set of square-free words? Several short first square-free words can be enumerated, but longer they can be gotten from short words somehow expanded. The first and foremost is the trial-and-error search. This straight search is fit to show that the square-free words subject to certain restrictions are finite in length or in number. Next come morphisms, repeatedly applied. Since the time of Thue's work in 1906, they have remained a sole tool to cope with different variations on repetitive strings. To be sure to yield square-free words the morphism might be required to be square-free, that is, when applied to the square-free words it produces square-free words as well.

To recognize a square-free morphism, or more generally $k-$(power)-free there are some tests. However, one does not need a square-free morphism to produce infinite square-free word, just needs it to be locally square-free, that is, on certain specific words. Usually, and the most simple trick is the iteration of h on a: $h(a), h^2(a), \dots$ all are square-free and, to simplify things further, $h^i(a)$ is a prefix of $h^{i+1}(a)$ for all $i = 1, 2, \dots$. So here comes the prolongability of h on a, they constitute an infinite square-free word $h^\omega(a)$, which is used to call a fixed point of h. According to [7], there is the following most simple and elegant morphism due to Istrail [10].

Proposition 1.2. *The endomorphism i on the ternary alphabet $A = \{0, 1, 2\}$ defined by $i(0) = 012, i(1) = 02, i(2) = 1$ has the square-free fixed point $i^\omega(0)$.*

The morphism i is not square-free as $i(010)$ contains a square, 0202. A morphism of this kind, a fixed point of its is square-free was termed weakly square-free (faiblement sans carré) by Crochemore in [7] and was explored in detail therein (characterizations, tests, ...).

Curiously, J. D. Currie [8] informed that Istrail's fixed point is mapped into Thue's word by the morphism h defined as $h(0) = 011, h(1) = 01, h(2) = 0$. I have verified this fact, and it turns out that h is unique to within composition with a repeated Thue morphism, that is, every morphism that maps Istrails's word onto Thue word has the form $h(t^i)$ for some exponent $i \geq 0$, where t is the Thue-Morse morphism $t(0) = 01, t(1) = 10$. This amazing fact makes Thue word and Istrail's morphism unique in the realm of words.

This paper is devoted to infinite square-free words on three symbols. The ternary alphabet is basic, vital and the most difficult for the square-freeness and overlap-freeness. Both concepts have recurred in many situations and have numerous applications, to the Burnside problem on groups and semigroups, for example, and are of intrinsic interests for the study of words. We produce numerous infinite square-free words for different purposes. For that there have been various characterizations and tests developed by precursor authors. Like primality, tests available, even in polynomial time, the determination of large prime numbers always is a demanding task.

Now we fix the terminology. We deal with a finite alphabet A of letters, the set A^* of words on A, the empty word ϵ, the set A^+ of nonempty words. For the word $w = a_1a_2\ldots a_n$ with $a_1, a_2, \ldots a_n$ the letters, n is the length of w, denoted $|w|$; by convention $|\epsilon| = 0$, the length of the empty word is null. The word u is a factor of w if there is a bloc $a_i \ldots a_{j-1}, 1 \leq i \leq j < n$ such that $u = a_i \ldots a_{j-1}$; this bloc, an occurrence of u, is at the position i and ends at the position $j - 1$ in w. A prefix of w is the word u which has a bloc starting at the position 1, a suffix, if it has a bloc ending at position n in w, an infix or internal factor, if it has a bloc starting at a position later than 1 and terminating at a position earlier than n.

A k-power, k a natural number, is k successive identical blocs; a square when $k = 2$. A word is k-free if it has no k-power factors; square-free when $k = 2$.

Let Δ be a finite subset of A^*. Denote, by convention $u_1u_2\ldots u_k = \epsilon$ when $k = 0$, $\Delta^* = \{u_1u_2\ldots u_k : u_i \in \Delta, i = 1, 2, \ldots, k; k = 0, 1, 2, \ldots\}$ and Δ^+ is the subset of the nonempty words of Δ^*. Considering Δ as an alphabet and each member of it as a letter, we call each product $u_1u_2\ldots u_k$ a Δ-word, which corresponds to a word $u = u_1u_2\ldots u_k$ on A. We say also that $u_1u_2\ldots u_k$ is Δ-square-free if it is square-free on the alphabet Δ. Of course, a Δ-square-free word may not lead to a square-free word $u_1u_2\ldots u_k$ on A, but if the latter is square-free on A, $u_1u_2\ldots u_k$ must be Δ-square-free. A morphism from Σ to Δ is square-free is equivalent to saying that every Δ-square-free word corresponds to a Σ-square-free word. By analogy, we term the set Δ *square-free* if every Δ-square-free word is square-free on the ground alphabet A, or equivalently, $\Delta = \{h(a) : a \in A\}$ for some square-free morphism h.

We extend the notion of factor on A to that of Δ-factor on the alphabet Δ in a usual manner. Also w is u-free if it does not contains u as a factor for $u \in A^*$; w is Δ-free if it is u-free for all u of Δ.

Now the key notion of overlap. Let u and v be words not necessarily distinct; u is said to overlap v if u has a suffix, not u nor v, nor empty that is a prefix of v, to wit, $u = rw, v = ws$, where $r, w, s \neq \epsilon$; u and v overlap if one of them overlap the other; u overlaps itself, then we say that u self-overlap, or u

is self-overlapping; w is an overlap, or an overlapping piece, a self-overlap, or an self-overlapping piece, etc. The set Δ is overlap-free if every pair of distinct words of its do not overlap, and total overlap-free if, in addition, every word of its does not overlap itself.

2. Tests for Square-free Morphisms

We state the characterizations developed by Berstel and made more precise by Crochemore [6], see also [7]. Let Δ be a subset of A^+, M the maximum and m the minimum length of the words of Δ, resp.

Proposition 2.1. *Δ is square-free if and only if every Δ-square-free word of length 3 and at most $\lfloor \frac{M-3}{m} \rfloor + 1$ is square-free. If $|\Delta| = 3$, Δ is square-free if and only if every Δ-square-free word of length 5 is square-free and 5 is the least.*

In this section I present the test in an explicit form convenient for the later purposes. But first, some technical notions.

Definition 2.2. Let K be an integer greater than 1. A subset Δ of A^* is said to have *property K* if for every word x of Δ

(K') x has no prefix of the form

$$x'y''x_1 \dots x_k x'$$

where

$$x' \in A^*, y, x_1, \dots, x_k \in \Delta,$$

y'' is a nonempty suffix of y, $0 \le k \le K-2$, for which $yx_1 \dots x_k x$ is Δ-square-free. or equivalently, $yx_1 \dots x_k$ is Δ-square-free if $k > 0$ and $y \neq x$ if $k = 0$, and

(K'') x has no suffix of the form

$$x''x_k \dots x_1 z' x''$$

where

$$x'' \in A^*, x_1, \dots, x_k, z \in \Delta,$$

z' is a nonempty prefix of z, $0 \le k \le K-2$, for which $xx_k \dots x_1 z$ is Δ-square-free. or equivalently, $x_1 \dots x_k z$ is Δ-square-free if $k > 0$ and $z \neq x$ if $k = 0$.

Note that, for $K = 2$, K' says that x is not of the form $x = x'y''x'x''$ and K'' says that z is not of the form $x = x'x''z'x''$. Observe that for two words u and v, uv contains a square if and only if u, or v contains a square, or u has a form forbidden by K' or v by K''. Therefore, if every word of Δ is square-free, the K property for $K = 2$ is equivalent to the that every Δ-word of length 2 is square-free.

Let now Δ be an overlap-free set, $x_1 \dots x_n \in \Delta^*$, $n > 2$, and $y_1 \dots y_m \in \Delta^*$, $m > 1$, be Δ-square-free words satisfying

$$x_1'' x_2 \dots x_{n-1} x_n' = y_1'' y_2 \dots y_{m-1} y_m'$$

where x_1'', y_1'' are nonempty suffix of x_1, y_1 and x_n', y_m' are nonemty prefix of x_n, y_m, respectively. For every occurrence x_i, $1 < i < n$, we have three possibilities:

(a) x_i occurs as an internal factor of some y_j, $1 \leq j \leq m$;
(b) some y_j, $1 < j < m$, occurs as an internal factor of x_i; and
(c) x_i coincides with some y_j, $1 \leq j \leq m$.
They result in the following issues.

Lemma 2.3. *If we have*
(a) then y_j violates K', or K'', or both for some $K \geq 3$;
(b) then x_i violates both K' and K'' for some $K \geq 3$; and finally,
(c) then $x_2 \dots x_{n-1}$ is a Δ-factor of $y_1 y_2 \dots y_m$, that is,

$$x_2 = y_{t+1}, \dots, x_{n-1} = y_{t+n-2}$$

for some t, $1 \leq t \leq m - n + 2$.

Proof. If x_i occurs inside of none of $y_1, y_2, \dots, y_m$ then x_i contains some y_j since x_i cannot overlap any two consecuitive of them (Δ-square-freeness of the two words and overlap-freeness of Δ). The remaining claim is by definition of overlap-freeness. The lemma is proved.

We abbreviate the longest common prefix of the two words u, v as $\mathrm{lcp}\,(u, v)$ and the longest common suffix as $\mathrm{lcs}\,(u, v)$. We say that a Δ-word is related if it contains a square. We go into a little more detail. A Δ-word xyz, or interchageably, a triple (x, y, z), $x, y, z \in \Delta$ is

(a) *ps-related* if $y = y'y''$, where y' is a nonempty common prefix of y and z, y'' is a nonempty common suffix of y and x. Thus xyz is not ps-related if and only if

$$|\mathrm{lcp}\,(y, z)| + |\mathrm{lcs}\,(y, x)| < |y|.$$

(b) *os-related* if

$$y = wz'x''w$$

where y' is a nonempty common prefix of y and z, y'' is a nonempty common suffix of y and x, w is a self-overlapping piece of y. Thus xyz is not os-related if and only if

$$|\mathrm{lcp}\,(y, wz)| + |\mathrm{lcs}\,(y, xw)| < |y|.$$

(c) *is-related* (*is* is for infix sandwich) if $x = z$

$$y = y'y''$$

and for some self-overlapping piece w of x, wy' is a prefix and $y''w$ is a suffix of x. Thus xyz is not is-related if and only if

$$|\mathrm{lcp}\,(x, wy)| + |\mathrm{lcs}\,(y, yw)| < |y| + 2|w|$$

for every self-overlap w of x.

The following assertions are more precise than Proposition 2.1.

Proposition 2.7. *Suppose that every word of Δ is square-free and Δ has K preperty for $K = 3$. Then a Δ-square-free word xyz of length 3 contains a square-free if and only if (x, y, z) is a ps-, or an os- or an is-related triple. Moreover, if Δ has property K for all $K \geq 3$ then a Δ-square-free word contains a square-free if and only if it contains a os- or is-related triple or a Δ-factor of the form $xryrz$ for $r \in \Delta^*$ for a ps-related triple (x, y, z).*

Proof. The if direction is a direct verification. For the converse, let $x_1x_2 \ldots x_k$ be a Δ-square-free word which contais contains a square $r'r'$. Under the hypothesis, by K-property for $K = 2$. every Δ-square-free word of length 2 is square-free, so $k \geq 3$. If $k = 3$, by K property for $K = 3$, x_1 and x_3 do not contain neither occurrence of r' in $r'r'$, so we have only the following case to consider

$$r' = x_1''x_2' = x_2''x_3'$$

where x_1'', x_2'' are a nonempty suffix of x_1, x_2 and x_2', x_3' are a nonempty prefix of x_2, x_3, respectively. If $x_1'' = x_2'', x_2' = x_3'$ which readily shows that $x_1x_2x_3$ is ps-related. If $|x_1''| < |x_2''|, |x_2'| > |x_3'|$ then $x_1''w = x_2'', wx_3' = x_2'$ and x_1 overlaps x_3 on the overlap w, hence $x_1 = x_3$ which self-overlaps on w and $x_1x_2x_1$ is is-related. If, finally, $|x_1''| > |x_2''|, |x_2'| < |x_3'|$ then $x_1'' = x_2''w, wx_3' = x_2'$, so x_2 is self-overlapping, thus $x_1x_2x_3$ is os-related that is the first claim.

Let now $k > 3$ and Δ have K property for all $K \geq 3$. We can assume that no proper Δ-subfactor of $x_1x_2 \ldots x_k$ contains $r'r'$. As before, we have only the following case to consider, for some m, $1 < m < k$,

$$r' = x_1''r_1x_m' = x_m''r_2x_k',$$

with x_1'' nonempty suffix of x_1, $r_1 = x_2 \ldots x_{m-1} \in \Delta^*$, x_m' a prefix of x_m, x_m'' a suffix of x_m, for which $x_m = x_m'x_m''$ $r_2 = x_{m+1} \ldots x_k \in \Delta^*$, x_k' nonempty prefix of x_k. Since $k > 3$, at least r_1 or r_2 is not empty, let it be r_1, the other case is completely similar. By Lemma 2.3, K property for all $K \geq 3$ implies that r_1 is Δ-factor of $x_m \ldots x_k$. Since $x_1'', x_k' \neq \epsilon$, we get $r_1 = r_2$ and $x_1'' = x_m'', x_m' = x_k'$

which shows that (x_1, x_m, x_k) is a ps-related triple that proves the last claim and the proposition.

We have not to verify the K property forever, because, roughly, k is bounded from above by $\frac{M-2}{m}$ and K can be any value beyond the maximum of such k plus 2, if exist. Precisely, by a more delicate inspection, we just have to check the Δ-square-freeness of some of those Δ-words that are factor of a word of Δ, of Δ-length k not exceeding $\lfloor\frac{M-3}{m}\rfloor + 1$ ($K = \lfloor\frac{M-3}{m}\rfloor + 2$) or $\frac{M-2}{m}$ ($K = \lfloor\frac{M-2}{m}\rfloor + 1$). Anyway, $k \leq \frac{M-3}{m} + 1$, the same bound given in [6] and $K \leq \frac{M-3}{m} + 2$. Thus, our manipulation is less arduous than testing every Δ-square-free words of Δ-length $\frac{M-3}{m} + 1$ for square-freeness by Proposition 2.1.

The following assertion prepares the prerequisites for the the notion of weakly square-free set, later.

Corollary 2.8. *Suppose that Δ has property K for all $K \geq 3$ and every Δ-square-free of length 2 word is square-free. Then Δ is square-free if and only if every Δ-square-free word of length 3 is squre-free, or more precisly, there are no ps-, os- or is-related triples over it.*

In the ensuing sections we construct some square-free triple, which are divided into four types as follows. Because the square-freeness of a word is not affected under reversal of the word and permutation of the letters of the alphabet, concerning the initial and the terminal letters of the words of $\Delta = \{x, y, z\}$ every product of two distinct words of which is square-free all we have are the following possibilities:

(I) $x = a \dots b, y = a \dots b$ and $z = a \dots b$;

(II) $x = a \dots b, y = a \dots b$ and $z = c \dots c$, or $z = c$;

(III) $x = a \dots a$ or $x = a$, $y = b \dots b$ or $y = b$ and $z = c \dots c$, or $z = c$;

(IIII) $x = a \dots c, y = a \dots c$ and $z = b \dots c$

which we call Type I, II, III and IIII, respectively. In what follows, we consider square-free words on the triple (x, y, z) of the first two types.

3. Type II

We consider the case when $z = c$, to this class belongs Istrail's example above. We try to clarify why it works, that is, why the triple $(012, 02, 1)$ makes up a weakly square-free morphism. Let $\Delta = \{x, y, z\}$ be a ternary set of words over A.

Definition 3.1. The triple Δ is weakly square-free if it has property K for all $K \geq 3$, every Δ-square-free word of length 3 is square-free except may be xyx or zyz or both.

Let now $A = \{a, b, c\}$ be a ternary alphabet. Put

$$\bar{a} = abc, \quad \bar{b} = ac, \quad \bar{c} = b$$

and

$$\bar{A} = \{\bar{a}, \bar{b}, \bar{c}\}.$$

Here is an immediate property of $\bar{A}$.

Proposition 3.2. *The triple $\bar{A}$ is weakly square-free with a unique related triple $\bar{a}\bar{b}\bar{a}$, which is ps-related, and every $\bar{A}$-word is $crbrc$-free and $arbra$-free for $r \in A^*$.*

Proof. The first statement is verified by definition. For the next one, it is enough to prove for $arbra$, the other case is symmetric (reversal). Suppose by a contradiction that some word of $\bar{A}^+$ contains $arbra$. Since a appears only as the initial letter of some words of $\bar{A}$, we get

$$arbr \in \bar{A}^+.$$

Further, b appears in an $\bar{A}$-word only as an $\bar{A}$-factor $\bar{b}$, or as the middle letter of an $\bar{A}$-factor $\bar{a}$. The first issue shows that

$$ar, r \in \bar{A}^*,$$

consequently, $a \in \bar{A}^*$, which is untrue. The second issue shows that

$$ar = r'a, r = cr'',$$

where $r', r'' \in \bar{A}^*$. Consequently, $r'a = ar = acr'' \in \bar{A}^*$, which is absurd because no $\bar{A}$-word terminates with a. The proposition is proved.

Consider now the Istrail's morphism i on A^*, defined as

$$i(a) = abc, \quad i(b) = ac, \quad i(c) = b$$

that is, we identify $i(a), i(b)$ and $i(c)$ with $\bar{a}, \bar{b}$ and $\bar{c}$, respectively. The Proposition 3.2 has an immediate consequence that for every square-free and $arbra$-free word u, $i(u)$, as such, $arbra$-free as well, is square-free, hence $i^\omega(a)$ is square-free. But we have more.

Let Δ be an arbitrary weakly square-free, possibly with related triples (x, y, x) and (z, y, z) and $h : A^* \to \Delta^*$ be a morphism, defined as

$$h(a) = x, \quad h(b) = y, \quad h(c) = z.$$

Proposition 3.3. *$h(i^n(w))$ is square-free for any square-free and $arbra$-free word w and integer $n \geq 0$.*

Proof. If $h(i^n(w))$ contains a square, by Proposition 2.7 it contains $xsysx$, as an A-word, for some $s \in A^*$, or it contains an H-square, as an H-word, where

$H = \{x, y, z\}$, or just the same, $i^n(w)$ contains a square. The latter is impossible by the preceding remark. Next, since two distinct words of Δ do not overlap, $i^n(w)$ is square-free, $s \in A^*$ and $xsysx$ must be an H-factor of $h(i^n(w))$. Let $s = h(r)$ for $r \in A^*$ we see that $arbra$ is a factor of $i^n(w)$ despite the assumption that proves the former and completes the proof.

Thus, starting from arbitrary square-free and $arbra$-free word w we get an infinite set of square-free words $i^n(w), n = 0, 1, 2, \ldots$. To get more, just map each $i^n(w)$ to A^+ by an arbitrary such morphism h. The most simple and obvious way is to start with $w = a$ to append the sequence $i(a), i^2(a), \ldots$ that makes up the Istrail's infinite square-free word $i^\omega(a)$. So we get the infinite square-free word $h(i^\omega(a))$ for a weakly square-free triple $\Delta = \{x, y, z\}$ of A^+.

Now we attend to determine a first few short $x, y, z : |z| \leq |y| \leq |x|$ such that (x, y, z) is weakly square-free. As a matter of fact, we find ones with a stronger requirement, just for limiting search. We call Δ *quasi-square-free* (or "strongly weakly square-free") if it is weakly square-free and totally overlap-free. We in what follows consider the case $z = c$ for the first try.

When $|y| < 6$, y either fails to exist or brings nothing new.

Let now $|y| \geq 6$; we demonstrate in detail how to proceed. As $z = c$ both x and y begin by abc or acb and end by acb or cab. There are two cases.

(a) y begins by abc and hence ends by acb (avoiding self-overlapping)

$$y = abc \ldots acb$$

then x should begin also by abc (y does not overlap x) and end also by acb (to not overlap y)

$$x = abc \ldots acb.$$

Moreover, x and y do not end with $cbacb$ or $acbcacb$ because yz or xz contains $cbacba$ or $acbcacbc$ otherwise.

(b) y begins by acb and hence ends by cab

$$y = acb \ldots cab$$

and hence x begins also by acb and ends by cab (to avoid self-overlapping)

$$x = acb \ldots cab.$$

In this case x and y avoid the suffix $bcab$ or $bcab$ for the square $bcabca$ is present otherwise in xzy or yzx.

We handle the case (a) first. The following (and their prefixes) are the candidates for the prefix of x and y of length up to 12. We list them as in a dictionary and when they fail to be one we indicate the reason thereafter. For example,

“$abc - a$: xzy or yzx: $(bca)^2$”, or “$abc - bac - aba - b$: $(ab)^2$”

means

“$abc-a$: xzy or yzx contains $(bca)^2$”, or “$abc-bac-aba-b$ contains $(ab)^2$”, resp.

We divide them into blocs of three letters each separated by a dash (for easier visualizing).

$abc - a$: xzy or yzx: $(bca)^2$

$abc - bab$: xy or yx: $(cbac)^2$

$abc - bac - aba - b$: $(cb)^2$

$abc - bac - aba - ca$: $(baca)^2$

$abc - bac - aba - cba$

$abc - bac - aba - cbc$

$abc - bac - aba - cba$ (*)

$abc - bac - aba - cbc$ (**)

$abc - bac - abc - ab$: $(cab)^2$

$abc - bac - abc - aca$: $(ca)^2$

$abc - bac - abc - acb$ (***)

$abc - bac - abc - ba$: zx or zy: $(cabcba)^2$

$abc - bac - abc - bc$: $(bc)^2$

$abc - bac - ac$: (ac^2)

$abc - bac - ba$: $(cba)^2$

$abc - bac - bca - bab$: $(ab)^2$

$abc - bac - bca - bac$

$abc - bac - bca - ca$: $(ca)^2$

$abc - bac - bca - cba$

$abc - bac - bca - cbc$: $(acba)^2$

$abc - bac - bcb - aba$: $(ba)^2$

$abc - bac - bc - abc$

$abc - bac - bc - aca$

$abc - bac - bc - acb$: $(cbacb)^2$

$abc - bc$: $(bc)^2$.

That is all for the length up to 12. Take notice of the lines marked with (*), (**) and (***). We claim that

$$x = abcbacabcacb, \quad y = abcbacabacb, \quad z = c$$

are the shortest words of the form (a) for which $\Delta = \{x, y, z\}$ is quasi-square-free that can be verified directly. Note that (x, y, x) is the only related triple in this case.

Now we treat the case (b). The resulting words are longer, so we now separately demonstrate the procedure for the prefixes and suffixes that we shall again employ in the sequel. I traced it back to [9], where F. Dejean used the same trick.

For the prefixes, by the same manipulation as above (we omit the routine details), the following (and their prefixes) are all the candidates for the prefix of x and y of length up to 9.

$acb - abc - aba$ (1)
$acb - abc - acb$ (2)
$acb - cab - aca$ (3)
$acb - cab - cba$ (4)

and the following (and their suffixes) are all the candidates for the suffix of x and y up to the length of 12

$cba - bca - cba - cab$ (5)
$aca - bca - cba - cab$ (6)
$bac - bca - cba - cab$ (7).

We see that there are no ones of them that could be x or y, hence x and y should have length exceeding 12. If there exists x or y of length not exceeding 18 then there is a bloc T of 3 letters ($= 9 + 12 - 18$) which occurs in a prefix $p, |p| \leq 9$, and a suffix $s, |s| \leq 12$, above, so that

$$p = p'Tp'', \quad s = s'Ts''$$

for which s' is a suffix of p' and p'' is a prefix of s''. We glue them to the word $p'Ts''$ that, if square-free, will be a candidate for x or y. Armed with that reasoning, we try to find two such $p'Ts''$ for a desired Δ with $z = c$. All we have found are listed below (several T may lead to the same word).

$acb - abc - acb - aca - b$, $T = abc$, (2) and (5)
$acb - cab - cba - bca - cba - cab$, $T = cba$, (4) and (5)
$acb - cab - aca - bca - cba - cab$, $T = aca$, (3) and (6).

It turns out, fortunately, that any two of them together with $z = c$ form a Δ that is quasi- square-free that we can quickly verify. Thus

$$\Delta = \{acbcabcbabcacbacab, \quad acbabcacbacab, \quad c\}$$

and

$$\Delta = \{c, \quad acbabcacbacab, \quad acbcabacabcacbacab\}$$

are of smallest total lengths $(18, 13, 1)$ among quasi-square-free sets of Type II for $z = c$.

For square-free triples of this type, with again,

$$z = c, \quad x = a \dots b, \quad y = a \dots b,$$

the procedure above — we omit the details — first brings the triple

$$x = acbabcbacab, \quad y = acbcacbacab, \quad z = c$$

of length $(11, 11, 1)$ and then the triple

$$x = abcbacabacb, \quad abcbaccacb, \quad z = c$$

of length $(11, 10, 1)$, which are readily verified to be square-free triples. The latter is the shortest square-free triple of Type II, in the sense that every square-free triple (x, y, z), $|x| \geq |y| \geq |z|$, of this type satisfies $10 \leq |y|, 11 \leq |x|$. I shall explain the detail in the follow-up part of this work.

4. Type I

We exhibit in this section some examples of Type I, including one that is quasi-square-free and one that is square-free itself. The shortest possible case is when $|z| = 4$ with only two issues $z = acab$ and $z = abcb$.

Let $z = acab$. Processing as in Section 3 leads to the triple

$$\Delta = (acbcacbabcb, \quad acbcabcb, \quad acab)$$

of lengths (11, 8, 4) which is quickly and routinely verified to be quasi-square-free.

The case $z = abcb$ leads to the triple

$$\Delta = (acabcbabcacb, \quad acabcacb, \quad abcb)$$

of length 12, 8 and 4, respectively.

Now the next shortest case $|z| = 5$. Usually, it is more demanding to find square-free triples, but here it is just opposite. There exists only one $z = abcab$ which leads to the triple

$$(acbcacb, \quad acabcb, \quad abcab).$$

We use Proposition 2.7 to verify that that triple is square-free. for leisure. First, there is no one of x, y, z which is a factor of another, so only the K-property for $K = 2$ matters and it is enough to ensure the square-freeness of the Δ-square-free words of length at most 3. As for length 3, there is no related triple; the only self-overlap is ab, followed and preceded by c. As for length 2, a quick inspection reveals the square-freeness of those Δ-square-free words and we are done.

This example has the shortest total length of those square-free triples of Type I. According to my calculation, this together with the triples

$$(abacabc, \quad acbabc, \quad bacbc)$$

of Type IIII, and

$$(abcbabcacb, \quad abcbacabacb, \quad c)$$

of Type II, only are of the smallest length of all, of course save for the ground alphabet, in the sense that any square-free triple (x, y, z), $|x| \geq |y| \geq |z|$ will have either $7 \leq |x|, 6 \leq |y|, 5 \leq |z|$ or $11 \leq |x|, 10 \leq |y|$, or both, uniquely. The detail will be explained in the follow-up part of this paper.

A small question of enumeration, a bid for continuation: what is the minimal length of a uniform square-free triple? 9 is definitely not; I guess 10.

References

[1] S.I. Adian, The Burnside Problem and Identities in Groups, Ergeb. Math. Grenzgeb. 95, Springer-Verlag, Berlin, 1979; [Russian, Nauka, 1975]

[2] J-P. Allouche, *Thue, Combinatorics on Words, and Conjectures Inspired by the Thue-Morse Sequence,* Journal de Théorie des Nombres de Bordeaux 27(2015), 375-388

[3] S.E. Arshon, *Proof of the Existence on Infinite Assymetric Sequences,* Mat. Sbornik (2) 44(1937), 769-779 (Russian)

[[4] D.R. Bean, A. Ehrenfeucht, G.F. McNulty, *Avoidable Patterns in Strings of Symbols,* Pacific Journal of Mathematics 85(1979), 261-294

[5] C. Choffrut, J. Karhumäki, Combinatorics on Words, in: Handbook of Formal Languages, v.1, G. Rozenberg, A. Salomaa, (Eds.), Springer, 1997

[6] M. Crochemore, *Sharp Characterizations of Square-free Morphisms,* Theoretical Computer Science 18 (1982), 221-226

[7] M. Crochemore, *Test sur les morphismes faiblement sans carré,* in: Combinatorics on Words (L.J. Cummings Eds.), Academic Press, 1983

[8] J.D. Currie, *Pattern Avoidance: themes and variations,* Theoretical Computer Science 339(2005), 7-18

[9] F. Dejean, *Sur Un Thérème de Thue,* Journal of Combinatorial Theory Ser. A 13(1972), 90-99

[10] S. Istrail, *On Irreducible Languages and Nonrational Numbers,* Bull. Math. Soc.Sci. Math. R. S. Roumaine. Tom 21 (69)(1977), nr. 3-4, 301-308

[11] G. Lallement, Semigroup and Combinatorial Applications, John Wiley and Sons, 1979

[12] P. S. Novikov, *On Periodic Groups,* Dokl. Acad. Nauk. SSSR 127(1959), nr. 4, 749-752; English translation, American Math. Soc. Transl. (2) (1965), 19-22

[13] E. Prouhet, *Mémoire sur quelques relations entre les puissances des nombres,* C. R. Acad. Sci. Paris 33(1851), 225.

Note about the linear complexity of new generalized cyclotomic binary sequences of period p^n

Vladimir Edemskiy
Novgorod State University, Russia*
Vladimir.Edemskiy@novsu.ru

1 Introduction

Linear complexity (L) is a very important merit factor for measuring unpredictability of pseudo-random sequences, which are often used as key stream sequences in stream ciphers. It is defined as the length of the shortest linear feedback shift register that can generate the sequence. The feedback function on this shift register can be deduced from knowledge of just $2L$ consecutive digits of the sequence. Thus, it is reasonable to suggest that 'good' sequences have $L > N/2$ (where N denotes the period of the sequence).

Cyclotomy is an old topic of elementary number theory. Classical and generalized cyclotomies have been used in the construction of sequences with desirable properties. Classical cyclotomy was first considered in detail by Gauss. Later, Ding and Helleseth introduced the generalized cyclotomy, which includes classical cyclotomy as a special case. New an approach was prepared in [6]. Based on the new generalized cyclotomic classes in [6], Xiao et al. presented a new family of cyclotomic binary sequences of period p^n and determined the linear complexity of the sequences in the case when $n = 2$ [7]. Further, these results was generalized in [2] for $n \geq 2$. It was shown in [2] that the linear complexity of new family of cyclotomic binary sequences of period p^n depends on a value $v = \gcd\left(\frac{p-1}{\mathrm{ord}_p(2)}, f\right)$, where $p = 1 + ef$ and $\mathrm{ord}_p(2)$ denote the order of 2 modulo p. In [2] the exact value of L was defined when v divides $f/2$ or

*The reported study was supported by Russian Foundation for Basic Research and Novgorod region under grant No. 18-41-530001.

$v = 2, f$. The experimental result indicates that Theorem 5 from [2] is true for $v = 4$, but the method from this paper can not be used in this case. So, our goal is generalizing the results [2] for this case.

2 The linear complexity

Let p be an odd prime and $p = ef + 1$, where e, f are positive integers and f is even. Let g be a primitive root modulo p. We define

$$\begin{aligned} &D_0^{(f)} = \left\{g^{t\cdot f} \ (\mathrm{mod} p) \,|\, 0 \le t < e\right\}, \text{ and} \\ &D_i^{(f)} = g^i D_0^{(f)} = \left\{g^i x \ (\mathrm{mod} p) : x \in D_0^{(f)}\right\}, \quad 1 \le i < f, \end{aligned} \tag{1}$$

and

$$\begin{aligned} &D_0^{(f/2)} = \left\{g^{t\cdot f/2} \ (\mathrm{mod} p) \,|\, 0 \le t < 2e\right\}, \text{ and} \\ &D_i^{(f/2)} = g^i D_0^{(f/2)} = \left\{g^i x \ (\mathrm{mod} p) : x \in D_0^{(f/2)}\right\}, \quad 1 \le i < f/2. \end{aligned} \tag{2}$$

The cosets $D_i^{(f)}$, $i = 0, 1, \cdots, f-1$, and $D_i^{(f/2)}$, $i = 0, 1, \cdots, f/2-1$ are called respectively *cyclotomic classes* of order f and $f/2$ with respect to p. It is well known that $\left\{D_0^{(f)}, D_1^{(f)}, \ldots, D_{f-1}^{(f)}\right\}$ forms a partition of $\mathbb{Z}_p^*$ and

$$\mathbb{Z}_p = \bigcup_{i=0}^{f-1} D_i^{(f)} \cup \{0\}.$$

Let b be an integer with $0 \le b < f$. Define two sets

$$\begin{aligned} &\mathcal{C}_0 = \bigcup_{i=f/2}^{f-1} D_{(i+b) \pmod f}^{(f)}, \text{ and} \\ &\mathcal{C}_1 = \bigcup_{i=0}^{f/2-1} D_{(i+b) \pmod f}^{(f)} \cup \{0\}. \end{aligned} \tag{3}$$

It is obvious that $\mathbb{Z}_p = \mathcal{C}_0 \cup \mathcal{C}_1$. Considered in [2] a family of almost balanced binary sequences $s^\infty = (s_0, s_1, s_2, \ldots)$ of period p can thus be defined as

$$s_i = \begin{cases} 0, & \text{if } i \ (\mathrm{mod}\ p) \in \mathcal{C}_0, \\ 1, & \text{if } i \ (\mathrm{mod}\ p) \in \mathcal{C}_1. \end{cases} \tag{4}$$

Let $S(x) = s_0 + s_1x + \cdots + s_{p-1}x^{p-1}$ for the cyclotomic sequences s^∞ defined in (4). Then, it is well known (see, for instance, [1]) that linear complexity of binary sequence s^∞ of period p is given by

$$L = N - \deg\Big(\gcd\big(x^p - 1, S(x)\big)\Big).$$

The above formula allows one to determine the linear complexity of s^∞ by examining the roots of $S(x)$ in an extension of $\mathbb{F}_2$ (the finite field of two elements). Let $\overline{\mathbb{F}}_2$ be an algebraic closure of $\mathbb{F}_2$ and let $\alpha \in \overline{\mathbb{F}}_2$ be a primitive p-th root of unity. Then

$$L = p - \left|\left\{S(\alpha^i) = 0 \,|\, i \in \mathbb{Z}_p\right\}\right|. \tag{5}$$

Denote by $\mathrm{ord}_p(2)$ an order of 2 modulo p. By [2] we have that if $v = \gcd(\frac{p-1}{\mathrm{ord}_p(2)}, f)$ and $v \,|\, \frac{f}{2}$, or $v = 2$ and $f \neq v$ then $S(\alpha^t) \neq 0$ for $t = 1, \dots, p-1$.

Our goal is to show that this statement is true for $v = 4$.

Theorem 1. *Let $p = ef + 1$ be an odd prime and $f \neq 4$ being an even positive integer. Let s^∞ be a generalized cyclotomic binary sequence of period p defined in* (4). *Let* $\mathrm{ord}_p(2)$ *denote the order of* 2 *modulo p and* $4 = \gcd\big(\frac{p-1}{\mathrm{ord}_p(2)}, f\big)$. *Then the linear complexity of s^∞ is given by $L = p$.*

By condition $S(1) = \frac{p+1}{2} \equiv 1 \pmod 2$. Further, we will show that $S(\alpha^t) \neq 0$ for $t = 1, 2, \dots, p-1$. We carry out the proof in several steps.

It can be easily seen from (1), (3) and (4) that

$$S(x) = 1 + \sum_{i=0}^{f/2-1} \sum_{t \in D^{(f)}_{i+b \pmod f}} x^t. \tag{6}$$

For simplicity of the presentation, we define polynomials

$$E_i(x) = \sum_{t \in D_i^{(f)}} x^t, \quad ,0 \le i < f, \tag{7}$$

$$F_i(x) = \sum_{t \in D_i^{(f/2)}} x^t, \quad ,0 \le i < f/2, \tag{8}$$

and

$$H_k(x) = \sum_{i=0}^{f/2-1} E_{i+k \pmod f}(x), \quad 0 \le k < f, \tag{9}$$

Notice that the subscripts i in $D_i^{(f)}, E_i(x)$ and $H_i(x)$ are all taken modulo f and the subscripts i in $D_i^{(f/2)}$ and $F_i(x)$ are all taken modulo the order $f/2$. In the rest of this paper the modulo operation will be omitted when no confusion can arise.

It can be easily seen from (6),(7) - (9) that $S(x) = 1 + H_b(x)$.

Suppose $2 \in D_u^{(f)}$ for some integer u. It is easily seen that $u \neq 0, u \equiv 4 \pmod{f}$. So $2 \in D_w^{(f/2)}, w \neq 0$ and $w \equiv 0 \pmod{2}$.

Some basic properties of these polynomials are given in the following lemmas.

Lemma 2.
(i) $E_i(\alpha^a) = E_{i+m}(\alpha)$ *for any* $a \in D_m^{(f)};, \ i, m = 0, 1, \ldots, f-1$*;*
(ii) $(E_i(\alpha^a))^2 = E_{i+u}(\alpha^a)$ *if* $2 \in D_u^{(f)}$*;*
(iii) $H_i(\alpha^a) + H_i(\alpha^{ag^{f/2}}) = H_i(\alpha^a) + H_{i+f/2}(\alpha) = 1$ *for* $i = 0, 1 \ldots, f/2 - 1$*;*
(iv) $F_i(\alpha^{g^k}) = F_{i+k}(\alpha)$ *for* $i = 0, 1 \ldots, f/2 - 1; k = 0, 1, \ldots, p-1$*;*
(v) $(F_i(\alpha^a))^2 = F_{i+w}(\alpha^a)$ *for* $i = 0, 1 \ldots, f/2 - 1; 2 \in D_w^{(f/2)}$*;*

Lemma 3. *Let* $\gcd(\frac{p-1}{\operatorname{ord}_p(2)}, f) = 4$ *and* $f \neq 4$*. If* $H_0(\alpha) = 1$ *then*

$$F_{2i}(\alpha) + F_{2i+1}(\alpha) = 1, \ \ i = 0, 1, \ldots, f/4 - 1.$$

Proof. Let $2 \in D_u^{(p)}$. Then $4 = \gcd(u, f)$, by a similar argument as in [2] we get that

$$1 = H_0(\alpha) = H_4(\alpha) = \cdots = H_{f-4}(\alpha)$$

and

$$0 = H_2(\alpha) = H_6(\alpha) = \cdots = H_{f-2}(\alpha)$$

So $H_{2i}(\alpha) + H_{2i+2}(\alpha) = 1$. Hence

$$E_{2i}(\alpha) + E_{2i+1}(\alpha) + E_{2i+f/2}(\alpha) + E_{2i+1+f/2}(\alpha) = 1.$$

By the definitions we have

$$D_{2i}^{(f)} \cup D_{2i+f/2}^{(f)} = D_{2i(\bmod f/2)}^{(f/2)}.$$

Thus $E_{2i}(\alpha) + E_{2i+f/2}(\alpha) = F_{2i}(\alpha)$ and $E_{2i+1}(\alpha) + E_{2i+1+f/2}(\alpha) = F_{2i+1}(\alpha)$. □

Let (i, j) be cyclotomic numbers of order $f/2$ modulo p, i.e., $(i, j) = |(D_i^{(f/2)} + 1) \cap D_j^{(f/2)}|$. Using $-1 = g^{(p-1)/2} = g^{ef/2}$, we obtain that $-1 \in D_0^{(f/2)}$. Hence $\sum_{j=0}^{f/2-1}(0, j) = |D_0^{(f/2)} - 1|$ and $\sum_{j=0}^{f/2-1}(1, j) = |D_0^{(f/2)}|$. By (2) $|D_0^{(f/2)}| = 2e$, thus we see that

$$\sum_{j=0}^{f/2-1}(0, j) \equiv 1 \pmod{2} \text{ and } \sum_{j=0}^{f/2-1}(1, j) \equiv 0 \pmod{2}. \tag{10}$$

The sums $\sum_{i\in D_j^{(f/2)}}\alpha^{ij}$ are also called Gauss period and by [5] (Proposition 8) we have the following statement when $f/2$ is even (see, also [3]).

Lemma 4.
(i) $(F_j(\alpha))^2=\sum_{i=0}^{f/2-1}(0,i)F_{i+j}(\alpha)$ *for* $j=0,1\dots,f/2-1$*; and*
(ii)$F_j(\alpha)F_{j+1}(\alpha)=\sum_{i=0}^{f/2-1}(1,i)F_{i+j}(\alpha)$ *for* $j=0,1\dots,f/2-1$.

Lemma 5. *Let* $f/2$ *is even and* $2\in D_w^{(f/2)}$*. Then* $(0,w)\equiv 1 \pmod 2$ *and* $(0,j)\equiv 0 \pmod 2$ *for* $j=0,1\dots,f/2-1$ *and* $j\neq w$.

Proof. Let $T(x)=F_w(x)+\sum_{i=0}^{f/2-1}(0,i)F_i(x)$. Since $F_i(1)=2e$, we see that $T(1)=0$ in $\mathbb{F}_2$. Further, by Lemma 2 (iv) we get $T(\alpha^{g^k})=F_w(\alpha^{g^k})+\sum_{i=0}^{f/2-1}(0,i)F_i(\alpha^{g^k})=F_{w+k}(\alpha)+\sum_{i=0}^{f/2-1}(0,i)F_{i+k}(\alpha)$ or by Lemma 4 $T(\alpha^{g^k})=F_{w+k}(\alpha)+(F_k(\alpha))^2=0$. Thus $T(x)$ have p roots and $\deg T(x)\le p-1$, hence $T(x)\equiv 0$ in a ring $GF(2)[x]$. In this case $(0,w)+1\equiv 0 \pmod 2$ and $(0,j)\equiv 0 \pmod 2$ for $j=0,1\dots,f/2-1$ and $j\neq w$. □

Lemma 6. *Let* $F_{2i}(\alpha)+F_{2i+1}(\alpha)=1,\ \ i=0,1,\dots,f/4-1$ *and* $2\in D_w^{(f/2)},w\neq 0$*. Then* $(1,0)+(1,1)\equiv 1 \pmod 2$.

Proof. We consider

$$G(x)=\sum_{i=0}^{f/4-1}\left((1,2i)+(1,2i+1)\right)F_{2i+1}(x)+F_1(x)+F_{1+w}(x)+\sum_{i=0}^{f/4-1}(1,2i+1).$$

We have that $-1\in D_0^{(f/2)}$ and w is an even, hence $\deg G(x)<p-1$.

1). Let $x=\alpha^{g^{2k}}$. Then

$$G(\alpha^{g^{2k}})=\sum_{i=0}^{f/4-1}\left((1,2i)+(1,2i+1)\right)F_{2i+1+2k}(\alpha)+$$
$$F_{1+2k}(\alpha)+F_{1+w+2k}(\alpha)+\sum_{i=0}^{f/4-1}(1,2i+1).$$

Since $F_{2i+1+2k}(\alpha)=1+F_{2i+2k}(\alpha)$, it follows by Lemma 4 that

$$\sum_{i=0}^{f/4-1}\left((1,2i)+(1,2i+1)\right)F_{2i+1+2k}(\alpha)=$$

$$\sum_{i=0}^{f/4-1}(1,2i)(1+F_{2i+2k})(\alpha)+\sum_{i=0}^{f/4-1}(1,2i+1)F_{2i+1+2k}(\alpha)=$$

$$\sum_{i=0}^{f/4-1}(1,2i)+\sum_{j=0}^{f/2-1}(1,j)F_{j+2k}(\alpha)=\sum_{i=0}^{f/4-1}(1,2i)+F_{2k}(\alpha)F_{2k+1}(\alpha).$$

By (10) we have that $\sum_{i=0}^{f/2-1}(1,j)\equiv 0 \pmod 2$, thus

$$G(\alpha^{g^{2k}})=F_{2k}(\alpha)F_{2k+1}(\alpha)+F_{1+2k}(\alpha)+F_{1+w+2k}(\alpha)$$

or

$$G(\alpha^{g^{2k}})=(1+F_{2k+1}(\alpha))F_{2k+1}(\alpha)+F_{1+2k}(\alpha)+F_{1+w+2k}(\alpha).$$

By Lemma 2 $(F_{2k+1}(\alpha))^2=F_{2k+1+w}(\alpha)$, hence $G(\alpha^{g^{2k}})=0$.

2). Let $x=\alpha^{g^{2k+1}}$. Then

$$G(\alpha^{g^{2k+1}})=\sum_{i=0}^{f/4-1}\left((1,2i)+(1,2i+1)\right)F_{2i+2+2k}(\alpha)+$$

$$F_{2+2k}(\alpha)+F_{2+w+2k}(\alpha)+\sum_{i=0}^{f/4-1}(1,2i+1).$$

Since $F_{2i+2+2k}(\alpha)=1+F_{2i+2k+2+1}(\alpha)$, it follows by Lemma 4 that

$$\sum_{i=0}^{f/4-1}\left((1,2i)+(1,2i+1)\right)F_{2i+2+2k}(\alpha)=$$

$$\sum_{i=0}^{f/4-1}(1,2i)F_{2i+2k+2}(\alpha)+\sum_{i=0}^{f/4-1}(1,2i+1)(1+F_{2i+1+2+2k}(\alpha))$$

$$=\sum_{j=0}^{f/2-1}(1,j)F_{j+2k+2}(\alpha)+\sum_{i=0}^{f/4-1}(1,2i+1)=F_{2k+2}(\alpha)F_{2k+3}(\alpha)+\sum_{i=0}^{f/4-1}(1,2i+1).$$

Thus $G(\alpha^{g^{2k}})=F_{2k+2}(\alpha)(1+F_{2k+2}(\alpha))+F_{2+2k}(\alpha)+F_{2+w+2k}(\alpha)$. By Lemma 2 $(F_{2k+2}(\alpha))^2=F_{2+2k+w}(\alpha)$, hence $G(\alpha^{g^{2k+1}})=0$.

So $G(x)$ have $p-1$ roots and $\deg G(x) < p-1$, hence $G(x)=0$ in a ring $GF(2)[x]$. In this case $(1,0)+(1,1) \equiv 1 \pmod 2$. □

Proof of Theorem 1

Let there exists h such that $S(\alpha^h)=0$. Then $H_b(\alpha^h)=H_{b+t}(\alpha)=1$, where $t : h \in D_t^{(f)}$. Without loss of generality, we can assume $b+t \equiv 0 \pmod f$ and $H_0(\alpha)=1$. By Lemmas 3 and 6 we get that $(1,0)+(1,1) \equiv 1 \pmod 2$. Using the properties of cyclotomic numbers ($(i,j)=(-i,i-j)$ and $(i,j)=(j,i)$ when $f/2$ is even, [4], formulae 11.6.35) we get that $(1,1)=(-1,0)=(0,f/2-1)$ and $(0,1)+(0,f/2-1) \equiv 1 \pmod 2$. We have a contradiction with Lemma 5 since $w \neq 1$ and $w \neq f/2-1$.

Remark 7. *If s^∞ is a sequence with a period p^n as in [2] then in the conditions of Theorem 1 $L = p^n$.*

References

[1] Cusick, T., Ding, C., Renvall, A.: Stream Ciphers and Number Theory. North-Holland mathematical library. Elsevier (2004).

[2] Edemskiy, V., Li, C., Zeng, X., Helleseth, T.: The linear complexity of generalized cyclotomic binary sequences of period p^n. Designs, Codes and Cryptography, 2018, 1-15, DOI: 10.1007/s10623-018-0513-2

[3] Edemskii, V. A.: On the linear complexity of binary sequences on the basis of biquadratic and sextic residue classes, Discret. Math. Appl. 20(1)(2010) 75-84; translation from Diskretn. Mat. vol. 22(4)(2010) 74-82.

[4] Hall, M.: Combinatorial Theory, Wiley, New York (1975)

[5] Myerson, G.: Period polynomials and Gauss sums for finite fields. Acta Arith. 39 (1981) 251-264.

[6] Zeng, X., Cai, H., Tang, X., Yang, Y.: Optimal frequency hopping sequences of odd length. IEEE Transactions on Information Theory **59**(5), 3237–3248 (2013).

[7] Xiao, Z., Zeng, X., Li, C., Helleseth, T.: New generalized cyclotomic binary sequences of period p^2. Des. Codes Cryptography 86(7)(2018) 1483-1497.

Научное издание

Пятый российско-финский симпозиум по дискретной математике

Издано в авторской редакции

Подписано в печать 06.05.2019. Бумага офсетная. Формат 60×84 1/16.
Гарнитура Times New Roman. Печать офсетная.
Усл. печ. л. 11,6. Уч.-изд. л. 10,2. Тираж 50 экз. Заказ № 431.
Отпечатано в ЗАО «Новгородский технопарк».
173003, Великий Новгород, ул. Б.Санкт-Петербургская, 41.
Тел. (816 2) 73-17-05.