A. Hakanen | V. Halava | P. Herva | J. Kari |
T. Laihonen | I. Petre | A. Saarela (Eds).

Proceedings of the Sixth Russian-Finnish Symposium on Discrete Mathematics

Turku Centre *for* Computer Science

TUCS Lecture Notes
No 31, October 2021

Proceedings of the Sixth Russian-Finnish Symposium on Discrete Mathematics (RuFiDiM 2021)

Anni Hakanen, Vesa Halava, Pyry Herva, Jarkko Kari,
Tero Laihonen, Ion Petre, and Aleksi Saarela (Eds.)

21 – 23 October, 2021
Turku, Finland

Editors

Anni Hakanen
Department of Mathematics and Statistics
University of Turku
Finland

Vesa Halava
Department of Mathematics and Statistics
University of Turku
Finland

Pyry Herva
Department of Mathematics and Statistics
University of Turku
Finland

Jarkko Kari
Department of Mathematics and Statistics
University of Turku
Finland

Tero Laihonen
Department of Mathematics and Statistics
University of Turku
Finland

Ion Petre
Department of Mathematics and Statistics
University of Turku
Finland

Aleksi Saarela
Department of Mathematics and Statistics
University of Turku
Finland

ISBN 978-952-12-4113-0
ISSN 1797-8831

Preface

The Russian-Finnish Symposium on Discrete Mathematics (RuFiDiM) conference series was initiated in 2011 to strengthen the cooperation between the Finnish and the Russian communities of researchers in discrete mathematics. The RuFiDiM symposia became established as international events, with contributions from all over the world.

The sixth Russian-Finnish Symposium on Discrete Mathematics conference (RuFiDiM) was organized by the Department of Mathematics and Statistics of University of Turku as an online symposium during October 21-23 2021. The conference was delayed by a year and a half due to the COVID-19 pandemic. Even in October 2021 we were forced to organize the symposium as an online event. Previous editions of the symposium were held in St. Petersburg (2011), Turku (2012), Petrozavodsk (2014), Turku (2017), and Veliky Novgorod (2019). The 2022 edition will be held in St. Petersburg during June 12-15, as a satellite event of the International Congress of Mathematicians.

RuFiDiM 2021 consisted of 5 invited talks and 20 contributed presentations. The invited speakers were Lauri Hella (Tampere University, Finland), Kaisa Matomäki (University of Turku, Finland), Alexander Tiskin (St. Petersburg State University, Russia), Yaokun Wu (Shanghai Jiao Tong University, China) and Ismael Yero (Universidad de Cádiz, Spain). The abstracts or extended abstracts of the contributions to the symposium are presented in these proceedings. They were selected by the symposium's scientific committee made of Vesa Halava, Juhani Karhumäki, Jarkko Kari, Dmitry Karpov, Tero Laihonen, Yuri Matiyasevitch, Vladimir Mazalov, Ion Petre, Ilya Ponomarenko, Svetlana Puzynina, Aleksi Saarela, and Mikhail Volkov.

The scientific spectrum of the contributions to the symposium offers a broad snapshot of the current research landscape in discrete mathematics in Finland and in Russia. The topics cover a very diverse set of topics: cellular automata, combinatorics on words, combinatorial optimization, game theory, graph theory, and quantum computing.

We are grateful to all authors who contributed to the symposium. We would like to thank the scientific committee for the time they spent reviewing the manuscripts submitted to the symposium. The symposium was supported by the Finnish Academy of Sciences (Mathematics Fund), the University of Turku, Turku Centre for Computer Science, and the Emmy Network Foundation.

Anni Hakanen, Vesa Halava, Pyry Herva, Jarkko Kari, Tero Laihonen, Ion Petre, Aleksi Saarela

Department of Mathematics and Statistics, University of Turku

Turku, October 2021

Organization

Scientific committee:

- Vesa Halava
- Juhani Karhumäki
- Jarkko Kari
- Dmitry Karpov
- Tero Laihonen
- Yuri Matiyasevich
- Vladimir Mazalov
- Ion Petre
- Ilya Ponomarenko
- Svetlana Puzynina
- Aleksi Saarela
- Mikhail Volkov

Organizing committee:

- Anni Hakanen
- Vesa Halava
- Pyry Herva
- Jarkko Kari
- Tero Laihonen
- Ion Petre
- Aleksi Saarela

Contents

Part I
Invited lectures

Dimensions of families of sets with applications to team semantics

Lauri Hella[1], Kerkko Luosto[1], and Jouko Väänänen*[2]

[1]Tampere University
[2]University of Helsinki

Abstract

In this extended abstract, we introduce three measures of complexity for families of sets. Each of the three measures, that we call dimensions, is defined in terms of the minimal number of convex subfamilies that are needed for covering the given family: for upper dimension, the subfamilies are required to contain a unique maximal set, for dual upper dimension a unique minimal set, and for cylindrical dimension both a unique maximal and a unique minimal set. In addition to considering dimensions of particular families of sets we study the behaviour of dimensions under operators that map families of sets to new families of sets. We identify natural sufficient criteria for such operators to preserve the growth class of the dimensions.

We apply the theory of our dimensions for proving new hierarchy results for logics with team semantics. First, we show that the standard logical operators preserve the growth classes of the families arising from the semantics of formulas in such logics. Second, we show that the upper dimension of $k+1$-ary dependence, inclusion, independence and exclusion atoms is in a strictly higher growth class than that of any k-ary atoms, whence the $k+1$-ary atoms are not definable in terms of any atoms of smaller arity.

1 Introduction

Families of sets are well-studied in discrete mathematics and set theory. Sperner families and downward closed families are examples of basic building blocks that can be used to analyse complex families. Considerations on ways how to represent a family as a union of more basic families leads us to several concepts of dimension. Given the finite size of the base set, we use our dimensions to associate families of subsets of the base set with better quantitative estimates than their mere size. We show that certain canonical

*The third author would like to thank the Academy of Finland, grant no: 322795. This project has received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (grant agreement No 101020762).

operations on families of sets preserve dimension. This allows us to isolate dimension bounded collections of families of sets.

By restricting attention to families of subsets of cartesian powers of finite sets we obtain finer distinctions. Such families arise in the context of so-called team semantics. In ordinary Tarski semantics of first order logic and its extensions by new logical operations any formula and any model of the appropriate kind can be associated with the set of assignments satisfying the formula in the model. It is natural to consider such a set as a subset of the cartesian power of the domain of the model. In team semantics satisfaction is defined with respect to sets ('teams') of assignments. Accordingly, any formula becomes associated with a family of subsets of such a cartesian power. We use our dimensions and preservation results for logical operations to prove new non-definability and hierarchy results for logics based on teams semantics. Examples of such logics are dependence logic, independence logic and inclusion logic.

The background of our work for this paper is the following. Ciardelli defined in his Master's Thesis [Cia09] a dimension concept, in the case of downward closed families, namely the cardinality of the set of maximal sets, or equivalently, the smallest number of power-sets that cover the family. He proved the preservation properties for basic propositional logic operations, including intuitionistic implication, and referred to them as Groenendijk inequalities. Hella, Luosto, Sano and Virtema [HLSV14] introduced a similar dimension concept in modal logic, including preservation of dimension results for logical operations of modal dependence logic. Hella and Stumpf [HS15] used a form of dimension to prove a succinctness result for the inclusion atom in modal inclusion logic. Lück and Vilander [LV19] generalized the notion of dimension from downward closed families to arbitrary families. They proved preservation of dimension under propositional operations, and computed the dimension of dependence and exclusion atoms in the context of propositional logic.

There are several other dimension concepts in discrete mathematics. Perhaps the most famous is the matroid rank, which coincides with the usual concept of dimension in the case of vector spaces and with degree of transcendence in the case of algebraically closed fields. However, our families do not necessarily satisfy the Exchange Axiom of matroids and therefore this concept does not work in our context. Another well-known dimension is the Vapnik–Chervonenkis- or VC-dimension. However VC-dimension is not preserved by logical operations in the sense that our dimension is. Therefore it does not serve our purpose in this paper. Still another dimension is the length of a disjunctive normal form in propositional logic. In the full paper we show we show that this is equivalent to one of the dimensions (cylindrical dimension) we investigate.

The concepts we introduce in this paper belong to discrete mathematics with no immediate connection to logic. Thus part of this paper can be read with no knowledge or interest in logic. However, our applications come from logic, more exactly from team semantics. We believe that our results are an interesting new contribution to discrete mathematics of families of sets. At the same time, we suggest that our results lead to a new approach to definability questions in team semantics and, in particular, yield a new strong hierarchy result (Theorem 5.5).

This extended abstract is a preliminary version of a forthcoming full paper which will cover more material both in the general theory of dimensions of families and applications in team semantics. Most of the proofs have been omitted in this version of the paper.

2 Basic notions

2.1 Families of sets

In the sequel, our applications will build on heavy use of combinatorial results in the subfield often called set-system combinatorics. We start with commonly used notions.

We use standard set-theoretic notation, including the shorthands $\bigcup \mathcal{A} = \bigcup_{A \in \mathcal{A}} A$ and $\bigcap \mathcal{A} = \bigcap_{A \in \mathcal{A}} A$, the latter being unambiguous only if $\mathcal{A} \neq \emptyset$. In addition, we write $[A, B] = \{C \mid A \subseteq C \subseteq B\}$, for any sets A and B. Note that if $A \not\subseteq B$, then $[A, B] = \emptyset$.

Definition 2.1. Let $\mathcal{A}$ be a family of sets. The family $\mathcal{A}$ is

- an *interval or cylinder*, if there exist A_0 and A_1 such that $A_0 \subseteq A_1$ and $\mathcal{A} = [A_0, A_1]$,
- *convex* if for all $S, T \in \mathcal{A}$, we have $[S, T] \subseteq \mathcal{A}$,
- *downwards closed* if $A \in \mathcal{A}$ and $S \subseteq A$ imply $S \in \mathcal{A}$
- a *Sperner family* if for all $S, T \in \mathcal{A}$ we have $S \not\subseteq T$,
- fulfills the *Zorn condition* if it is closed under unions of chains: if $\mathcal{C}$ is a chain (i.e., a family linearly ordered by inclusion), then $\bigcup \mathcal{C} \in \mathcal{C}$,
- *closed under unions* if for every subfamily $\mathcal{B} \subseteq \mathcal{A}$, we have $\bigcup \mathcal{B} \in \mathcal{A}$.

Note that if a family of sets is downward closed or a Sperner family, then it is also convex. The concept of a upward closed family is also useful in set theory but is lacking here, as applications of our methods are very much leaning towards downward closed families.

For $\mathcal{A}$ a family of sets, we denote the family of all maximal (with respect to inclusion) sets in $\mathcal{A}$ by $\mathrm{Max}(\mathcal{A})$. Similarly, $\mathrm{Min}(\mathcal{A})$ is the set of all minimal sets in $\mathcal{A}$. Observe that $\mathrm{Max}(\mathcal{A})$ and $\mathrm{Min}(\mathcal{A})$ are always Sperner families.

Definition 2.2. A family of set $\mathcal{A}$ is *dominated (by $\bigcup \mathcal{A}$)* if $\bigcup \mathcal{A} \in \mathcal{A}$. The family $\mathcal{A}$ is *supported* (by $\bigcap \mathcal{A}$) if $\mathcal{A}$ is nonempty and $\bigcap \mathcal{A} \in \mathcal{A}$. Naturally, we say that $\mathcal{A}$ is *dominated convex* if it is dominated and convex. Similarly, $\mathcal{A}$ is *supported convex* if it is supported and convex.

In other words, a family $\mathcal{A}$ is dominated by a set D if and only if D is the largest element in $\mathcal{A}$ with respect to inclusion. Similarly, $\mathcal{A}$ is supported by a set S if and only if S is the smallest element in $\mathcal{A}$ with respect to inclusion. We spell out some of the easily seen connections between the basic concepts in the following lemma.

Lemma 2.3. *Let $\mathcal{A} \subseteq \mathcal{P}(X)$ and denote $\mathcal{A}^{\mathsf{d}} = \{X \setminus A \mid A \in \mathcal{A}\}$.*

1. *The family $\mathcal{A}$ is an interval iff it is dominated, supported and convex.*
2. *$\mathcal{A}$ is convex iff $\mathcal{A}^{\mathsf{d}}$ is convex.*
3. *$\mathcal{A}$ is dominated iff $\mathcal{A}^{\mathsf{d}}$ is supported.*

We proceed to the central dimension concepts which will be studied throughout this paper. The *upper dimension* was first defined for downwards closed in the paper of Hella, Luosto, Sano and Virtema [HLSV14] and subsequently generalized for arbitrary families by Lück and Vilander in [LV19]. The definition presented here is an equivalent reformulation of the latter. We also introduce two new dimension concepts: *dual upper dimension* and *cylindrical dimension.*

Definition 2.4. Let $\mathcal{A}$ be a family of sets. We say that a subfamily $\mathcal{G} \subseteq \mathcal{A}$ *dominates* $\mathcal{A}$ if there exist dominated convex families $\mathcal{A}_G$, $G \in \mathcal{G}$, such that $\bigcup_{G\in\mathcal{G}} \mathcal{A}_G = \mathcal{A}$ and $\bigcup \mathcal{A}_G = G$, for each $G \in \mathcal{G}$. The subfamily $\mathcal{K} \subseteq \mathcal{A}$ *supports* $\mathcal{A}$ if there exist supported convex families $\mathcal{S}_K$, $K \in \mathcal{K}$ such that $\bigcup_{K\in\mathcal{K}} \mathcal{S}_K = \mathcal{A}$ ja $\bigcap \mathcal{S}_K = K$, for each $K \in \mathcal{K}$.

Definition 2.5. Let $\mathcal{A}$ be a family of sets.

1. The *upper dimension* of $\mathcal{A}$ is $\mathrm{D}(\mathcal{A}) = \min\{|\mathcal{G}| \mid \mathcal{G} \text{ dominates the family } \mathcal{A}\}$.
2. The *dual upper dimension* of $\mathcal{A}$ is $\mathrm{D}^{\mathrm{d}}(\mathcal{A}) = \min\{|\mathcal{G}| \mid \mathcal{G} \text{ supports the family } \mathcal{A}\}$.
3. The *cylindrical dimension* of $\mathcal{A}$ is
   $\mathrm{CD}(\mathcal{A}) = \min\{|I| \mid \text{there are sets } A_i, B_i \text{ for } i \in I \text{ such that } \bigcup_{i\in I}[A_i, B_i] = \mathcal{A}\}$.

2.2 Operators

In addition to studying the dimensions of fixed families of sets we are also interested in the behaviour of dimensions under various operators. An operator for families of sets on a fixed base set X is a function $\Delta\colon \mathcal{P}(\mathcal{P}(X))^n \to \mathcal{P}(\mathcal{P}(X))$ for some positive integer n. In some applications we consider more general operators of the form $\Delta\colon \mathcal{P}(\mathcal{P}(X))^n \to \mathcal{P}(\mathcal{P}(Y))$ with different base sets X and Y. We list in the next example some natural set-theoretic operators that we will study further in the forthcoming sections.

Example 2.6. (a) *Union and intersection.* The union operator $\Delta^X_\cup\colon \mathcal{P}(\mathcal{P}(X))^2 \to \mathcal{P}(\mathcal{P}(X))$ on the base set X is defined by $\Delta^X_\cup(\mathcal{A}, \mathcal{B}) = \mathcal{A} \cup \mathcal{B}$. Similarly, the intersection operator $\Delta^X_\cap\colon \mathcal{P}(\mathcal{P}(X))^2 \to \mathcal{P}(\mathcal{P}(X))$ on X is defined by $\Delta^X_\cap(\mathcal{A}, \mathcal{B}) = \mathcal{A} \cap \mathcal{B}$.

(b) *Complementation.* Complementation on X is the unary operator $\Delta^X_c\colon \mathcal{P}(\mathcal{P}(X)) \to \mathcal{P}(\mathcal{P}(X))$ defined by $\Delta^X_c(\mathcal{A}) = \mathcal{P}(X) \setminus \mathcal{A}$.

(c) *Tensor disjunction, conjunction and negation.* The idea of tensor disjunction[1] $\Delta^X_\vee$ and tensor conjunction $\Delta^X_\wedge$ is to take unions and intersections inside the families: $\Delta^X_\vee(\mathcal{A}, \mathcal{B}) = \{A \cup B \mid A \in \mathcal{A}, B \in \mathcal{B}\}$ and $\Delta^X_\wedge(\mathcal{A}, \mathcal{B}) = \{A \cap B \mid A \in \mathcal{A}, B \in \mathcal{B}\}$. Similarly, pushing complementation inside a given family, we obtain tensor negation: $\Delta^X_\neg(\mathcal{A}) = \{X \setminus A \mid A \in \mathcal{A}\}$.

[1] We call this operator tensor *disjunction*, since it gives the team semantics for disjunction.

(d) *Projections.* Let $f\colon X \to Y$ be a surjective function. The (abstract) projection operator corresponding to f is obtained by lifting f to a function $\Delta_f\colon \mathcal{P}(\mathcal{P}(X)) \to \mathcal{P}(\mathcal{P}(Y))$ in the usual way: $\Delta_f(\mathcal{A}) = \{f[A] \mid A \in \mathcal{A}\}$, where $f[A]$ denotes the image $\{f(a) \mid a \in A\}$ of A under f.

(e) *Universal projections.* Given a surjection $f\colon X \to Y$, let $\mathcal{R}_f^U \subseteq \mathcal{P}(X)\times\mathcal{P}(Y)$ be the relation $\{(B, A) \mid B = f[A]$ and $f^{-1}[\{b\}] \subseteq A$ for all $b \in B\}$. The corresponding universal projection Δ_f^U is defined by $\Delta_f^U(\mathcal{A}) = \{B \mid (B, A) \in \mathcal{R}_f^U$ for some $A \in \mathcal{A}\}$.

(f) In the concrete case $X = X_0 \times \cdots \times X_{m-1}$, $Y = X_0 \times \cdots X_{i-1} \times X_{i+1} \times \cdots \times X_{m-1}$, and f is the function $f(a_0, \ldots, a_{m-1}) = (a_0, \ldots, a_{i-1}, a_{i+1}, \ldots, a_{m-1})$ (i.e., f is the projection to coordinates $j \neq i$), we denote the projection Δ_f by $\Delta^X_{\exists i}$ and the universal projection Δ_f^U by $\Delta^X_{\forall i}$.

Note that the union and intersection operators $\Delta^X_\cup$ and $\Delta^X_\cap$ do not depend on the base set X. Thus, in the sequel we will denote these operators simply by $\cup$ and $\cap$. The same holds for tensor disjunction and conjunction, whence we will use the notation $\mathcal{A} \vee \mathcal{B} := \Delta^X_\vee(\mathcal{A}, \mathcal{B})$ and $\mathcal{A} \wedge \mathcal{B} := \Delta^X_\wedge(\mathcal{A}, \mathcal{B})$.

2.3 Families of teams

The general concept of a family of sets arises naturally in numerous contexts. In this paper our focus is on families of sets arising in logic, with applications in logic in mind. These families are families of sets on the base set of the form of a cartesian products M^m. This particular form of the base set permits dimension computations which do not arise in the abstract setting. In particular, we can fix m and ask how does the dimension of a family depend on $|M|$.

In classical logic one associates with a given formula $\phi(x_0, \ldots, x_{m-1})$ with the free variables $x_0, \ldots, x_{m-1}$ and a given structure M the set of m-tuples satisfying the formula ϕ in M:

$$\|\phi\|^M = \{(a_0, \ldots, a_{m-1}) \in M^n : M \models \phi(a_0, \ldots, a_{m-1})\}.$$

Such sets of m-tuples are called definable subsets of M^m. The definable subsets of M^m form a Boolean algebra with Boolean operations corresponding to the logical operations of first order logic. The study of this algebra is a well-known method in logic.

In the same way as classical logic gives rise to definable sets of m-tuples, team semantics and dependence logic [Vää07] give rise to definable families of sets of m-tuples. If M is a model, a *team* in M is a set of assignments s (i.e. functions) which map a set $\mathrm{dom}(s) = \{x_0, \ldots, x_{m-1}\}$ of variables, called the domain of s, to M. Thus a team can be identified with a subset of M^m. Every formula ϕ of dependence logic, or another logic based on team semantics, with free variables in $\vec{x} = (x_0, \ldots, x_{m-1})$ gives rise to the set of teams

$$\|\phi\|^{M,\vec{x}} = \{X \subseteq M^m : M \models_X \phi\}, \tag{1}$$

where $M \models_X \phi$ is the satisfaction relation defined below. We consider the families $\|\phi\|^{M,\vec{x}}$ a special case of families of subsets of M^m.

If ϕ is a formula of first order logic, then $\|\phi\|^{M,\vec{x}}$ is downward closed, dominated and supported by $\emptyset$. If ϕ is a formula of dependence logic, then $\|\phi\|^{M,\vec{x}}$ is downward closed and supported by $\emptyset$ but not necessarily dominated. Many of the results of this paper hold for arbitrary families of sets but when applied to families of the form $\|\phi\|^{M,\vec{x}}$, results about dependence and independence logics obtain.

In order to make (1) more exact we now recall the inductive definition of $M \models_X \phi$ from [Vää07]. If $a \in M$, then $s(a/x)$ is the unique assignment s' such that $s'(x) = a$ and $s'(y) = s(y)$ for variables y in the domain of s other than x. If $F : X \to \mathcal{P}(M) \setminus \{\emptyset\}$, then $X[F/x] = \{s(a/x) : a \in F(s)\}$. Finally, $X[M/x] = \{s(a/x) : a \in M, s \in X\}$.

Definition 2.7. 1. $M \models_X \phi$, where ϕ is atomic or negated atomic if and only if every assignment s in X satisfies ϕ.

2. $M \models_X \phi \wedge \psi$ if and only if $M \models_X \phi$ and $M \models_X \psi$.
3. $M \models_X \phi \vee \psi$ if and only if $X = Y \cup Z$ such that $M \models_Y \phi$ and $M \models_Z \psi$. (Tensor disjunction)
4. $M \models_X \exists x\phi$ if and only if there is $F : X \to \mathcal{P}(M) \setminus \{\emptyset\}$ such that $M \models_{X[F/x]} \phi$.
5. $M \models_X \forall x\phi$ if and only if $M \models_{X[M/x]} \phi$.

This defines $M \models_X \phi$ for every first order ϕ. By Definition 2.7.1, for every first order literal (i.e., atomic or negated atomic) ϕ we have $\|\phi\|^{M,\vec{x}} = \{\vec{a} \in M^m \mid M \models \phi(\vec{a})\}$. Note further that for composite ϕ the family $\|\phi\|^{M,\vec{x}'}$ can be obtained from the corresponding families $\|\psi\|^{M,\vec{x}}$ for the components ψ of ϕ (with appropriate $\vec{x}'$, see below) by applying one of the natural operators introduced in Example 2.6:

$$\begin{array}{lcl} \|\phi \wedge \psi\|^{M,\vec{x}'} & = & \|\phi\|^{M,\vec{x}} \cap \|\psi\|^{M,\vec{x}} \\ \|\phi \vee \psi\|^{M,\vec{x}'} & = & \|\phi\|^{M,\vec{x}} \vee \|\psi\|^{M,\vec{x}} \\ \|\exists x_i\phi\|^{M,\vec{x}'} & = & \Delta^{M^m}_{\exists i}(\|\phi\|^{M,\vec{x}}) \\ \|\forall x_i\phi\|^{M,\vec{x}'} & = & \Delta^{M^m}_{\forall i}(\|\phi\|^{M,\vec{x}}) \end{array}$$

Here $\vec{x}'$ is $\vec{x}$ in the case of conjunction and disjunction, while in the case of quantifiers, $\vec{x}'$ is obtained from $\vec{x}$ by deleting the component x_i.

We now recall the extension of $M \models_X \phi$ from first order ϕ to new non-first order atoms.

Definition 2.8. 1. *Dependence atom*: $M \models_X =(\vec{x}, y)$ if and only if $s(\vec{x}) = s'(\vec{x})$ implies $s(\vec{y}) = s'(\vec{y})$ for all $s, s' \in X$.

2. *Inclusion atom*: $M \models_X \vec{x} \subseteq \vec{y}$ if and only if for every $s \in X$ there is $s' \in X$ such that $s(\vec{x}) = s'(\vec{y})$. (We assume $\mathrm{len}(\vec{x}) = \mathrm{len}(\vec{y})$.)
3. *Exclusion atom*: $M \models_X \vec{x} \mid \vec{y}$ if and only if for every $s, s' \in X$ we have $s(\vec{x}) \neq s'(\vec{y})$. (We assume $\mathrm{len}(\vec{x}) = \mathrm{len}(\vec{y})$.)

4. *Independence atom*: $M \models_X \vec{x} \perp_{\vec{z}} \vec{y}$ if and only if for every $s, s' \in X$ such that $s(\vec{z}) = s'(\vec{z})$ there is $s'' \in X$ such that $s''(\vec{x}) = s(\vec{x})$ and $s''(\vec{y}) = s'(\vec{y})$. The atom $\vec{x} \perp \vec{y}$ is called a *pure* independence atom, while $\vec{x} \perp_{\vec{z}} \vec{y}$ is the *relativized* independence atom.

3 Dimension calculations

3.1 Convex shadows

In this subsection, we develop some auxiliary tools for performing concrete dimension calculations.

Definition 3.1. Let $\mathcal{A}$ be a family of sets and $A \in \mathcal{A}$. The *convex shadow of A in the family $\mathcal{A}$* is the family

$$\partial_A(\mathcal{A}) = \{B \subseteq A \mid [B, A] \subseteq \mathcal{A}\}.$$

Similarly, the *dual convex shadow* of A in $\mathcal{A}$ is

$$\partial^A(\mathcal{A}) = \{B \in \mathcal{A} \mid A \subseteq B,\ [A, B] \subseteq \mathcal{A}\}.$$

A set $A \in \mathcal{A}$ is called *critical* in $\mathcal{A}$ if its convex shadow is maximal in the family $\{\partial_B(\mathcal{A}) \mid B \in \mathcal{A}\}$. We use the notation $\mathrm{Crit}(\mathcal{A}) = \{A \in \mathcal{A} \mid A \text{ critical in } \mathcal{A}\}$. Similarly, we define the notion of *dual criticality*. We denote the family of dually critical sets in $\mathcal{A}$ by $\mathrm{Crit}^{\mathrm{d}}(\mathcal{A})$.

Lemma 3.2. *Let $\mathcal{A}$ be a family of sets and $A \in \mathcal{A}$.*

1. *$\partial_A(\mathcal{A})$ is the largest dominated convex family $\mathcal{C} \subseteq \mathcal{A}$ with $\bigcup \mathcal{C} = A$. Similarly, $\partial^A(\mathcal{A})$ is the largest supported convex family $\mathcal{C} \subseteq \mathcal{A}$ with $\bigcap \mathcal{C} = A$.*
2. *A family $\mathcal{G} \subseteq \mathcal{A}$ dominates $\mathcal{A}$ iff $\bigcup_{G \in \mathcal{G}} \partial_G(\mathcal{A}) = \mathcal{A}$. Dually, $\mathcal{H} \subseteq \mathcal{A}$ supports $\mathcal{A}$ iff $\bigcup_{H \in \mathcal{H}} \partial^H(\mathcal{A}) = \mathcal{A}$.*
3. *If $\mathcal{G}$ dominates $\mathcal{A}$, then $\mathrm{Max}(\mathcal{A}) \subseteq \mathcal{G}$, and if $\mathcal{H}$ supports $\mathcal{A}$, then $\mathrm{Min}(\mathcal{A}) \subseteq \mathcal{H}$.*
4. *If $\mathcal{A}$ is finite, then $\mathcal{A}$ and $\mathrm{Crit}(\mathcal{A})$ satisfy Zorn condition.*
5. *Suppose that $\mathrm{Crit}(\mathcal{A})$ satisfy Zorn condition. Then if $\mathcal{G} \subseteq \mathcal{A}$ dominates $\mathcal{A}$, then there is a family $\mathcal{G}'$ dominating $\mathcal{A}$ such that $\mathcal{G}' \subseteq \mathrm{Crit}(\mathcal{A})$ and $|\mathcal{G}'| \leq |\mathcal{G}|$. The dual result also holds.*

Convex shadows and dual convex shadows are maximal *subfamilies* satisfying the appropriate properties. The similar operations that produce superfamilies instead of subfamilies are called hulls. We shall utilize these latter concepts in later sections.

Definition 3.3. Let $\mathcal{A}$ be a family of sets.

1. The *convex hull* of $\mathcal{A}$ is $\mathcal{H}(\mathcal{A}) = \bigcup_{A, A' \in \mathcal{A}} [A, A']$.
2. The *dominated (convex) hull* of $\mathcal{A}$ is $\mathcal{H}_*(\mathcal{A}) = \bigcup_{A \in \mathcal{A}} [A, \bigcup \mathcal{A}]$.

3. The *supported (convex) hull* is $\mathcal{H}^*(\mathcal{A}) = \bigcup_{A\in\mathcal{A}} [\bigcap \mathcal{A}, A]$.

If the family of sets is finite, we may drop the braces from the notation in the customary manner, writing $\mathcal{H}_*(A_0, \ldots, A_{k-1})$ instead of $\mathcal{H}_*(\{A_0, \ldots, A_{k-1}\})$. Note the special cases $\mathcal{H}_*(A, B) = [A, A\cup B]\cup[B, A\cup B]$ and $\mathcal{H}^*(A, B) = [A\cap B, A]\cup[A\cap B, B]$.

Lemma 3.4. *Let $\mathcal{A}$ be a family of sets. Then*

1. *$\mathcal{H}(\mathcal{A})$ is the least convex family containing $\mathcal{A}$,*
2. *$\mathcal{H}_*(\mathcal{A})$ is the least dominated convex family containing $\mathcal{A}$ and*
3. *$\mathcal{H}^*(\mathcal{A})$ is the least supported convex family containing $\mathcal{A}$.*

3.2 Dimensions of particular families

In this subsection, we list the dimensions of some concrete families of sets that are relevant to team semantics but certainly are familar from other contexts, too.

For non-empty base sets X and Y, here is a list of families that we consider:

$$\begin{aligned}\mathcal{F} &= \{f \subseteq X\times Y \mid f \text{ is a mapping }\},\\ \mathcal{I}_\subseteq &= \{R\subseteq X\times X \mid \mathrm{dom}(R)\subseteq \mathrm{rg}(R)\},\\ \mathcal{I}_\perp &= \{A\times B \mid A\subseteq X,\, B\subseteq Y\} \text{ and}\\ \mathcal{X} &= \{R\subseteq X\times X \mid \mathrm{dom}(R)\cap\mathrm{rg}(R)=\emptyset\}.\end{aligned}$$

Theorem 3.5. *Let X and Y be finite base sets with $\ell = |X| \geq 2$ and $n = |Y| \geq 2$. Then:*

$$\begin{array}{lll}
\mathrm{D}(\mathcal{F}) = n^\ell, & \mathrm{D}^{\mathrm{d}}(\mathcal{F}) = 1, & \mathrm{CD}(\mathcal{F}) = \mathrm{D}(\mathcal{F}),\\
\mathrm{D}(\mathcal{I}_\subseteq) = 2^\ell - \ell, & \mathrm{D}^{\mathrm{d}}(\mathcal{I}_\subseteq) = 1 + \sum_{k=2}^{\ell}\binom{\ell}{k}k^k, & \mathrm{CD}(\mathcal{I}_\subseteq) = \mathrm{D}^{\mathrm{d}}(\mathcal{I}_\subseteq),\\
\mathrm{D}(\mathcal{I}_\perp) = (2^\ell-\ell-1)(2^n-n-1)+\ell+n, & \mathrm{D}^{\mathrm{d}}(\mathcal{I}_\perp) = (2^\ell-\ell-1)(2^n-n-1)+1, & \mathrm{CD}(\mathcal{I}_\perp) = \mathrm{D}(\mathcal{I}_\perp),\\
\mathrm{D}(\mathcal{X}) = 2^\ell - 2, & \mathrm{D}^{\mathrm{d}}(\mathcal{X}) = 1, & \mathrm{CD}(\mathcal{X}) = \mathrm{D}(\mathcal{X}).
\end{array}$$

The proof of Theorem 3.5 is based on a careful analysis of (dual) convex shadows and critical sets (see Definition 3.1) for each of the families.

3.3 Dimensions of definable families

We have defined three dimension concepts for totally arbitrary families of sets on a finite base set. We now apply these concepts to definable families of subsets of a cartesian product M^m. In particular, we are interested in calculating the three dimensions for families of the form $\|\phi\|^{M,\vec{x}}$.

Lemma 3.6. *If ϕ is first order, then* $\mathrm{D}(\|\phi\|^{M,\vec{x}}) = \mathrm{D}^{\mathrm{d}}(\|\phi\|^{M,\vec{x}}) = \mathrm{CD}(\|\phi\|^{M,\vec{x}}) = 1$.

Proof. The claim follows from the fact that if ϕ is first order, then $M \models_X \phi$ if and only if $s \in X$ implies $M \models \phi(s(\vec{x}))$ for all s. Thus for first order ϕ the set $\|\phi\|^{M,\vec{x}}$ is always the power-set of a set. This makes the dimension computations trivial. □

As alluded to in Section 2.3, team semantics permits the extension of first order logic by a number of new atoms (see Definition 2.8) leading to dependence logic, inclusion logic, exclusion logic and independence logic. In order to estimate the dimensions of families definable in these logics we first note the following consequence of Theorem 3.5:

Theorem 3.7. *Suppose* $|M| = n$.

1. *Let* α *be the dependence atom* $=(\vec{x}, y)$, *where* $\mathrm{len}(\vec{x}) = m$, *and let* $\vec{z} = \vec{x}y$. *Then* $\mathrm{D}(\|\alpha\|^{M,\vec{z}}) = \mathrm{CD}(\|\alpha\|^{M,\vec{z}}) = n^{n^m}$ *and* $\mathrm{D}^{\mathrm{d}}(\|\alpha\|^{M,\vec{z}}) = 1$.
2. *Let* α *be the inclusion atom* $\vec{x} \subseteq \vec{y}$, *where* $\mathrm{len}(\vec{x}) = \mathrm{len}(\vec{y}) = m$, *and let* $\vec{z} = \vec{x}\vec{y}$. *Then* $\mathrm{D}(\|\alpha\|^{M,\vec{z}}) = 2^{n^m} - n^m$ *and* $\mathrm{D}^{\mathrm{d}}(\|\alpha\|^{M,\vec{z}}) = \mathrm{CD}(\|\alpha\|^{M,\vec{z}}) = 1 + \sum_{k=2}^{n^m} \binom{n^m}{k} k^k$.
3. *Let* α *be the independence atom* $\vec{x} \perp \vec{y}$, *where* $\mathrm{len}(\vec{x}) = m$ *and* $\mathrm{len}(\vec{y}) = k$, *and let* $\vec{z} = \vec{x}\vec{y}$. *Then* $\mathrm{D}(\|\alpha\|^{M,\vec{z}}) = \mathrm{CD}(\|\alpha\|^{M,\vec{z}}) = (2^{n^m} - n^m - 1)(2^{n^k} - n^k - 1) + n^m + n^k$ *and* $\mathrm{D}^{\mathrm{d}}(\|\alpha\|^{M,\vec{z}}) = (2^{n^m} - n^m - 1)(2^{n^k} - n^k - 1) + 1$.
4. *Let* α *be the exclusion atom* $\vec{x} \mid \vec{y}$, *where* $\mathrm{len}(\vec{x}) = \mathrm{len}(\vec{y}) = m$, *and let* $\vec{z} = \vec{x}\vec{y}$. *Then* $\mathrm{D}(\|\alpha\|^{M,\vec{z}}) = \mathrm{CD}(\|\alpha\|^{M,\vec{z}}) = 2^{n^m} - 2$ *and* $\mathrm{D}^{\mathrm{d}}(\|\alpha\|^{M,\vec{z}}) = 1$.

We may notice that, keeping m and k fixed, the upper and the cylindrical dimension of the dependence atom grows faster than the respective dimensions of the other atoms. Varying m and k we obtain a host of comparisons between dimensions of the atoms. These will become relevant in Section 5 when we combine the atoms with logical operations.

4 Growth classes and operators

4.1 Growth classes

As we apply our dimensional techniques to definability problems on the class of finite structures, we are constantly facing the dilemma that it is usually not sufficient to consider a single structure and families of sets arising from team semantics in that structure, but we rather have to consider the class of all appropriate finite structures. That means that we have to accept the possibility that the size of the base set may change, which calls for a dynamical way to handle matters. To that end, we consider growth classes.

In the definitions that follow, we generalize the arithmetical notation in the pointwise fashion, e.g., for functions $f, g\colon \mathbb{N} \to \mathbb{N}$ we set $f + g$ to be the function $\mathbb{N} \to \mathbb{N}$ such that $(f + g)(n) = f(n) + g(n)$, for $n \in \mathbb{N}$, and $f \leq g$ means that $f(n) \leq g(n)$ holds for every $n \in \mathbb{N}$.

Definition 4.1. A set $\mathbb{O}$ of mappings $f\colon \mathbb{N} \to \mathbb{N}$ is a *growth class* if the following conditions hold for all $f, g\colon \mathbb{N} \to \mathbb{N}$:

1. If $g \in \mathbb{O}$ and $f \leq g$, then $f \in \mathbb{O}$.
2. If $f, g \in \mathbb{O}$, then $f + g \in \mathbb{O}$ and $fg \in \mathbb{O}$.

We are interested in the following particular classes: For $k \in \mathbb{N}$, the class $\mathbb{E}_k$ consist all $f\colon \mathbb{N} \to \mathbb{N}$ such that there exists a polynomial $p\colon \mathbb{N} \to \mathbb{N}$ of degree k and with coefficients in $\mathbb{N}$ such that $f \leq 2^p$. In addition, $\mathbb{F}_k$ is the class of functions $f\colon \mathbb{N} \to \mathbb{N}$ such that there exists a polynomial $p\colon \mathbb{N} \to \mathbb{N}$ of degree k and with coefficients in $\mathbb{N}$ such that for every $n \in \mathbb{N} \setminus \{0, 1\}$ we have that

$$f(n) \leq n^{p(n)}.$$

Note that $\mathbb{E}_0$ is the class of bounded functions and $\mathbb{F}_0$ the class of functions of polynomial growth. The following is immediate:

Proposition 4.2. *Each $\mathbb{E}_k$ and $\mathbb{F}_k$ (for $k \in \mathbb{N}$) is a growth class. Furthermore, we have*

$$\mathbb{E}_0 \subsetneq \mathbb{F}_0 \subsetneq \mathbb{E}_1 \subsetneq \mathbb{F}_1 \subsetneq \cdots \subsetneq \mathbb{E}_k \subsetneq \mathbb{F}_k.$$

Definition 4.3. To each formula ϕ with free variables in $\vec{x}$ allowing a team-semantical interpretation we relate the following *dimension functions*:

$$\begin{aligned}
&\mathrm{Dim}_{\phi,\vec{x}}\colon \mathbb{N} \to \mathrm{Card}, && \mathrm{Dim}_{\phi,\vec{x}}(n) = \sup\left\{\mathrm{D}(\|\phi\|^{M,\vec{x}}) \mid M \text{ is a model}, |M| = n\right\},\\
&\mathrm{Dim}^{\mathrm{d}}{}_{\phi,\vec{x}}\colon \mathbb{N} \to \mathrm{Card}, && \mathrm{Dim}^{\mathrm{d}}{}_{\phi,\vec{x}}(n) = \sup\left\{\mathrm{D}^{\mathrm{d}}(\|\phi\|^{M,\vec{x}}) \mid M \text{ is a model}, |M| = n\right\},\\
&\mathrm{CDim}_{\phi,\vec{x}}\colon \mathbb{N} \to \mathrm{Card}, && \mathrm{CDim}_{\phi,\vec{x}}(n) = \sup\left\{\mathrm{CD}(\|\phi\|^{M,\vec{x}}) \mid M \text{ is a model}, |M| = n\right\}.
\end{aligned}$$

4.2 Kripke-operators

Our goal in this section is to find natural criteria for operators to preserve growth classes. We start by defining a class of operators that is inspired by the Kripke semantics of modal logic. Let $\mathcal{R}$ be an $(n+1)$-ary relation on the powerset $\mathcal{P}(X)$ of some nonempty set X. Then we define a corresponding operator $\Delta_{\mathcal{R}}\colon \mathcal{P}(\mathcal{P}(X))^n \to \mathcal{P}(\mathcal{P}(X))$ by the condition

$$A \in \Delta_{\mathcal{R}}(\mathcal{A}_0, \ldots, \mathcal{A}_{n-1}) \iff \exists A_0 \in \mathcal{A}_0 \ldots \exists A_{n-1} \in \mathcal{A}_{n-1} : (A, A_0, \ldots, A_{n-1}) \in \mathcal{R}.$$

Note that $\Delta_{\mathcal{R}}$ can be seen as the n-ary second-order version of the function mapping the truth set of a formula φ to the truth set of $\Diamond\varphi$ in a Kripke model.

Definition 4.4. Let X be a set. A function $\Delta\colon \mathcal{P}(\mathcal{P}(X))^n \to \mathcal{P}(\mathcal{P}(X))$ is a *(second-order) Kripke-operator*[2], if there is a relation $\mathcal{R} \subseteq \mathcal{P}(X)^{n+1}$ such that $\Delta = \Delta_{\mathcal{R}}$.

In the next example we go through the operators introduced in Example 2.6, and check which of them are Kripke-operators.

[2]This notion is defined by Lück [Lüc20]; he calls functions satisfying the condition just "operators".

Example 4.5. (a) Intersection of families is a Kripke-operator on any base set X: If $\mathcal{A}, \mathcal{B} \subseteq \mathcal{P}(X)$ and $C \in \mathcal{P}(X)$, then $C \in \mathcal{A} \cap \mathcal{B}$ if and only if there exist $A \in \mathcal{A}$ and $B \in \mathcal{B}$ such that $(C, A, B) \in \mathcal{R}_\cap$, where $\mathcal{R}_\cap$ is the relation $\{(D, D, D) \mid D \in \mathcal{P}(X)\}$.

(b) Union of families on X is *not* a Kripke-operator: for any relation $\mathcal{R} \subseteq (\mathcal{P}(X))^3$ and any nonempty family $\mathcal{A} \subseteq \mathcal{P}(X)$ we have $\Delta_\mathcal{R}(\mathcal{A}, \emptyset) = \emptyset \neq \mathcal{A} = \mathcal{A} \cup \emptyset$.

(c) It is also easy to see that complementation Δ_c^X is not a Kripke-operator: $\Delta_\mathcal{R}(\emptyset) = \emptyset$ for any relation $\mathcal{R} \subseteq (\mathcal{P}(X))^2$, but $\Delta_c^X(\emptyset) = \mathcal{P}(X) \neq \emptyset$.

(d) Tensor disjunction on X is a Kripke-operator: clearly $\mathcal{A} \vee \mathcal{B} = \Delta_{\mathcal{R}_\vee}(\mathcal{A}, \mathcal{B})$, where $\mathcal{R}_\vee = \{(A \cup B, A, B) \mid A, B \in \mathcal{P}(X)\}$.

(e) Projections are Kripke-operators. Indeed, if $f\colon X \to Y$ is a surjection, then clearly $\Delta_f = \Delta_{\mathcal{R}_f}$, where $\mathcal{R}_f = \{(f[A], A) \mid A \in \mathcal{P}(X)\}$. Note further that universal projections are actually by their definition Kripke-operators: $\Delta_f^U = \Delta_{\mathcal{R}_f^U}$.

An important property of Kripke-operators is that they preserve unions of families:

Lemma 4.6 (Union Lemma)**.** *Let $\Delta_\mathcal{R}\colon \mathcal{P}(\mathcal{P}(X))^n \to \mathcal{P}(\mathcal{P}(X))$ be a Kripke-operator, and let $\mathcal{A}_i^k \in \mathcal{P}(\mathcal{P}(X))$, $k \in K_i$, be families of sets for some index sets K_i, $i < n$. Then*

$$\Delta_\mathcal{R}(\bigcup_{k \in K_0} \mathcal{A}_0^k, \ldots, \bigcup_{k \in K_{n-1}} \mathcal{A}_{n-1}^k) = \bigcup_{\vec{k} \in K} \Delta_\mathcal{R}(\mathcal{A}_0^{k_0}, \ldots, \mathcal{A}_{n-1}^{k_{n-1}}),$$

where we use the notation $\vec{k} = (k_0, \ldots, k_{n-1})$ and $K = K_0 \times \cdots \times K_{n-1}$.

Proof. Using the notation $\mathcal{A}_i = \bigcup_{k \in K_i} \mathcal{A}_i^k$ for $i < n$ the left hand side of the equation can be written as $\mathcal{A} := \Delta_\mathcal{R}(\mathcal{A}_0, \ldots, \mathcal{A}_{n-1})$. The claim follows now from the chain of equivalences below:

$$\begin{aligned}
A \in \mathcal{A} &\iff \forall i < n\, \exists A_i \in \mathcal{A}_i : (A, A_0, \ldots, A_{n-1}) \in \mathcal{R} \\
&\iff \forall i < n\, \exists k_i \in K_i\, \exists A_i \in \mathcal{A}_i^{k_i} : (A, A_0, \ldots, A_{n-1}) \in \mathcal{R} \\
&\iff \exists \vec{k} \in K : A \in \Delta_\mathcal{R}(\mathcal{A}_0^{k_0}, \ldots, \mathcal{A}_{n-1}^{k_{n-1}}) \\
&\iff A \in \textstyle\bigcup_{\vec{k} \in K} \Delta_\mathcal{R}(\mathcal{A}_0^{k_0}, \ldots, \mathcal{A}_{n-1}^{k_{n-1}}).
\end{aligned}$$

□

Kripke-operators that preserve the property of being dominated (and/or supported) and convex have a crucial role in our considerations. This is because for such an operator $\Delta_\mathcal{R}$ the (corresponding) dimension of the image $\Delta_\mathcal{R}(\mathcal{A}_0, \ldots, \mathcal{A}_{n-1})$ is at most the product of the dimensions of $\mathcal{A}_i$, $i < n$, and consequently, $\Delta_\mathcal{R}$ preserves growth classes.

Definition 4.7. Let $\Delta\colon \mathcal{P}(\mathcal{P}(X))^n \to \mathcal{P}(\mathcal{P}(X))$ be an operator. We say that Δ *weakly preserves dominated (supported, resp.) convexity* if $\Delta(\mathcal{A}_0, \ldots, \mathcal{A}_{n-1})$ is dominated (supported, resp.) and convex or $\Delta(\mathcal{A}_0, \ldots, \mathcal{A}_{n-1}) = \emptyset$ whenever $\mathcal{A}_i$ is dominated and convex for each $i < n$.

Theorem 4.8. *Let $\Delta_{\mathcal{R}}\colon \mathcal{P}(\mathcal{P}(X))^n \to \mathcal{P}(\mathcal{P}(X))$ be a Kripke-operator, and let $\mathcal{A} = \Delta(\mathcal{A}_0, \ldots, \mathcal{A}_{n-1})$.*

1. *If Δ weakly preserves dominated convexity then $\mathrm{D}(\mathcal{A}) \leq \mathrm{D}(\mathcal{A}_0) \cdot \ldots \cdot \mathrm{D}(\mathcal{A}_{n-1})$.*
2. *If Δ weakly preserves supported convexity then $\mathrm{D}^{\mathrm{d}}(\mathcal{A}) \leq \mathrm{D}^{\mathrm{d}}(\mathcal{A}_0) \cdot \ldots \cdot \mathrm{D}^{\mathrm{d}}(\mathcal{A}_{n-1})$.*
3. *If Δ weakly preserves both dominated and supported convexity then $\mathrm{CD}(\mathcal{A}) \leq \mathrm{CD}(\mathcal{A}_0) \cdot \ldots \cdot \mathrm{CD}(\mathcal{A}_{n-1})$.*

Proof. (a) By Definition 2.5, for each $i < n$ there are dominated and convex subfamilies $\mathcal{A}_i^k \subseteq \mathcal{A}_i$, $k \in K_i$, such that $\mathcal{A}_i = \bigcup_{k \in K_i} \mathcal{A}_i^k$ and $|K_i| = \mathrm{D}(\mathcal{A}_i)$. For each tuple $\vec{k} := (k_0, \ldots, k_{n-1})$ in $K := K_0 \times \cdots \times K_{n-1}$, let $\mathcal{A}_{\vec{k}}$ denote the family $\Delta(\mathcal{A}_0^{k_0}, \ldots, \mathcal{A}_{n-1}^{k_{n-1}})$. By our assumption, each $\mathcal{A}_{\vec{k}}$ is either dominated and convex, or empty. By Lemma 4.6, $\mathcal{A} = \bigcup_{\vec{k} \in K} \mathcal{A}_{\vec{k}}$. Thus we see that $\mathrm{D}(\mathcal{A}) \leq |K| = |K_0| \cdot \ldots \cdot |K_{n-1}| = \mathrm{D}(\mathcal{A}_0) \cdot \ldots \cdot \mathrm{D}(\mathcal{A}_{n-1})$.

Claim (b) is proved in the same way just by replacing dominated convexity by supported convexity. Finally, to prove (c) it suffices to observe that a non-empty family is an interval if and only if it is dominated, supported and convex. □

As seen in Example 4.5, there are well-behaved operators that are not Kripke-operators, but on the other hand, most of the operators arising in our applications are Kripke-operators. Moreover, we can prove relatively simple exact characterizations for weak preservation of dominated convexity and supported convexity for Kripke-operators. We will state these characterizations in the full paper.

4.3 Local Kripke-operators

Below we will use the notation

$$\mathcal{R}[A] := \{(A_0, \ldots, A_{n-1}) \mid (A, A_0, \ldots, A_{n-1}) \in \mathcal{R}\}.$$

Many natural Kripke-operators $\Delta_{\mathcal{R}}$ are local in the sense that the relation $\mathcal{R}[A]$ is completely determined by its behaviour on singletons $\{a\} \subseteq A$.

Definition 4.9. A Kripke-operator $\Delta_{\mathcal{R}}\colon \mathcal{P}(\mathcal{P}(X))^n \to \mathcal{P}(\mathcal{P}(X))$ is *local*[3] if, for any $A \in \mathcal{P}(X)$, $\mathcal{R}[A]$ is determined by the relations $\mathcal{R}[\{a\}]$, $a \in A$, as follows:

$$(A_0, \ldots, A_{n-1}) \in \mathcal{R}[A] \iff \text{for each } a \in A \text{ there is } (A_0^a, \ldots, A_{n-1}^a) \in \mathcal{R}[\{a\}] \text{ such that } A_i = \bigcup_{a \in A} A_i^a \text{ for } i < n.$$

Lück [Lüc20] proved that all local Kripke-operators Δ preserve flatness: if $\mathcal{A}_i$, $i < n$, are flat (i.e., dominated and downward closed), then $\Delta(\mathcal{A}_0, \ldots, \mathcal{A}_{n-1})$ is also flat. We generalize this result to dominated convexity.

Theorem 4.10. *If $\Delta_{\mathcal{R}}\colon \mathcal{P}(\mathcal{P}(X))^n \to \mathcal{P}(\mathcal{P}(X))$ is a local Kripke-operator for a finite X, then it weakly preserves dominated convexity.*

[3] Lück [Lüc20] defined this notion under the name "transversal".

On the other hand, it is not the case that all local Kripke-operators weakly preserve supported convexity. This is seen in the next example.

Example 4.11. Let $X = \{a, b\}$, and let $\mathcal{R}$ be the relation $\{(Y, X) \mid Y \neq \emptyset\} \subseteq \mathcal{P}(X)^2$. Then $\Delta_{\mathcal{R}}$ is local, but it does not weakly preserve supported convexity, since $\mathcal{H}^*(X) = \{X\}$ is convex and supported, but its image $\Delta_{\mathcal{R}}(\{X\}) = \{\{a\}, \{b\}, X\}$ is not supported.

To avoid the problem exhibited in the example above, we consider the following additional requirement for (local) Kripke-operators:

Definition 4.12. A Kripke-operator $\Delta_{\mathcal{R}} \colon \mathcal{P}(\mathcal{P}(X))^n \to \mathcal{P}(\mathcal{P}(X))$ is *separating* if $A_i \cap B_i = \emptyset$ for $i < n$ whenever $(A_0, \ldots, A_{n-1}) \in \mathcal{R}[\{a\}]$, $(B_0, \ldots, B_{n-1}) \in \mathcal{R}[\{b\}]$ and $a \neq b$.

Theorem 4.13. *If $\Delta_{\mathcal{R}} \colon \mathcal{P}(\mathcal{P}(X))^n \to \mathcal{P}(\mathcal{P}(X))$ is a local and separating Kripke-operator for a finite X, then it weakly preserves supported convexity.*

5 Applications

We can now apply our results to obtain hierarchy results for extensions of first order logic by various team-based atoms. We start by observing that the operators corresponding to the usual first-order connectives (except negation) and quantifiers are local and separating.

Lemma 5.1. *Let M be a model. The Kripke-operators $\cap$, $\vee$, $\Delta_{\exists i}^{M^m}$, and $\Delta_{\forall i}^{M^m}$ on M^m are local and separating.*

As a corollary, we get the following preservation result for the growth classes of the dimension functions of formulas.

Corollary 5.2. *Let $\mathcal{L}$ be an extension of first-order logic by a set A of atoms. Assume that* $\mathrm{dim} \in \{\mathrm{Dim}, \mathrm{Dim}^{\mathrm{d}}, \mathrm{CDim}\}$ *and* $\mathbb{C} \in \{\mathbb{E}_k, \mathbb{F}_k \mid k \in \mathbb{N}\}$. *If* $\mathrm{dim}_{\alpha,\vec{x}} \in \mathbb{C}$ *for every atom $\alpha \in A$ and every $\vec{x}$ containing the free variables of α, then* $\mathrm{dim}_{\phi,\vec{y}} \in \mathbb{C}$ *for every $\mathcal{L}$-formula ϕ and every $\vec{y}$ containing the free variables of ϕ.*

In order to apply this corollary for concrete logics $\mathcal{L}$, we need to consider the length of variable-tuples allowed in the atoms. Let us therefore specify the concept of arity for our atoms:

Definition 5.3. We say the dependence atom $=(\vec{x}, y)$ is k-ary, if $\mathrm{len}(\vec{x}) = k$, the inclusion atom $\vec{x} \subseteq \vec{y}$ is k-ary if $\mathrm{len}(\vec{x}) = \mathrm{len}(\vec{y}) = k$, the independence atom $\vec{x} \perp \vec{y}$ is k-ary if $\max\{\mathrm{len}(\vec{x}), \mathrm{len}(\vec{y})\} = k$, and the exclusion atom $\vec{x} \mid \vec{y}$ is k-ary if $\mathrm{len}(\vec{x}) = \mathrm{len}(\vec{y}) = k$.

Using Theorem 3.7 we can now determine the growth classes of the dimension functions for each of the k-ary atoms. However, there is a subtle detail that we have not mentioned earlier: the dual upper dimension $\mathrm{D}^{\mathrm{d}}(\|\phi\|^{M,\vec{x}})$ may increase if we add (dummy) variables in the tuple $\vec{x}$. Fortunately, we can prove that this increase can only lift the dimension function $\mathrm{Dim}^{\mathrm{d}}{}_{\phi,\vec{x}}$ from the growth class $\mathbb{E}_k$ to $\mathbb{F}_k$, and $\mathbb{F}_k$ is closed with respect to the increase. Moreover, the upper dimension $\mathrm{D}(\|\phi\|^{M,\vec{x}})$ is independent of the tuple $\vec{x}$.

Theorem 5.4. *Let $\mathcal{L}$ be an extension of first-order logic by a set A of dependence, inclusion, independence and exclusion atoms.*

1. *If all atoms in A are at most k-ary, then $\mathrm{Dim}_{\phi,\vec{x}}, \mathrm{Dim}^{\mathrm{d}}{}_{\phi,\vec{x}}, \mathrm{CDim}_{\phi,\vec{x}} \in \mathbb{F}_k$ for every $\mathcal{L}$-formula ϕ and every $\vec{x}$.*
2. *If all dependence atoms in A are less than k-ary, and other atoms are at most k-ary, then $\mathrm{Dim}_{\phi,\vec{x}} \in \mathbb{E}_k$ for every $\mathcal{L}$-formula ϕ and every $\vec{x}$.*
3. *If all inclusion and independence atoms in A are at most k-ary, then $\mathrm{Dim}^{\mathrm{d}}{}_{\phi,\vec{x}} \in \mathbb{F}_k$ for every $\mathcal{L}$-formula ϕ and every $\vec{x}$.*

Using the first clause of Theorem 5.4, we can now prove the promised arity hierarchy result for our atoms:

Theorem 5.5. *1. Each k-ary dependence atom $=(\vec{x}, y)$ is not definable in the extension of first-order logic by less than k-ary dependence atoms and at most k-ary inclusion, independence and exclusion atoms.*

2. *Each k-ary inclusion atom $\vec{x} \subseteq \vec{y}$ is not definable in the extension of first-order logic by less than k-ary dependence, inclusion, independence and exclusion atoms.*
3. *Each k-ary independence atom $\vec{x} \perp \vec{y}$ is not definable in the extension of first-order logic by less than k-ary dependence, inclusion, independence and exclusion atoms.*
4. *Each k-ary exclusion atom $\vec{x} \mid \vec{y}$ is not definable in the extension of first-order logic by less than k-ary dependence, inclusion, independence and exclusion atoms.*

Proof. To prove the first claim, observe that by Theorem 3.7, $\mathrm{Dim}_{=(\vec{x},y),\vec{x}y}(n) = n^{n^k}$, whence $\mathrm{Dim}_{=(\vec{x},y),\vec{x}y} \notin \mathbb{E}_k$. On the other hand, by the first clause of Theorem 5.4 we have $\mathrm{Dim}_{\phi,\vec{x}y} \in \mathbb{E}_k$ for any formula ϕ in the extension of first-order logic by the atoms stipulated in the claim. Thus, no such formula ϕ can define the atom $=(\vec{x}, y)$.

The rest of the claims are proved in the same way. □

Earlier hierarchy results have been for sentences. [HS15] Kontinen-Durand [DK12] show that $k-1$-ary dependence atom is weaker than k-ary dependence atom for sentences in vocabulary having arity k. Miika Hannula [Han18] showed (using similar results of Grohe on transitive closure and fixpoint operator) that inclusion logic with $k-1$-ary inclusion atoms is strictly weaker than inclusion logic with k-ary inclusion atoms for sentences when $k \geq 2$. Galliani-Hannula-Kontinen [GHK13] showed that independence logic with $k-1$-ary independence atoms is strictly weaker than independence logic with k-ary independence atoms on the level of sentences.

References

[Cia09] Ivano Ciardelli. Inquisitive semantics and intermediate logics. Master's thesis, University of Amsterdam, 2009.

[DK12] Arnaud Durand and Juha Kontinen. Hierarchies in dependence logic. *ACM Trans. Comput. Log.*, 13(4):Art. 31, 21, 2012.

[GHK13] Pietro Galliani, Miika Hannula, and Juha Kontinen. Hierarchies in independence logic. In Simona Ronchi Della Rocca, editor, *Computer Science Logic 2013 (CSL 2013), CSL 2013, September 2-5, 2013, Torino, Italy*, volume 23 of *LIPIcs*, pages 263–280. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2013.

[Han18] Miika Hannula. Hierarchies in inclusion logic with lax semantics. *ACM Trans. Comput. Log.*, 19(3):16:1–16:23, 2018.

[HLSV14] Lauri Hella, Kerkko Luosto, Katsuhiko Sano, and Jonni Virtema. The expressive power of modal dependence logic. In *Advances in modal logic. Vol. 10*, pages 294–312. Coll. Publ., London, 2014.

[HS15] Lauri Hella and Johanna Stumpf. The expressive power of modal logic with inclusion atoms. In *Proceedings Sixth International Symposium on Games, Automata, Logics and Formal Verification*, volume 193 of *Electron. Proc. Theor. Comput. Sci. (EPTCS)*, pages 129–143. EPTCS, [place of publication not identified], 2015.

[Lüc20] Martin Lück. *Team logic: axioms, expressiveness, complexity.* PhD thesis, University of Hanover, Hannover, Germany, 2020.

[LV19] Martin Lück and Miikka Vilander. On the succinctness of atoms of dependency. *Log. Methods Comput. Sci.*, 15(3):Paper No. 17, 28, 2019.

[Vää07] Jouko Väänänen. *Dependence logic*, volume 70 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 2007. A new approach to independence friendly logic.

Singmaster's conjecture in the interior of Pascal's triangle

Kaisa Matomäki*

Department of Mathematics and Statistics
University of Turku, Finland

Abstract

In 1971, David Singmaster conjectured that any natural number greater than one only appears in Pascal's triangle a bounded number of times. In the talk I will discuss what is known about this conjecture, concentrating on a recent result in joint work with Maksym Radziwill, Xuancheng Shao, Terence Tao, and Joni Teräväinen that establishes the conjecture in the interior region of the triangle.

While the problem is combinatorial, we use number theoretic and analytic tools. In particular an important analytic input in our proof is Vinogradov's estimate for exponential sums over primes.

*The author was supported by the Academy of Finland grant no. 285894.

Sparsity and treelikeness of high dimensional $(0,1)$ arrays

Yaokun Wu

Shanghai Jiao Tong University

Abstract

We propose new methods to measure the sparsity and treelikeness of $(0,1)$ arrays. Since $(0,1)$ arrays can be identified with clutters, partition systems, simplicial complexes, and so on, these measures lead to new viewpoints about those widely-studied structures. We will report some of our results and conjectures in this line of research.

This talk is based on the following three papers joint with Qian and Xiong:

1. Yaokun Wu, Yanzhen Xiong, Sparse $(0,1)$ arrays and tree-like partition systems, https://math.sjtu.edu.cn/faculty/ykwu/data/Paper/sparsity1001.pdf
2. Chengyang Qian, Yaokun Wu, Yanzhen Xiong, Collapsibility of oriented matroids, https://math.sjtu.edu.cn/faculty/ykwu/data/Paper/Hyperplane_arrangement.pdf
3. Chengyang Qian, Yaokun Wu, Yanzhen Xiong, Collapsibility and sparsity of d-partite clut ters, In preparation.

On general position problems in graphs

Ismael G. Yero

Universidad de Cádiz, Departamento de Matemáticas, Algeciras, Spain
ismael.gonzalez@uca.es

Given a connected graph G, a *general position set* of G is a set of vertices $S \subseteq V(G)$ for which there are no three vertices lying on a common shortest path (geodesic) of G. The cardinality of a largest general position set, shortly called a *gp-set*, is the *general position number* $\mathrm{gp}(G)$ of G. This concept was recently and independently introduced in [2, 3]. Further on, a series of several other investigations on the topics has been developed. Among such works, there has been made a generalization which is presented as follows.

Let $d \in \mathbb{N}$. Then $S \subseteq V(G)$ is a *general d-position set* if the following holds:

$$\{u, v, w\} \in \binom{S}{3}, v \in I_G(u, w) \Rightarrow d_G(u, w) > d\,, \tag{1}$$

where $d_G(u, w)$ denotes the shortest-path distance in G between u and w, and $I_G(u, w) = \{x \in V(G) : \ d_G(u, w) = d_G(u, x) + d_G(x, w)\}$ is the *interval* between u and w. That is, the set S is a general d-position set if no three different vertices from S lie on a common geodesic of length at most d. It is said that vertices u, v, w that fulfill condition (1) lie in *general d-position*. The cardinality of a largest general d-position set of G is the *general d-position number* of G and is denoted by $\mathrm{gp}_d(G)$. The concept above were introduced in [1].

In this talk, there will be given several contributions concerning the general position and the general d-position numbers of graphs. Specifically, the following points shall be addressed.

- The general position number of some Cartesian product graphs.
- Monotonic behavior of $\mathrm{gp}_d(G)$ with respect to the suitable values of d.
- The NP-completeness of the decision problem concerning finding $\mathrm{gp}_d(G)$ for any value of d.
- Some other structural characterization of general d-position and some relationships with other topics including strong resolving graphs and dissociation sets.

References

[1] S. Klavžar, D. F. Rall, I. G. Yero, General d-position sets, *Ars Mathematica Contemporanea* 21 (2021), article # P1.03.

[2] P. Manuel, S. Klavžar, A general position problem in graph theory, *Bulletin of the Australian Mathematical Society* **98** (2018), 177–187.

[3] S. V. Ullas Chandran, G. Jaya Parthasarathy, The geodesic irredundant sets in graphs, *International Journal of Mathematical Combinatorics* **4** (2016), 135–143.

Part II
Contributed talks

On tree sizes in a random forest

Irina Cheplyukova and Yuri Pavlov

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

We consider a Galton-Watson branching process G starting with N particles, where the number of offspring of any particle ξ has the distribution

$$p_k = \mathbf{P}\{\xi = k\} = \frac{h(k+1)}{(k+1)^\tau}, \quad k = 0, 1, 2, \ldots, \quad \tau \in (2, 3), \tag{1}$$

where $h(x) > 0$ is a slowly varying function. Branching processes of this type are successfully used in the study of the structure and dynamics of random graphs intended for modeling complex communication networks, such as the Internet [1]. We take a subset of the realizations of G such that the number of particles that existed in the process before its extinction is equal to $N + n$. The set $\mathcal{F}_{N,n}$ of all realisations of the Galton-Watson process G conditioned to have n offspring with the probability measure induced by this process in a natural way is called a Galton-Watson forest with N trees and n non-root vertices. Let us assume that the process G is critical, i. e. $\mathbf{E}\xi = 1$. The most comprehensive reviews of such random forests are given in [2, 3, 4]. However, the known results on Galton-Watson forests were obtained under the condition that the offspring distribution of the branching process has a finite second moment. It is easy to see that the distribution (1) has an infinite variance. It is therefore interesting to study the properties of such random forests.

Any forest in $\mathcal{F}_{N,n}$ consists of N root trees, the roots of which correspond to the initial particles of the process G. The size of a tree is the number of its vertices including the root. We denote by μ_r the number of trees of size r in a forest from $\mathcal{F}_{N,n}$. The limit distributions of these random variables for different relations between the parameters N and n tending to infinity are obtained. Let $\xi(\lambda)$ denote an auxiliary random variable with the distribution

$$p_k(\lambda) = \mathbf{P}\{\xi(\lambda) = k\} = \frac{\lambda^k p_k}{F(\lambda)}, \quad k = 0, 1, 2, \ldots, \tag{2}$$

where $0 < \lambda < 1$, and

$$F(\lambda) = \sum_{k=0}^{\infty} p_k \lambda^k.$$

Let ν denote a random variable equal to the number of particles that existed in a branching process starting with one particle when the number of offspring of any particle had the distribution (2). Let also $q_k = q_k(\lambda) = \mathbf{P}\{\nu = k\}, \quad k = 1, 2, \ldots,$

$$\sigma_{rr}^2 = q_r \left(1 - q_r - \frac{(a-r)^2}{b^2} q_r\right),$$

where $a = a(\lambda) = \mathbf{E}\nu, \quad b^2 = b^2(\lambda) = \mathbf{D}\nu$. A random variable μ_r equal to the number of trees of a given size is the most important characteristic of the Galton-Watson forest structure. The following is true.

Theorem. *Let $N, n \to \infty, r$ be a fixed natural number, $\lambda = \lambda(N, n)$ be determined by the relation*

$$\frac{\lambda F'(\lambda)}{F(\lambda)} = \frac{n}{N+n}$$

and one of the following conditions be satisfied:

1. $n/N \to 0, \qquad N\,(n/N)^{r-1} \to \infty, \qquad r > 2;$
2. $0 < C_1 \leqslant n/N \leqslant C_2 < \infty;$
3. $n/N \to \infty$ and there are positive constants Δ, ω, where $\omega < 1/2$, such that

$$\left(\frac{n}{N}\right)^2 = O\left(N^{\omega}(1-\lambda)^{1+\Delta}\right). \tag{3}$$

Then,

$$\mathbf{P}\{\mu_r = k\} = \frac{1 + o(1)}{\sigma_{rr}\sqrt{2\pi N}} e^{-u_r^2/2}.$$

for a positive integer k uniformly with respect to $u_r = (k - Nq_r) \,/\, \left(\sigma_{rr}\sqrt{N}\right)$ lying in any fixed finite interval. In addition, the statement of the theorem remains true with $r \to \infty$, if condition 1 is supplemented with the requirement $Nq_r \to \infty$, r in condition 2 equals $o(\ln N)$, and the relation $r = O\,(n/N)$ is added to condition 3.

References

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

[2] Kolchin V.F. *Random mappings.* Transaction series in mathematics and engineering. Optimization software Inc. Publication division. New York, 1986.

[3] Kolchin V.F. *Random graphs.* 2nd. ed. Cambridge: Cambridge Univ.Press, 2010.

[4] Pavlov Yu.L. *Random forests.* Utrecht: VSP, 2000.

The notes about the symmetric 4-adic complexity of quaternary sequences obtained from two Legendre sequences

Vladimir Edemskiy

Yaroslav-the-Wise Novgorod State University
Veliky Novgorod, 173003, Russia
vladimir.edemsky@novsu.ru

1 Introduction

Pseudorandom sequences with low autocorrelation, high linear complexity and m-adic complexity, are widely used in many areas of communication and cryptography. Since the quadrature modulations are preferred in the digital communication systems, binary and quaternary sequences have drawn more interests. A sequence is said to have optimal autocorrelation if the maximal out-of-phase autocorrelation magnitude is as small as possible. For quaternary sequences with period N, $N \equiv 2 \pmod 4$ the least value modulo of the out-of-phase autocorrelation is equal to 2 [10]. There is a well-known method for constructing quaternary sequences from two binary sequences using inverse Gray mapping. In particular, balanced quaternary sequences with even period and optimal autocorrelation property obtained from two ideal sequences were presented in [10]. Further, Kim et al. proposed new quaternary sequences with optimal autocorrelation constructed from Legendre sequences [5].

The notations of the shortest feedback with carry shift registers and 2-adic complexity binary sequences were proposed in [6, 7]. Many papers have been devoted to the study of the 2 -adic complexity of binary sequences [9, 12, 13] (see also the references here). Further, the results form [6, 7] were generalized for m-ary sequences in [11, 3], where $m > 2$ is integer. m -adic complexity of a sequence over the ring of integers modulo m is defined as the length of the shortest feedback with carry shift registers which is able to construct this sequence. For m-adic complexity of sequence $w(t) = (w_0, w_1, \ldots, w_{T-1})$ over $\mathbb{Z}_m$ with period T (denoted by $\Phi_m(w(t))$) we have

$$\Phi_m(w(t)) = \left\lfloor \log_m \left(\frac{m^T - 1}{\gcd(S_w(m), m^N - 1)} + 1 \right) \right\rfloor, \tag{1}$$

where $S_w(x) = \sum_{i=0}^{T-1} w_i x^i \in \mathbb{Z}[x]$ and $\lfloor h \rfloor$ is the greatest integer that is less than or equal to h.

Due to the rational approximation algorithm, m-adic complexity has become one of the most important cryptographic measures [6, 11]. Thus, it is interesting to study the m -adic

complexity of known sequences and to find families of sequences with high m -adic complexity. Comparing with the binary sequences, the m-adic complexity of quaternary sequences with small autocorrelation has not been fully researched. The 4-adic complexity of quaternary sequences with period $2p$ is considered in [8] and the generalized cyclotomic quaternary sequences with period equal to the product of two different primes is studied in [1]. Very recently, the 4-adic complexity of quaternary sequences presented in [10, 5] was studied in [14, 15].

A symmetric 2-adic complexity $\bar{\Phi}(w(t)) = \min(\Phi(w(t)), \Phi(\tilde{w}(t)))$ as a new measure for binary sequences was proposed in [4], here $\tilde{w}(t) = (w_{T-1}, w_{T-2}, \ldots, w_0)$ is the reciprocal sequence of $w(t)$. According to [4], the symmetric 2-adic complexity is better than 2-adic complexity when measuring the security of a binary periodic sequence. Therefore, it is also interesting to consider the symmetric 4-adic complexity of quaternary sequences. In this paper, we study the symmetric 4-adic complexity of quaternary sequences with optimal autocorrelation from [5]. In conclusion, we made a comment about the estimation of k-error 4-adic complexity.

2 Definitions of sequences

In this section, we recall the definition of sequences from [5].

Let p be an odd prime. Denote by $\mathbf{QR}_p$ and $\mathbf{NQR}_p$ the sets of quadratic residues and quadratic nonresidues modulo p, respectively. Let $b_0(t), b_1(t)$ be Legendre sequences of period p defined as

$$b_0(t) = \begin{cases} 0, & \text{if } t \pmod p = 0, \\ 0, & \text{if } t \pmod p \in \mathbf{QR}_p, \\ 1, & \text{if } t \pmod p \in \mathbf{NQR}_p. \end{cases}$$

and

$$b_1(t) = \begin{cases} 1, & \text{if } t \pmod p = 0, \\ 0, & \text{if } t \pmod p \in \mathbf{QR}_p, \\ 1, & \text{if } t \pmod p \in \mathbf{NQR}_p. \end{cases}$$

It is well known that these sequences have an ideal autocorrelation when $p \equiv 3 \pmod 4$ (its out-of-phase autocorrelation coefficients equals -1) and optimal autocorrelation when $p \equiv 1 \pmod 4$ (its out-of-phase autocorrelation coefficients belong to the set $\{-3, 1\}$).

Also we define two binary sequences with period $2p$ as

$$s_0(t) = \begin{cases} b_0(t), & \text{if } t \equiv 0 (\bmod 2), \\ b_1(t), & \text{if } t \equiv 1 (\bmod 2). \end{cases} \tag{2}$$

and

$$s_1(t) = \begin{cases} b_0(t), & \text{if } t \equiv 0 (\bmod 2), \\ b_1(t) \oplus 1, & \text{if } t \equiv 1 (\bmod 2). \end{cases}, \tag{3}$$

where $\oplus$ denotes the addition over Z_2.

The well-known Gray mapping $\phi : \mathbb{Z}_4 \to \mathbb{Z}_2 \times \mathbb{Z}_2$ is defined as

$$\phi(0) = (0,0),\ \phi(1) = (0,1),\ \phi(2) = (1,1),\ \phi(3) = (1,0).$$

Thus, we can obtain a quaternary sequence from two binary sequences using the inverse Gray mapping.

Let $q_1(t)$ be the quaternary sequence of period $2p$ defined by

$$q_1(t) = \phi^{-1}(s_0(t), s_1(t)). \tag{4}$$

According to [5] balanced quaternary sequence $q_1(t)$ have optimal autocorrelation value for $p \equiv 1 \pmod 4$ (its out-of-phase autocorrelation coefficients belong to the set $\{-2, 0\}$).

Also we define two other binary sequences with period $2p$ as

$$s_2(t) = \begin{cases} b_0(t), & \text{if } t \equiv 0 (\bmod 2), \\ b_0(t), & \text{if } t \equiv 1 (\bmod 2). \end{cases} \tag{5}$$

and

$$s_3(t) = \begin{cases} b_1(t), & \text{if } t \equiv 0 (\bmod 2), \\ b_1(t) \oplus 1, & \text{if } t \equiv 1 (\bmod 2). \end{cases} \tag{6}$$

Let $q_2(t)$ be the quaternary sequence of period $2p$ defined by

$$q_2(t) = \phi^{-1}(s_2(t), s_3(t)). \tag{7}$$

According to [5] balanced quaternary sequence $q_2(t)$ also have optimal autocorrelation value for $p \equiv 3 \pmod 4$.

3 The symmetric 4-adic complexity of sequences

In this section we present our main results.

Theorem 1. *Let $s_0(t)$ and $s_1(t)$ be binary sequences defined by* (2) *and* (3) *for Legendre sequences $b_0(t)$ and $b_1(t)$. Let the quaternary sequence $q_1(t)$ with period $2p$, $p \equiv 1 \pmod 4$ be defined in* (4)*. Then for the symmetric 4-adic complexity of $q_1(t)$ we have*

$$\bar{\Phi}_4(q_1(t)) = \begin{cases} 2p-2, & \text{if } p \equiv 13 (\bmod 20), \\ 2p-1, & \text{if } p \not\equiv 13 (\bmod 20). \end{cases}$$

Proof. Let $S_0(X) = \sum_{i \in \mathbf{QR}_p} X^i$, $S_1(X) = \sum_{i \in \mathbf{NQR}_p} X^i$ and $S_{q_1}(X) = \sum_{t=0}^{2p-1} q_1(t) X^t$. Here, $S_1(X)$ is the generating polynomial of sequence $b_0(t)$. Using the definitions of considered sequences we get

$$S_{q_1}(X) = 2(1+X^p)S_1(X) + 2X^p + X(X^{2p}-1)/(X^2-1). \tag{8}$$

Then

$$S_{q_1}(4) = 2(1+4^p)S_1(4) + 2 \cdot 4^p + 4(4^{2p}-1)/15$$

and we see that $4\tilde{S}_{q_1}(4) \equiv S_{q_1}(4) \pmod{4^{2p}-1}$, where $\tilde{S}_{q_1}(4)$ is the generating polynomial of the reciprocal sequence of $q_1(t)$. The properties of $S_0(4)$ and $S_1(4)$ were studied in [2]. Using its, we can find $\gcd\left(S_{q_1}(4), 4^{2p}-1\right)$ and complete the proof of this theorem using (1). □

According to Theorem 1 the sequence $q_1(t)$ have high symmetric 4-adic complexity.

Now we consider second family of quaternary sequences $q_2(t)$ proposed in [5].

Theorem 2. *Let $s_2(t)$ and $s_3(t)$ be binary sequences defined by* (5) *and* (6) *for Legendre sequences $b_0(t)$ and $b_1(t)$. Let the quaternary sequence $q_2(t)$ with period $2p$, $p \equiv 3 \pmod 4$ be defined in* (7)*. Then for the symmetric 4-adic complexity of $q_2(t)$ we have*

$$\bar{\Phi}_4(q_2(t)) = \begin{cases} 2p-2, & \text{if } p \equiv 7 (\bmod 20), \\ 2p, & \text{if } p \not\equiv 7 (\bmod 20). \end{cases}$$

Proof. In this case,

$$S_{q_2}(X) = 2(1+X^p)S_1(X) + 1 - X^p + X(X^{2p}-1)/(X^2-1) \tag{9}$$

and

$$\tilde{S}_{q_2}(X) = 2(1+X^p)S_0(X) + 1 - X^p + X(X^{2p}-1)/(X^2-1). \tag{10}$$

Thus, we get

$$S_{q_2}(4) = 2(1+4^p)S_1(4) + 1 - 4^p + 4(4^{2p}-1)/15$$

and

$$4\tilde{S}_{q_2}(4) \equiv 2(1+4^p)S_0(4) + 1 - 4^p + 4(4^{2p}-1)/15 \pmod{4^{2p}-1}.$$

We can prove Theorem 2 in the same way as Theorem 1. □

The statements of Theorems 1 and 2 are consistent with the results from [15].

Let $w(t) = (w_0, w_1, \ldots, w_{T-1})$ be a sequence over $\mathbb{Z}_m$ with period T. For integers $k \geq 0$, the k-error m-adic complexity over $\mathbb{Z}_m$ of $(w(t))$, denoted by $\Phi_{k,m}(w(t))$, is the smallest m-adic complexity (over $\mathbb{Z}_m$) that can be obtained by changing at most k terms of the sequence per period, i.e.

$$\Phi_{k,m}(w(t)) = \min_{d(w(t),u(t)) \leq k} \Phi_m(u(t)),$$

where the minimum is extended over all T -periodic sequences $u(t) = (u_0, u_1, \ldots, u_{T-1})$, for which the Hamming distance, denoted as $d(w(t), u(t))$, of the vectors $(w_0, w_1, \ldots, w_{T-1})$ and $(u_0, u_1, \ldots, u_{T-1})$ is at most k. For a sequence to be cryptographically strong, its m-adic complexity should be large, and at the same time not significantly reduced by changing a few terms.

Using (8), (9) and (10) we obtain the following statement.

Lemma 3. *Let quaternary sequences $q_1(t)$ and $q_2(t)$ be defined by* (4) *and* (7)*, respectively. Then*

$$\bar{\Phi}_{1,4}(q_i(t)) \leq p+1, \ i = 0, 1.$$

Thus, we see that 4-adic complexity of these sequences is significantly reduced by changing one term. In general case, according to (8), (9) and (10) the k-error 4-adic complexity $\bar{\Phi}_{k,4}(q_i(t))$ of considered quaternary sequences defines the k-error 4-adic complexity $\bar{\Phi}_{k,4}(b_i(t))$ of Legendre sequences over $\mathbb{Z}_4$.

References

[1] V. Edemskiy, and Z. Chen.: On the 4-adic complexity of the two-prime quaternary generator. — arXiv:2106.05483 [cs.CR] 10 Jun 2021.

[2] V. Edemskiy, and N. Sokolovski.: (2020) Linear Complexity of New q-ary Generalized Cyclotomic Sequences of Period 2 . In LNCS, vol. 12020, pp. 551-559. Springer

[3] M. Goresky, and A. Klapper. Algebraic Shift Register Sequences, Cambridge University Press, 2012

[4] H. Hu, and D. Feng.: On the 2-adic complexity and the k-error 2-adic complexity of periodic binary sequences,' IEEE Trans. Inf. Theory, vol.54, pp. 874-883, 2008.

[5] Y-S. Kim, J-W. Jang, S-H. Kim, and J-S No.: New Quaternary Sequences with Ideal Autocorrelation Constructed from Legendre Sequences, IEICE Trans. Fund. Electron, vol. E96-A (9), pp. 1872-1882, 2013.

[6] A. Klapper, and M. Goresky.: Cryptanalysis based on 2-adic rational approxiamtion. In: CRYPTO 1995, LNCS, vol.963, pp. 262-273, 1995.

[7] A. Klapper, and M. Goresky.: Feedback shift registers, 2-adic span, and combiners with memory. Journal of Cryptology, vol. 10, pp. 111-147, 1997.

[8] S. Qiang, Y. Li, M. Yang, and K. Feng.: The 4-adic complexity of a class of quaternary cyclotomic sequences with period $2p$, CoRR abs/2011.11875 (2020)

[9] Y. Sun, T. Yan, Z. Chen, and L.Wang.: The 2-adic complexity of a class of binary sequences with optimal autocorrelation magnitude, Cryptogr. Commun., vol. 12, pp. 675-683, 2020.

[10] X. Tang, C. Ding.: New classes of balanced quaternary and almost balanced binary sequences with optimal autocorrelation value, IEEE Trans. Inf. Theory, vol. 56, pp. 6398-6405, 2010.

[11] J. Xu, and A. Klapper.: (1999) Feedback with Carry Shift Registers over $Z/(N)$. In: Ding C., Helleseth T., Niederreiter H. (eds) Sequences and their Applications. Discrete Mathematics and Theoretical Computer Science. Springer, London. https://doi.org/10.1007/978-1-4471-0551-0-29

[12] L. Zhang, J. Zhang, M. Yang, and K. Feng.: On the 2-Adic Complexity of the Ding-Helleseth-Martinsen Binary Sequences, IEEE Trans. Inform. Theory, vol. 66(7), pp. 4613-4620, 2020.

[13] C. Zhao, Y. Sun, and T. Yan.: Further results on the 2-adic complexity of a class of balanced generalized cyclotomic sequences. CoRR abs/2102.12098 (2021)

[14] X. Jing, M. Yang, and K. Feng.: 4-Adic Complexity of Interleaved Quaternary Sequences. arXiv:2105.13826v1 [cs.IT] 28 May 2021

[15] M. Yang, S. Qiang, X. Jing, K. Feng, and D. Lin. On the 4-Adic Complexity of Quaternary Sequences with Ideal Autocorrelation. arXiv:2107.03574v2 [cs.IT] 13 Jul 2021

Scattered Factor Universality - The Power of the Remainder

Pamela Fleischmann, Bernhard Sebastian Germann, and Dirk Nowotka

Department of Computer Science
Kiel University, Germany

fpa@informatik.uni-kiel.de, stu121684@mail.uni-kiel.de, dn@informatik.uni-kiel.de

Abstract

Scattered factor (circular) universality was firstly introduced by Barker et al. in 2020. A word w is called k-universal for some natural number k, if every word of length k of w's alphabet occurs as a scattered factor in w; it is called circular k-universal if a conjugate of w is k-universal. Here, a word $u = u_1 \cdots u_n$ is called a scattered factor of w if u is obtained from w by deleting parts of w, i.e. there exist (possibly empty) words $v_1, \ldots, v_{n+1}$ with $w = v_1 u_1 v_2 \cdots v_n u_n v_{n+1}$. In this work, we solve two problems, left open in the aforementioned paper, namely a generalisation of one of their main theorems to arbitrary alphabets and a slight modification of another theorem such that we characterise the circular universality in terms of universality. Moreover, we present an algorithm computing the circular universality of a word w over the alphabet Σ in time $\mathcal{O}(|\Sigma||w|)$.

1 Introduction

By deleting letters from a word one obtains another word, a *scattered factor* (also known as *subword* or *subsequence*). More formally, a word $u = u_1 \cdots u_n$ is a scattered factor of w if there exist (possibly) empty words $v_1, \ldots, v_{n+1}$ with $w = v_1 u_1 \cdots v_n u_n v_{n+1}$. For instance, `latin` is a scattered factor of `dalmatian` but `lama` is not. Scattered factors are a fundamental concept in mathematics and computer science: whenever data are transmitted via a lossy channel or in aligning DNA-sequences, scattered factors are the formal model to describe the incomplete data (e.g., [8]). Thus, it is not astonishing that scattered factors are strongly related to partial words [2]. *Parikh matrices* and *subword histories* use scattered factors to encode numerical properties of words into matrices, thus connecting the world of words and languages with the world of vectors and matrices (see [24, 26, 27]). From an algorithmic point of view, scattered factors are crucial in some classical problems: the longest common subsequence, the shortest common supersequence, and the string-to-string correction problem [22, 3, 29]. On the

other hand, scattered factors are also used in logic theories and have applications in formal software verifcation [30, 13, 20].

The line of research that led to this work began with Higman [15], who showed that in any infinite set of words there are always two words such that one is a scattered factor of the other, albeit only as an application of a more general theorem about partial orderings on an abstract algebra and without explicitly defining scattered factors. Later in 1967 Haines [12] explicitly introduced scattered factors and rediscovered Higman's result. In the seminal work [28] from 1975, Simon used this partial ordering to define the equivalence relation $\sim_k$, now known as the *Simon congruence*, where $x \sim_k y$ iff x and y have the same set of scattered factors of a fixed length k. In 1991, Hebrard introduced the *arch factorisation*, which is a very powerful tool in investigating the scattered factors of a word [14]. A very profound overview from a mathematical point of view can be found in [21, Chapter 6], where Simon and Sakarovitch expand Simon's previous work.

In this work we focus on a special $\sim_k$-class of words. A word $w \in \Sigma^*$ is called *k-universal* if its set of scattered factors of length k is Σ^k. For instance, `anana` is 2-universal over $\{\mathtt{a}, \mathtt{n}\}$ but `banana` is only 1-universal over $\{\mathtt{a}, \mathtt{b}, \mathtt{n}\}$. Notice that this notion is equivalent to the notion of *richness* introduced in [17, 18] in the context of piecewise testable languages; as in [1] we prefer the notion of universality for avoiding confusion with the notion of richness w.r.t. palindromes. While the classical universality problem, which asks whether a given language $L \subseteq \Sigma^*$ is equal to Σ^*, and many variants of it, as well as the universality problem for (partial) words, which asks given an ℓ whether there exists a word $w \in \Sigma^*$ that contains all words of length ℓ exactly once as a factor are well studied (see [16, 10, 25, 19] and [23, 7, 4, 11] and the references therein), the universality problem for scattered factors just recently received attention (see [6, 1, 5, 9] and the references therein).

Our contribution. Following the line of research started in [1], we investigate the (circular) universality of words. In particular, we study the universality of repetitions, which leads to several characterisations of its growth by the remainder of the arch factorisation. We show that intervals on which the universality of repetitions is constant, correspond to either ascending or descending chains of the remainder of those repetitions. These insights into the behaviour of the remainder of the arch factorisation are linked to the circular universality such that we are able to present results on two open problems of [1]. As a consequence, we also get an efficient algorithm to compute the circular universality of a word.

Structure of the work. In Section 2 we present the basic notions and in Section 3 we study the remainder of the arch factorisation and especially its growth behaviour on repetitions. Afterwards, in Section 4, we connect the previous results and define ascending and descending chains of the remainder, which leads to our main results, the generalisations of Theorem 22 and Theorem 23 from [1].

2 Preliminaries

Let $\mathbb{N} = \{1, 2, \dots\}$ denote the natural numbers. Set $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$ and $\mathbb{N}_{\geq k} = \{n \in \mathbb{N} \mid n \geq k\}$ for all $k \in \mathbb{N}_0$. We also define the discrete interval $[i, j] = \{i, i+1, \dots, j\}$ for $i, j \in \mathbb{N}_0$. Define for a function $f : \mathbb{N}_0 \to \mathbb{N}_0$ with $f(0) = 0$ the *backward difference* in $x \in \mathbb{N}$ by $\nabla f(x) = f(x) - f(x-1)$ and call ∇ the *backward difference operator* and $\nabla f(x)$ the *growth* of f in x. Set $\nabla f(0) = 0$.

An *alphabet* Σ is a finite set of symbols, called *letters*. A *word* w is a finite sequence of letters from a given alphabet and its length $|w|$ is the number of w's letters. For $i \in [1, |w|]$ let $w[i]$ denote the i^{th} letter of w. The set of all finite words over the alphabet Σ, denoted by Σ^*, is the free monoid generated by Σ with concatenation (product) as operation and the neutral element is the empty word ε, i.e. the word of length 0. Set $\Sigma^+ = \Sigma^* \setminus \{\varepsilon\}$ and $\Sigma^k = \{w \in \Sigma^* \mid |w| = k\}$ for some $k \in \mathbb{N}$. Let $u, w \in \Sigma^*$ be words. Then u is called a *factor* of w, if $w = xuy$ for some words x and y over Σ. If $x = \varepsilon$ (resp., $y = \varepsilon$) then u is called a *prefix* (resp., *suffix*) of w. A factor (resp. prefix, suffix) u of w is called a *proper* factor (resp., prefix, suffix), if $u \notin \{w, \varepsilon\}$. If $w = xy$ then we define $x^{-1}w = y$ and $wy^{-1} = x$. We say that a letter $\mathtt{a} \in \Sigma$ *occurs* in w, if $\mathtt{a}$ is a factor of w. We denote the set of all letters that occur in w by $\operatorname{alph}(w)$. Furthermore two words $u_1, u_2 \in \Sigma^*$ are called *prefix-compatible* (resp., *suffix-compatible*) if one is a prefix (resp., suffix) of the other. Two words w and u are said to be *conjugate* to each other if there exist words $x, y \in \Sigma^*$ such that $w = xy$ and $u = yx$. We denote the *reversal* of a word by w^R, i.e. if $|w| = n$ then $w^R = w[n] \cdot w[n-1] \cdot \ldots \cdot w[1]$. If we have words $w_i \in \Sigma^*$ for all $i \in [1, n]$ and some $n \in \mathbb{N}$, then we define $\prod_{i=k}^{n} w_i = w_k \cdot \ldots \cdot w_n$. In the special case $w_1 = w_2 = \ldots = w_n = w$ we also write $w^n = \prod_{i=1}^{n} w$ and call w^n the n^{th} power of w.

Now, we introduce the notions around scattered factor universality ([1]).

Definition 1. A word $u \in \Sigma^*$ is called a *scattered factor* (or *subword*) of $w \in \Sigma^*$ if there exist $x_1, \dots, x_{|u|+1} \in \Sigma^*$ such that $w = x_1 u[1] x_2 \cdots x_{|u|} u[|u|] x_{|u|+1}$. We denote the set of all scattered factors of a given word $w \in \Sigma^*$ by $\operatorname{ScatFact}(w)$ and the set of all scattered factors of a given length $k \in \mathbb{N}_0$ by $\operatorname{ScatFact}_k(w)$.

Definition 2. For a $k \in \mathbb{N}_0$, a word $w \in \Sigma^*$ is called *k-universal* (w.r.t Σ) if $\operatorname{ScatFact}_k(w) = \Sigma^k$ and called *circular* k-universal (w.r.t. Σ) if there exists a conjugate v of w such that v is k-universal. We define the *universality index* of w as the maximal k such that w is k-universal and denote it by $\iota(w)$; analogously $\zeta(w)$ denotes the *circular universality index* of w.

Remark 3. By definition, the universality is w.r.t. to a given alphabet Σ. Notice, that we have immediately $\iota(w) = 0 = \zeta(w)$ if $\operatorname{alph}(w) \subsetneq \Sigma$. Therefore, we implicitly assume w.l.o.g. $\Sigma = \operatorname{alph}(w)$ from now on. Thus, we also assume $\iota(w) > 0$ at any time without mentioning it. For abbreviation, we set $\sigma = |\Sigma|$.

Since this work focuses on the (circular) universality index of powers of $w \in \Sigma^*$, we introduce the following parametrisation.

Definition 4. For $w \in \Sigma^*$ define $\iota_w : \mathbb{N}_0 \to \mathbb{N}_0$; $s \mapsto \iota(w^s)$ and $\zeta_w : \mathbb{N}_0 \to \mathbb{N}_0$; $s \mapsto \zeta(w^s)$.

The following remark captures properties of ι_w and ζ_w for a given $w \in \Sigma^*$.

Remark 5. For $w \in \Sigma^*$ and all $s \in \mathbb{N}_0$ we have first, $\iota(w^s) = \iota_w(s) = \sum_{i=1}^{s} \nabla\iota_w(i)$, $\iota(w) \leq \nabla\iota_w(s) \leq \iota(w)+1$, and $\nabla\iota_w(1) = \iota(w)$. Therefore, $s\iota(w) \leq \iota_w(s) \leq s\iota(w)+s-1$ with
1. $\iota_w(s) = sk$ iff $\nabla\iota_w(i) = k$ for all $i \in [1,s]$ and
2. $\iota_w(s) = sk+s-1$ iff $\nabla\iota_w(i) = k+1$ for all $i \in [2,s]$.
The binary words ab and baab satisfy the first and second property, resp. For an arbitrary alphabet $\Sigma = \{\mathtt{a}_1, \ldots, \mathtt{a}_\sigma\}$, the word $\mathtt{a}_1 \ldots \mathtt{a}_\sigma$ satisfies the first property, and for the second property an example is given in Remark 43.

Next we recall the arch factorisation introduced by Hebrard in [14].

Definition 6. Let $w \in \Sigma^*$. The factorisation $w = \mathrm{ar}_1(w) \cdot \ldots \cdot \mathrm{ar}_k(w) \cdot r(w)$, for some $k \in \mathbb{N}_0$, is called *arch factorisation* if for all $i \in [1,k]$ we have $\mathrm{ar}_i(w) = u_i\mathtt{a}_i$ for some $u_i \in \Sigma^*$ and $\mathtt{a}_i \in \Sigma$, $\mathrm{alph}(u_i) \neq \Sigma$, $\mathrm{alph}(u_i\mathtt{a}_i) = \Sigma$, and $\mathrm{alph}(r(w)) \neq \Sigma$. Furthermore, we define the *modus* as $m(w) = \mathtt{a}_1 \cdot \ldots \cdot \mathtt{a}_k$. We call $\mathrm{ar}_i(w)$ the i^{th} arch, $r(w)$ the remainder, and denote the set of letters that occur in the remainder by $\mathcal{R}(w) = \mathrm{alph}(r(w))$.

Remark 7. Note, that for all $w \in \Sigma^*$ and appropriate $i \in \mathbb{N}$, $m(w)[i]$ occurs exactly once in $\mathrm{ar}_i(w)$ and the number of arches of a word w is $\iota(w)$. In [1, Proposition 10] a linear time algorithm to compute w's arch factorisation is given. In examples we will visualise the arch factorisation with the use of brackets. For example, we will write $(\mathtt{abc}) \cdot (\mathtt{cbba}) \cdot (\mathtt{caaab}) \cdot \mathtt{a}$ to indicate the three arches abc, cbba, and caaab and the remainder (without brackets) a.

In [1] the dynamic between universality and circular universality is studied. Naïvely, one would expect that the universality of powers of w grows linearly with its universality, i.e. $\nabla\iota(w^s) = \iota(w)$ for all $s \in \mathbb{N}$. But this is not always the case. Instead, its actual growth is related to the circular universality of w. The following statements about (circular) universality from [1] are fundamental and the basis for our work.

Lemma 8 ([1])**.** For $w \in \Sigma^*$, we have $\iota(w) = \iota(w^R)$ and $\iota(w) \leq \zeta(w) \leq \iota(w)+1$.

Theorem 9 ([1])**.** *Let $w \in \Sigma^*$ and $k = \iota(w)$. For all $s \in \mathbb{N}$, if $\zeta(w) = k+1$ then $\iota(w^s) = sk+s-1$.*

Theorem 10 ([1])**.** *Let $|\Sigma| = 2$, $w \in \Sigma^*$ with $k = \iota(w)$, and $s \in \mathbb{N}$. Then $\iota(w^s) = sk+s-1$ if $\zeta(w) = k+1$ and $\iota(w^s) = sk$ otherwise.*

As stated in [1], neither Theorem 10 nor the converse of Theorem 9 hold for ternary alphabets: considering $w = (\mathtt{babc}) \cdot (\mathtt{caab}) \cdot \mathtt{c}$, we have $\zeta(w) = \iota(w)$ and $\iota(ww) = 2\iota(w)+1$. We finish the preliminaries with a lemma that follows the line of arguments repeatedly used in [1].

Lemma 11. Let $w \in \Sigma^*$. If $\nabla\iota_w(s) = \iota(w)$ for all $s \in \mathbb{N}$ then also $\nabla\zeta_w(s) = \iota(w)$ for all $s \in \mathbb{N}$.

Proof. Let $\nabla\iota_w(s) = k$ for all $s \in \mathbb{N}$. Now suppose that $\nabla\zeta_w(s_0) = k+1$ for some $s_0 \in \mathbb{N}$ and choose s_0 to be minimal with this property. Then we have $\zeta_w(s_0) = s_0k + 1$. This implies that $\zeta_w(2s_0) \geq 2s_0k + 2$. Therefore, we get $\iota_w(2s_0) \geq 2s_0 + 1$ by Lemma 8. This is a contradiction to our assumption that $\nabla\iota_w(s) = k$ for all $s \in \mathbb{N}$. Thus there cannot be such an s_0. □

3 The Growth Behaviour of the Universality

In this section, our goal is to find a characterisation for the previous example: for $w = \texttt{babccabc}$, we have $k = \iota(w) = 2$. Then we obtain $\iota(w^2) = 2k + 1$ and $\iota(w^3) = 3k + 1$ again. This means $\nabla\iota_w(2) = k + 1$, but $\nabla\iota_w(3) = k$. Thus, we seek criteria to determine whether $\nabla\iota_w(s_0)$ is k or $k + 1$ for a given s_0. Having this purpose in mind, we now look at the arch factorisation of w^2: the first k arches of w^2 are those of w but the next arch begins with the remainder $r(w)$ (which may be empty) and ends with a non-empty prefix p of w. The remaining arches are those of $p^{-1}w$. Thus $\iota(w^2) = k + 1 + \iota(p^{-1}w)$ or, equivalently, $\nabla\iota_w(2) = 1 + \iota(p^{-1}w)$. Clearly, by increasing the length of p, we decrease $\iota(p^{-1}w)$. So we get $\nabla\iota_w(2) = k + 1$ iff p is not *too long*. Thus, how long does p have to be, and what is the longest prefix p that we can remove from w without reducing its universality? Answering these questions will yield the characterisation that we are striving to. Regarding the first question, p must be long enough for the equation $\mathrm{alph}(r(w)p) = \Sigma$ to hold, since only then $r(w)p$ is an arch of w^2. The second question is answered by the following lemma.

Lemma 12. For $w \in \Sigma^*$, the word $p = r(w^R)^R$ is the longest prefix of w such that $\iota(p^{-1}w) = \iota(w)$ holds.

Proof. The claim follows from the facts that $q = r(w^R)$ is the longest suffix of w^R such that $\iota(w^Rq^{-1}) = \iota(w^R)$, and that $\iota(u) = \iota(u^R)$ for all $u \in \Sigma^*$. □

For instance, if $w = \texttt{nabananab}$, we have $r(w^R)^R = \texttt{an}$, and indeed, if we remove $\texttt{na}$ from the beginning of w, $\iota(\texttt{bananab}) = 2$ still holds.

In our considerations above we looked at the arch factorisation of w^2. This can be generalised to the concatenation of two arbitrary words w and u. The answer to the question, whether $\iota(wu)$ equals $\iota(w) + \iota(u) + 1$ or $\iota(w) + \iota(u)$, is given by a slightly more general version of [1, Proposition 18].

Proposition 13. *Let $u, w \in \Sigma^*$ with $k = \iota(w)$ and $\ell = \iota(u)$. Then $\iota(wu) = k + \ell + 1$ if and only if* $\mathrm{alph}(r(w)r(u^R)) = \Sigma$.

Proof. From the arch factorisations of w and u^R, respectively, follows immediately that if $\mathrm{alph}(r(w)r(u^R)) = \Sigma$ then $\iota(wu) = k + \ell + 1$. Now on the other hand assume that $\mathrm{alph}(r(w)r(u^R)) \neq \Sigma$. We can factorise wu as $wu = w(u^R)^R = \left[\prod_{i=1}^{k} \mathrm{ar}_i(w)\right] \cdot r(w) \cdot r(u^R)^R \cdot \left[\prod_{i=1}^{\ell} \mathrm{ar}_{\ell+1-i}(u^R)^R\right]$, i.e., as the product of the arch factorisation of w and the reversal of the arch factorisation of u^R. Then one can see that $\iota(wu) = k + \iota(r(w)u)$.

Now it is left to show that $\iota(r(w)u) < \ell + 1$. We will determine $\iota(r(w)u)$ by looking as usual at its arch factorisation. First, there exists a prefix p of u such that the first arch of $r(w)u$ is $\mathrm{ar}_1(r(w)u) = r(w)p$. Then it follows from the assumption that p has to be longer than $r(u^R)^R$, i.e. $|p| > \left|r(u^R)^R\right|$. And so, by Lemma 12 $\iota(p^{-1}u) < \ell$ holds. Therefore, finally, $\iota(r(w)u) = \iota(r(w)p) + \iota(p^{-1}u) < 1 + \ell$. □

Proposition 13 implies immediately the desired characterisation of the growth of ι_w, i.e. $\nabla\iota_w$, using $w^s = w^{s-1} \cdot w$.

Corollary 14. Let $w \in \Sigma^*$, $k = \iota(w)$ and $s \in \mathbb{N}$. Then we have $\nabla\iota_w(s) = k + 1$ if and only if $\mathrm{alph}(r(w^{s-1})r(w^R)) = \Sigma$.

Proof. The claim follows by Proposition 13 applied on on w^{s-1} and w. □

Corollary 14 is fundamental to the remainder of this chapter. It gives us a useful tool to investigate the universality of repetitions w^s. It implies that the growth $\nabla\iota_w$ and the remainder mapping $s \mapsto r(w^s)$ of repetitions depend on each other. Thus we can gain insight into the behaviour of $\nabla\iota_w$ by studying $s \mapsto r(w^s)$ and vice versa. In particular, we are interested in the question under which circumstances we gain eventual periodicity in the growth. Notice that $r(w^s)$ depends recursively on $r(w^{s-1})$ by the equation $r(w^s) = r(w^{s-1} \cdot w)$. However, we can slightly refine this notion: since removing whole arches from a word does not change its remainder, we have the following observation.

Remark 15. Let $w \in \Sigma^*$ and $s \in \mathbb{N}$. Then $r(w^s) = r(r(w^{s-1})w)$. Thus, there is always a word $u \in \Sigma^*$ with $\mathrm{alph}(u) \subsetneq \Sigma$ such that $r(w^s) = r(uw)$.

Now, we investigate when $r(uw)$ and $r(w)$ differ (or more generally $r(uw)$ and $r(vw)$ for some $v \in \Sigma^* \backslash \{u\}$ with $\mathrm{alph}(v) \subsetneq \Sigma$). Consider, for motivation, $w = (\mathtt{abbc}) \cdot (\mathtt{caab}) \cdot \mathtt{caa}$. If $u \in \{\mathtt{a}, \mathtt{b}\}^*$ then in uw, u simply adds to the first arch of w without bringing any significant change into the arch factorisation. This happens because $\mathtt{c}$ does not occur in u leading to $r(uw) = r(w)$. Now consider $u = \mathtt{c}$. This time, regarding uw, u causes the factor $\mathtt{bc}$ to get *released* from w's first arch and $\mathtt{ab}$ gets released from w's second arch and *binds* $\mathtt{c}$, the first letter of w's remainder, to build a third arch. Thus by prepending u to w, changes in the arch factorisation get carried through the whole word. Finally, let $u = \mathtt{caa}$. The arch factorisations of $\mathtt{c}w$ and uw do not differ significantly from each other since the last letter of $\mathrm{ar}_1(uw)$ is $\mathtt{b}$ and adding any number of the letter $\mathtt{a}$ to $\mathtt{c}$ has no effect. Notice that in all cases, we only argued using $\mathrm{alph}(u)$ but neither on the number of letters nor their position. In fact, for any $u \in \Sigma^*$ with $\mathrm{alph}(u) \subsetneq \Sigma$, $\mathrm{alph}(u)$ is the only relevant information about u for the computation of $r(uw)$, since we assumed $\iota(w) > 0$.

Lemma 16. If $u, v, w \in \Sigma^*$ with $\mathrm{alph}(u) = \mathrm{alph}(v) \subsetneq \Sigma$ then $r(uw) = r(vw)$.

Proof. The first arch of uw is formed by u and the shortest prefix p of w such that $\mathrm{alph}(u) \cup \mathrm{alph}(p) = \Sigma$. Thus p depends solely on $\mathrm{alph}(u)$. This makes p also the shortest prefix such that $\mathrm{alph}(v) \cup \mathrm{alph}(p) = \Sigma$. Hence $r(uw) = r(p^{-1}w) = r(vw)$. □

Now, we return our attention to the equation $r(w^{s_0}) = r(r(w^{s_0-1})w)$ for some $s_0 \in \mathbb{N}_0$. If the letters occurring in $r(w^{s_0})$ and $r(w^{s_0-1})$ are the same, Lemma 16 implies that $s \mapsto r(w^s)$ stays constant beginning at s_0. And even more generally, we get in the same way that, if for some $t_0 \in \mathbb{N}_0$ the letters occurring in $r(w^{s_0})$ and $r(w^{t_0})$ are the same, then $r(w^{s_0+1}) = r(w^{t_0+1})$, i.e., the mapping $s \mapsto r(w^s)$ is periodic beginning at $\min\{ s_0, t_0 \}$. The following lemma proves this observation. Recall that we defined $\mathcal{R}(w) = \mathrm{alph}(r(w))$.

Lemma 17. Let $w \in \Sigma^*$ and let $s, t \in \mathbb{N}_0$. If $\mathcal{R}(w^s) = \mathcal{R}(w^t)$ then $r(w^{s+i}) = r(w^{t+i})$ for all $i \in \mathbb{N}$.

Proof. Let $\mathcal{R}(w^s) = \mathcal{R}(w^t)$. We show by induction that $r(w^{s+i}) = r(w^{t+i})$ for all $i \in \mathbb{N}$. For $i = 1$, we get $r(w^{s+1}) = r(r(w^s)w) = r(r(w^t)w) = r(w^{t+1})$ by Lemma 16. For $i > 1$, assume that $r(w^{s+i}) = r(w^{t+i})$. Then we get $r(w^{s+i+1}) = r(r(w^{s+i})w) = r(r(w^{t+i})w) = r(w^{t+i+1})$. □

The converse of Lemma 17 is not necessarily true: considering $w = (\mathtt{acab}) \cdot \mathtt{b}$, we have $r(w^2) = r(w^3) = r(w^s)$ for all $s \geq 2$, but $\mathcal{R}(w) \neq \mathcal{R}(w^2)$. Notice also, that Lemma 17 does not hold for $i = 0$. For $w = (\mathtt{ab}) \cdot \mathtt{b}$ we have $\mathcal{R}(w) = \mathcal{R}(w^2)$, but $r(w) \neq r(w^2)$. But indeed, if we only care about the letters in the remainders, then we can extend Lemma 17 to all $i \in \mathbb{N}_0$ and the converse immediately holds as well.

Lemma 18. Let $w \in \Sigma^*$ and let $s, t \in \mathbb{N}_0$. Then we have $\mathcal{R}(w^{s+i}) = \mathcal{R}(w^{t+i})$ for all $i \in \mathbb{N}_0$ if and only if $\mathcal{R}(w^s) = \mathcal{R}(w^t)$.

Proof. Let $\mathcal{R}(w^s) = \mathcal{R}(w^t)$. Then Lemma 17 implies that $r(w^{s+i}) = r(w^{t+i})$ for all $i \in \mathbb{N}$. Hence $\mathcal{R}(w^{s+i}) = \mathcal{R}(w^{t+i})$ for all $i \in \mathbb{N}_0$. The other direction follows immediately by $i = 0$. □

Lemma 18 implies the desired periodicity property of the growth.

Proposition 19. *The growth of the universality index, $\nabla \iota_w$, is eventually periodic.*

Proof. Since the mapping $s \mapsto \mathcal{R}(w^s)$ can only have finitely many values (Σ is finite), there exist $s_0, t_0 \in \mathbb{N}_0$ with $s_0 \neq t_0$ such that $\mathcal{R}(w^{s_0}) = \mathcal{R}(w^{t_0})$ and thus Lemma 18 implies that $s \mapsto \mathcal{R}(w^s)$ is periodic. The claim follows by Corollary 14. □

The following lemma shows that s and t can be bound by σ and leads to a theorem capturing the above considerations.

Lemma 20. For all $w \in \Sigma^*$ we have $|\{ \mathcal{R}(w^s) \mid s \in \mathbb{N}_0 \}| \leq \sigma$.

Proof. For all $s \in \mathbb{N}_0$ the remainder $r(w^s)$ is a suffix of w. Therefore these remainders are pairwise suffix-compatible with each other, and consequently also the sets $\mathcal{R}(w^s)$ are pairwise comparable regarding inclusion, i.e. the set $\{ \mathcal{R}(w^s) \mid s \in \mathbb{N}_0 \}$ is totally ordered. Thus we can order them by some bijective mapping $\pi : \mathbb{N}_0 \to \mathbb{N}_0$ such that $\mathcal{R}(w^{\pi(j)}) \supseteq \mathcal{R}(w^{\pi(j+1)})$ for all $j \in \mathbb{N}_0$. But since also each set contains less than σ elements, i.e., $0 \leq |\mathcal{R}(w^s)| < \sigma$ for all $s \in \mathbb{N}_0$, it follows that $s \mapsto \mathcal{R}(w^s)$ has at most σ different values. □

Theorem 21. *For all $w \in \Sigma^*$ there exist $s, t \in [0, \sigma]$ with $s < t$ such that*
1. $r(w^{s+i}) = r(w^{t+i})$ for all $i \in \mathbb{N}$,
2. $\mathcal{R}(w^{s+i}) = \mathcal{R}(w^{t+i})$ for all $i \in \mathbb{N}_0$, and
3. $\nabla\iota_w(s+i) = \nabla\iota_w(t+i)$ for all $i \in \mathbb{N}$.

Proof. By Lemma 20 there exist $s < t \in [0, \sigma]$ such that $\mathcal{R}(w^s) = \mathcal{R}(w^t)$. Then the first claim follows by Lemma 17 and the second by Proposition 18. The third claim follows by combining the second claim with Corollary 14. □

Theorem 21 states that beginning at $s+1$, the quantity $\nabla\iota_w$ has the period $t-s$. So, given an $n \in \mathbb{N}$ we can divide $[1, n]$ into $[1, s]$ (before $\nabla\iota_w$ is periodic) and $[s+1, n]$ (containing the periodic part). By division with remainder, we obtain $\ell, m \in \mathbb{N}_0$ such that $n - s = \ell \cdot (t-s) + m$ and thus, the subinterval $[s+1, s+\ell(t-s)]$ contains ℓ full periods while $[s+\ell(t-s)+1, n]$ is the rest. This observation motivates the following Proposition.

Proposition 22. *Let $w \in \Sigma^*$ and let $n \in \mathbb{N}$ with $n \geq \sigma$. Then there exist $\ell, m, s, t \in \mathbb{N}_0$ with $s < t \leq \sigma$, $m < t - s$, and $n - s = \ell \cdot (t-s) + m$ such that $\iota_w(n) = \iota_w(s+m) + \ell \cdot (\iota_w(t) - \iota_w(s))$.*

Proof. Let s and t be minimal such that $s < t$ and $\mathcal{R}(w^s) = \mathcal{R}(w^t)$. By Theorem 21 we have $s, t \leq \sigma$. Then there are by division with remainder $m, \ell \in \mathbb{N}_0$ such that $n - s = \ell \cdot (t-s) + m$ with $m < t - s$. It follows by Theorem 21 that

$$\begin{aligned}\iota_w(n) = \sum_{i=1}^{n} \nabla\iota_w(i) &= \left[\sum_{i=1}^{s} \nabla\iota_w(i)\right] + \ell \cdot \left[\sum_{i=s+1}^{t} \nabla\iota_w(i)\right] + \left[\sum_{i=s+1}^{s+m} \nabla\iota_w(i)\right] \\ &= \iota_w(s+m) + \ell \cdot \left[\sum_{i=s+1}^{t} \nabla\iota_w(i)\right] = \iota_w(s+m) + \ell \cdot (\iota_w(t) - \iota_w(s)),\end{aligned}$$

which was to be shown. □

Proposition 23. *Given $w \in \Sigma^*$, we can compute $\iota_w(n)$ for all $n \in \mathbb{N}_0$ in constant time with a preprocessing time of $\mathcal{O}(\sigma|w|)$.*

Proof. We only have to compute the minimal $s, t \in \mathbb{N}_0$ with $\mathcal{R}(w^s) = \mathcal{R}(w^t)$ and $\iota_w(i)$ for all $i \in [0, \sigma]$ once, taking in total $\mathcal{O}(\sigma|w|)$ time. Afterwards, by Proposition 22, we can compute $\iota_w(n)$ for all $n \in \mathbb{N}_0$ in constant time. □

In the rest of this work we will usually only need the notion of constancy and not of periodicity. Thus we restate Lemma 17 and Proposition 18 for the case $s = t - 1$. The claims follow directly by the lemma and the proposition.

Lemma 24. Let $w \in \Sigma^*$ and $s_0 \in \mathbb{N}$. If $\mathcal{R}(w^{s_0-1}) = \mathcal{R}(w^{s_0})$ then $r(w^s) = r(w^{s_0})$ for all $s \geq s_0$.

Proposition 25. *Let $w \in \Sigma^*$and $s_0 \in \mathbb{N}$. Then we have $\mathcal{R}(w^s) = \mathcal{R}(w^{s_0})$ for all $s \geq s_0 - 1$ if and only if $\mathcal{R}(w^{s_0-1}) = \mathcal{R}(w^{s_0})$.*

Hence, if $\mathcal{R}(w^{s_0-1}) = \mathcal{R}(w^{s_0})$ holds for any $s_0 \in \mathbb{N}$ then the mappings $s \mapsto r(w^s)$ and $s \mapsto \mathcal{R}(w^s)$ are both eventually constant.

4 Chaining the Remainder

Section 3 established by Corollary 14 a correspondence between the growth $\nabla\iota_w$ and the remainder mapping $s \mapsto r(w^s)$. We achieved this corollary by interpreting w^s recursively as $w^{s-1} \cdot w$. But if we interpret it as $w \cdot w^{s-1}$ instead then we find another useful relationship that we capture in the following lemma.

Lemma 26. Let $w \in \Sigma^*$ and $s \in \mathbb{N}_0$. Then the following two statements hold:
1. If $\nabla\iota_w(s+1) = \iota(w)$ then $r(w^s)$ is a suffix of $r(w^{s+1})$.
2. If $\nabla\iota_w(s+1) = \iota(w)+1$ then $r(w^{s+1})$ is a suffix of $r(w^s)$.

Proof. Set $k = \iota(w)$. First note that $r(w^{s+1}) = r(r(w)w^s)$ holds. Second, let $\ell = \iota(w^s)$ be the universality of w^s. Now we examine the arch factorisation of $r(w)w^s = r(w) \cdot \prod_{i=1}^{\ell} \mathrm{ar}_i(w^s)$. For all $i \in [1,\ell]$ there exist factors $x_i, y_i \in \Sigma^*$ such that the arches of w^s are factorised by $\mathrm{ar}_i(w^s) = x_i y_i$ and such the arches of $r(w)w^s$ are factorised by $\mathrm{ar}_i(r(w)w^s) = r(w)x_1$, if $i = 1$ and $\mathrm{ar}_i(r(w)w^s) = y_{i-1}x_i$, if $i \geq 2$. Now the question is whether the remaining factor $y_\ell r(w^s)$ contains yet another arch or whether it is already the remainder of $r(w)w^s$.
Case 1: Assume that it is already the remainder, i.e., that $r(r(w)w^s) = y_\ell r(w^s)$ holds. Then $r(w)w^s$ has exactly ℓ arches and hence w^{s+1} has $k+\ell$ arches. In other words, $\nabla\iota_w(s+1) = k$. But, since $r(w^{s+1}) = r(w)w^s$, it also follows that $r(w^s)$ is a suffix of $r(w^{s+1})$.
Case 2: Now assume that $y_\ell r(w^s)$ contains yet another arch. Then there exist factors $x_{\ell+1}, y_{\ell+1} \in \Sigma^*$ such that $r(w^s) = x_{\ell+1}y_{\ell+1}$, $\mathrm{ar}_{\ell+1}(r(w)w^s) = y_\ell x_{\ell+1}$ and $r(r(w)w^s) = y_{\ell+1}$. Then with similar arguments as in the previous case it follows that $\nabla\iota_w(s+1) = k+1$ and also that $r(w^{s+1}) = y_{\ell+1}$ is a suffix of $r(w^s)$. Thus, so we have either the case that $\nabla\iota_w(s+1) = k$ and $r(w^s)$ is a suffix of $r(w^{s+1})$, or the case that $\nabla\iota_w(s+1) = k+1$ and $r(w^{s+1})$ is a suffix of $r(w^s)$. □

Combining Corollary 14 and Lemma 26 implies that if $r(w^s)$ is *long enough* then $\nabla\iota_w(s+1) = k+1$, which implies that $r(w^{s+1})$ is a suffix of $r(w^s)$. Thus, now $r(w^{s+1})$ may have become *so short* that in the next step we get $\nabla\iota_w(s+2) = k$. This is exactly what happens for $w = (\mathtt{babc}) \cdot (\mathtt{caab}) \cdot \mathtt{c}$. The other case is symmetrical: if $r(w^s)$ is not *long enough* then $\nabla\iota_w(s+1) = k$, which implies that $r(w^s)$ is a suffix of $r(w^{s+1})$. Thus, now $r(w^{s+1})$ may have become *long enough* for $\nabla\iota_w(s+2) = k+1$. Also note, that the converses of Lemma 26 do not necessarily hold if $r(w^s) = r(w^{s+1})$. Considering $w = (\mathtt{ab}) \cdot \mathtt{a}$, we get $\nabla\iota_w(2) = 1$ and $r(w) = \mathtt{a} = r(w^2)$. On the other hand, if $w = (\mathtt{aab}) \cdot \mathtt{b}$ then $\iota(w) = 1$, but $\nabla\iota_w(2) = 2$ and $r(w) = \mathtt{b} = r(w^2)$. But as soon as two successive remainders are equal or even if only their set of occurring letters are equal, then $s \mapsto r(w^s)$ is eventually constant. Thus, it seems useful to consider the cases, where these conditions are excluded, explicitly. We state them in the following two corollaries.

Corollary 27. Let $w \in \Sigma^*$ and $s \in \mathbb{N}_0$. If $r(w^s) \neq r(w^{s+1})$, then
1. $\nabla\iota_w(s+1) = k$ iff $r(w^s)$ is a (proper) suffix of $r(w^{s+1})$ and
2. $\nabla\iota_w(s+1) = k+1$ iff $r(w^{s+1})$ is a (proper) suffix of $r(w^s)$.

Corollary 28. Let $w \in \Sigma^*$ and $s \in \mathbb{N}_0$ with $\mathcal{R}(w^s) \neq \mathcal{R}(w^{s+1})$. Then we obtain
1. $\nabla\iota_w(s+1) = k$ iff $r(w^s)$ is a (proper) suffix of $r(w^{s+1})$ iff $\mathcal{R}(w^s) \subsetneq \mathcal{R}(w^{s+1})$ and 2. $\nabla\iota_w(s+1) = k+1$ iff $r(w^{s+1})$ is a (proper) suffix of $r(w^s)$ iff $\mathcal{R}(w^s) \supsetneq \mathcal{R}(w^{s+1})$.

However, usually we do not know whether $s \mapsto r(w^s)$ is eventually constant, i.e. whether Corollary 28 is applicable. So now the following lemma gives a criterion to decide whether this condition is satisfied.

Lemma 29. For all $w \in \Sigma^*$, $s \mapsto r(w^s)$ is eventually constant iff $\nabla\iota_w$ is.

Proof. From Corollary 14 follows immediately that if $s \mapsto r(w^s)$ is eventually constant then $\nabla\iota_w$ is, too. Thus, assume that $\nabla\iota_w$ is eventually constant. Then there is $s_0 \in \mathbb{N}$ such that $\nabla\iota_w(s) = \ell$ for all $s \geq s_0$, where ℓ is either k or $k+1$.
Case $\ell = k$: Then Lemma 26 implies that there is an infinite ascending chain $\mathcal{R}(w^{s_0}) \subseteq \mathcal{R}(w^{s_0+1}) \subseteq \ldots$. But since $\mathcal{R}(w^s) \subseteq \Sigma$ for all $s \in \mathbb{N}$ and Σ is finite, it follows that the chain is not strictly increasing. Hence, there is some $t \geq s_0$ such that $\mathcal{R}(w^t) = \mathcal{R}(w^{t+1})$ and thus $s \mapsto r(w^s)$ is eventually constant.
Case $\ell = k+1$: This case is analogous to the previous one. □

Applying Lemma 29 gives a new insight regarding the characterisation when $\zeta(w) = \iota(w) + 1$ holds.

Corollary 30. Let $w \in \Sigma^*$ and $k = \iota(w)$. If $\zeta(w) = k+1$ then $s \mapsto r(w^s)$ is eventually constant.

We will usually apply Lemma 26 and Corollary 28 in the following way: an interval $[\ell+1, n]$ on which we have $\nabla\iota_w(s) = k$ implies that there is an ascending chain $\mathcal{R}(w^\ell) \subseteq \mathcal{R}(w^{\ell+1}) \subseteq \ldots \subseteq \mathcal{R}(w^n)$. Notice that we cannot conclude that $\nabla\iota_w(s) = k$ holds on $[\ell+1, n]$ by the existence of such a chain since there may be equality in some steps. However, if we exclude $\mathcal{R}(w^s) = \mathcal{R}(w^n)$ for all $s \geq n-1$, i.e., $s \mapsto \mathcal{R}(w^s)$ is not yet constant, then we know that the chain from $\mathcal{R}(w^\ell)$ to $\mathcal{R}(w^n)$ is strict, and such a strictly ascending chain implies $\nabla\iota_w(s) = k$ on $[\ell+1, n]$ (the case where $\nabla\iota_w(s) = k+1$ on $[\ell+1, n]$ is symmetrical with descending chains). This way Lemma 26 and Corollary 28 can be used to translate questions about ι_w and ζ_w into questions about chains of sets.

In the following two subsections we investigate ascending and descending chains in more detail. By improvements of Lemma 29, we are able to generalise the two aforementioned results from [1].

4.1 Ascending Chains. So far, we established that an interval $[\ell+1, n]$ on which $\nabla\iota(w^s) = k$ holds implies an ascending chain $\mathcal{R}(w^\ell) \subseteq \ldots \subseteq \mathcal{R}(w^n)$ and if that chain is strict then the implication holds also in the other direction. The following lemma gives us a structural property about a strictly ascending chain of length exactly σ, where σ is the size of the alphabet.

Lemma 31. Let $w \in \Sigma^*$ and $\ell \in \mathbb{N}_0$. If $\mathcal{R}(w^\ell) \subsetneq \ldots \subsetneq \mathcal{R}(w^{\ell+\sigma-1})$ is a strictly ascending chain of length σ then we have $|\mathcal{R}(w^s)| = s - \ell$ for all $s \in [\ell, \ell+\sigma-1]$.

Proof. By the definition of the remainder we have $0 \leq |\mathcal{R}(u)| < \sigma$ for all $u \in \Sigma^*$. Thus, the claim follows by $0 \leq \left|\mathcal{R}(w^\ell)\right| < \ldots < \left|\mathcal{R}(w^{\ell+\sigma-1})\right| < \sigma$. □

By Lemma 31, strictly ascending chains of length $\sigma + 1$ cannot exist.

Corollary 32. Let $w \in \Sigma^*$, $\ell, n \in \mathbb{N}_0$, and $\mathcal{R}(w^\ell) \subsetneq \ldots \subsetneq \mathcal{R}(w^{\ell+n-1})$ be a strictly ascending chain of length n. Then $n \leq \sigma$.

Proof. If there was a strictly ascending chain with length $\sigma + 1$ then Lemma 31 would imply $\sigma - 1 = \left|\mathcal{R}(w^{\ell+\sigma-1})\right| < \left|\mathcal{R}(w^{\ell+\sigma})\right|$ and thus $\left|\mathcal{R}(w^{\ell+\sigma})\right| = \sigma$. This is a contradiction since not all letters can occur in the remainder. □

Remark 33. In fact, there actually exists a strictly ascending chain of length σ. For $\Sigma = \{\, \mathtt{a}_1, \ldots, \mathtt{a}_\sigma \,\}$ set $w = \prod_{i=1}^{\sigma} \mathtt{a}_i^2$. Then we have $\iota(w) = 1$, $\nabla\iota_w(s) = 1$ for all $s \in [1, \sigma - 1]$ and $\nabla\iota_w(\sigma) = 2$. Furthermore $\mathcal{R}(w^0) \subsetneq \ldots \subsetneq \mathcal{R}(w^{\sigma-1})$ is a strictly ascending chain of length σ.

Corollary 32 leads to the following proposition, which states that if we have $\nabla\iota_w(s) = k$ for the first $\sigma - 1$ repetitions then $\nabla\iota_w$ is already constant.

Proposition 34. *Let $w \in \Sigma^*$, $k = \iota(w)$. If $\nabla\iota_w(s) = k$ for all $s \in [1, \sigma]$ then $\nabla\iota_w(s) = k$ for all $s \in \mathbb{N}$.*

Proof. Let $\nabla\iota_w(s) = k$ for all $s \in [1, \sigma]$. Then Lemma 26 gives us the ascending chain $\mathcal{R}(w^0) \subseteq \ldots \subseteq \mathcal{R}(w^\sigma)$. By Corollary 32 this chain is not strict. Therefore there exists an $s_0 \in [1, \sigma]$ such that $\mathcal{R}(w^{s_0-1}) = \mathcal{R}(w^{s_0})$. Then Proposition 25 implies that $s \mapsto \mathcal{R}(w^s)$ is eventually constant with $\mathcal{R}(w^s) = \mathcal{R}(w^{s_0-1})$ for all $s \geq s_0 - 1$. Consequently it follows from Corollary 14 that $\nabla\iota_w(s) = \nabla\iota_w(s_0) = k$ for all $s \geq s_0$. □

Even though the bound σ in Proposition 34 is tight, we can still improve the statement in another way. If we consider the *circular* universality ζ_w instead of the plain universality ι_w then we can lower the bound to $\sigma - 1$. Before we present the corresponding proposition, we prove two auxiliary lemmata.

Lemma 35. Let $w \in \Sigma^*$ and $k = \iota(w)$. If each letter $\mathtt{a} \in \Sigma$ occurs only once in each arch of w and at most once in the remainder $r(w)$ then $\nabla\zeta_w(s) = k$ for all $s \in \mathbb{N}$.

Proof. Let $\mathtt{a} \in \Sigma$ such that $\mathtt{a}$ does not occur in $r(w)$. Then by assumption $\mathtt{a}$ occurs k times in w and therefore sk times in w^s. So $\zeta_w(s)$ is bounded by sk. However, it is also at least sk. Hence $\zeta_w(s) = sk$. □

Lemma 36. Let $w \in \Sigma^*$, $k = \iota(w)$. Let there be a word $y \in \Sigma^*$ and a letter $\mathtt{a} \in \Sigma$ such that $|\mathrm{alph}(y)| \leq \sigma - 2$ and such that $\mathtt{a}y\mathtt{a}$ is a factor of some conjugate v of w. If $\nabla\zeta_w(s) = k$ holds for all $s \in [1, \sigma - 1]$ then we have $\nabla\iota_w(s) = k$ for all $s \in \mathbb{N}$.

Proof. Because $\mathtt{a}y\mathtt{a}$ is a factor of v, there exist factors $x, z \in \Sigma^*$ such that $v = x\mathtt{a}y\mathtt{a}z$. Then $u = \mathtt{a}zx\mathtt{a}y$ is a conjugate of w, too. Now suppose that $\nabla\iota_w$ grew in the σ^{th} step by $k + 1$, i.e., $\nabla\iota_w(\sigma) = k + 1$. Then the same holds for the circular universality of u in at least

some step, i.e., $\nabla\zeta_u(t) = k+1$ for some $t \in \mathbb{N}$. This now implies by Lemma 11 that the same must hold for its plain universality, i.e., we have $\nabla\iota_u(t') = k+1$ for some $t' \in \mathbb{N}$. However, Proposition 34 states that any such growth must have already occurred in the interval $[1,\sigma]$, i.e., there is some $t'' \in [1,\sigma]$ with that property. But since by assumption $\nabla\zeta_w(s) = k$ for all $s \in [1,\sigma-1]$, the only possible value is $t'' = \sigma$. Thus far we have shown that $\nabla\iota_u(s) = k$ if $s \in [1,\sigma-1]$ and $\nabla\iota_u(s) = k+1$ if $s = \sigma$. The first case gives us by Lemma 26 the ascending chain $\mathcal{R}(u^0) \subseteq \ldots \subseteq \mathcal{R}(u^{\sigma-1})$ and the second case implies that this chain is strict. Then Lemma 31 is applicable, resulting in $|\mathcal{R}(u^s)| = s$ for all $s \in [1,\sigma-1]$. Now note that by Lemma 8 these arguments can be analogously applied to u^R as well. Consequently we can follow that $\left|\mathcal{R}((u^R)^s)\right| = s$ for all $s \in [1,\sigma-1]$. And so we have in particular $\left|\mathcal{R}(u^{\sigma-1})\right| = \sigma-1$ and $\left|\mathcal{R}(u^R)\right| = 1$. Therefore, since by assumption $|\mathrm{alph}(\mathtt{a}y)| \leq \sigma-1$, it follows from the construction of u that both $\mathtt{a} \in \mathcal{R}(u^{\sigma-1})$ and $\mathcal{R}(u^R) = \{\,\mathtt{a}\,\}$. However, this implies that $\mathrm{alph}(r(u^{\sigma-1})r(u^R)) = \mathcal{R}(u^{\sigma-1}) \neq \Sigma$ and hence we have $\nabla\iota_u(\sigma) = k$ by Corollary 14. This is a contradiction and so the supposition $\nabla\iota_w(\sigma) = k+1$ must be false. Thus we have $\nabla\iota_w(s) = k$ not only on the interval $[1,\sigma-1]$, but on $[1,\sigma]$. The claim follows by Proposition 34. □

Proposition 37. *Let $w \in \Sigma^*$. Then we have $\nabla\iota_w(s) = k$ for all $s \in \mathbb{N}$ if and only if $\nabla\zeta_w(s) = k$ for all $s \in [1,\sigma-1]$.*

Proof. First let $\nabla\zeta_w(s) = k$ for all $s \in [1,\sigma-1]$. If each letter occurs only once in each arch of w and at most once in the remainder $r(w)$, then the claim already follows by Lemma 35. So now assume that there exists some letter $\mathtt{a} \in \Sigma$ that occurs at least twice in an arch or the remainder of w. Since the last letter of an arch is unique this implies that the conditions of Lemma 36 are met. Then the claim follows. The other direction follows immediately by Lemma 11. □

With Proposition 37 we can finally achieve our first main goal of generalising Theorem 10 to alphabets of arbitrary size.

Theorem 38. *Let $w \in \Sigma^*$ with $k = \iota(w) > 0$ and let $s \in \mathbb{N}$.*
1. If $\zeta(w) = k+1$ then $\iota(w^s) = sk+s-1$.
2. If $\nabla\zeta_w(t) = k$ for all $t \in [1,\sigma-1]$ then $\iota(w^s) = sk$.

Proof. The claim follows by combining Theorem 9 and Proposition 37. □

Remark 39. Considering again $w = \prod_{i=1}^{\sigma} \mathtt{a}_i^2$ shows that the bound $\sigma-1$ in Proposition 37 is tight. The word $u = \mathtt{a}_1 \left[\prod_{i=2}^{n} \mathtt{a}_i^2\right] \mathtt{a}_1$ is a conjugate of w with $\nabla\iota_u(s) = 1$ for all $s \leq \sigma-2$ and $\nabla\iota_u(\sigma-1) = 2$. Thus, we have $\nabla\zeta_w(s) = 1$ for all $s \leq \sigma-2$ and $\nabla\zeta_w(\sigma-1) = 2$.

4.2 Descending Chains. Now, we discuss descending chains instead of ascending chains. We begin by searching for the longest strictly descending chain that is possible. The following lemma gives us a structural property about such a chain of length exactly σ and is symmetrical to Lemma 31.

Lemma 40. Let $w \in \Sigma^*$ and $\ell \in \mathbb{N}_0$. If $\mathcal{R}(w^\ell) \supsetneq \ldots \supsetneq \mathcal{R}(w^{\ell+\sigma-1})$ is a strictly descending chain of length σ then $\left|\mathcal{R}(w^{\ell+s})\right| = \sigma - 1 - s$ for all $s \in [0, \sigma-1]$.

Proof. The proof is symmetrical to the proof of Lemma 31. □

Analogously to Corollary 32, there cannot be a strictly descending chain of length $\sigma+1$. Surprisingly, such a chain of length σ leads to a contradiction as well. First, we present an auxiliary lemma.

Lemma 41. Let $w \in \Sigma^*$ and $\ell, n \in \mathbb{N}_0$. If $\mathcal{R}(w^\ell) \supsetneq \ldots \supsetneq \mathcal{R}(w^{\ell+\sigma-1})$ is a strictly descending chain of length σ then $\mathcal{R}(w) \supsetneq \ldots \supsetneq \mathcal{R}(w^\sigma)$ is one as well.

Proof. We can apply Lemma 40. It implies that $\mathcal{R}(w^\ell) = \sigma - 1$, and hence $\ell \neq 0$. It also implies that $s \mapsto \mathcal{R}(w^s)$ assumes σ different values on the interval $[\ell, \ell+\sigma-1]$, i.e., all possible values by Lemma 20. Therefore $\mathcal{R}(w^{\ell-1})$ is one of them, i.e., we have $\mathcal{R}(w^{\ell-1}) = \mathcal{R}(w^{\ell+m})$ for some $m \in [0, \sigma-1]$. However, by Corollary 14 their successors are also equal, i.e., $\mathcal{R}(w^\ell) = \mathcal{R}(w^{\ell+m+1})$. Hence, since the chain is strict, $m = \sigma - 1$ is the only possible value for m. Thus, since $\left|\mathcal{R}(w^{\ell+\sigma-1})\right| = 0$ by Lemma 40, it follows that $\mathcal{R}(w^{\ell-1}) = \emptyset$, and consequently $r(w^{\ell-1}) = \varepsilon = r(w^0)$. Then Lemma 17 implies that $r(w^s) = r(w^{\ell-1+s})$ for all $s \in \mathbb{N}_0$, and therefore $\mathcal{R}(w) \supsetneq \ldots \supsetneq \mathcal{R}(w^\sigma)$ is a strictly descending chain of length σ, too. □

Proposition 42. *Let $w \in \Sigma^*$ and $\ell, n \in \mathbb{N}_0$. If $\mathcal{R}(w^\ell) \supsetneq \ldots \supsetneq \mathcal{R}(w^{\ell+n-1})$ is a strictly descending chain of length n then $n \leq \sigma - 1$.*

Proof. The structure of this contradiction proof is the following: first we argue that one can assume $\ell = 1$. Second we argue that the conjugates of w obtained by cyclic shifts of whole arches give us strictly descending chains, too. Third we follow that each arch and the remainder end with the same letter. Last we show that this leads to a contradiction.

Suppose that $n > \sigma - 1$. Then in particular there is a strictly descending chain of length σ. By Lemma 41 we can assume w.l.o.g. that $\ell = 1$. So we have that $\mathcal{R}(w) \supsetneq \ldots \supsetneq \mathcal{R}(w^\sigma)$ is a strictly descending chain. Now let $j \in [0, k]$ and $w_j = \left[\prod_{i=j+1}^{k} \mathrm{ar}_i(w)\right] r(w) \left[\prod_{i=1}^{j} \mathrm{ar}_i(w)\right]$. In other words, w_j is a conjugate of w obtained by cyclic shifts of full arches of w and in particular $w_0 = w$. Then for all $s \in \mathbb{N}$ the arch factorisation $w_j^s = \left[\prod_{i=j+1}^{\iota(w^s)} \mathrm{ar}_i(w^s)\right] r(w^s) \left[\prod_{i=1}^{j} \mathrm{ar}_i(w^s)\right]$ contains at least $\iota(w^s)$ arches and thus $\iota(w_j^s) \geq \iota(w^s)$. Next, since $\mathcal{R}(w^\sigma)$ is empty by Lemma 40, it follows that $\nabla\iota_w(\sigma+1) = k$, and so by Theorem 9 we necessarily have $k = \zeta(w) \geq \iota(w_j)$. Hence by Remark 5, we get $\iota(w_j^s) \leq sk + s - 1$ for all $s \in \mathbb{N}$. However, because the chain is strict, Corollary 28 implies that $\nabla\iota_w(s) = k+1$ on the interval $[2, \sigma]$ and thus $\iota(w^s) = sk + s - 1$ for all $s \in [1, \sigma]$. Consequently we get for all $s \in [1, \sigma]$ that $\iota(w_j^s) \leq \iota(w^s)$. But moreover note that, since $r(w^\sigma) = \varepsilon$, we have $\iota(w_j^{\sigma+1}) = \iota(w^{\sigma+1})$ by definition of w_j. Thus far we have shown that $\iota(w_j^s) = \iota(w^s)$ for all $s \in [1, \sigma+1]$. This implies for all $s \in [2, \sigma]$ that $\nabla\iota(w_j^s) = k+1$ and $\nabla\iota(w_j^{\sigma+1}) = k$. By Corollary 28 we have that $\mathcal{R}(w_j) \supsetneq \ldots \supsetneq \mathcal{R}(w_j^\sigma)$ is also a strictly descending chain. We can apply Lemma 40 on this chain, too, and get

$\left|\mathcal{R}(w_j)\right| = \sigma - 1$ and $\left|\mathcal{R}(w_j^{\sigma-1})\right| = 1$. Since, moreover, $\nabla\iota(w_j^\sigma) = k+1$ by Corollary 14 implies $\mathrm{alph}(r(w_j^{\sigma-1})r(w_j^R)) = \Sigma$, $\left|\mathcal{R}(w_j^R)\right| = \sigma - 1$ and $\mathcal{R}(w_j^{\sigma-1}) \cap \mathcal{R}(w_j^R) = \emptyset$ follow. Next let $\mathtt{a}_j \in \mathcal{R}(w_j^{\sigma-1})$ be the letter that occurs in $r(w_j^{\sigma-1})$. Note that $\mathtt{a}_j$ is also the last letter of w_j. Then, since $\mathcal{R}(w_j^{\sigma-1})$ and $\mathcal{R}(w_j^R)$ are disjunct, we have $\mathtt{a}_j \notin \mathcal{R}(w_j^R)$. And so, since all letters of Σ except $\mathtt{a}_j$ occur in $r(w_j^R)^R$ and it is also a prefix of the first arch of w_j, i.e. , $\mathrm{ar}_1(w_j)$, the last letter of $\mathrm{ar}_1(w_j)$ has to be $\mathtt{a}_j$, because the last letter of an arch is unique. However, by construction of w_j we have that $\mathrm{ar}_1(w_j)$ is a suffix of w_{j+1} for all $j < k$. This implies that $\mathtt{a}_j$ is the last letter of w_{j+1} and hence $\mathtt{a}_j = \mathtt{a}_{j+1}$ for all $j < k$, and inductively we get $\mathtt{a}_j = \mathtt{a}_0$ for all $j \leq k$. In other words, every arch and also the remainder of w ends with the same letter $\mathtt{a}_0$. Now note that $w_k = r(w)\left[\prod_{i=1}^k \mathrm{ar}_i(w)\right]$. Then, since $r(w_k^R)^R$ and $r(w)$ are both prefixes of w_k and in both occur exactly $\sigma - 1$ different letters, we get $\mathcal{R}(w_k^R) = \mathcal{R}(w)$. But we have on the one hand $\mathtt{a}_0 \in \mathcal{R}(w)$, since $\mathtt{a}_0$ is the last letter of w, and on the other hand also $\mathtt{a}_0 \notin \mathcal{R}(w_k^R)$. This is a contradiction, i.e., $n \leq \sigma - 1$. □

Remark 43. The word $w = \mathtt{a}_\sigma \left[\prod_{i=1}^\sigma \mathtt{a}_i^2\right]^{\sigma-2} \left[\prod_{i=1}^{\sigma-1} \mathtt{a}_i\right]$ over $\Sigma = \{\, \mathtt{a}_1, \ldots, \mathtt{a}_\sigma \,\}$ witnesses that a strictly descending chain of length $\sigma - 1$ actually exists: we have $\iota(w) = \sigma - 1$ and $\nabla\iota_w(s) = \sigma$ for all $s \in [1, n-1]$ as well as $\nabla\iota_w(\sigma) = \sigma - 1$ and $\zeta(w) = \sigma - 1$. Furthermore, $\mathcal{R}(w) \supsetneq \ldots \supsetneq \mathcal{R}(w^{\sigma-1})$ is a strictly descending chain of length $\sigma - 1$.

With Proposition 42 we can achieve our second main goal: the following theorem is a reasonable modification of Theorem 9 such that its converse holds.

Theorem 44. *For $w \in \Sigma^*$ the following statements are equivalent:*
1. $\nabla\iota_w(s) = k+1$ for all $s \in [2, \sigma]$,
2. $\nabla\iota_w(s) = k+1$ for all $s \in \mathbb{N}_{\geq 2}$,
3. $\zeta(w) = k+1$.

Proof. Firstly, let $\nabla\iota_w(s) = k+1$ for all $s \in [2, \sigma]$. Then Lemma 26 gives us the descending chain $\mathcal{R}(w) \supseteq \ldots \supseteq \mathcal{R}(w^\sigma)$. By Lemma 32 this chain is not strict and thus, $\nabla\iota_w(s) = k+1$ for all $s \in \mathbb{N}_{\geq 2}$. This proves the first implication. Now let $\nabla\iota_w(s) = k+1$ for all $s \geq 2$. Then, again, the chain $\mathcal{R}(w) \supseteq \mathcal{R}(w^2) \supseteq \ldots$ is not strict. Hence the mapping $s \mapsto r(w^s)$ is eventually constant. Thus there exists $t \geq 2$ such that $r(w^t) = r(w^{t+1})$. Therefore, we have $r(r(w^t)w) = r(w^{t+1}) = r(w^t)$. Note that, since $\nabla\iota_w(t+1) = k+1$, we have $\iota(r(w^t)w) = k+1$. Since, moreover, removing the remainder does not change the universality of a word, $\iota(r(w^t) \cdot w \cdot r(w^t)^{-1}) = k+1$ follows. Because the word $r(w^t) \cdot w \cdot r(w^t)^{-1}$ is a conjugate of w, we have $\zeta(w) = k+1$. This proves the second implication. Finally, let $\zeta(w) = k+1$. Then Theorem 9 implies immediately that $\nabla\iota_w(s) = k+1$ for all $s \in [2, \sigma]$. □

Finally, Theorem 44 provides an algorithm to compute the circular universality of a word w in $\mathcal{O}(\sigma|w|)$, which is, if $\sigma < |w|$ holds, better than the naïve approach by computing $\iota(v)$ for every conjugate v of w.

Theorem 45. *Given a word $w \in \Sigma^*$, we can compute $\zeta(w)$ in time $\mathcal{O}(\sigma|w|)$.*

Proof. By [1, Proposition 10] we can compute $\iota(w^\sigma)$ in $\mathcal{O}(\sigma|w|)$. Let $k = \iota(w)$. If $\iota(w^\sigma) = \sigma k + \sigma - 1$, then $\zeta(w) = k + 1$, else $\zeta(w) = k$. □

5 Conclusion

The main goal of this work was to improve certain results from [1] on the connection between the universality of repetitions and the circular universality, namely Theorem 9 and Theorem 10.

At first we focused our investigation on repetitions. In Section 3 we showed that the growth of the universality of repetitions can be characterised by their remainders and that the growth is eventually periodic beginning its periodicity latest after σ repetitions. Thus, the universality of all other repetitions can be computed in constant time. In Section 4 we found that one can translate questions about the universality of repetitions into questions about ascending or descending chains of the remainders of those repetitions. The investigation of strictly ascending chains led to a tight bound on the length of the longest possible strictly ascending chain and the connection of such chains with the circular universality, gives the extension of Theorem 10 to alphabets of arbitrary size. On the other hand, on investigating strictly descending chains, we found a tight bound on the length of such chains, which is surprisingly one step shorter than the ascending equivalent. This lead to a modification of Theorem 9 such that its converse holds, too, and also to an efficient algorithm to compute the circular universality of a word.

It remains an interesting open problem to characterise the class of words, for which the remainder of some proper repetition is the empty word. We propose to call such words *perfect k-universal*. Furthermore, one could extend the study of k-universality from finite words to infinite words, e.g. one could study the universality of the sequence of finite prefixes of aperiodic infinite words.

References

[1] L. Barker, P. Fleischmann, K. Harwardt, F. Manea, and D. Nowotka. Scattered factor-universality of words. In *DLT 2020*, volume 12086 of *LNCS*, pages 14–28, 2020.

[2] F. Blanchet-Sadri. Algorithmic combinatorics on partial words. *Int. J. Found. Comput. Sci.*, 23(06):1189–1206, 2012.

[3] K. Bringmann and M. Künnemann. Multivariate fine-grained complexity of longest common subsequence. In *Proc. SODA 2018*, pages 1216–1235. SIAM, 2018.

[4] H.Z.Q. Chen, S. Kitaev, T. Mütze, and B.Y. Sun. On universal partial words. *Electronic Notes in Discrete Mathematics*, 61:231–237, 2017.

[5] J.D. Day, P. Fleischmann, M. Kosche, T. Koß, F. Manea, and S. Siemer. The edit distance to k-subsequence universality. In *STACS 2021*, volume 187, pages 25:1–25:19, 2021.

[6] J.D. Day, P. Fleischmann, F. Manea, and D. Nowotka. k-spectra of weakly-c-balanced words. In *DLT 2019*, pages 265–277, 2019.

[7] N.G. de Bruijn. A combinatorial problem. *Koninklijke Nederlandse Akademie v. Wetenschappen*, 49:758–764, 1946.

[8] C. H. Elzinga, S. Rahmann, and H. Wang. Algorithms for subsequence combinatorics. *Theor. Comput. Sci.*, 409(3):394–404, 2008.

[9] P. Gawrychowski, M. Kosche, T. Koß, F. Manea, and S. Siemer. Efficiently testing Simon's congruence. In *STACS 2021*, volume 187, pages 34:1–34:18, 2021.

[10] P. Gawrychowski, M. Lange, N. Rampersad, J.O. Shallit, and M. Szykula. Existential length universality. In *STACS 2020*, volume 154, pages 16:1–16:14, 2020.

[11] B. Goeckner, C. Groothuis, C. Hettle, B. Kell, P. Kirkpatrick, R. Kirsch, and R.W. Solava. Universal partial words over non-binary alphabets. *Theor. Comput. Sci*, 713:56–65, 2018.

[12] L. H. Haines. On free monoids partially ordered by embedding. *J. Comb. Theory, Series A*, 6:94–98, 1969.

[13] S. Halfon, P. Schnoebelen, and G. Zetzsche. Decidability, complexity, and expressiveness of first-order logic over the subword ordering. In *Proc. LICS 2017*, pages 1–12, 2017.

[14] J.-J. Hebrard. An algorithm for distinguishing efficiently bit-strings by their subsequences. *Theo. Comp. Sci.*, 82(1):35–49, 1991.

[15] G. Higman. Ordering by divisibility in abstract algebras. *Proceedings of the LMS*, s3-2(1):326–336, 1952.

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

[17] P. Karandikar and P. Schnoebelen. The height of piecewise-testable languages with applications in logical complexity. In *CSL 2016*, volume 62 of *LIPIcs*, pages 37:1–37:22, 2016.

[18] P. Karandikar and P. Schnoebelen. The height of piecewise-testable languages and the complexity of the logic of subwords. *Log. Methods Comput. Sci.*, 15(2), 2019.

[19] M. Krötzsch, T. Masopust, and M. Thomazo. Complexity of universality and related problems for partially ordered NFAs. *Inf. Comput.*, 255:177–192, 2017.

[20] D. Kuske and G. Zetzsche. Languages ordered by the subword order. In *Proc. FOSSACS 2019*, volume 11425, pages 348–364, 2019.

[21] M. Lothaire. *Combinatorics on Words*. Cambridge University Press, 1997.

[22] D. Maier. The complexity of some problems on subsequences and supersequences. *J. ACM*, 25(2):322–336, 1978.

[23] M.H. Martin. A problem in arrangements. *Bull. Amer. Math. Soc.*, 40(12):859–864, 12 1934.

[24] A. Mateescu, A. Salomaa, and S. Yu. Subword histories and Parikh matrices. *J. Comput. Syst. Sci.*, 68(1):1–21, 2004.

[25] N. Rampersad, J. Shallit, and Z. Xu. The computational complexity of universality problems for prefixes, suffixes, factors, and subwords of regular languages. *Fundam. Inf.*, 116(1-4):223–236, January 2012.

[26] A. Salomaa. Connections between subwords and certain matrix mappings. *Theor. Comput. Sci.*, 340(2):188–203, 2005.

[27] S. Seki. Absoluteness of subword inequality is undecidable. *Theor. Comput. Sci.*, 418:116–120, 2012.

[28] I. Simon. Piecewise testable events. In *Automata Theory and Formal Languages*, pages 214–222, 1975.

[29] R.A. Wagner and M.J. Fischer. The string-to-string correction problem. *J. ACM*, 21(1):168–173, 1974.

[30] G. Zetzsche. The complexity of downward closure comparisons. In *Proc. ICALP 2016*, volume 55 of *LIPIcs*, pages 123:1–123:14, 2016.

Abelian Nivat's conjecture for non-rectangular patterns Extended abstract

Nikolai Geravker and Svetlana Puzynina

Saint-Petersburg State University

Abstract

In this paper, we study the relation between periodicity of two-dimensional words and their abelian pattern complexity. A pattern $\mathcal{P}$ in $\mathbb{Z}^n$ is the set of all translations of some finite subset F of $\mathbb{Z}^n$. An F-factor of an infinite word is a finite word restricted to F. Then the pattern complexity over a pattern $\mathcal{P}$ counts the number of distinct F-factors of an infinite word. Two finite words are called abelian equivalent if for each letter of the alphabet, they contain the same numbers of occurrences of this letter. The abelian pattern complexity counts the number of F-factors up to abelian equivalence. As the main result of the paper, we characterize two-dimensional convex patterns with the following property: if abelian pattern complexity over a pattern $\mathcal{P}$ is equal to 1, then the word is fully periodic. Similar result holds for a function on $\mathbb{Z}^2$ instead of a word and for constant sums instead of abelian complexity equal to 1. In dimensional 1, we get a necessary condition for patterns for which there exist non-constant functions with constant sums.

1 Introduction

One of the most studied topics in combinatorics on words is complexity of infinite words, both in the one-dimensional and in the multidimensional case. First steps in complexity theory of words were made by Morse and Hedlund in 1938. They introduced the notion of a complexity of an infinite word as a function $p(n)$ which counts, for each integer n, the number of its distinct factors (i.e., blocks of consecutive letters) of length n. They proved that if for an infinite word its complexity function is bounded, then the word is periodic [11]:

Theorem 1 (Morse, Hedlund, 1938)**.** *Let* $\mathbf{w}$ *be a one-dimensional infinite word. Then the following statements are equivalent:*

- $\mathbf{w}$ *is periodic;*
- *there exists* n *such that* $p_{\mathbf{w}}(n) \leqslant n$*;*
- *there exist* n_0 *and* C *such that* $p_{\mathbf{w}}(n) \leqslant C$ *for all* $n \geqslant n_0$*;*

Nivat's conjecture [12] is a generalization of Theorem 1 to two dimensions. A two-dimensional word $\mathbf{w}$ is an element of $A^{\mathbb{Z}^2}$, where A is a finite set called an alphabet. A word $\mathbf{w}$ is called *periodic* if there exist a vector $p \in \mathbb{Z}^2$ such that $\mathbf{w}(x) = \mathbf{w}(x+p)$ for all $x \in \mathbb{Z}^2$. A complexity of a two-dimensional word $\mathbf{w}$ is a function $p_{\mathbf{w}}(m,n)$ counting for each $m,n \in \mathbb{N}$ the number of distinct rectangular $m \times n$ blocks.

Conjecture 1 (Nivat, 1997)**.** *Let* $\mathbf{w}$ *be a two-dimensional word. If there exists* m,n *such that* $p_{\mathbf{w}}(m,n) \leqslant mn$ *then* $\mathbf{w}$ *is periodic.*

Nivat's conjecture remains open despite of efforts of different scientists. It has been proven is some weak forms, for example, in an asymptotic form by Kari, Szabados [9]. In a series of papers, it was shown that $p_{\mathbf{w}}(m,n) \leqslant mn/C$ is enough to guarantee the periodicity of $\mathbf{w}$, with the biggest constant $C = 2$ [3]. Some versions of Nivat's conjecture and minimal complexity in two or more dimensions were studied in [1, 2, 4, 8].

The main objective of this paper is finding generalizations of Theorem 1 and Conjecture 1 for abelian pattern complexity. We recall that two words u and v in A^* are said to be *abelian equivalent*, denoted by $u \sim_{ab} v$, if and only if the numbers of occurrences of each letter are the same in both words. The *abelian complexity* $a_{\mathbf{w}}(n)$ of a (one-dimensional) word $\mathbf{w}$ is the function counting number of distinct abelian classes of factors of length n [15, 16]. This definition can be extended to two or more dimensions.

For one-dimensional words an abelian analogue of Theorem 1 is straightforward: clearly, the condition $a_{\mathbf{w}}(n) = 1$ implies that $\mathbf{w}$ is n-periodic. For two-dimensional words, the abelian modifications of Nivat's conjecture have been studied in [13]. It was shown that there exists an aperiodic word $\mathbf{w}$ and integers m and n such that $a_{\mathbf{w}}(m,n) = 1$. However, for an aperiodic recurrent two-dimensional word $\mathbf{w}$ there exist infinitely many pairs of numbers m,n such that $a_{\mathbf{w}}(m,n) \geqslant 3$.

A related concept of maximal pattern complexity has been introduced by Kamae and Zamboni in 2002 [7]. A pattern $\mathcal{P}$ can be defined as a finite subset of integers $\{i_1, \ldots, i_k\}$, taken up to a shift. A pattern complexity of a word $\mathbf{w}$ over this pattern is the number of distinct subwords of the form $\mathbf{w}_{n+i_1} \ldots \mathbf{w}_{n+i_k}$, with $n \in \mathbb{N}$. The maximal pattern complexity $p^*_{\mathbf{w}}(k)$ of a word $\mathbf{w}$ is defined as a function counting, for each k, the supremum of the pattern complexities for patterns defined by sets of size k. Similarly to factor complexity and abelian complexity, the maximal pattern complexity also gives a characterization of periodicity in the one-dimensional case: An infinite one-dimensional word $\mathbf{w}$ is eventually periodic if and only if $p^*_{\mathbf{w}}(k) < 2k$ for some integer k [7]. The abelian pattern complexity also gives a characterization of aperiodicity in terms of so-called aperiodicity by projection [5, 6].

In this paper, we are interested in a related concept of pattern complexity, when we fix the pattern instead of taking the maximum among all patterns of a given size. The main problem we study is the following: find a characterization of patterns such that for each word $\mathbf{w}$ the condition $a_{\mathbf{w}}(\mathcal{P}) = 1$ implies that $\mathbf{w}$ is a periodic word. We call such patterns *abelian rigid*. We also consider a variant of this problem when instead of a word we consider a function with finitely many values, and instead of unary abelian pattern complexity we consider constant sums in the figures of the pattern. Clearly,

such a function can also be considered as a word with letters corresponding to values of the function, and if we prove under certain conditions periodicity of all functions with finitely many values, the periodicity of words in these conditions follows immediately. In dimension 1, it is easy to see that all patterns are abelian rigid. We then find a necessary condition on a pattern for existence of non-unary words with abelian pattern complexity 1 over this pattern. This is generalized to a necessary and sufficient condition for functions. As the main result, we characterize abelian rigid convex patterns for two-dimensional words.

2 Definitions and notation

In the paper, we mostly follow the usual terminology of combinatorics on words from [10]. Let A be a finite set and n be an integer. A function from $\mathbb{Z}^n$ to A is called an *n-dimensional word on the alphabet A*. The elements of A are called *letters*.

Let $\mathbf{w}$ be an n-dimensional word and u be a vector in $\mathbb{Z}^n$. If $\mathbf{w}(x) = \mathbf{w}(x+u)$ for any $x \in \mathbb{Z}^n$, then $\mathbf{w}$ is called *u-periodic*. A word is *periodic* if there exists a vector u such that the word u-periodic. A word is *fully periodic* if there exist n linearly independent vectors $u_1, u_2, \ldots, u_n \in \mathbb{Z}^n$ such that the word is u_i-periodic for all $i = 1, 2, \ldots n$.

Let $\mathbf{w}$ be an n-dimensional word. Its *complexity* is defined as a function $p_{\mathbf{w}} : \mathbb{N}^d \to \mathbb{N}$ counting for each $(n_1, \ldots, n_d)$ the number of distinct $n_1 \times \cdots \times n_d$-blocks (or factors) of $\mathbf{w}$. Similarly, its *abelian complexity* is defined as a function counting the number of abelian classes of $n_1 \times \cdots \times n_d$-factors of $\mathbf{w}$.

A finite subset of $\mathbb{Z}^n$ is called *a figure of* $\mathbb{Z}^n$. Let F_1 and F_2 be figures of $\mathbb{Z}^n$. If there exists a translation τ such that $\tau(F_1) = F_2$, then we say that F_1 and F_2 are *equivalent* and write $F_1 \sim F_2$. An equivalence class under $\sim$ is called a *pattern*.

Let F be a figure of $\mathbb{Z}^n$. A *figure with weights* F^w in $\mathbb{Z}^n$ is a finite set of pairs $\{(u, g_u) | u \in \mathbb{Z}^n; g_u \in \mathbb{Z}\}$, where the integer g_u is called the weight of a point u. Let F_1^w and F_2^w be figures with weights in $\mathbb{Z}^n$. If there exists a translation τ such that

$$F_2^w = \{(\tau(u), g_u) | (u, g_u) \in F_1^w\},$$

then we say that F_1^w and F_2^w are *equivalent* and write $F_1^w \sim_g F_2^w$. An equivalence class under $\sim_g$ is called *a pattern with weights*.

Definition 1. *Let $\mathcal{P}$ be a pattern with weights in the n-dimensional space and $F_{\mathcal{P}}$ be the figure of $\mathcal{P}$ such that for each $i \in 1, 2, \ldots, n$ the minimal i'th coordinate of the points of $F_{\mathcal{P}}$ is equal to 0. The figure $F_{\mathcal{P}}$ is called* the canonical figure *of the pattern $\mathcal{P}$.*

The *polynomial of a pattern $\mathcal{P}$* is defined by

$$Poly_{\mathcal{P}}(x) = \sum_{(t, g_t) \in F_{\mathcal{P}}} g_t x^t,$$

where $x^t = x_1^{t_1} x_2^{t_2} \cdots x_n^{t_n}$.

A natural generalization of the notion of a complexity is the pattern complexity. Let $F^w = \{(u_1, g_1), \ldots, (u_l, g_l)\}$ be a figure with weights, and $A = \{a_1, a_2, \ldots, a_k\}$ be an alphabet. We can consider the ring $\mathbb{Z}[a_1, a_2, \ldots, a_k]$ of linear combinations over variables from A. A linear polynomial

$$\sum_{i=1}^{l} \mathbf{w}(u_i) g_i \in \mathbb{Z}[a_1, a_2 \ldots a_k]$$

is called a *linear combination of the word* $\mathbf{w}$ *over* F^w and is denoted by $H^{\mathbf{w}}_{F^w}$. We say that $H^{\mathbf{w}}_{F^w}$ is a $\mathcal{P}$*-linear combination* if F^w belongs to the pattern (with weights) $\mathcal{P}$. Essentially, the $\mathcal{P}$-linear combination gives the sum of the elements from F with their weights.

The *abelian pattern complexity* $a_{\mathbf{w}}(\mathcal{P})$ of $\mathbf{w}$ is the function counting the number of distinct $\mathcal{P}$-linear combinations of $\mathbf{w}$. If all the weights are equal to 1, then we have the abelian pattern complexity counting the number of abelian equivalence classes of $\mathcal{P}$-factors, i.e., factors of $\mathbf{w}$ restricted to figures from $\mathcal{P}$. When we have weights, the occurrences of each letter are counted with corresponding multiplicities (which could also be negative).

Definition 2. *A pattern* $\mathcal{P}$ *is called* abelian rigid *if* $a_{\mathbf{w}}(\mathcal{P}) = 1$ *only for fully periodic words* $\mathbf{w}$.

The main problem we are interested in is the characterization of abelian rigid patterns.

3 Results

In the paper, we obtain a classification of abelian rigid patterns with weights on the line and classification of abelian rigid convex patterns on the plane. Also, in the one-dimensional case, we give a necessary condition on a pattern $\mathcal{P}$ for existence of a non-unary word with pattern abelian complexity over $\mathcal{P}$ equal to 1 in terms of cyclotomic polynomials.

3.1 One-dimensional space

In this subsection, all words are one-dimensional. First we remark that in the one-dimensional case, all patterns are abelian rigid:

Proposition 1. *If* $a_{\mathbf{w}}(\mathcal{P}) = 1$ *for some one-dimensional pattern* $\mathcal{P}$ *with weights, then* $\mathbf{w}$ *is periodic.*

The same statement can be also made for functions with finitely many values and for patterns with weights.

We recall that the n'th cyclotomic polynomial is defined by

$$\Phi_n(x) = \prod_{1 \leqslant k \leqslant n; (k,n)=1} (x - e^{2\pi i \frac{k}{n}}).$$

Theorem 2. *Let $\mathcal{P}$ be a pattern with weights, and let the alphabet A be a finite subset of complex numbers. Then there exists a non-zero word* $\mathbf{w}$ *such that*

$$\sum_{x \in F} \mathbf{w}(x) g_x = 0 \text{ for all } F \in \mathcal{P} \tag{1}$$

if and only if there exists n such that $Poly_{\mathcal{P}}(x)$ is divisible by $\Phi_n(x)$ in the ring $\mathbb{Q}[x]$.

As a corollary, we get a necessary condition for a pattern for existence of non-constant words with abelian complexity equal to 1.

Corollary 1. *If $\mathcal{P}$ is a one-dimensional pattern $\mathcal{P}$ with weights such that $a_{\mathbf{w}}(\mathcal{P}) = 1$ for some non-constant word* $\mathbf{w}$*, then there exists an integer n such that $Poly_{\mathcal{P}}(x)$ is divisible by $\Phi_n(x)$ in the ring $\mathbb{Q}[x]$.*

This condition is not sufficient. For example, for a pattern corresponding to $\Phi_6 = x^2 - x + 1$ there is no non-constant word with abelian complexity equal to 1 over this pattern. To see it, it is enough to check words up to length 4.

3.2 Two-dimensional space

Throughout this subsection $\mathbf{w}$ denotes a two-dimensional word.

Definition 3. *A figure F (without weights) is called* convex *if $F = conv_{\mathbb{R}^2}(F) \cap \mathbb{Z}^2$, where $conv_{\mathbb{R}^2}(F)$ is the convex hull of the set F in the two-dimensional Euclidean space. A pattern $\mathcal{P}$ is called* convex *if all figures of this pattern are convex.*

Let $v \in \mathbb{Z}^2$ be a vector and n be a natural number. The polynomial of the form $l(v, n) = \sum_{i=0}^{n} x^{iv}$ is called *strongly linear*.

The following theorem is the main result in the two-dimensional case.

Theorem 3. *Let $\mathcal{P}$ be a convex pattern. Then $Poly_{\mathcal{P}}$ has a non-trivial strongly linear divisor if and only if $\mathcal{P}$ is not abelian rigid.*

Moreover, both directions of the theorem hold in a stronger form. In fact, we proved that a strongly linear divisor implies the existence of aperiodic words also for arbitrary patterns with weights. The reversed direction holds not only for words, but also for integer-valued functions with constant sums.

The proof of existence of a non-periodic word is fairly easy by construction. The hard part was the proof of abelian rigidity. Here we used a more involved version of a method of R-prolongable words used e.g. in [14] for particular shapes.

Also, we can reformulate Theorem 3 in terms of *relatively prime* patterns. Let u be an integer vector and $\mathcal{P}$ be a convex pattern. If a line parallel to u intersects the pattern in several integer points, the number of such points is called the length of the intersection. Now consider all lines that are parallel to the vector u and intersect some figure of $\mathcal{P}$ (say, the canonical one). If the greatest common divisor of the lengths of the intersections of the set of such lines is equal to 1, then the pattern $\mathcal{P}$ is called u-relatively

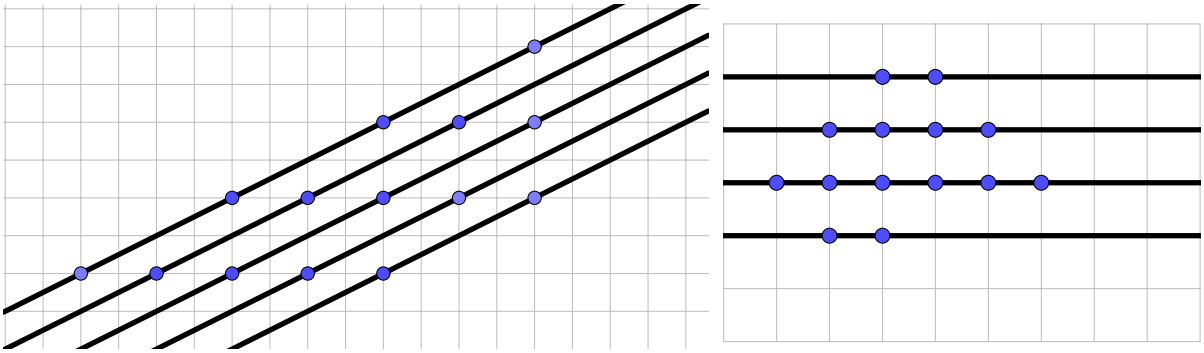

Figure 1: Example of $(2,1)$-relatively prime (on the left) and not relatively prime (not $(1,0)$-relatively prime) pattern (on the right)

prime. It is called *relatively prime* if $\mathcal{P}$ is u-relatively prime for each vector u. On Fig. 3.2 one can see an example of a relatively prime pattern and an example of non-relatively prime pattern. It is not hard to see that for a pattern being non-relatively prime is equivalent to the condition of divisibility by a strongly linear divisor. So, Theorem 3 is equivalent to the following theorem.

Theorem 4. *Let $\mathcal{P}$ be a convex pattern. Then $\mathcal{P}$ is relatively prime if and only if $\mathcal{P}$ is abelian rigid.*

4 Conclusions and future research

In this extended abstract, we consider patterns for which abelian complexity is equal to 1 only for fully periodic words. In the two-dimensional case we found a characterization of convex patterns $\mathcal{P}$ satisfying this condition (Theorem 3). An interesting problem is finding a generalization of this characterization for non-convex patterns, i.e., characterizing patterns $\mathcal{P}$ such that abelian pattern complexity for these pattern equals 1 only for periodic words. The same question is open in dimensions bigger than 2.

5 Acknowledgements

This research is supported by the Foundation for the Advancement of Theoretical Physics and Mathematics “BASIS”.

References

[1] J. Cassaigne: Double Sequences with Complexity $mn + 1$. Journal of Automata, Languages and Combinatorics 4 (1999): 153–170.

[2] J. Cassaigne: Subword complexity and periodicity in two or more dimensions. Developments in Language Theory 1999: 14–21.

[3] V. Cyr, B. Kra: Nonexpansive $\mathbb{Z}^2$-subdynamics and Nivat's conjecture. Trans. Amer. Math. Soc. 367 (2015), 6487–6537.

[4] F. Durand, M. Rigo: Multidimensional extension of the Morse-Hedlund theorem. European Journal of Combinatorics 34(2), 2011.

[5] T. Kamae, H. Rao, Yu-M. Xue, Maximal pattern complexity of two-dimensional words, Theoretical Computer Science, Volume 359, Issue 114, 2006, pp. 15–27.

[6] T. Kamae, S. Widmer and L. Q. Zamboni: Abelian maximal pattern complexity of words. Ergodic Theory and Dynamical Systems 35 (2015): 142–151.

[7] T. Kamae and L.Q. Zamboni, Sequence entropy and the maximal pattern complexity of infinite words, Ergod. Th. & Dynam. Sys. 22 (2002), 1191–1199.

[8] J. Kari, E. Moutot: Decidability and Periodicity of Low Complexity Tilings. STACS 2020: 14:1–14:12

[9] J. Kari, M. Szabados: An algebraic geometric approach to Nivat's conjecture. Information and Computation, Volume 271, April 2020, 104481

[10] M. Lothaire: Algebraic combinatorics on words. Cambridge University Press, 2002.

[11] M. Morse, G. Hedlund: Symbolic dynamics. Amer. J. Math. 60 (1938), 815–866.

[12] M. Nivat: Invited talk at ICALP'97.

[13] S. A. Puzynina: Aperiodic Two-Dimensional Words of Small Abelian Complexity. Electron. J. Comb. 26(4): P4.15 (2019)

[14] S. A. Puzynina, Sergey V. Avgustinovich: On periodicity of two-dimensional words. Theor. Comput. Sci. 391(1-2): 178-187 (2008)

[15] G. Richomme, K. Saari, L. Q. Zamboni: Abelian complexity of minimal subshifts. J. London Math. Society 83 (2011), 79–95.

[16] A. Saarela: Ultimately Constant Abelian Complexity of Infinite Words. Journal of Automata, Languages and Combinatorics 14 (2009), 255–258.

On Vertices that are in Every Metric Basis of a Unicyclic Graph

Anni Hakanen[1], Ville Junnila[1], Tero Laihonen[1], and Ismael G. Yero[2]

[1]Department of Mathematics and Statistics, University of Turku, Finland
[2]Department of Mathematics, Universidad de Cádiz, Spain

All the graphs considered in this extended abstract are simple, undirected and connected. For a given graph G, the distance $d(u, v)$ between two vertices $u, v \in V(G)$ is the length of a shortest path between u and v. A set of vertices $R \subseteq V(G)$ is called a *resolving set* for G if for any pair of distinct vertices $u, v \in V(G)$, there exists a vertex $w \in R$ such that $d(w, u) \neq d(w, v)$. The cardinality of the smallest possible resolving set for G is the *metric dimension* of G, denoted by $\dim(G)$. A resolving set of cardinality $\dim(G)$ is a *metric basis* of G. Such concepts were (independently) introduced in [3] and [2].

It is natural to ask if a graph has vertices belonging to every metric basis. It was shown in [1], that for every integers k, r with $k \geq 2$ and $0 \leq r \leq k$, there exists a graph G with metric dimension k having r vertices that belong to every metric basis of G.

Definition 1. A vertex $v \in V(G)$ is a *basis forced vertex* of the graph G if it is contained in every metric basis of G.

Clearly, all graphs do not have basis forced vertices. Considering basis forced vertices we can show the following result.

Theorem 2. *Any finite graph has a metric basis that does not contain any cut-vertices.*

The graph has to be finite for Theorem 2 to hold. For example, the bi-infinite path consists of only cut-vertices, and thus any resolving set contains only cut-vertices.

The number of basis forced vertices in a graph is bounded by the following theorem.

Theorem 3. *If G is a graph with n vertices and $k > 0$ basis forced vertices, then $k \leq n - \dim(G) - 1$. Moreover, we have $k \leq \frac{n-1}{2}$.*

If we want to construct connected graphs with, say, k basis forced vertices and as few edges as possible, then the following construction will be useful. Notice that P_n denotes a path on n vertices.

Theorem 4. *Let G_i be connected graphs such that $G_i \not\simeq P_n$ for $i = 1, \ldots, k$, and let all G_i be vertex disjoint. Let g_i be a fixed element of $V(G_i)$ such that g_i is in some metric basis of G_i. Let W be the graph with*

$$V(W) = \bigcup_{i=1}^{k} V(G_i) \quad \text{and} \quad E(W) = \{\{g_i, g_j\} \mid i \neq j\} \cup \bigcup_{i=1}^{k} E(G_i),$$

i.e. the graph we obtain by connecting every g_i with one another. A set $R \subseteq V(W)$ is a metric basis of W if and only if

$$R = \bigcup_{i=1}^{k} R_i \setminus \{g_i\}$$

where R_i is a metric basis of G_i that contains g_i for each $i = 1, \ldots, k$. Consequently,

$$\dim(W) = \sum_{i=1}^{k} \dim(G_i) - k.$$

Unicyclic graphs are good candidates for the graphs G_i above. We have the following result.

Theorem 5. *If G is a unicyclic graph, then it can have at most 2 basis forced vertices.*

We have found unicyclic graphs with just one basis forced vertex in addition to unicyclic graphs with two basis forced vertices.

Acknowledgements

Ismael G. Yero has been partially supported by the Spanish Ministry of Science and Innovation through the grant PID2019-105824GB-I00. Tero Laihonen has been partially supported by the Academy of Finland through the grant 338797.

References

[1] P. S. Buczkowski, G. Chartrand, C. Poisson, and P. Zhang. On k-dimensional graphs and their bases. *Period. Math. Hung.*, 46(1):9–15, 2003. doi: 10.1023/A:1025745406160.

[2] F. Harary and R. Melter. On the metric dimension of a graph. *Ars Comb.*, 2:191–195, 1976.

[3] 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.

Local identifying and local locating-dominating codes in graphs

Pyry Herva and Tero Laihonen*

Department of Mathematics and Statistics, University of Turku, Finland
pysahe@utu.fi and terolai@utu.fi

1 Introduction and preliminaries

Let $G = (V, E)$ be a simple, connected and undirected graph with vertex set V and edge set $E \subseteq \{\{u, v\} \mid u, v \in V, u \neq v\}$. The (graphic) *distance* $d(u, v)$ of two vertices $u, v \in V$ of G is the number of edges in some shortest path between u and v.

We call any non-empty subset $C \subseteq V$ of vertices of a graph $G = (V, E)$ a *code* (in the graph G). The elements of C are called *codewords* and the elements of $V \setminus C$ are called *non-codewords*. If there is a codeword of C of distance at most r from any vertex of G then C is an *r-covering code*. The *r-identifying set* $I_{C,r}(u)$ of vertex $u \in V$ with respect to a code C is defined as

$$I_{C,r}(u) = B_r(u) \cap C$$

where $B_r(u) = \{v \in V \mid d(v, u) \leq r\}$ is the ball of radius r centered at u. If C or r are known from the context we may just write $I(u) = I_C(u) = I_r(u) = I_{C,r}(u)$. Note that C is an r-covering code if and only if $I_{C,r}(u) \neq \emptyset$ for every $u \in V$.

We say that an r-covering code $C \subseteq V$ is an *r-identifying code* if the r-identifying sets are unique for every vertex of G, i.e., if for every $u, v \in V, u \neq v$ we have $I_{C,r}(u) \neq I_{C,r}(v)$. An r-covering code $C \subseteq V$ is an *r-locating-dominating code* if the r-identifying sets are unique for every non-codeword vertex of G, i.e., if for every $u, v \in V \setminus C, u \neq v$ we have $I_{C,r}(u) \neq I_{C,r}(v)$. The concept of identifying codes was introduced by Karpovsky, Chakrabarty and Levitin in [11] in 1998 and the concept of locating-dominating codes was introduced by Slater in [14, 15] in 1980's. Since their discovery these classes (and many related classes) of codes have been extensively studied in different graphs over the years. See the website [13] for a comprehensive list of references around the topic.

We introduce two new classes of covering codes derived from identifying and locating-dominating codes and some results concerning them (see also [7]). A related concept in

*Research supported by the Academy of Finland grant 338797

the context of local metric dimensions has been considered, see e.g. [12]. Two different vertices of $G = (V, E)$ are *neighbours* or *adjacent* if there is an edge between them, that is, if their distance is 1. We say that an r-covering code C is a *local r-identifying code* if $I_{C,r}(u) \neq I_{C,r}(v)$ for all neighbours $u, v \in V$. An r-covering code C is a *local r-locating-dominating code* if $I_{C,r}(u) \neq I_{C,r}(v)$ for all neighbours $u, v \in V \setminus C$. There is an hierarchy between introduced classes of codes: They are all covering codes, locating-dominating and local identifying codes are both local locating-dominating codes, and identifying codes are locating-dominating codes and also local identifying codes. Depending on the graph these inclusions may or may not be strict. For example, it is quite easy to see that in paths (finite or infinite) and in sufficiently large cycles the classes of identifying and local identifying codes are the same.

We say that a code in a certain class of covering codes in a finite graph is *optimal* if its size is the smallest among every code in the class. We also consider optimality with respect to densities in certain infinite graphs (for the definitions of the densities see Section 3). We will study the sizes of optimal local 1-identifying codes in binary hypercubes and the densities of optimal local 1-identifying and local 1-locating-dominating codes in some infinite grids. In some cases we obtain precise results but in most of the cases we prove a lower bound for the size (or density) of an optimal code in the graph in consideration.

Important concept in finding lower bounds for sizes of optimal codes is the concept of *share* introduced by Slater in [16]. Let C be an r-covering code in graph G. The (r-)share $s(c) = s_r(c)$ of a codeword $c \in C$ is defined as

$$s(c) = \sum_{u \in B_r(c)} \frac{1}{|I_{C,r}(u)|}$$

which is well defined since C is an r-covering code.

Lemma 1. *Let C be an r-covering in a finite graph $G = (V, E)$. If $s(c) \leq \alpha$ for every $c \in C$ then*

$$|C| \geq \frac{|V|}{\alpha}.$$

Thus an upper bound for the share of an arbitrary codeword provides a lower bound for the size of the code. We have a similar lemma for shares and densities in some infinite graphs which we will discuss in Section 3.

Finally, we say that a graph G is *triangle-free* if it does not contain any triangles, i.e., if it does not contain any 3-cycles as induced subgraphs. It is easy to see that a code in a triangle-free graph is a local 1-locating-dominating code if and only if it is a 1-covering code.

2 Local 1-identifying codes in binary hypercubes

Let us denote by $\mathbb{F} = \{0, 1\}$ the binary field and let $n \geq 1$ be an integer. The set of length n binary words is denoted by $\mathbb{F}^n$ as usual. The *Hamming distance* $d_H(\mathbf{x}, \mathbf{y})$

of two binary words $\mathbf{x}, \mathbf{y} \in \mathbb{F}^n$ is the number of coordinates in which they differ. The *binary n-dimensional hypercube* or the *binary n-dimensional Hamming space* is the graph $G = (V, E)$ where $V = \mathbb{F}^n$ and $E = \{\{\mathbf{x}, \mathbf{y}\} \mid d_H(\mathbf{x}, \mathbf{y}) = 1\}$, i.e., two binary words are adjacent in the binary hypercube if and only if their Hamming distance is 1. In fact it is easy to see that the Hamming distance between two binary words is the same as their graphic distance in the binary hypercube. Thus from now on by $\mathbb{F}^n$ we mean the graph.

We will study local 1-identifying codes in binary hypercubes which we will from now on call simply local identifying codes. Let us denote by $M^L(n)$ the cardinality of an optimal local identifying code and by $M(n)$ the cardinality of an optimal identifying code in the n-dimensional binary hypercube. Even though there have been much research concerning identifying codes in binary hypercubes the exact value of $M(n)$ is known only for $2 \leq n \leq 7$. These known values of $M(n)$ are listed in Table 1. Note that $M(1)$ and $M^L(1)$ are not defined since there are no identifying or local identifying codes in the binary 1-dimensional hypercube $\mathbb{F}$.

Before stating general bounds for numbers $M^L(n)$ let us mention some lemmas which are useful in many constructions. The *direct sum* of two codes $C_1 \subseteq \mathbb{F}^n$ and $C_2 \subseteq \mathbb{F}^m$ is the code

$$C_1 \oplus C_2 = \{(\mathbf{c}_1, \mathbf{c}_2) \in \mathbb{F}^{n+m} \mid \mathbf{c}_1 \in C_1, \mathbf{c}_2 \in C_2\} \subseteq \mathbb{F}^{n+m}.$$

The following two lemmas have analogous counterparts in the context of identifying codes. Also the proofs are very similar.

Lemma 2. *Let $C \subseteq \mathbb{F}^n$ be a local identifying code. Then the code $C' = \mathbb{F} \oplus C \subseteq \mathbb{F}^{n+1}$ is a local identifying code if and only if $|I(\mathbf{c})| \geq 2$ for every $\mathbf{c} \in C$.*

Lemma 3. *Let $C \subseteq \mathbb{F}^n$ be a local identifying code. Then the code $\mathbb{F}^2 \oplus C \subseteq \mathbb{F}^{n+2}$ is a local identifying code too and hence $M^L(n+2) \leq 4M^L(n)$.*

Next two lemmas give some sufficient conditions for a code to be a local identifying code.

Lemma 4. *Let $C \subseteq \mathbb{F}^n$ be a code such that $|I(\mathbf{c})| \geq 3$ for every $\mathbf{c} \in C$ and $|I(\mathbf{x})| \geq 1$ for every $\mathbf{x} \in \mathbb{F}^n \setminus C$. Then C is a local identifying code.*

Lemma 5. *Let $C \subseteq \mathbb{F}^n$ be a code such that $|I(\mathbf{c})| = 1$ for every $\mathbf{c} \in C$ and $|I(\mathbf{x})| \geq 2$ for every $\mathbf{x} \in \mathbb{F}^n \setminus C$. Then C is a local identifying code.*

By proving an upper bound for the share of an arbitrary codeword of an arbitrary local identifying code we are able to prove the following theorem which provides a lower bound for $M^L(n)$ for every $n \geq 3$.

Theorem 6. *For every $n \geq 3$*

$$M^L(n) \geq \frac{3 \cdot 2^n}{3n - 2}.$$

For comparison we have

$$M(n) \geq \frac{n \cdot 2^n}{1 + n + \binom{n}{2}} = \frac{n \cdot 2^{n+1}}{2 + n(n+1)}$$

n	$M(n)$	$M^L(n)$
2	3	2
3	4	4
4	7	6
5	10	8
6	19	12 - 16
7	32	21 - 32

Table 1: Known values of $M(n)$ (see [2] for references) and our contributions concerning the values of $M^L(n)$ for $n \in [2, 7]$.

stated and proved in [11]. By general constructions we obtain the following upper bounds for $M^L(n)$.

Theorem 7. *Let $m \geq 3$ and $n = 2^m - 2$. Then*

$$M^L(n) \leq 2^{2^m - m - 1}.$$

Theorem 8. *Let $m, k \geq 2$ and $n = 2^m + k - 1$. Then*

$$M^L(n) \leq 2^{2^m + k - m - 1}.$$

We see that in binary hypercubes the optimal local identifying codes are (at least in some cases) much smaller than the optimal identifying codes. For example by Theorems 6 and 8 we are able to conclude that $M^L(9) \in \{62, 63, 64\}$ while $M(9) \in \{101, \ldots, 112\}$ ([11, 2]). More generally we see that for arbitrarily large $n = 2^m + k - 1$ where k is "small" the upper bound of Theorem 8 is close to the lower bound of Theorem 6. This means that the lower bound is quite good and cannot be significantly improved.

3 Local 1-identifying and local 1-locating-dominating codes in infinite grids

By an infinite grid we mean a graph with vertex set $\mathbb{Z}^2$. We study local 1-identifying and local 1-locating-dominating codes – which we from now on call simply local identifying and local locating-dominating codes – in four different grids which we will define next.

- *Square grid* is the graph $\mathcal{S} = (\mathbb{Z}^2, E_{\mathcal{S}})$ where

$$E_{\mathcal{S}} = \{\{\mathbf{u}, \mathbf{v}\} \mid \mathbf{u} - \mathbf{v} \in \{(\pm 1, 0), (0, \pm 1)\}\}.$$

- *Hexagonal grid* is the graph $\mathcal{H} = (\mathbb{Z}^2, E_{\mathcal{H}})$ where

$$E_{\mathcal{H}} = \{\{\mathbf{u} = (i, j), \mathbf{v}\} \mid \mathbf{u} - \mathbf{v} \in \{(\pm 1, 0), (0, (-1)^{i+j+1})\}\}.$$

- *Triangular grid* is the graph $\mathcal{T} = (\mathbb{Z}^2, E_{\mathcal{T}})$ where

$$E_{\mathcal{T}} = \{\{\mathbf{u}, \mathbf{v}\} \mid \mathbf{u} - \mathbf{v} \in \{(\pm 1, 0), (0, \pm 1), (1, 1), (-1, -1)\}\}.$$

- *King grid* is the graph $\mathcal{K} = (\mathbb{Z}^2, E_{\mathcal{K}})$ where

$$E_{\mathcal{K}} = \{\{\mathbf{u}, \mathbf{v}\} \mid \mathbf{u} - \mathbf{v} \in \{(\pm 1, 0), (0, \pm 1), (\pm 1, \pm 1)\}\}.$$

Next we will define the concept of *density of a code* in these infinite grids. So, let G be any of these grids and let $C \subseteq \mathbb{Z}^2$ be a code in G. The density $D(C)$ of C is then defined by

$$D(C) = \limsup_{n \to \infty} \frac{|C \cap Q_n|}{|Q_n|}$$

where $Q_n = \{(i, j) \in \mathbb{Z}^2 \mid |i| \leq n,\ |j| \leq n\}$. We say that a code in some class is optimal if it has the smallest density among the codes in the same class. We will denote by $\gamma^{ID}(G)$, $\gamma^{LD}(G)$, $\gamma^{L-ID}(G)$ and $\gamma^{L-LD}(G)$ the densities of optimal identifying, locating-dominating, local identifying and local locating-dominating codes, respectively, in G. The numbers $\gamma^{ID}(G)$ and $\gamma^{LD}(G)$ are all known when G is the square, triangular or king grid. The number $\gamma^{LD}(\mathcal{H})$ is also known while the number $\gamma^{ID}(\mathcal{H})$ is currently still unknown. Note that interestingly the exact value of the density of optimal 2-identifying codes in the hexagonal grid is however known to be $\frac{4}{19}$ [10]. In Table 2 the known values are listed. For the number $\gamma^{ID}(\mathcal{H})$ we have given an interval in which we know it belongs.

G	$\mathcal{S}$	$\mathcal{H}$	$\mathcal{T}$	$\mathcal{K}$
$\gamma^{ID}(G)$	$\frac{7}{20}$ ([1])	$\frac{5}{12}$ - $\frac{3}{7}$ ([6, 4])	$\frac{1}{4}$ ([11])	$\frac{2}{9}$ ([3, 5])
$\gamma^{LD}(G)$	$\frac{3}{10}$ ([16])	$\frac{1}{3}$ ([9])	$\frac{13}{57}$ ([8])	$\frac{1}{5}$ ([9])

Table 2: Known values for the densities of optimal identifying and locating-dominating codes in infinite grids.

We will study the densities of optimal local identifying and local locating-dominating codes in these four grids. Since square and hexagonal grids are triangle-free we have the following theorem. See Figures 1 and 2 for constructions.

Theorem 9.

$$\gamma^{L-LD}(\mathcal{S}) = \frac{1}{5}$$

and

$$\gamma^{L-LD}(\mathcal{H}) = \frac{1}{4}.$$

For the other classes of codes of our interest we will prove lower bounds for the density of an optimal code in the class. The following lemma is commonly known and used.

Lemma 10. *Let G be an infinite grid and let $C \subseteq \mathbb{Z}^2$ be an r-covering code in G. If $s(c) \leq \alpha$ for every $c \in C$ then $D(C) \geq \frac{1}{\alpha}$.*

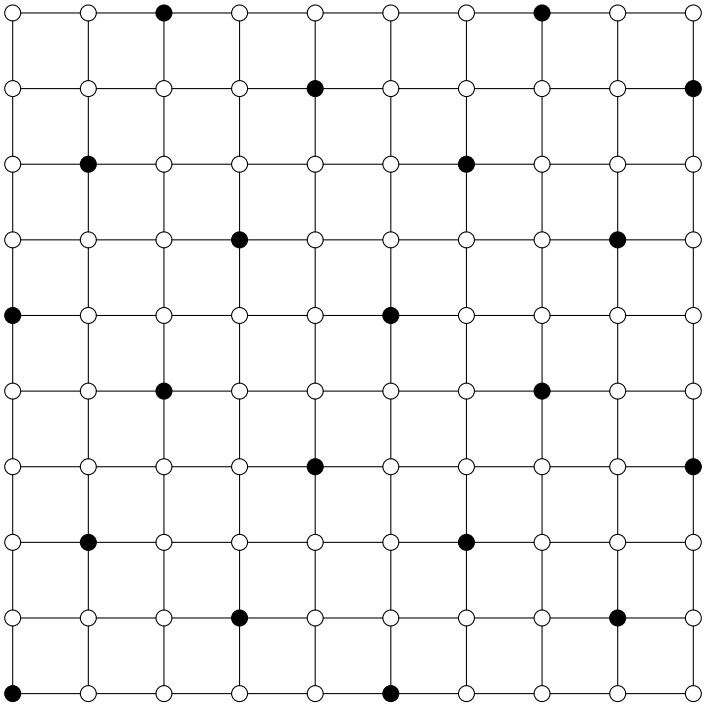

Figure 1: An optimal local locating-dominating code which is also an optimal 1-covering code in the square grid.

Thus by finding an upper bound for the share of an arbitrary codeword of a code we obtain a lower bound for the density of the code. By analyzing the possible shares of codewords of local identifying and local locating-dominating codes in the grids we get lower bounds for the numbers $\gamma^{L-ID}(G)$ and $\gamma^{L-LD}(G)$ for different grids G. On the other hand, since any identifying code is also a local identifying code and any locating-dominating code is also a local locating-dominating code, the optimal densities (and an upper bound for optimal density in the case of identifying codes in the hexagonal grid) in Table 2 give upper bounds for the densities. Moreover in Figure 3 we have constructed a local identifying code of density $\frac{3}{11}$ in the square grid. This is a better upper bound than $\frac{7}{20}$ provided by Table 2. Thus we have the following theorems.

Theorem 11.

$$\gamma^{L-ID}(\mathcal{S}) \in \left[\frac{6}{23}, \frac{3}{11}\right].$$

Theorem 12.

$$\gamma^{L-ID}(\mathcal{H}) \in \left[\frac{6}{17}, \frac{3}{7}\right].$$

Theorem 13.

$$\gamma^{L-LD}(\mathcal{T}) \in \left[\frac{2}{11}, \frac{13}{57}\right].$$

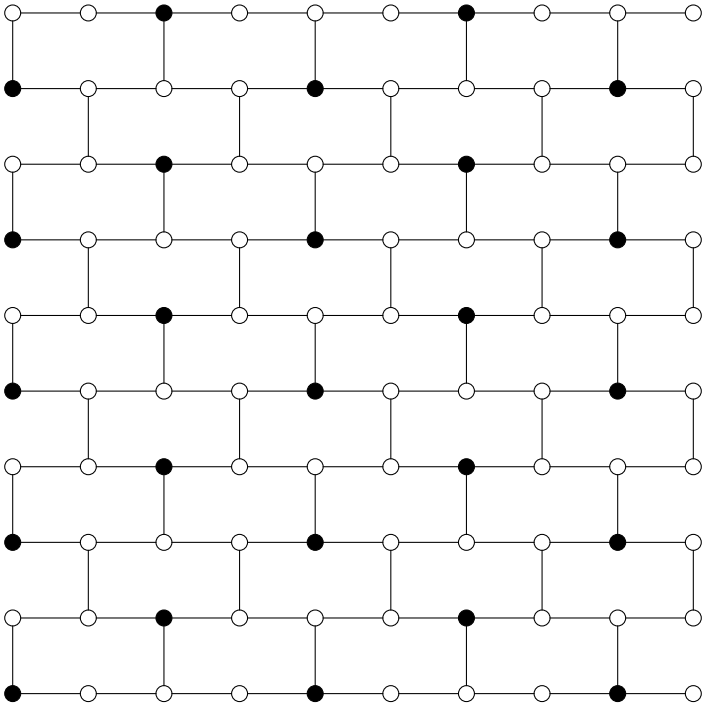

Figure 2: An optimal local locating-dominating code which is also an optimal 1-covering code in the hexagonal grid.

For $\gamma^{L-ID}(\mathcal{T})$ we get a precise value. This is because the lower bound we observe using shares is the same than the upper bound from Table 2. This means that optimal identifying and local identifying codes in the triangular grid have the same densities.

Theorem 14.

$$\gamma^{L-ID}(\mathcal{T}) = \frac{1}{4} = \gamma^{ID}(\mathcal{T}).$$

Theorem 15.

$$\gamma^{L-LD}(\mathcal{K}) \in \left[\frac{3}{17}, \frac{1}{5}\right].$$

Theorem 16.

$$\gamma^{L-ID}(\mathcal{K}) \in \left[\frac{4}{19}, \frac{2}{9}\right].$$

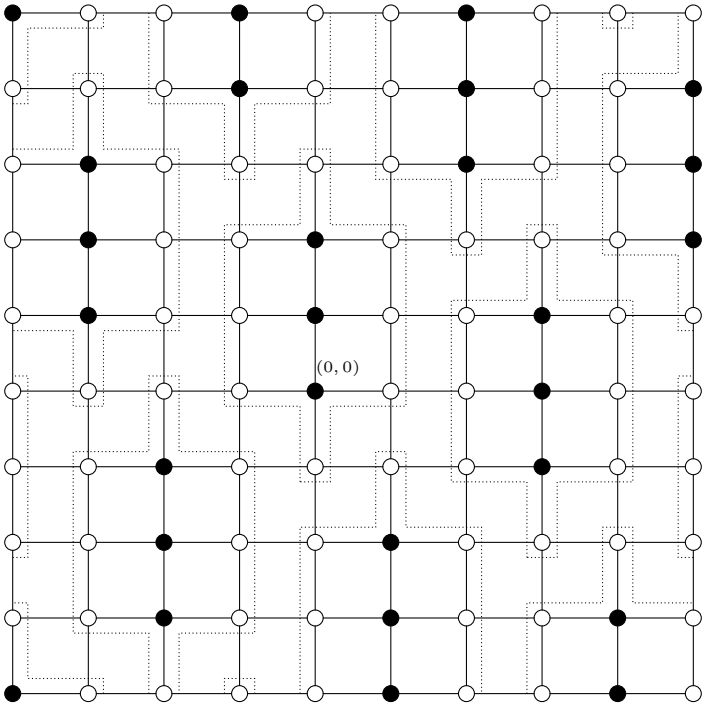

Figure 3: A local identifying code of density $\frac{3}{11}$ in the square grid.

References

[1] Y. Ben-Haim and S. Litsyn. Exact minimum density of codes identifying vertices in the square grid. *SIAM Journal on Discrete Mathematics*, 19:69–82, 2005.

[2] I. Charon, G. Cohen, O. Hudry, and A. Lobstein. New identifying codes in the binary hamming space. *European Journal of Combinatorics*, 32, 2010.

[3] I. Charon, O. Hudry, and A. Lobstein. Identifying codes with small radius in some infinite regular graphs. *Electronic Journal of Combinatorics*, 9(1), 2002.

[4] G. Cohen, I. Honkala, and A. Lobstein. Bounds for codes identifying vertices in the hexagonal grid. *SIAM Journal on Discrete Mathematics*, 13:492–504, 2000.

[5] G. Cohen, I. Honkala, and A. Lobstein. On codes identifying vertices in the two-dimensional square lattice with diagonals. *IEEE Trans. on Comput.*, 50:174–176, 2001.

[6] A. Cukierman and G. Yu. New bounds on the minimum density of an identifying code for the infinite hexagonal grid. *Discrete Applied Mathematics*, 161:2910–2924, 2013.

[7] P. Herva. Lokaali identifiointi graafeissa. *Master's thesis*, University of Turku, February 2020.

[8] I. Honkala. An optimal locating-dominating set in the infinite triangular grid. *Discrete Mathematics*, 306:2670–2681, 2006.

[9] I. Honkala and T. Laihonen. On locating-dominating sets in infinite grids. *European Journal of Combinatorics*, 27:218–227, 2006.

[10] V. Junnila and T. Laihonen. Optimal lower bound for 2-identifying codes in the hexagonal grid. *Electronic Journal of Combinatorics*, 19(2), 2012.

[11] M. G. Karpovsky, K. Chakrabarty, and L. B. Levitin. On a new class of codes for identifying vertices in graphs. *IEEE Transactions on Information Theory*, IT-44:599–611, 1998.

[12] S. Klavžar and M. Tavakoli. Local metric dimension of graphs: Generalized hierarchical products and some applications. *Applied Mathematics and Computation*, 2020.

[13] A. Lobstein. Watching systems, identifying, locating-dominating and discriminating codes in graphs. `https://www.lri.fr/~lobstein/debutBIBidetlocdom.pdf`.

[14] D. F. Rall and P. J. Slater. On location-domination numbers for certain classes of graphs. *Congr. Numer.*, 45:97–106, 1984.

[15] P. J. Slater. Dominating and reference sets in a graph. *J. Math. Phys. Sci.*, 22:445–455, 1988.

[16] P. J. Slater. Fault-tolerant locating dominating sets. *Discrete Mathematics*, 249:179–189, 2002.

Generalized measure-theoretic entropy and Lyapunov exponents for G-equivariant functions

Toni Hotanen

University of Turku, Finland

Abstract

Measure-theoretic entropy is an useful invariant for measure-preserving dynamical systems, which tells something about the complexity of the system. In this paper we develop a new notion of measure-theoretic entropy for endomorphisms of measure-preserving systems. We require the systems to use actions of amenable groups as we need properties of those groups to define our entropy. We show that our entropy has analogous versions of the expected properties of the classical entropy.

Lyapunov exponents were defined for cellular automata three decades ago by Shereshevsky, although they have existed in the context of differentiable systems for over a hundred years. We generalize Shereshevsky's notion of Lyapunov exponents for endomorphisms of topological dynamical systems over zero-dimensional compact metric spaces. We show that our entropy and Lyapunov exponents are tied together by an upper bound relation.

1 Introduction

Measure-theoretic entropy is an important invariant in ergodic theory. Entropy can be thought of as a measure of complexity of a system, but the notion is also used in definition of chaos. Measure-theoretic entropy was developed by Kolmogorov in [6] and improved upon by Sinai in [12] hence it often alternatively goes by the name Kolmogorov-Sinai entropy as a tribute to its creators.

Measure-theoretic entropy is preserved by taking measure-theoretic conjugacies (isomorphisms) and therefore can be used to classify some measure-preserving dynamical systems. The task of showing whether two systems were isomorphic was difficult prior to the notion of entropy. For instance the question by von Neumann from 1930s of whether the two Bernoulli shifts with distributions $(\frac{1}{2}, \frac{1}{2})$ and $(\frac{1}{3}, \frac{1}{3}, \frac{1}{3})$ were isomorphic remained open for few decades. Kolmogorov showed that since these systems have different entropies, they can not be isomorphic. The question of whether two Bernoulli shifts with same entropies were isomorphic gained a lot of attention in the following years. The celebrated article [10] by Ornstein gave a positive answer to the question. For a great historical account on this development see [4].

Our interest lies in the study of G-equivariant measure-preserving functions; especially cellular automata (CA). When $G = \mathbb{Z}$, the classical measure-theoretic entropy can be used to tell many non-conjugate systems apart. But when G has more complex structure the same doesn't necessarily hold. For instance according to [8] it was conjectured by Shereshevsky that the topological entropies for multidimensional cellular automata are always either zero or infinite. The conjecture was later shown false by Meyerovitch in [7] and in the same paper the author also described a method of constructing a cellular automaton with finite measure-theoretic entropy. While multidimensional CA with finite non-zero entropies exist, the fact that the problem remained open for more than a decade indicates that such CA are at least somewhat rare. Furthermore the problem is still open in a more general setting. In addition there exists classes of CA, such that each of its members have zero or infinite topological entropy. For example in [2] D'amico et al. proved that the class of multidimensional linear CA have such property. Therefore we would like to have an invariant that gives a more refined classification.

In this paper we define a measure-theoretic entropy for G-equivariant measure-preserving functions with respect to a given subgroup $H \leq G$. We show that this entropy is invariant under a stronger notion of conjugacy and it is finite if the subgroup H is suitably selected. Similar efforts in defining such an entropy have been already made in [1] by Blanchard and Tisseur for CA over $\mathbb{Z}^2$. But while their definition can be generalized for $\mathbb{Z}^d$, where $d > 1$, something else is required if we want to consider more general groups. We take these steps in the more general direction and define a measure-theoretic entropy for endomorphisms of measure-preserving dynamical systems over groups that are countable, discrete and amenable.

Lyapunov exponents tell the rate of divergence of close points in a dynamical system. For one dimensional cellular automata they were first introduced in [11] and an upper bound relation between them and measure-theoretic entropy was proven. Tisseur generalized the notion for two dimensional cellular automata in [13] and showed a similar relation between their two-dimensional entropy. We generalize Shereshevsky's and Tisseur's definitions for topological dynamical systems over zero-dimensional compact metric spaces, which are G-equivariant for some group action. In this context the group does not have to be amenable. We show that the Lyapunov exponents can be used to compute an upper bound for our entropy, when the group we are considering has a normal subgroup, such that the set of left cosets forms a group isomorphic to $\mathbb{Z}$.

2 Preliminaries

Let G be a group and X be a set. We denote the identity element of G by 1_G, where we omit the subscript if the group it belongs to to is clear from context. A (left) *group action* is a mapping $\varphi : G \times X \to X$, such that $\varphi(g, \varphi(h, x)) = \varphi(gh, x)$ and $\varphi(1, x) = x$, for each $g \in G$, $h \in G$ and $x \in X$. If we are considering only a single group action, we omit the notation of φ entirely and instead use the shorthand notation $gx = \varphi(g, x)$. We will use the notation $Gx = \{gx \mid g \in G\}$ for the *orbit* of each point $x \in X$. It is clear from the definition that the function $f_g : X \to X$, such that $f_g(x) = gx$ for each $x \in X$

is a bijection for each $g \in G$. We will use the notation g for both the group element and the function f_g, whenever doing so does not lead to ambiguities.
Let X be a set. A *σ-algebra* of a set X, is such a collection of subsets of X, that empty set belongs to it and it is closed under taking countable unions and complements. If $\mathcal{Y}$ is a collection of subsets of X, then the smallest σ-algebra containing $\mathcal{Y}$ is called the σ-algebra generated by $\mathcal{Y}$, which is denoted as $\sigma(\mathcal{Y})$ and $\mathcal{Y}$ is called a *generator* of $\sigma(\mathcal{Y})$. A *measure* μ is a function $\mu : \mathcal{B} \to [0, \infty]$, such that $\mu(\emptyset) = 0$ and $\mu(\bigcup_{i \in I} A_i) = \sum_{i \in I} \mu(A_i)$, where $\mathcal{B}$ is a σ-algebra, I is a countable index set and $A_i \cap A_j = \emptyset$ for each disjoint $i \in I$ and $j \in I$. The sets $A \in \mathcal{B}$ are called *measurable*. A measure μ is a *probability measure* if its codomain is the interval $[0, 1]$ and $\mu(X) = 1$. A triple $(X, \mathcal{B}, \mu)$ is a *measure space* if μ is an arbitrary measure and furthermore it is a *probability space* if μ is a probability measure.
Let $(X_i, \mathcal{B}_i, \mu_i)$ be two measure spaces, where $i \in \{0, 1\}$. A function $f : X_0 \to X_1$ is called *measurable*, if $f^{-1}(A) \in \mathcal{B}_0$ for each $A \in \mathcal{B}_1$, where naturally $f^{-1}(A) = \{x \mid f(x) \in A)\}$. A measurable function is called *measure-preserving* if furthermore $\mu_0(f^{-1}(A)) = \mu_1(A)$ for every $A \in \mathcal{B}_1$. If f is a measure-preserving function, then we call the measure μ *f-invariant*. Let $(X, \mathcal{B}, \mu)$ be a probability space and let G be a group acting on X. We call μ *G-invariant* if the function $g : X \to X$, is measure-preserving for each $g \in G$ and we call such G measure-preserving. A *measure-preserving dynamical system* is a tuple $(X, \mathcal{B}, \mu, \kappa)$, where $(X, \mathcal{B}, \mu)$ is a probability space and κ is either a measure-preserving function or a group.
A *partition* α of a set X is such a collection of pairwise disjoint subsets of X, that the union of all elements in the partition equals X. If α and β are such partitions of the set X, that for each $A \in \alpha$, there exists $B \in \beta$, such that $A \subseteq B$, then α is a *refinement* of β. We denote the *join* of two partitions α and β as $\alpha \vee \beta = \{A \cap B \mid A \in \alpha, B \in \beta\}$, which is clearly a refinement of both partitions. A join of $n+1$ partitions is denoted as $\bigvee_{i=0}^{n} \alpha_i = \alpha_n \vee \bigvee_{i=0}^{n-1} \alpha_i$, where α_i is a partition of X for each $i \in \mathbb{N}$, such that $0 \leq i \leq n$. More generally a join over a finite index set F is denoted as $\alpha_F = \bigvee_{g \in F} \alpha_g$ and furthermore if F is a subset of a group, then each $\alpha_g = g^{-1}(\alpha)$. A partition is a *finite partition*, if it contains finitely many elements and it is a *measurable partition* if each of its elements are measurable. For each $x \in X$ we will denote $\alpha(x) = A$, where $A \in \alpha$ is such that $x \in A$. Let $\mathcal{B}$ be a σ-algebra of a set X. A sequence (α_i) of partitions of X is a *generating partition* of $\mathcal{B}$ if for each $i \in \mathbb{N}$, α_{i+1} is a refinement of α_i and $\sigma(\bigcup_{i \in \mathbb{N}} \alpha_i) = \mathcal{B}$.
Let $(X, \mathcal{B}, \mu, f)$ be a measure-preserving dynamical system. A *measure-theoretic entropy* of a partition α is defined as $H_\mu(\alpha) = \sum_{A \in \alpha} -\mu(A) \log(\mu(A))$ and a *conditional measure-theoretic entropy* of a finite partition β, given α is defined as $H_\mu(\beta|\alpha) = \sum_{A \in \alpha} \sum_{B \in \beta} -\mu(A \cap B) \log(\frac{\mu(A \cap B)}{\mu(A)})$. For convenience we will define $0 \log 0 = 0$. The *measure-theoretic entropy of a system* with respect to a partition α is defined as $h_\mu(f, \alpha) = \lim_{n \to \infty} \frac{H_\mu(\alpha^n)}{n}$, where

$\alpha^n = \bigvee_{i=0}^{n-1} f^{-i}(\alpha)$ and $f^{-1}(\alpha) = \{f^{-1}(A) \mid A \in \alpha\}$. Finally a *measure-theoretic entropy of a system* is $h_\mu(f) = \sup_\alpha\{h_\mu(f,\alpha) \mid \alpha$ is a finite and measurable partition of $X\}$.

2.1 Measure-Theoretic Entropy

The basic facts contained in the following two lemmas and their proofs can be found in many introductory texts to ergodic theory, for example in [14]. We use them in the next section without explicitly referring to them.

Lemma 1. *The following properties hold for the (conditional) measure-theoretic entropy:*

$$\begin{aligned}
&H_\mu(\alpha \vee \beta) \leq H_\mu(\alpha) + H_\mu(\beta|\alpha)\\
&H_\mu(\alpha \vee \beta|\gamma) \leq H_\mu(\alpha|\gamma) + H_\mu(\beta|\alpha \vee \gamma)\\
&H_\mu(\beta|\alpha) \leq H_\mu(\beta)\\
&H_\mu(\beta) \leq H_\mu(\alpha) \text{ if } \alpha \text{ is a refinement of } \beta\\
&H_\mu(\beta|\alpha) \leq H_\mu(\beta'|\alpha) \text{ if } \beta' \text{ is a refinement of } \beta\\
&H_\mu(\beta|\alpha') \leq H_\mu(\beta|\alpha) \text{ if } \alpha' \text{ is a refinement of } \alpha\\
&h_\mu(\beta) \leq h_\mu(\alpha) + H_\mu(\beta|\alpha)\\
&h_\mu(\alpha) = h_\mu(\alpha^n) \text{ for each } n \in \mathbb{N}
\end{aligned}$$

Lemma 2. *Let X be a set and $\mathcal{B}$ be a σ-algebra. Let (α_i) be a generating sequence of partitions. Then for any partition β we have that for every ϵ there exist such n_ϵ, that*

$$H_\mu(\beta|\alpha_n) < \epsilon,$$

whenever $n > n_\epsilon$

2.2 Amenable Groups

There are several equivalent ways to define amenable groups. We will use the definition given by Følner, as we will use his sequences in the definition of our entropy.

Definition 1. *Let G be a group. If there exists a sequence (F_n) of finite subsets of G, such that for each $g \in G$ and $\epsilon > 0$, there exists n_ϵ, such that $|gF_n \triangle F_n| \leq \epsilon|F_n|$, whenever $n > n_\epsilon$, then the sequence (F_n) is called a Følner sequence. If a group admits a Følner sequence it is called amenable.*

Lemma 3. *Let G be a group and (F_n) be a Følner sequence. Let (H_n) be a sequence of finite subsets of G. Then there exists a subsequence (F_{n_i}), such that $(H_i F_{n_i})$ is a Følner sequence.*

Lemma 4. *Let G be a group, such that G/N and N are amenable groups. Let $T = \{t_1, t_2, ..., t_k\}$ be such that $< t_1N, t_2N, ..., t_kN >$ is a minimal generator of G/N. Then for any Følner sequence $(F_n^{G/N})$ of G/N, there exists a Følner sequence (F_n^N) of N,*

such that $(T_n F_n^N)$ *is a Følner sequence of* G*, where* T_n *is a finite subset of* $< T >$ *and* $\varphi(T_n) = (F_n^{G/N})$*, where* $\varphi : G \to G/N$ *is the canonical epimorphism.*

Denote by $\mathrm{Fin}(G)$ the set of finite subsets of a group G. Let $f : \mathrm{Fin}\ (G) \to \mathbb{R}$.

f is called *non-decreasing* if	$f(F) \leq f(E)$ for each $F \subseteq E$.
f is called *non-negative* if	$0 \leq f(F)$ for each $F \neq \emptyset$.
f is called *shift invariant* if	$f(F) = f(Fg)$ for each $g \in G$.
f is called *sub-additive* if	$f(F \cup E) \leq f(F) + f(E)$ for each $E, F \in \mathrm{Fin}(G)$.

The following theorem, which we will need in our definition is due to Ornstein and Weiss and can be found in [9].

Theorem 1 (Ornstein - Weiss)**.** *Let* G *be an amenable group. Let* $f : Fin(G) \to \mathbb{R}$ *be non-negative, non-decreasing, shift invariant and sub-additive and let* (F_n) *be a Følner sequence. Then a limit*

$$\lim_{n\to\infty} \frac{f(F_n)}{|F_n|}$$

exists and is independent of the choice of the Følner sequence.

Ornstein and Weiss used their theorem in their generalization of measure-theoretic entropy for actions of amenable groups.

Definition 2. *Let* $(X, \mathcal{B}, \mu, G)$ *be a measure-preserving dynamical system. The measure-theoretic entropy of the group action with respect to a partition* α *is defined as*

$$\bar{h}^G_{\mu,\alpha} = \lim_{n\to\infty} \frac{H_\mu(\alpha_{F_n})}{|F_n|},$$

where (F_n) *is an arbitrary Følner sequence. Furthermore the measure-theoretic entropy of the group action is defined as*

$$\bar{h}^G_\mu = \sup\{\bar{h}^G_{\mu,\alpha} \ [\ \alpha \text{ is a partition of } X\}.$$

2.3 Topological Dynamical Systems and Cellular Automata

Definition 3. *A pair* (X, f) *is a dynamical system, where* X *is a compact metric space and* f *is either a continuous group action* $f : G \times X \to X$ *or a continuous function* $f : X \to X$*.*

Definition 4. *A cellular automaton is a* 4*-tuple* (G, Σ, w, V)*, where* G *is a finitely generated group,* Σ *is a finite set of symbols,* $w : \Sigma^k \to \Sigma$ *is a local rule and* $V = (g_1, g_2, \ldots, g_k) \in G^k$ *is a neighbourhood. A global rule is a function* $f : \Sigma^G \to \Sigma^G$*, such that* $f(c)_g = w(c_{gg_1}, c_{gg_2}, \ldots c_{gg_k})$*, where* $c \in \Sigma^G$ *and* $c_g = c(g)$*.*

Definition 5. *A cellular automaton* (G, Σ, w, V) *is called* g_i*-permutive if a function* $\varphi : \Sigma \to \Sigma$ *defined as* $\varphi(x) = w(c_{g_1}, c_{g_2}, \ldots c_{g_{i-1}}, x, c_{g_{i+1}} \ldots c_{g_k})$ *is permutive for each* $c \in \Sigma^G$*.*

3 Entropy

In this section we define a new type of measure-theoretic entropy for measure-preserving dynamical systems. Our definition generalizes the usual definition of measure-theoretic entropy for G-equivariant functions of measure-preserving dynamical systems.

We start by defining an auxiliary function from the collection of finite subsets of a given group to the set of real numbers. After that we show that the function has the properties defined in the beginning of the section, when it is an endomorphism.

Definition 6. *Let $(X, \mathcal{B}, \mu, G)$ be a measure-preserving dynamical system. Let $f : X \to X$ be a measure-preserving endomorphism. Define $h_{\mu,\alpha} : Fin(G) \to \mathbb{R}$, such that*

$$h_{\mu,\alpha}(F) = \lim_{n\to\infty} \frac{H_\mu((\alpha_F)^n)}{n}.$$

Definition 7. *Let X and Y be sets such that a group G acts on them. A mapping $f : X \to Y$ is G-equivariant, if f commutes with every group element, i.e. $f \circ g = g \circ f$ for every $g \in G$. If $Y = X$, then f is an endomorphism.*

Lemma 5. *Let $(X, \mathcal{B}, \mu, G)$ be a measure-preserving dynamical system and f a measure-preserving endomorphism, then the function $h_{\mu,\alpha}$ is non-decreasing, non-negative, shift invariant and sub-additive.*

Combining the above lemma together with the theorem of Ornstein and Weiss we are able to define our entropy in Definition 8.

Definition 8. *Let $(X, \mathcal{B}, \mu, G)$ be a measure-preserving dynamical system, where G is amenable and let f be a measure-preserving endomorphism. Let $H \leq G$ and (F_n) be a Følner sequence of H. We define a (H, f)-entropy of the system with respect to a partition α to be*

$$h^H_{\mu,\alpha} = \lim_{n\to\infty} \frac{h_{\mu,\alpha}(F_n)}{|F_n|}.$$

By Lemma 5 and Theorem 1 the limit exists and is independent of the choice of the Følner sequence.

We define a (H, f)-entropy of the system to be

$$h^H_\mu = \sup\{h^H_{\mu,\alpha} \mid \alpha \text{ is a partition of } X.\}$$

Notice that letting $H = \{1\}$ gives the usual definition of the measure-theoretic entropy. In this sense our entropy is a generalization of the classical measure-theoretic entropy.

In the next lemma we show that just like in the usual measure-theoretic entropy, one can calculate the entropy as the limit of of a generating sequence of partitions.

Lemma 6. *Let $(X, \mathcal{B}, \mu, G)$ be a measure-preserving dynamical system, where G is amenable and let f be a measure-preserving endomorphism. Let $H \leq G$. If (α_n) is a generating sequence, then*

$$\lim_{n\to\infty} h^H_{\mu,\alpha_n} = h^H_\mu.$$

Lemma 7. *Let $(X, \mathcal{B}, \mu, G)$ be a measure-preserving dynamical system, where G is amenable and let f be a measure-preserving endomorphism. Let $H \leq G$. Let (F_n) be a Følner sequence of H and $m \geq 0$. Then for any partition α, we have that $h^H_{\mu,\alpha} = h^H_{\mu,\alpha^m_F}$.*

From the above lemma we get the following corollary, which is analogous to the property of having a dynamically generating sequence in the setting of the usual measure-theoretic entropy.

Corollary 1. *Let $(X, \mathcal{B}, \mu, G)$ be a measure-preserving dynamical system, where G is amenable and let f be a measure-preserving endomorphism. If (α_i) is such a generating sequence, that for every $i \in \mathbb{N}$, there exists such $m_i \in \mathbb{N}$ and a finite subset H_i of H, that $\alpha_i = \alpha^{m_i}_{H_i}$, then $h^H_{\mu,\alpha} = h^H_\mu$.*

The following lemma shows that a strong factor of a given measure-preserving dynamical system, cannot have a larger entropy, than the original system. As an obvious corollary, we get that strongly isomorphic systems have the same entropy.

Lemma 8. *Let $i \in \{1, 2\}$ and $(X_i, \mathcal{B}_i, \mu_i, G)$ be two measure-preserving dynamical systems, where G is amenable and let f_i be measure-preserving endomorphisms of their respective systems. Let $H \leq G$. If there exists a measure-preserving G-equivariant mapping $T : X_1 \to X_2$, such that $T \circ f_1 = f_2 \circ T$, then $h^H_{\mu_1} \geq h^H_{\mu_2}$.*

Example 1. *Let H_3 be the Heisenberg group generated by x, y, z, where $x = (1, 0, 0)$, $y = (0, 1, 0)$ and $z = (0, 0, 1)$. The product of two elements (u, v, w) and (u', v', w') of the group is defined as $(u + u', v + v' + uw', w + w')$. Let $H =< y, z >$, then*

$$(F_n^{-1}) = \{(a, b, c) \in H_3 \mid a = 0, 0 \leq b < n \text{ and } 0 \leq c < n\}$$

is a Følner sequence of H. Let us consider a probability space $(\mathbb{F}_2^{H_3}, \mathcal{B}, \mu)$, where $\mathbb{F}_2$ is the Galois field of two elements, $\mathcal{B}$ is the Borel σ-algebra of $\mathbb{F}_2^{H_3}$ and μ is the uniform measure. Let α be a partition containing the sets

$$\{c \in \mathbb{F}_2^{H_3} \mid c(1_{H_3}) = a\},$$

for every $a \in \mathbb{F}_2$. Let us consider the group action $(H_3, \mathbb{F}_2^{H_3}) \to \mathbb{F}_2^{H_3}$, such that $hc(h') = c(h^{-1}h')$ i.e. the left shift.

Let $f : \mathbb{F}_2^{H_3} \to \mathbb{F}_2^{H_3}$ be a CA, such that $f(c)(h) = c(hx) + c(hy) + c(h) \mod 2$. For a partition α let $\alpha(c)$ denote the element A of α, such that $c \in A$. Now $\alpha_{F_n^{-1}}$ is a partition containing the sets

$$\{c' \in \mathbb{F}_2^{H_3} \mid c_{|F_n} = c'_{|F_n}\},$$

for every $c \in \mathbb{F}_2^{H_3}$.

It is easy to show that $h_\mu(f) = \infty$. *On the other hand we can show with a straightforward, albeit cumbersome computation that* $h^H_{\mu,\alpha} = \log(2)$, *which gives a lower bound for the entropy* h^H_μ. *Next lemma applies to the situation of this example as our CA was* x*-permutive,* $H \trianglelefteq H_3$ *and* $H_3/H \cong \mathbb{Z}$ *and gives us a much quicker way to estimate the entropy.*

Lemma 9. *Let* G *be such an amenable group that there exists* $N \trianglelefteq G$, *such that* $G/N \cong \mathbb{Z}$ *and let* $g \in G$ *be such that* $< gN >= G/N$. *Let* $\mathcal{A} = (G, \Sigma, w, V)$ *be a cellular automaton and let* μ *be the uniform measure. The following three implications hold:*

If there exists $k_1 \in \mathbb{Z}_+$, *such that* $\mathcal{A}$ *is* g^{k_1}*-permutive, then* $h^N_\mu \geq k_1 \log(|\Sigma|)$.

If there exists $k_2 \in \mathbb{Z}_+$, *such that* $\mathcal{A}$ *is* g^{-k_2}*-permutive, then* $h^N_\mu \geq k_2 \log(|\Sigma|)$.

If there exists $k_1 \in \mathbb{Z}_+$ *and* $k_2 \in \mathbb{Z}_+$, *such that* $\mathcal{A}$ *is* g^{k_1}*-permutive and* g^{-k_2}*-permutive, then* $h^N_\mu \geq (k_1 + k_2) \log(|\Sigma|)$.

Combining the above lemma with Theorem 3, we get a large class of CA that we can compute the h^N_μ entropy of.

4 Lyapunov exponent

In this section we generalize the notion of Lyapunov exponents by Shereshevsky in [11] of one-dimensional cellular automata to endomorphisms of topological dynamical systems over zero-dimensional compact metric spaces. The zero-dimensionality comes to play when we require the existence of topologically generating open partitions. Notice that in this section we do not require groups to be amenable. In the context of cellular automata our definition of λ^H_α can be thought of as the maximum speed of which a difference in the cells far from H propagates to the cells of H.

Definition 9. *Let* X *be a metric space. Then for a subset* $Y \subseteq X$ *the diameter of* Y *is defined as* $diam(Y) = \sup\{d(x, y) \mid x \in Y \text{ and } y \in Y\}$. *For a family* α *of subsets of* X *the diameter of* α *is defined as* $diam(\alpha) = \sup\{diam(A) \mid A \in \alpha\}$.

Definition 10. *Let* X *be a metric space. Let* α *be a cover of* X. *Then* α *is topologically* G*-generating if* $\lim_{n\to\infty} diam(\alpha_{B_n}) = 0$ *and topologically* f*-generating if* $\lim_{n\to\infty} diam(\alpha^n) = 0$.

Definition 11. *Let* X *be a set,* G *be a group acting on it and* f *be a self-map with domain* X. *Let* α *be a partition of* X *and* $H \subseteq G$ *and denote* $H^C = (G \setminus H)^{-1}$. *Define*

$$L^H_{\alpha,n}(x) = \inf\{k \in \mathbb{N} \mid f^i(\alpha_{B_k H^C}(x)) \subseteq \alpha_{H^C}(f^i(x)) \text{ for each } i < n\}.$$

Furthermore for $Y \subseteq X$, *we define*

$$L^H_{\alpha,n}(Y) = \sup\{L^H_{\alpha,n}(x) \mid x \in Y\}.$$

For $L^H_{\alpha,n}(X)$, we will use the shorthand notation $L^H_{\alpha,n}$. Finally we define

$$\lambda^H_\alpha(Y) = \limsup_{n\to\infty} \frac{L^H_{\alpha,n}(Y)}{n},$$

and give it the name Lyapunov exponent of the set Y, with respect to α and H. If Y is a singleton $\{x\}$, we call it the Lyapunov exponent of the point x and denote it as $\lambda^H_{\alpha,n}(x)$ and if $Y = X$, we call it just the Lyapunov exponent and denote it by λ^H_α.

While our definition above is for more general setting than what was stated in the beginning of this section, we require the additional structure for the Lyapunov exponents to have several desired properties.

Lemma 10. *Let (X, G) be a dynamical system and f its endomorphism. Let α be a topologically G-generating open partition of X. Let $H \subseteq G$ and denote $H^C = (G \setminus H)^{-1}$. Then*

$$L^H_{\alpha,n}(Y) = \min\{k \in \mathbb{N} \mid f^i(\alpha_{B_k H^C}(x)) \subseteq \alpha_{H^C}(f^i(x)) \text{ for each } i < n \text{ and } x \in Y\}$$

exists for any $Y \subseteq X$ and $n \in \mathbb{N}$.

The following lemma is by Fekete in [3].

Lemma 11 (Fekete's subadditive lemma)**.** *Let (x_n) be a sequence of real numbers. If the inequality $x_{n+m} \leq x_n + x_m$ holds for every n and m in $\mathbb{N}$, then*

$$\lim_{n\to\infty} \frac{x_n}{n} = \inf\{\frac{x_n}{n} \mid n \in \mathbb{N}\}.$$

Lemma 12. *Let (X, G) be a dynamical system and f its endomorphism. Let α be a topologically G-generating open partition of X. Let $H \subseteq G$ be such that $H^C B_i = B_i H^C$ for each $i \in \mathbb{N}$, where $H^C = (G \setminus H)^{-1}$. If $Y \subseteq X$ is such that the implication if $x \in Y$, then $gx \in Y$, holds for each $g \in G$, then*

$$L^H_{\alpha,i+j}(Y) \leq L^H_{\alpha,i}(Y) + L^H_{\alpha,j}(f^i(Y)).$$

Proof. Denote $I = L^H_{\alpha,i}(Y)$ and $J = L^H_{\alpha,j}(f^i(Y))$. Let $x \in Y$, then for every $g \in B_J$, we have that

$$\begin{aligned} f^{i+j}(\alpha_{B_{I+J}H^C}(x)) &= f^{i+j}(\alpha_{B_I H^C B_J}(x)) \\ &\subseteq f^{i+j}(\alpha_{B_I H^C g}(x)) \\ &= f^{i+j}(\alpha_{B_I H^C}(gx)) \\ &\subseteq f^j(\alpha_{H^C}(f^i(gx))) \\ &= f^j(\alpha_{H^C g}(g^{-1}g(f^i(x)))) \\ &= f^j(\alpha_{H^C g}(f^i(x))). \end{aligned}$$

Therefore

$$\begin{aligned} f^{i+j}(\alpha_{B_{I+J}H^C}(x)) &\subseteq f^j(\alpha_{H^C B_J}(f^i(x))) \\ &= f^j(\alpha_{B_J H^C}(f^i(x))) \\ &\subseteq \alpha_{H^C}(f^{i+j}(x)), \end{aligned}$$

which means that $L^H_{\alpha,i+j}(Y) \leq L^H_{\alpha,i}(Y) + L^H_{\alpha,j}(f^i(Y))$. □

Corollary 2. *Let (X, G) be a dynamical system and f its endomorphism. Let α_G be a topologically G-generating open partition of X. Let $H \subseteq G$ be such that $H^C B_i = B_i H^C$ for each $i \in \mathbb{N}$, where $H^C = (G \setminus H)^{-1}$. If $Y \subseteq X$ is such that if $x \in Y$, then $gx \in Y$ and $f^i(x) \in y$, for every $g \in G$ and $i \in \mathbb{N}$, then*

$$\lambda_\alpha^H(Y) = \lim_{n\to\infty} \frac{L_{\alpha,n}^H(Y)}{n}.$$

Proof. By Lemma 12, we have that $L_{\alpha,i+j}^H(Y) \leq L_{\alpha,i}^H(Y) + L_{\alpha,j}^H(f^i(Y))$ and since $f^i(Y) \subseteq Y$ the claim follows from Fekete's subadditive lemma 11. □

We can analogously prove a measure-theoretic version of the above by using Kingman's Theorem from [5].

Theorem 2 (Kingman's subadditive ergodic theorem)**.** *Let $(X, \mathcal{B}, \mu)$ be a probability space. If f is a measure-preserving function and (g_n) is a sequence of L^1 functions such that*

$$g_{i+j}(x) \leq g_i(x) + g_j(f^i(x)),$$

then there exists a function $g : X \to \mathbb{R} \cup \{-\infty, \infty\}$, such that almost everywhere we have that

$$\lim_{n\to\infty} \frac{g_n(x)}{n} = g(x) \geq -\infty$$

and g is μ-invariant. If furthermore f is μ-ergodic, then g is constant almost everywhere.

Corollary 3. *Let $(X, \mathcal{B}, \mu, G)$ be a measure-preserving dynamical system, where X is a compact metric space and let f be a measure-preserving endomorphism. Let α_G be a topologically G-generating open partition of X. Let $H \subseteq G$ be such that $H^C B_i = B_i H^C$ for each $i \in \mathbb{N}$, where $H^C = (G \setminus H)^{-1}$. Then we have that*

$$\lambda_\alpha^H(Gx) = \lim_{n\to\infty} \frac{L_{\alpha,n}^H(Gx)}{n}.$$

The following splitting property allows us to consider several Lyapunov exponents on their own. We can then guarantee that a difference does not propagate to the intersection of our selected subsets.

Definition 12. *Let (X, G) be a dynamical system and f its endomorphism. A partition α is called strongly irreducible if whenever $x \in X$, $y \in X$, $H \subseteq G$ and $H' \subseteq G$ such that $H \cap H' = \emptyset$ implies that $\alpha_H(x) \cap \alpha_{H'}(y) \neq \emptyset$.*

Lemma 13. *Let X be a compact metric space, G a group acting on it, f an endomorphism, α a partition of X and $Y \subseteq X$. Let $\mathcal{H}$ be such a collection of subsets of G, that for each $H \in \mathcal{H}$, there exists $B_H \subseteq G$, such that $y \in \alpha_{B_H H}(x)$ implies that $f(y) \in \alpha_H(f(x))$, for every $x \in Y$. If α is strongly irreducible then $y \in \alpha_A(x)$ implies that $f(y) \in \alpha_K(f(x))$, for every $x \in Y$, where*

$$A = \bigcap_{H\in\mathcal{H}} B_H H$$

and

$$K = \bigcap_{H \in \mathcal{H}} H.$$

5 Upper Bound

Theorem 3. *Let $(X, \mathcal{B}, \mu, G)$ be a measure-preserving, strongly irreducible dynamical system, where $\mathcal{B}$ is the Borel σ-algebra of X and let f be a measure-preserving endomorphism. Let $N \trianglelefteq G$, such that $G/N \cong \mathbb{Z}$. Let $g \in G$ be such that $< gN >= G/N$. Let α be G-generating. Then*

$$h_\mu^N \leq \bar{h}_\mu^G(\lambda_\alpha^{H_+} + \lambda_\alpha^{H_-}),$$

where $H_\pm^{-1} = J_\pm N$ and $J_\pm = \{g^i \mid i > 0\}^{\pm 1}$

Using the above theorem we can show that the lower bounds established in Lemma 9 are actually the exact values of the entropies. Therefore we have a large class of cellular automata for which we can compute our entropy.

6 Conclusion

In this work we defined a new kind of measure-theoretic entropy for G-equivariant measure-preserving functions. We also generalized the notion of Lyapunov exponents for G-equivariant functions. We showed that these concepts are especially useful when G has a normal subgroup N, such that $G/N \cong \mathbb{Z}$. In such a situation the entropy is finite and can be used to show that two systems are not strongly conjugate. Our entropy may turn out useful in the study of cellular automata over Heisenberg group or Lamplighter group for example, as both have a coset isomorphic to $\mathbb{Z}$.

Future directions of this work could include defining the analogous topological entropy and consider their connections. For instance does the variational principle hold? A lot is still unknown about connections of entropy and Lyapunov exponents to different dynamical properties of one-dimensional cellular automata. It would be interesting to show if all the known connections hold in the more general setting. For instance what can we say about the values of our entropy and Lyapunov exponents in context of linear cellular automata? We were able to compute entropies for a class of permutive CA in a fairly general setting. We would also like to know if there is a class of G-equivariant functions that can be classified in terms of our entropy analogous to the classification of Bernoulli shifts.

Acknowledgements

The author acknowledges the emmy.network foundation under the aegis of the Fondation de Luxembourg for its financial support.

References

[1] François Blanchard and Pierre Tisseur. Entropy rate of higher-dimensional cellular automata. 06 2012.

[2] Michele D'amico, Giovanni Manzini, and Luciano Margara. On computing the entropy of cellular automata. In Kim G. Larsen, Sven Skyum, and Glynn Winskel, editors, *Automata, Languages and Programming*, pages 470–481, Berlin, Heidelberg, 1998. Springer Berlin Heidelberg.

[3] M. Fekete. Über die verteilung der wurzeln bei gewissen algebraischen gleichungen mit ganzzahligen koeffizienten. *Mathematische Zeitschrift*, 17:228–249.

[4] Anatole Katok. Fifty years of entropy in dynamics: 1958 – 2007. *Journal of Modern Dynamics*, 1, 10 2007.

[5] J. F. C. Kingman. The ergodic theory of subadditive stochastic processes. *Journal of the Royal Statistical Society: Series B (Methodological)*, 30(3):499–510, 1968.

[6] A. N. Kolmogorov. New metric invariant of transitive dynamical systems and endomorphisms of lebesgue spaces. *Doklady of Russian Academy of Sciences*, 119(N5):851–864, 1958.

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

[8] G. Morris and T. Ward. Entropy bounds for endomorphisms commuting with k actions. *Israel J. Math*, 106:1–12, 1997.

[9] D. Ornstein and B. Weiss. Entropy and isomorphism theorems for actions of amenable groups. *Journal d'Analyse Mathématique*, 48:1–141, 1987.

[10] Donald Ornstein. Bernoulli shifts with the same entropy are isomorphic. *Advances in Mathematics*, 4(3):337–352, 1970.

[11] M. A. Shereshevsky. Lyapunov exponents for one-dimensional cellular automata. *Journal of Nonlinear Science*, 2(1):1–8, Mar 1992.

[12] Y. Sinai. On the concept of entropy of dynamical system. *Soviet Mathematics*, 4:768–771, 01 1959.

[13] Pierre Tisseur. Always finite entropy and lyapunov exponents of two-dimensional cellular automata. 03 2005.

[14] P. Walters. *An Introduction to Ergodic Theory*. Graduate texts in mathematics. Springer-Verlag, 1982.

Optimal Stopping in the Job Allocation Problem

Anna Ivashko

Institute of Applied Mathematical Research
Karelian Research Centre RAS
Petrozavodsk, Russia
aivashko@krc.karelia.ru

Keywords: Optimal stopping problem, job allocation, balls-and-bins problem

In this paper, we study the following discrete time optimal stopping problem connected with the job allocation problem.

We consider the process where jobs arrive randomly one at a time to servers. There are N periods of time. In each period with probability p only one new server can be added in the system. We want to select the time moment to stop the process. If we stop then we obtain the gain according to load of the system. We obtain 1 for every server with exactly one job and loses $1/2$ for every server with two or more jobs. The aim is to maximize the expected payoff.

This problem can be modelled using the balls-and-bins problem ([1, 2]). The balls-and-bins problem is a classic problem in probability theory that has many applications in computer science: shared-memory emulations, efficient hashing schemes, randomized load balancing of tasks on servers, and routing of packets within parallel networks and data centers.

State $(i_0, i_1; k)$ means that there are k bins in the game: i_0 empty bins, i_1 bins with exactly one ball, and $k - i_0 - i_1$ bins with two or more balls.

The optimal value function $v_n(i_0, i_1; k)$ at step n being the maximum expected payoff you can achieve starting from state $(i_0, i_1; k)$ can be obtained from the optimality equation

$$
\begin{aligned}
&v_n(i_0, i_1; k) = \max\left\{i_1 - \frac{1}{2}(k - i_0 - i_1); \bar{v}_n(i_0, i_1; k)\right\},\ n = 1, ..., N-1,\ k = 1, ..., n+1;\\
&v_N(i_0, i_1; k) = i_1 - \frac{1}{2}(k - i_0 - i_1),\ k = 1, ..., N+1;\\
&i_0 + i_1 \le k,
\end{aligned}
$$

where

$$\bar{v}_n(i_0,i_1;k) = p\left[\frac{i_0+1}{k+1}v_{n+1}(i_0,i_1+1;k+1) + \frac{i_1}{k+1}v_{n+1}(i_0+1,i_1-1;k+1)\right.$$
$$\left.+\frac{k-i_0-i_1}{k+1}v_{n+1}(i_0+1,i_1;k+1)\right]$$
$$+(1-p)\left[\frac{i_0}{k}v_{n+1}(i_0-1,i_1+1;k) + \frac{i_1}{k}v_{n+1}(i_0,i_1-1;k) + \frac{k-i_0-i_1}{k}v_{n+1}(i_0,i_1;k)\right],$$

The optimal value function at the beginning of the process has the form

$$v_0(1,0;1) = pv_1(1,1;2) + (1-p)v_1(0,1;1).$$

For this problem, the construction of optimal payoffs was described. Optimal payoffs and strategies were numerically modeled for different parameters of the problem. A simple-form strategy approximated to the optimal one was suggested.

References

1. Kolchin, V. F. (1978). *Random allocations*. Winston [usw.]: Washington.

2. Tijms, H. (2017). *One-Step Improvement Ideas and Computational Aspects*. In: Markov Decision Processes in Practice. International Series in Operations Research & Management Science (Boucherie, R. and van and N. Dijk, eds), Vol. 248, pp. 3–32. Springer, Cham.

Quantum Algorithm for the Longest Trail Problem

Kamil Khadiev and Ruslan Kapralov

Kazan Federal University, Kazan, Russia
email: kamilhadi@gmail.com

Abstract

We present the quantum algorithm for the Longest Trail Problem. The problem is to search the longest edge-simple path for a graph with n vertexes and m edges. Here edge-simple means no edge occurs in the path twice, but vertexes can occur several times. The running time of our algorithm is $O^*(1.728^m)$.

1 Introduction

Quantum computing [17, 2, 1] is one of the hot topics in computer science of the last decades. There are many problems where quantum algorithms outperform the best-known classical algorithms. Some of them can be founded here [8, 13]. Problems for graphs are examples of such problems [15, 14, 3, 10]. One of the most important performance metrics in this regard is *query complexity*; and we investigate problems using this metric for complexity.

In this paper, we consider the Longest Trail Problem (LTP). The problem is the following one. Let us consider a graph with n vertexes and m edges. The problem is to search the *longest edge-simple* path. Here *edge-simple* means no edge occurs in the path twice, but vertexes can occur several times. The *longest* means the path has the maximal possible number of edges.

The problem is strongly related to the longest path problem (LPP) that is searching the longest *vertex-simple* path. Here *vertex-simple* means no vertex occurs in the path twice.

There are many practical applications of these problems, for example, [6, 18].

Both problems are NP-hard [16]. The NP-hardness of LTP problem was discussed in [7].

The simple classical solution for the problem can be a brute force algorithm that checks all possible paths and searching the required one. Such solution works in $O(m!) = O(m^m)$ running time. This solution can be used as a base of a quantum algorithm because the classical algorithm solves a search problem. Therefore, we can use Grover Search algorithm [11, 5] and obtain a quantum algorithm that works in $O(\sqrt{m!}) = O(m^{0.5m})$. At the same time, there is a better classical algorithm that is based on the

Dynamic programming approach [4, 12]. This classical algorithm for the LTP problem works in $O^*(2^m)$ running time, where O^* hides polylog factors. The algorithm is not a simple search algorithm. That is why we cannot directly use the Grover Search algorithm for quantum speed-up, and we cannot obtain a complexity $O^*(1.4^m)$ using this way. We present a quantum algorithm that works in $O^*(1.728^m)$ running time. The algorithm on Grover Search algorithm [11, 5], quantum minimum finding algorithm [9, 10] and quantum ideas for dynamic programming on Boolean cube [3].

The structure of the paper is the following. Section 2 contains preliminaries. Then, we discuss algorithm in Section 3.

2 Preliminaries

2.1 The Longest Trail Problem

Let $G = (V, E)$ be an unweighted, underacted graph, where V is a set of vertexes, and E is a set of edges. Let $m = |E|$ be the number of edges and $n = |V|$ be the number of vertexes.

Let a sequence of edges $P = (e_{i_1}, \ldots, e_{i_\ell})$ be a path if each sequentially pair of edges e_{i_j} and $e_{i_{j+1}}$ has common vertex, for $j \in \{1, \ldots, \ell - 1\}$. A path is edge-simple if the sequence has no duplicates i.e., for any $j \neq j'$ we have $e_{i_j} \neq e_{i_{j'}}$. Let $|P| = \ell$ be the length of a path P. Let $\mathcal{P}(G)$ be the set of all possible paths for a graph G.

The problem is to the longest path i.e., any path P_{long} such that $|P_{long}| = max\{|P| : P \in \mathcal{P}(G)\}$.

2.2 Quantum Query Model

We use the standard form of the quantum query model. Let $f : D \to \{0, 1\}, D \subseteq \{0, 1\}^N$ be an N variable function. An input for the function is $x = (x_1, \ldots, x_N) \in D$ where $x_i \in \{0, 1\}$ for $i \in \{1, \ldots, N\}$.

We are given oracle access to the input x, i.e. it is realized by a specific unitary transformation usually defined as $|i\rangle|z\rangle|w\rangle \to |i\rangle|z + x_i \pmod 2\rangle|w\rangle$ where the $|i\rangle$ register indicates the index of the variable we are querying, $|z\rangle$ is the output register, and $|w\rangle$ is some auxiliary work-space. It can be interpreted as a sequence of control-not transformations such that we apply inversion operation (X-gate) to the second register that contains $|z\rangle$ in a case of the first register equals i and the variable $x_i = 1$. We interpret the oracle access transformation as N such controlled transformations for each $i \in \{1, \ldots, N\}$.

An algorithm in the query model consists of alternating applications of arbitrary unitaries independent of the input and the query unitary, and a measurement in the end. The smallest number of queries for an algorithm that outputs $f(x)$ with a probability that is at least $\frac{2}{3}$ on all x is called the quantum query complexity of the function f and is denoted by $Q(f)$. We refer the readers to [17, 2, 1] for more details on quantum computing.

In this paper's quantum algorithms, we refer to the quantum query complexity as the quantum running time. We use modifications of Grover's search algorithm [11, 5] as quantum subroutines. For these subroutines, time complexity is more than query complexity for additional log factor.

3 Algorithm

We discuss our algorithm in this section. Let us consider a function $L : 2^E \times E \times E \to \mathbb{R}$ where 2^E is the set of all subsets of E. The function L is such that $L(S, v, u)$ is the length of the longest path that uses only edges from the set S, starts from the edge v, and finishes in the edge u.

Let the function $F : 2^E \times E \times E \to \mathbb{R}$ be such that $F(S, v, u)$ is the longest path that uses only edges from the set S, starts from the edge v, and finishes in the edge u.

It is easy to see that $L(\{v\}, v, v) = 1$ and $F(\{v\}, v, v) = (v)$ for any $v \in E$ because the set has only one edge and it is the only path in the set.

Another property of these functions is

Property 1 *Suppose $S \in 2^E, v, u \in E$, an integer $k \leq |S|$. The function L is such that*

$$L(S, v, u) = \max_{S' \subset S, |S'|=k, y \in S'} \big(L(S', v, y) + L((S \backslash S') \cup \{y\}, y, u)\big)$$

and $F(S, u, v)$ is the path that is concatenation of corresponding paths.

Proof. Let $P^1 = F(S', v, y)$ and $P^2 = F((S \backslash S') \cup \{y\}, y, u)$. The path $P = P^1 \circ P^2$ belongs to S', starts from v and finishes in u, where $\circ$ means concatenation of paths excluding the duplication of common edge y. Because of definition of L, we have $L(S, v, u) \geq |P|$.

Assume that there is $T = (e_1, \ldots, e_\ell)$ such that $\ell = |T| = L(S, v, u)$ and $|T| > |P|$. Let us select S'' such that $|S''| = k, S'' \subset S$ and there is $j < |T|$ such that $R^1 = e_1, \ldots, e_j \in S''$ and $R^2 = e_j, e_{j+1}, \ldots, e_\ell \notin S'' \backslash \{e_j\}$. Then $|R^1| \leq |P^1|$ and $|R^2| \leq |P^2|$ by definition of F and L. Therefore, $|R| = |R^1| + |R^2| - 1 \leq |P^1| + |P^2| - 1 = |P|$. We obtain a contradiction with assumption. □

As a corollary we obtain the following result:

Corollary 1 *Suppose $S \in 2^E, v, u \in E$, $\mathcal{I}(u)$ is the set of all edges that has common vertex with u. The function L is such that*

$$L(S, v, u) = \max_{y \in S \backslash \{u\}, y \in \mathcal{I}(u)} (L(S \backslash \{u\}, v, y) + 1)$$

and $F(S, u, v)$ is the path that is the corresponding path.

Using this idea, we construct the following algorithm.

Step 1. Let $\alpha = 0.055$. We classically. compute $L(s, v, u)$ and $F(S, v, u)$ for $|S| = (1 - \alpha)\frac{m}{4}$ and $v, u \in E$

Step 2. Let $E_4 \subset E$ be such that $|E_4| = \frac{m}{4}$. Then, we have

$$L(E_4, u, v) = \max_{E_\alpha \subset E_4, |E_\alpha| = (1-\alpha)m/4, y \in E_\alpha} \left(L(E_\alpha, v, y) + L((E_4 \backslash E_\alpha) \cup \{y\}, y, u)\right).$$

Let $E_2 \subset E$ be such that $|E_2| = \frac{m}{2}$. Then, we have

$$L(E_2, u, v) = \max_{E_4 \subset E_2, |E_4| = m/4, y \in E_4} \left(L(E_4, v, y) + L((E_2 \backslash E_4) \cup \{y\}, y, u)\right).$$

Finally,

$$L(E, u, v) = \max_{E_2 \subset E, |E_2| = m/2, y \in E_2} \left(L(E_2, v, y) + L((E \backslash E_2) \cup \{y\}, y, u)\right).$$

We can compute $L(E, u, v)$ and corresponding $F(E, u, v)$ using three nested procedures for maximum finding. As such procedure, we use Durr-Hoyer [9, 10] quantum minimum finding algorithm.

Note that the error probability for the Durr-Hoyer algorithm is at most 0.1. So, we use the standard boosting technique to decrease the total error probability to constant by $O(m)$ repetition of the maximum finding algorithm in each level.

Let us present the implementation of Step 1. Assume that $\mathcal{I}(u)$ is the sequence of edges that have a common vertex with the edge u. Let us present a recursive function GetLen(S, v, u) for $S \in 2^E, u, v \in E$ with cashing that is Dynamic Programming approach in fact. The function is based on Corollary 1.

Algorithm 1 GetLen(S, v, u).

```
if v = u and S = {v} then                                   ▷ Initialization
    L({v}, v, v) ← 1
    F({v}, v, v) ← (v)
end if
if L(S, v, u) is not computed then
    len ← −1
    path ← ()
    for y ∈ I(u) do
        if y ∈ S\{u} and GetLen(S\{u}, v, y) + 1 > len then
            len ← L(S\{u}, v, y) + 1
            path ← F(S\{u}, v, y) ∪ u
        end if
    end for
    L(S, v, u) ← len
    F(S, v, u) ← path
end if
return L(S, v, u)
```

Algorithm 2 STEP1.

for $S \in 2^E$ such that $|S| = (1-\alpha)\frac{m}{4}$ **do**
  for $v \in E$ **do**
    for $u \in E$ **do**
      if $v \in S$ and $u \in S$ **then**
        GETLEN(S, v, u) ▷ We are computing $L(S, v, u)$ and $F(S, v, u)$ but we are not needing this results at the moment. We need it for Step 2.
      end if
    end for
  end for
end for

Let QMAX$((x_1, \ldots, x_N))$ be the implementation of the quantum maximum finding algorithm [9] for a sequence $x_1, \ldots, x_N$.

The most nested quantum maximum finding algorithm for some $E_4 \subset E, |E_4| = \frac{m}{4}$ and $u, v \in E$ is

$$\text{QMAX}((L(E_\alpha, v, y) + L((E_4 \backslash E_\alpha) \cup \{y\}, y, u) : E_\alpha \subset E_4, |E_\alpha| = (1-\alpha)\frac{m}{4}, y \in E_\alpha))$$

The middle quantum maximum finding algorithm for some $E_2 \subset E, |E_2| = \frac{m}{2}$ and $u, v \in E$ is

$$\text{QMAX}((L(E_4, v, y) + L((E_2 \backslash E_4) \cup \{y\}, y, u) : E_4 \subset E_2, |E_4| = n/4, y \in E_4))$$

Note that $|E_4| = m/4$ and $|E_2 \backslash E_4| = m/4$. We use the invocation of QMAX (the most nested quantum maximum finding algorithm) instead of $L(E_4, v, y)$ and $L(E_2 \backslash E_4, y, u)$.

The final quantum maximum finding algorithm for some $u, v \in E$ is

$$\text{QMAX}((L(E_2, v, y) + L((E \backslash E_2) \cup \{y\}, y, u) : E_2 \subset E, |E_2| = m/2, y \in E_2))$$

Note that $|E_2| = m/2$ and $|E \backslash E_2| = m/2$. We use the invocation of QMAX (the middle quantum maximum finding algorithm) instead of $L(E_2, v, y)$ and $L((E \backslash E_2) \cup \{y\}, y, u)$.

The procedure QMAX returns not only the maximal value, but the index of the target element. Therefore, by the "index" we can obtain the target paths using F function. So the result path is $P = P^1 \circ P^2$, where P^1 is the result path for $L(E_2, v, y)$ and P^2 is the result path for $L((E \backslash E_2) \cup \{y\}, y, u)$.

$P^1 = P^{1,1} \circ P^{1,2}$, where $P^{1,1}$ is the result path for $L(E_4, v, y)$ and $P^{1,2}$ is the result path for $L((E_2 \backslash E_4) \cup \{y\}, y, u)$. By the same way we can construct $P^2 = P^{2,1} \circ P^{2,2}$.

$P^{1,1} = P^{1,1,1} \circ P^{1,1,2}$, where $P^{1,1,1}$ is the result path for $L(E_\alpha, v, y)$ and $P^{1,1,2}$ is the result path for $L((E_4 \backslash E_\alpha) \cup \{y\}, y, u)$. Note, that this values were precomputed classically, and were stored in $F(E_\alpha, v, y)$ and $F((E_4 \backslash E_\alpha) \cup \{y\}, y, u)$ respectively.

By the same way we can construct

$$P^{1,2} = P^{1,2,1} \circ P^{1,2,2},$$

$$P^{2,1} = P^{2,1,1} \circ P^{2,1,2},$$

$$P^{2,2} = P^{2,2,1} \circ P^{2,2,2}.$$

The final Path is

$$P = P^1 \circ P^2 = (P^{1,1} \circ P^{1,2}) \circ (P^{2,1} \circ P^{2,2}) =$$

$$\Big((P^{1,1,1} \circ P^{1,1,2}) \circ (P^{1,2,1} \circ P^{1,2,2})\Big) \circ \Big((P^{2,1,1} \circ P^{2,1,2}) \circ (P^{2,2,1} \circ P^{2,2,2})\Big)$$

Let us present the final algorithm as Algorithm 3.

Algorithm 3 Algorithm for LTP.

```
STEP1()
len ← −1
path ← ()
for v ∈ E do
    for u ∈ E do
        currentLen ← QMAX((L(E_2, v, y) + L((E\E_2) ∪ {y}, y, u) : E_2 ⊂ E, |E_2| = m/2, y ∈ E_2))
        if len < currentLen then
            len ← currentLen
            path ← ((P^{1,1,1} ∘ P^{1,1,2}) ∘ (P^{1,2,1} ∘ P^{1,2,2})) ∘ ((P^{2,1,1} ∘ P^{2,1,2}) ∘ (P^{2,2,1} ∘ P^{2,2,2}))
        end if
    end for
end for
return path
```

The complexity of the algorithm is presented in the next theorem.

Theorem 1 *Algorithm 3 solves LTP with* $O^*(1.728^m)$ *running time and constant bounded error.*

Proof. The correctness of the algorithm follows from the above discussion. Let us present an analysis of running time.

Complexity of Step 1 (Classical preprocessing) is

$$O^*\left(\binom{m}{(1-\alpha)\frac{m}{4}}\right) = O^*(1.728^m).$$

Complexity of Step 2 (Quantum part) is complexity of three nested Durr-Hoyer maximum finding algorithms. Due to [9, 11, 10, 1], the complexity is

$$O^*\left(\sqrt{\binom{m}{m/2}}\cdot\sqrt{\binom{m/2}{m/4}}\cdot\sqrt{\binom{m/4}{\alpha m/4}}\right)=O^*(1.728^m).$$

We invoke Step 1 and Step 2 sequentially. Therefore the total complexity is the sum of complexities for these steps. So, the total complexity is $O^*(1.728^m)$.

Only Step 2 has an error probability. The most nested invocation of the Durr-Hoyer algorithm has an error probability 0.1. Let us repeat it $2m$ times and choose the maximal value among all invocations. The algorithm has an error only if all invocations have an error. Therefore, the error probability is $0.1^{2m} = 100^{-m}$.

Let us consider the middle Durr-Hoyer algorithm's invocation. The probability of success is the probability of correctness of maximum finding and the probability of input correctness, i.e., the correctness of all the nested Durr-Hoyer algorithm's invocations. It is

$$0.9\cdot(1-100^{-m})^{\gamma}, \text{ where } \gamma=\binom{m/2}{m/4}$$

$$\geq 0.8, \text{ for enough big } m.$$

So, the error probability is at most 0.2.

Let us repeat the middle Durr-Hoyer algorithm $2m$ times and choose the maximal value among all invocations. Similar to the previous analysis, the error probability is $0.2^{2m} = 25^{-m}$.

Therefore, the total success probability that is the final Durr-Hoyer algorithm's success probability is the following one.

$$0.9\cdot(1-25^{-m})^{\beta}, \text{ where } \beta=\binom{m}{m/2}$$

$$> 0.8, \text{ for enough big } m.$$

Therefore, the total error probability is at most 0.2. □

Acknowledgments

The research is funded by the subsidy allocated to Kazan Federal University for the state assignment in the sphere of scientific activities, project No. 0671-2020-0065; supported by the Kazan Federal University Strategic Academic Leadership Program.

References

[1] F. Ablayev, M. Ablayev, J. Z. Huang, K. Khadiev, N. Salikhova, and D. Wu. On quantum methods for machine learning problems part i: Quantum tools. *Big Data Mining and Analytics*, 3(1):41–55, 2019.

[2] A. Ambainis. Understanding quantum algorithms via query complexity. In *Proc. Int. Conf. of Math. 2018*, volume 4, pages 3283–3304, 2018.

[3] Andris Ambainis, Kaspars Balodis, Jānis Iraids, Martins Kokainis, Krišjānis Prūsis, and Jevgēnijs Vihrovs. Quantum speedups for exponential-time dynamic programming algorithms. In *Proceedings of the Thirtieth Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 1783–1793. SIAM, 2019.

[4] Richard Bellman. Dynamic programming treatment of the travelling salesman problem. *Journal of the ACM (JACM)*, 9(1):61–63, 1962.

[5] Michel Boyer, Gilles Brassard, Peter Høyer, and Alain Tapp. Tight bounds on quantum searching. *Fortschritte der Physik*, 46(4-5):493–505, 1998.

[6] Vasek Chvatal David L. Applegate, Robert E. Bixby and William J. Cook. *The traveling salesman problem: a computational study.* Princeton University Press, 2007.

[7] Marzio De Biasi. Is the longest trail problem easier than the longest path problem?, 2014. Stack Exchange. Theoretical Computer Science. https://cstheory.stackexchange.com/questions/20682/is-the-longest-trail-problem-easier-than-the-longest-path-problem.

[8] Ronald de Wolf. *Quantum computing and communication complexity.* 2001.

[9] C. Dürr and P. Høyer. A quantum algorithm for finding the minimum. *arXiv:quant-ph/9607014*, 1996.

[10] Christoph Dürr, Mark Heiligman, Peter Høyer, and Mehdi Mhalla. Quantum query complexity of some graph problems. In *International Colloquium on Automata, Languages, and Programming*, pages 481–493. Springer, 2004.

[11] 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.

[12] Michael Held and Richard M Karp. A dynamic programming approach to sequencing problems. *Journal of the Society for Industrial and Applied mathematics*, 10(1):196–210, 1962.

[13] Stephen Jordan. Quantum algorithms zoo, 2021. http://quantumalgorithmzoo.org/.

[14] K. Khadiev, D. Kravchenko, and D. Serov. On the quantum and classical complexity of solving subtraction games. In *Proceedings of CSR 2019*, volume 11532 of *LNCS*, pages 228–236. 2019.

[15] K. Khadiev and L. Safina. Quantum algorithm for dynamic programming approach for dags. applications for zhegalkin polynomial evaluation and some problems on dags. In *Proceedings of UCNC 2019*, volume 4362 of *LNCS*, pages 150–163. 2019.

[16] Eugene L Lawler. *Combinatorial optimization: networks and matroids*. Courier Corporation, 2001.

[17] M. A Nielsen and I. L Chuang. *Quantum computation and quantum information*. Cambridge univ. press, 2010.

[18] Jacob Scott, Trey Ideker, Richard M Karp, and Roded Sharan. Efficient algorithms for detecting signaling pathways in protein interaction networks. *Journal of Computational Biology*, 13(2):133–144, 2006.

On the Steiner variant for the general position problem on graphs

Sandi Klavžar[1,2], Dorota Kuziak*[3], Iztok Peterin[2], and Ismael G. Yero[3]

[1]University of Ljubljana, Slovenia
[2]University of Maribor, Slovenia
[3]Universidad de Cádiz, Algeciras, Spain

Abstract

For a given graph G and a set $W \subseteq V(G)$, the Steiner distance of W is the smallest possible size among all connected subgraph of G containing W. Such subgraph is indeed a tree, that is frequently called a Steiner W-tree. A set of vertices $A \subseteq V(G)$ is called a k-Steiner general position set for G if every set $B \subseteq A$ having cardinality k, and every Steiner B-tree T_B satisfy that $V(T_B) \cap A = B$. In relation to this, the k-Steiner general position number $\mathrm{sgp}_k(G)$ of the graph G stands for the cardinality of a largest possible k-Steiner general position set in G. Several contributions on the k-Steiner general position number of graphs are given in this work.

AMS Subject Classification (2010): 05C12.

1 Introduction

The Steiner general position problem on graphs raised up in [2], in connection with the lastly intensively studied general position problem on graphs, which in turns has its roots in some older problems arising in computational geometry. That is for instance, the problem to finding the maximum number of points that can be placed in the $n \times n$ grid so that no three points lie on a line is known as the *no-three-in-line problem* and was posed back in 1917 by Dudeney [1]. Recently, several studies on the standard general position problem on graphs have been published, by taking the starting points independently introduced in [3, 4]. In this work, a new approach of the general position problem is studied.

We now formally define the necessary concepts, and for any other basic terminology, the reader can use any basic graph theory book. The *distance* $d_G(u, v)$ between two vertices u and v of G is the minimum number of edges on a u, v-path in G. If there is

*Corr. author email: *dorota.kuziak@uca.es*

no such path, then we set $d_G(u,v) = \infty$. A *general position set* of a graph G is a set of vertices $S \subseteq V(G)$ such that no three vertices from S lie on a common geodesic. The cardinality of a largest possible general position set is the *general position number* $\mathrm{gp}(G)$ of G.

For a nonempty set $W \subseteq V(G)$, the *Steiner distance* of W, denoted by $d_G(W)$, is the minimum size of a connected subgraph of G containing W. Such a subgraph is clearly a tree called a *Steiner W-tree*. If G is not connected and the vertices of W lie in at least two components of G, then no Steiner W-tree exists and we set $d_G(W) = \infty$.

Let $k \in \mathbb{N}$ and let G be a graph. Then $A \subseteq V(G)$ is a *k-Steiner general position set* if for every set $B \subseteq A$ of cardinality k (from now on a k-set), and for every Steiner B-tree T_B, it follows that $V(T_B) \cap A = B$. In other words, A is a k-Steiner general position set if no $k+1$ distinct vertices from A lie on a common Steiner B-tree, where $B \subseteq A$ and $|B| = k$. Clearly, if $|A| \leq k$, then A is k-Steiner general position set. Hence we may define the *k-Steiner general position number* of G, denoted by $\mathrm{sgp}_k(G)$, as the cardinality of a largest k-Steiner general position set in G. A k-Steiner general position set of cardinality $\mathrm{sgp}_k(G)$ will be called a *k-sgp-code*. Note that $\mathrm{sgp}_2(G) = \mathrm{gp}(G)$.

2 Main results

We next make a resume of the most significant known contributions concerning the Steiner general position problem on graphs. For their proofs, we suggest the reader the recent published article [2].

We introduce first k-Steiner cliques, a concept that might be of interest also elsewhere. If $k \geq 2$ is a fixed integer, then $A \subseteq V(G)$ is a *k-Steiner clique* if $G[B]$ (subgraph induced by B) is connected for every k-set $B \subseteq A$. The cardinality of a largest k-Steiner clique will be denoted by $s\omega_k(G)$. Note that $s\omega_2(G) = \omega(G)$ (where $\omega(G)$ is the clique number of G).

Remark 2.1 [2] *If G is a connected graph and $k \in [2 : n(G) - 1]$, then*

$$\max\{k, \omega(G)\} \leq s\omega_k(G) \leq \mathrm{sgp}_k(G) \leq n(G)\,.$$

If $n > k$, then $s\omega_k(P_n) = k$, hence the first inequality in Remark 2.1 is sharp. If $n > k \geq 3$, then $s\omega_k(K_n - M) = n$, where M is a matching of K_n.

Proposition 2.2 [2] *Let G be a graph and let $k \in [2 : n(G) - 1]$. Then, $\mathrm{sgp}_k(G) = n(G)$ if and only if G is $(n(G) - k + 1)$-connected.*

Corollary 2.3 [2] *The equality chain $\mathrm{sgp}_2(G) = \cdots = \mathrm{sgp}_{n(G)-1}(G) = n(G)$ holds if and only if G is a complete graph.*

We next show that, a bit surprisingly, it is in general not true that a k-Steiner general position set is also a k'-Steiner general position set for some $k' > k$.

Proposition 2.4 [2] *For every $k \geq 3$ there exist a graph $G^{(k)}$ and a set $A_k \subseteq V(G^{(k)})$ such that A_k is a $(k-1)$-Steiner general position set and is not a k-Steiner general position set of $G^{(k)}$.*

We now center our attention into the k-Steiner general position number of several graph classes.

Theorem 2.5 [2] *If T is a tree with $n(T) \geq 3$, $\ell(T)$ leaves, and $k \in [2 : n(T)-1]$, then*

$$\mathrm{sgp}_k(T) = \begin{cases} \ell(T); & k \leq \ell(T), \\ k; & k > \ell(T). \end{cases}$$

Theorem 2.6 [2] *If $n \geq 3$ and $k \in [2 : n-1]$, then* $\mathrm{sgp}_k(C_n) = \begin{cases} k; & k \in \left[\left\lfloor \frac{2n}{3} \right\rfloor : n-2\right], \\ k+1; & \text{otherwise.} \end{cases}$

The join $G \vee H$ of disjoint graphs G and H is the graph with vertex set $V(G \vee H) = V(G) \cup V(H)$ and edge set

$$E(G \vee H) = E(G) \cup E(H) \cup \{gh : g \in V(G), h \in V(H)\}.$$

Let G be a graph and let $A \subseteq V(G)$ be a set of vertices of cardinality at least k. Then we say that A is a *k-Steiner join-critical set* of G if for each k-subset B of A we have $d_{G[A]}(B) \neq k$. That is, A is a k-Steiner join-critical set if there exists no k-set $B \subseteq A$ such that a Steiner B-tree in $G[A]$ contains $k+1$ vertices. By $\mathrm{sjc}_k(G)$ we denote the cardinality of a largest k-Steiner join-critical set. For a given set $D \subseteq V(G)$, if every connected component of $G[D]$ is of order at most k, then D is k-Steiner join-critical. For the particular case in which $D = V(G)$, if every connected component of G has order at most k, then $\mathrm{sjc}_k(G) = n(G)$. Note also that, by definition, if $k \geq n(G)$, then $\mathrm{sjc}_k(G) = n(G)$.

Theorem 2.7 [2] *If G and H are graphs and $k \in [2 : n(G \vee H) - 1]$, then*

$$\mathrm{sgp}_k(G \vee H) = \max\{s\omega_k(G \vee H), \mathrm{sjc}_k(G), \mathrm{sjc}_k(H)\}.$$

We next give some applications of Theorem 2.7.

Corollary 2.8 [2] *The following assertions hold for positive integers k, n, r, s.*

(i) If $k \in [2 : r+s-1]$, then $\mathrm{sgp}_k(K_{r+s}) = \mathrm{sgp}_k(K_r \vee K_s) = r+s$.

(ii) If $n \geq 6$ and $k \in [2 : n-1]$, then $\mathrm{sgp}_k(W_n) = \mathrm{sgp}_k(K_1 \vee C_{n-1}) = \max\{k+1, n - 2 - \left\lfloor \frac{n-2}{k+1} \right\rfloor\}$.

(iii) If $n \geq 4$ and $k \in [2 : n-1]$, then $\mathrm{sgp}_k(F_n) = \mathrm{sgp}_k(K_1 \vee P_{n-1}) = \max\{k+1, n - 1 - \left\lfloor \frac{n-1}{k+1} \right\rfloor\}$.

(iv) If $r \leq s$ and $k \in [2 : r+s-1]$, then

$$\mathrm{sgp}_k(K_{r,s}) = \mathrm{sgp}_k(\overline{K}_r \vee \overline{K}_s) = \begin{cases} \max\{s, \min\{k-1, r\} + k - 1\}; & k \leq s, \\ r+s; & k > s. \end{cases}$$

(v) If $k \in [2 : r+s-1]$, then $\mathrm{sgp}_k(K_r \vee \overline{K}_s) = \begin{cases} r + \min\{s, k-1\}; & k > \min\{r, s\}, \\ \max\{r+k-1, s\}; & k \leq \min\{r, s\}. \end{cases}$

Let G and H be two graphs. The lexicographic product $G \circ H$ is a graph with $V(G \circ H) = V(G) \times V(H)$. Two vertices (g, h) and (g', h') are adjacent if $gg' \in E(G)$ or $(g = g'$ and $hh' \in E(H))$.

Let k and ℓ be two positive integers with $k \leq \ell$. A set $A \subseteq V(G)$ is a $[k : \ell]$-*Steiner general position set* of a graph G, or a $[k : \ell]$-sgp set for short, if it is a j-Steiner general position set for every $j \in [k : \ell]$. The cardinality of a largest $[k : \ell]$-sgp set for G is represented as $\mathrm{sgp}_{[k:\ell]}(G)$. The family of all $[k : \ell]$-sgp sets of a graph G is denoted by $\mathcal{G}_{k,\ell}$. For every k-general Steiner position set S, we partition S into two sets $\mathcal{I}_S$ and $\mathcal{J}_S$, where $\mathcal{I}_S$ contains all isolated vertices in the subgraph of $G[S]$ and $\mathcal{J}_S = S \setminus \mathcal{I}_S$. Every set of vertices of cardinality at most k is a $[k : \ell]$-sgp set.

Theorem 2.9 [2] *Let G and H be nontrivial graphs, let G be connected, and let $k \in [2 : n(G) \cdot n(H) - 1]$. If $j = \left\lceil \frac{k}{n(H)} \right\rceil$ and $\ell = \min\{k, n(G)\}$, then*

$$\mathrm{sgp}_k(G \circ H) \geq \begin{cases} \max_{S \in \mathcal{G}_{2,k}} \{|\mathcal{I}_S| \mathrm{sjc}_k(H) + |\mathcal{J}_S| s\omega_k(H)\}; & k \leq n(H), \\ \mathrm{sgp}_{[j:\ell]}(G) n(H); & n(H) < k < n(G) \cdot n(H). \end{cases}$$

Moreover, the equality holds if $k > (n(G) - 1)n(H)$.

An interesting particular case of the result above is the next one, where an equality can be reached.

Theorem 2.10 [2] *If G and H are nontrivial graphs where G is connected, then*

$$\mathrm{gp}(G \circ H) = \max_{S \in \mathcal{G}_{2,2}} \{|\mathcal{I}_S| \mathrm{sjc}_2(H) + |\mathcal{J}_S| \omega(H)\}.$$

With P_∞ we denote the two ways infinite path. Let $V(P_\infty) = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ where i is adjacent to j if and only if $|i - j| = 1$. The infinite grid $P_\infty \,\square\, P_\infty$ is the Cartesian product of two infinite paths, that is $V(P_\infty \,\square\, P_\infty) = \{(i, j) : i, j \in \mathbb{Z}\}$ and $(i, j)(k, \ell) \in E(P_\infty \,\square\, P_\infty)$ when $|i - j| + |k - \ell| = 1$.

Theorem 2.11 [2] $\mathrm{sgp}_k(P_\infty \,\square\, P_\infty) \geq 2k$.

Acknowledgements

Sandi Klavžar and Iztok Peterin acknowledge the financial support from the Slovenian Research Agency (research core funding No. P1-0297 and projects J1-9109, J1-1693, J1-2452, N1-0095). Dorota Kuziak and Ismael G. Yero have been partially supported by the Spanish Ministry of Science and Innovation through the grant PID2019-105824GB-I00.

References

[1] H.E. Dudeney, Amusements in Mathematics, Nelson, Edinburgh, 1917.

[2] S. Klavžar, D. Kuziak, I. Peterin, I. G. Yero, A Steiner general position problem in graph theory, Comp. Applied Math. 40(6) (2021) article # 223.

[3] P. Manuel, S. Klavžar, A general position problem in graph theory, Bull. Aust. Math. Soc. 98 (2018) 177–187.

[4] S. V. Ullas Chandran, G. Jaya Parthasarathy, The geodesic irredundant sets in graphs, Int. J. Math. Combin. 4 (2016) 135–143.

The Hats game. The power of constructors

Aleksei Latyshev, joint with Konstantin Kokhas

The Hats game: Several sages wearing colored hats occupy the vertices of a graph. Each sage can have a hat of one of k colors. Each sage tries to guess the color of his own hat merely on the basis of observing the hats of his neighbors without exchanging any information. A predetermined guessing strategy is winning if it guarantees at least one correct individual guess for every assignment of colors.

Let $HG(G)$ be the maximum k for which the sages have a deterministic winning strategy. Usually relations of $HG(G)$ with other graph parameters (such as maximal degree, diameter, clique number, etc) are studied. And one of the interesting question is whether the planarity of graph imposes any constraint on $HG(G)$.

Currently boundness of $HG(G)$ for planar graphs is an open question. Bradshaw [2] showed that for outerplanar graphs $HG(G) < 2^{125000}$. On the other hand little is known about the lower bound either: Alon and Chizewer [1] proved the existence of a planar graph G with $HG(G) = 12$.

In this presentation, based on [4], we propose recipes of building an outerplanar graph G with $HG(G) = 6$ and a planar graph G with $HG(G) = 14$. This recipe widely uses a "constructors" machinery, proposed in papers [3] and [5]. Thus, it shows once again that "constructor"-theorems are useful not only for investigate more general problem with a variable number of hats, but also for obtaining state of the art results in the classical Hats game.

References

[1] Alon, N., and Chizewer, J. On the hat guessing number of graphs. *arXiv:2107.05995 [cs, math]* (2021).

[2] Bradshaw, P. On the hat guessing number of a planar graph class. *arXiv:2106.01480 [math]* (2021).

[3] Kokhas, K., and Latyshev, A. Cliques and constructors in "hats" game. i. *Journal of Mathematical Sciences 255*, 1 (2021), 39–57.

[4] Kokhas, K. P., and Latyshev, A. S. The hats game. the power of constructors. *Journal of Mathematical Sciences 255*, 2 (2021), 124–131.

[5] Kokhas, K. P., Latyshev, A. S., and Retinskiy, V. I. Cliques and constructors in "hats" game. II. *Journal of Mathematical Sciences 255*, 1 (2021), 58–70.

Three ways to locate-dominate every vertex in a graph

Tuomo Lehtilä*

Université Claude Bernard Lyon 1, LIRIS, F-69622 Lyon, France.
Department of Mathematics and Statistics,
University of Turku, FI-20014 Turku, Finland.
tuomoleh@gmail.com

Abstract

We consider $(1, \leq \ell)$-locating-dominating codes of type B, multiple intruder locating-dominating codes (MILD codes) and open-irredundant sets. In particular, we show that the two first mentioned are equivalent with each other when $\ell \geq \Delta(G) + 1$ and they are also equivalent with the complement of open irredundant set. With these equivalences we expand results between these concepts. Moreover, we show that the maximum irredundance number $IR(G)$ is a general lower bound for these codes. It has been shown that these codes contain at least half of vertices in any graph. We discuss how to attain this bound in some graph classes. Moreover, we show that deciding whether there exists a MILD code containing exactly half of vertices in a graph, is an $\mathcal{NP}$-complete problem.

Keywords: Graph theory; domination; location-domination; open-irredundant; irredundancy

Let $G = (V, E)$ be an undirected, simple and finite graph and $N[v]$ be the *closed neighbourhood* of the vertex $v \in V$, that is, the set of vertices adjacent to v and v itself. Moreover, for a set of vertices $C \subseteq V$, we denote the *I-set* of v by

$$I_G(C; v) = I(v) = N[v] \cap C.$$

If the set C is non-empty, we will call it *code* and its members *codewords*.

Slater and Rall have introduced in the 1980s locating-dominating codes [16]. A set of vertices C is a *locating-dominating code* in G if C is *dominating*, that is, each vertex has a non-empty I-set, and if each non-codeword has a unique I-set among the non-codewords, that is, for each $u, v \in V \setminus C$, we have

$$I(u) \neq I(v). \tag{1}$$

*Research supported by the Jenny and Antti Wihuri Foundation and the Finnish Cultural Foundation.

We extend the notation of I-sets for sets of vertices in a natural way, for $X \subseteq V$, we say that

$$I(X) = \bigcup_{v \in X} I(v).$$

One of the major motivations to study location-domination has been *sensor networks*. In them, the vertices of a graph represent locations and edges connections between locations. Now, a codeword $c \in C$ represents a location with a sensor and if $c \in I(u)$, then the location at vertex u is monitored by a sensor at a location depicted by codeword vertex c. If the sensors are placed according to the locating-dominating code and we have an intruder in a location without a sensor (non-codeword vertex), then we can recognize the location just by comparing the I-sets due to Definition (1).

However, this approach is problematic if there can be multiple intruders in the network. To solve that problem, Honkala et al. [10] introduced $(1, \leq \ell)$-*locating-dominating codes of types A and B* (for short $(1, \leq \ell)$-LDA and -LDB codes). These are locating-dominating codes which have capability to locate at most ℓ intruders in the network simultaneously. In general, the $(1, \leq \ell)$-LDA codes are larger and more demanding than the $(1, \leq \ell)$-LDB codes. The reader may find more information about these codes in [3, 12, 13, 14].

In this paper, we are especially interested in a situation where ℓ is very large. Let $\Delta(G)$ ($\delta(G)$) denote the maximum (minimum) degree of the graph G. It is possible to show that if $\ell \geq \Delta(G) + 1$, then all $(1, \leq \ell)$-LDA codes contain every vertex in G. Moreover, another related class of dominating codes, $(1, \leq \ell)$-identifying codes, do not even exist in a graph G when $\ell \geq \delta(G) + 1$, [11, Theorem 8]. However, the same is not true for $(1, \leq \ell)$-LDB codes. The $(1, \leq \ell)$-LDB code C is defined in the following way, for any two distinct sets $X, Y \subseteq V \setminus C$ with $|X|, |Y| \leq \ell$ we have

$$I(X) \neq I(Y).$$

When $\ell = 1$, these codes are just normal locating-dominating codes. Moreover, each $(1, \leq \ell + 1)$-LDB code is also a $(1, \leq \ell)$-LDB code.

We can show that, in any graph G each $(1, \leq \ell)$-LDB code is also a $(1, \leq \ell + 1)$-LDB code if $\ell \geq \Delta(G) + 1$, and vice versa. Moreover, this lower bound for ℓ is tight in some graphs; there are graphs for which some $(1, \leq \Delta(G))$-LDB codes are not $(1, \leq \Delta(G)+1)$-LDB codes. Furthermore, there exists a family of graphs $\mathcal{G}$, for which there exists a $(1, \leq \ell)$-LDB code which is not a $(1, \leq \ell + 1)$-LDB code for each $1 \leq \ell \leq \Delta(G)$ when $G \in \mathcal{G}$. In Figure 1, we give an example graph for $\Delta(G) = 4$. Due to this, we will concentrate on the $(1, \leq \Delta(G) + 1)$-LDB codes. The cardinality of the smallest possible, *optimal*, $(1, \leq \ell)$-LDB code in the graph G is denoted by $\gamma_\ell^{LDB}(G)$. Now, our considerations give the following chain of inequalities and equalities:

$$\gamma^{LD}(G) \leq \gamma_2^{LDB}(G) \leq \cdots \leq \gamma_{\Delta(G)+1}^{LDB}(G) = \gamma_{\Delta(G)+2}^{LDB}(G).$$

Besides LDB-codes, we need to define open-irredundant sets, they were originally introduced by Farley and Shacham [5] and have been since studied in, for example,

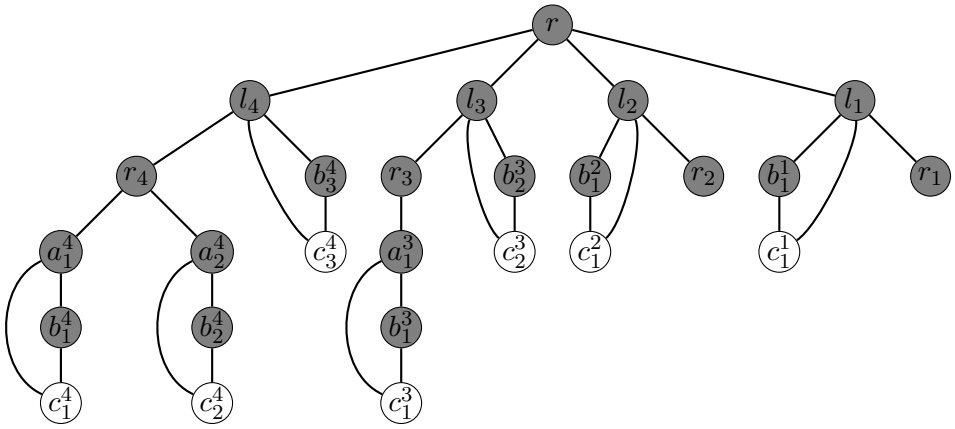

Figure 1: Gray vertices form the smallest possible $(1, \leq \Delta(G)+1)$-LDB code.

[1, 2, 4, 6, 7, 15]. We say that S is an *open-irredundant set* if for each $v \in S$ we have

$$N(v) \setminus N[S \setminus \{v\}] \neq \emptyset.$$

This set is also called *external private neighbourhood of* v or $epn[v, S]$. We link this concept to LDB-codes with the following lemma:

Lemma 1. *A set of vertices $S \subseteq V$ is open irredundant if and only if $V \setminus S$ is a $(1, \leq \Delta(G)+1)$-LDB code.*

Besides open-irredundancy, we are also interested in recently introduced [17, 18] *multiple intruder locating-dominating codes* (MILD codes). A code $C \subseteq V$ is a MILD code if for each non-codeword $u \in V \setminus C$ there exists a codeword $c \in C$ such that

$$N(c) \cap (V \setminus C) = \{u\}.$$

The cardinality of a maximum open-irredundant set in graph G is denoted by $OIR(G)$ and the cardinality of a minimum MILD code by $\gamma^{ML}(G)$.

Interestingly, also MILD codes are equivalent with the two previous sets.

Theorem 2. *Let G be a graph and $C \subseteq V$ be a code in G. Then the following three conditions are equivalent:*

1. *C is a $(1, \leq \Delta(G)+1)$-LDB code;*
2. *C is a MILD code and*
3. *$V \setminus C$ is an open-irredundant set.*

Theorem 2 immediately gives the following equality for an n-vertex graph G:

$$\gamma^{LDB}_{\Delta(G)+1}(G) = \gamma^{ML}(G) = n - OIR(G). \tag{2}$$

Although these concepts have been studied in multiple articles, there are surprisingly many open questions left to study. For $(1, \leq \ell)$-LDB codes this is probably due to the existence of the two parameters and many results acquired for MILD codes already existed for open-irredundant sets. Moreover, since these three properties are equivalent, any new result for one of them increases our understanding for all of them.

A well-known property of complements of open-irredundant sets and MILD codes is that they contain at least half of the vertices in any graph. Thus, a trivial lower bound for these codes has been presented as

$$\gamma^{ML}(G) \geq n/2$$

for an n-vertex graph G. Interestingly, this lower bound can also be achieved. If C is a MILD code in G with $\gamma^{ML}(G) = n/2$, then every codeword in C has exactly one adjacent non-codeword and each non-codeword has exactly one adjacent codewords. Thus, we partition the graph into two equal parts which are connected exactly by a perfect matching. This, raises a natural question, which graphs admit a MILD code with $\gamma^{ML}(G) = n/2$?

For a tree T, Golumbic and Laskar [7] have mentioned that $OIR(T) = m(T)$ where $m(T)$ is the matching number of T. Since $m(T) + \alpha(T) = n$ for any tree T, where $\alpha(T)$ is the independence number of T, we have

$$\gamma^{ML}(T) = \alpha(T).$$

Hence, we have $\gamma^{ML}(T) = n/2$ in a tree T if and only if we have a perfect matching in T. However, using (k, δ, ρ) graph partitions defined by Heggernes and Telle [9], we can give following result showing that the question is hard in the case of general graphs.

Theorem 3. *Let G be a graph on n vertices. Then it is an $\mathcal{NP}$-complete problem to decide whether G admits a MILD code with cardinality $n/2$.*

However, as we have seen for trees, for some graph classes the problem is easy to solve. We give following result for Cartesian products of graphs.

Theorem 4. *Let $G = (V, E_1)$ and $G' = (U, E_2)$ be connected graphs and let $D = G \square G' = (V \times U, E)$ be a graph on n vertices. Then graph D admits a MILD code with cardinality $n/2$ if and only if G (or G') admits a MILD code with cardinality $|V(G)|/2$ (or $|V(G')|/2$).*

Besides $\gamma^{ML}(G) \geq n/2$, the MILD codes are lacking in (good) known general bounds and the same is true for $(1, \leq \Delta(G) + 1)$-LDB codes. However, we know something for open-irredundant sets. Farley and Shacham have shown in [5] for any graph G with $\delta(G) \geq 1$ that

$$\gamma(G) \leq OIR(G) \leq IR(G),$$

where $\gamma(G)$ is the cardinality of the minimum dominating set in G and $IR(G)$ is the cardinality of the maximum irredundant set in G. A set of vertices S is *irredundant* in G if we have $N[v] \setminus N[S \setminus \{v\}] \neq \emptyset$ for each $v \in S$. Thus, we have

$$n - \gamma(G) \geq \gamma^{ML}(G) \geq n - IR(G).$$

We present a new (tight) general lower bound in the following theorem.

Theorem 5. *Let G be a graph, then $\gamma^{ML}(G) \geq IR(G)$.*

When we append this inequality to the well-known domination chain [8], we get that

$$ir(G) \leq \gamma(G) \leq i(G) \leq \alpha(G) \leq \Gamma(G) \leq IR(G) \leq \gamma^{ML}(G),$$

where $ir(G)$ is the minimum size of any maximum irredundant set, $i(G)$ is the minimum size of any maximal independent set and $\Gamma(G)$ is the maximum size of any minimal dominating set in G.

Acknowledgments

I would like to thank Ville Junnila and Tero Laihonen for the fruitful discussions on the topic.

References

[1] E. Cockayne, O. Favaron, S. Finbow, and C. M. Mynhardt. Open irredundance and maximum degree in graphs. *Discrete mathematics*, 308(23):5358–5375, 2008.

[2] E. Cockayne and S. Finbow. Generalised irredundance in graphs: Nordhaus-gaddum bounds. *Discussiones Mathematicae Graph Theory*, 24(1):147–160, 2004.

[3] G. Exoo, V. Junnila, and T. Laihonen. On location-domination of set of vertices in cycles and paths. *Congressus Numerantium*, 202:97–112, 2010.

[4] A. M. Farley and A. Proskurowski. Computing the maximum order of an open irredundant set in a tree. *Congressus Numerantium*, 41:219–228, 1984.

[5] A. M. Farley and N. Shacham. Senders in broadcast networks: open-irredundancy in graphs. *Congressus Numerantium*, 38:47–57, 1983.

[6] O. Favaron. A note on the open irredundance in a graph. *Congressus Numerantium*, 66:316–318, 1988.

[7] M. C. Golumbic and R. C. Laskar. Irredundancy in circular arc graphs. *Discrete Applied Mathematics*, 44(1-3):79–89, 1993.

[8] T. W. Haynes, S. T. Hedetniemi, and P. J. Slater. *Fundamentals of Domination in Graphs. 1998.* Marcel Dekker, New York, 1998.

[9] P. Heggernes and J. A. Telle. Partitioning graphs into generalized dominating sets. *Nordic Journal of Computing*, 5(2):128–142, 1998.

[10] I. Honkala, T. Laihonen, and S. Ranto. On locating-dominating codes in binary Hamming spaces. *Discrete Mathematics and Theoretical Computer Science*, 6(2), 2004.

[11] T. Laihonen and S. Ranto. Codes identifying sets of vertices. In *Lecture Notes in Computer Science*, volume 2227, pages 82–91, 2001.

[12] M. Pelto. On locating-dominating codes for locating large numbers of vertices in the infinite king grid. *Australasian Journal of Combinatorics*, 50:127–140, 2011.

[13] M. Pelto. On (r,$\leq$ 2)-locating-dominating codes in the infinite king grid. *Advances in Mathematics of Communications*, 6(1):27–38, 2012.

[14] M. Pelto. Optimal (r,$\leq$ 3)-locating–dominating codes in the infinite king grid. *Discrete Applied Mathematics*, 161(16-17):2597–2603, 2013.

[15] D. F. Rall. On well-dominated direct, cartesian and strong product graphs. *arXiv preprint arXiv:2105.09797*, 2021.

[16] D. F. Rall and P. J. Slater. On location-domination numbers for certain classes of graphs. *Congressus Numerantium*, 45:97–106, 1984.

[17] K. Venugopal and K. A. Vidya. Multiple intruder locating dominating sets. *International Journal of Scientific Research in Mathematical and Statistical Sciences*, 6(2):394–398, 2019.

[18] K. Venugopal and K. A. Vidya. Multiple intruder locating dominating sets in graphs: An algorithmic approach. *Communications in Mathematics and Applications*, 11(2):259–269, 2020.

Cooperative game theory and network analysis

Vladimir V. Mazalov

Institute of Applied Mathematical Research
Karelia Research Center of Russian Academy of Science
vmazalov@krc.karelia.ru

Abstract

The methods of cooperative game theory are used for the analysis of the network structure. First, a cooperative game and its characteristic function associated with the graph is determined. Then the solution of the cooperative game is derived. The solution can be in the form of the core, the Shapley value, the Myerson value, the Owen value, etc. Depending on the type of characteristic function, the value of the cooperative game can be interpreted as the measure of centrality of vertices and edges, or it can be a measure of communicability. The use of cooperative game theory methods can help in graph clustering problems. In this case, the method of finding Nash-stable coalition partitions in a cooperative game is used.

We demonstrate how this approach can be used for ranking the corpus of texts of a news portal. Each text is assigned a vertex of a certain graph, and its structure is determined based on the semantic connectivity of the texts. As a measure of centrality, the Myerson value is used in a cooperative game on a graph, where the number of simple paths in a subgraph of a certain length is chosen as a characteristic function. The operation of the ranking algorithm is illustrated by numerical examples related to a specific news portal.

References

Avrachenkov, K.E.; Kondratev, A.Y.; Mazalov, V.V.; Rubanov, D.G. Network partitioning algorithm as cooperative games. Computational Social Networks, 5, 2018, pp. 1–28.

Aspects of stability in multiobjective integer linear programming problem with objective partitioning

Yury Nikulin[1] and Vladimir Emelichev[2]

[1]University of Turku, Department of Mathematics and Statistics, FIN-20014 Turku, Finland, yurnik@utu.fi
[2]Belarusian State University, Faculty of Mechanics and Mathematics, BLR-220030 Minsk, Belarus, vemelichev@gmail.com

Abstract

In a multiobjective problem of integer linear programming, parametrization of optimality principle is introduced by dividing a set of objectives into a family of disjoint subsets. The introduction of this principle makes possible to connect two classical optimality sets, namely, extreme and Pareto. The admissible independent perturbations in such problem is formed by a set of additive matrices, with arbitrary Hölder's norms specified in the solution and criterion spaces. The lower and upper bounds for the radius of stability are obtained. The main result is complemented with several important corollaries.

Keywords: Multiobjective integer programming, a set of extreme solutions, stability radius, Hölder's norms, post-optimal analysis.

1 Introduction

This work continues research started in [1], where stability aspects of the multiobjective ILP with the set of extreme solutions problem were scrutinized. In this work we generalize some of the results for the case of parametrized optimality. The parametrized optimality principle that was first introduced in [2] by dividing a set of objectives into a family of disjoint subsets. While [2] deals with the type of stability known as quasistability, the recent paper tackles the classical concept of stability. The paper is organized as follows. In section 2, we formulate parametric optimality and introduce basic concepts. In section 3, we formulate and prove the main result regarding the lower and upper bounds for the stability radius. Section 4 lists most important corollaries.

2 Main definitions and problem formulation

Consider a multicriteria integer linear programming problem (ILP) in the following formulation. Let $C=[c_{ij}] \in \mathbf{R}^{m\times n}$ be a matrix whose rows are denoted by $C_i=(c_{i1}, c_{i2}, ..., c_{in}) \in \mathbf{R}^n$, $i \in N_m=\{1, 2, ...,m\}$, $m \geq 1$. Let $x=(x_1, x_2, ..., x_n)^T \in X \subset \mathbf{Z}^n$, $n \geq 2$, and the number of elements of the set X is finite and greater than one. On the set of (admissible) solutions X, we define a vector linear criterion

$$Cx = (C_1x, C_2x, \ldots, C_mx)^T \longrightarrow \min_{x\in X}. \tag{1}$$

In the space $\mathbf{R}^k$ of arbitrary dimension $k \in \mathbf{N}$, we introduce a binary relation that generates the Pareto optimality principle [3]:

$$y \succ y' \Rightarrow y \geq y' \ \& \ y \neq y',$$

where $y = (y_1, y_2, \ldots, y_k)^T \in \mathbf{R}^k$, $y' = (y'_1, y'_2, \ldots, y'_k)^T \in \mathbf{R}^k$. The symbol $\overline{\succ}$ denotes the negation of the relation $\succ$.

Let $\emptyset \neq I \subseteq N_m, |I| =v$, and let C_I denote the submatrix of the matrix $C \in \mathbf{R}^{m\times n}$ consisting of rows of this matrix with the numbers from I, i.e.

$$C_I=(C_{i_1}, C_{i_2}, ..., C_{i_v})^T, \quad I=\{i_1, i_2, ..., i_v\},$$

$$1 \leq i_1<i_2< ... <i_v \leq m, \quad C_I \in \mathbf{R}^{v\times n}.$$

Let $s \in N_m$, and let $N_m=\cup_{k\in N_s} I_k$ be a partition of the set N_m into s nonempty sets, i.e. $I_k \neq \emptyset$, $k \in N_s$, and $i \neq j \Rightarrow I_i \cap I_j=\emptyset$. For this partition, we introduce a set of $(I_1, I_2, ..., I_s)$-efficient solutions according to the formula:

$$G^m(C, I_1, I_2, ..., I_s) =$$

$$\{x \in X : \ \exists k \in N_s \ (X(x, C_{I_k}) = \emptyset)\}, \tag{2}$$

where

$$X(x, C_I) = \{x' \in X : \ C_Ix \ \succ \ C_Ix'\}.$$

Sometimes for brevity we denote this set by $G^m(C)$.

Obviously, any N_m-efficient solution $x \in G^m(C, N_m)$ ($s= 1$) is Pareto optimal, i.e. efficient solution to problem (1). Therefore, the set $G^m(C, N_m)$ is the Pareto set [3]:

Denote

$$X(x, C) =\{x' \in X : \ Cx \geq Cx' \ \& \ Cx \neq Cx'\},$$

which is a set of solutions $x' \in X$ such that x' dominates x in Pareto sense in problem (1). Therefore, we have

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

In the other extreme case, when $s=m$, $G^m(C, \{1\},\{2\}, ...,\{m\})$ is a set of extreme solutions (see e.g. [4]). This set is denoted by $E^m(C)$. Thereby, we have:

$$E^m(C) =\{x \in X : \ \exists k \in N_m \ \ \forall x' \in X \ \ (C_kx \ \overline{\succ} \ C_kx')\}=$$

$$\{x \in X : \ \exists k \in N_m \ \ \forall x' \in X \ \ (C_k x \leq C_k x')\}.$$

It is easy to see that the set of extreme solutions is composed of the best solutions for each of the m criteria. So, in this context, the parametrization of the optimality principle refers to the introduction of such a characteristic of the binary preference relation that allows us to connect the well-known choice functions, parameterizing them from the Pareto to the extreme.

Denoted by $Z^m(C, I_1, I_2, \ldots, I_s)$, the multicriteria ILP problem consists in finding the set $G^m(C, I_1, I_2, \ldots, I_s)$. Sometimes, for the sake of brevity, we use the notation $Z^m(C)$ for this problem. Denote $Z^m_B(C)$ the problem with Boolean variables.

It is easy to see that the set $P^1(C) = E^1(C)$ is the set of optimal solutions to the scalar (single-criterion) problem $Z^1(C, N_1)$, where $C \in \mathbf{R}^n$.

For any nonempty subset $I \subseteq N_m$ we introduce the notation

$$P(C_I) = \{x \in X : \ \forall x' \in X \ \ (C_I x \succcurlyeq C_I x')\},$$

i.e.

$$P(C_I) = \{x \in X : \ X(x, C_I) = \emptyset\}.$$

Then, by virtue of (2), we obtain

$$G^m(C, I_1, I_2, \ldots, I_s) = \{x \in X : \ \exists k \in N_s \ \ (x \in P(C_{I_k}))\}. \tag{3}$$

Therefore, we have

$$G^m(C, I_1, I_2, \ldots, I_s) = \underset{k \in N_s}{\cup} P(C_{I_k}), \ \ N_m = \underset{k \in N_s}{\cup} I_k.$$

It is obvious that all the sets given here are nonempty for any matrix $C \in \mathbf{R}^{m \times n}$.

Before formulating the main result regarding the stability radius bounds in the next section, we need to prove five supplementary statements presented in this section as lemmas.

From (3), we get the following straightforward statement.

Lemma 1. *A solution $x \notin G^m(C, I_1, I_2, \ldots, I_s)$ if and only if for any index $k \in N_s$ the solution $x \notin P(C_{I_k})$.*

In the space of solutions $\mathbf{R}^n$, we define an arbitrary Hölder's norm l_p, $p \in [1,\infty]$, i.e. by the norm of a vector $a = (a_1, a_2, ..., a_n)^T \in \mathbf{R}^n$ we mean the number

$$\|a\|_p = \begin{cases} \left(\sum_{j \in N_n} |a_j|^p\right)^{1/p} & \text{if} \ \ 1 \leq p < \infty, \\ \max\{|a_j| : \ j \in N_n\} & \text{if} \ \ p = \infty. \end{cases}$$

In the space of criteria $\mathbf{R}^m$, we define an arbitrary Hölder's norm l_q, $q \in [1,\infty]$, and $l_p \neq l_q$. By the norm of the matrix $C \in \mathbf{R}^{m \times n}$ with the rows C_i, $i \in N_m$, we mean the norm of a vector whose components are the norms of the rows of the matrix. By that, we have

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

Obviously,

$$\|C_i\|_p \le \|C_I\|_{pq} \le \|\mathrm{C}\|_{pq},\ i \in I \subseteq N_m. \tag{4}$$

So, it is easy to see that for any $a=(a_1, a_2, \ldots, a_n)^T \in \mathbf{R}^n$ with

$$|a_j| = \alpha, \quad j \in N_n,$$

the following equality holds

$$\|a\|_p = \alpha n^{1/p} \tag{5}$$

for any $p \in [1,\infty]$.

In the solution space $\mathbf{R}^n$ along with the norm l_p, $p \in [1,\infty]$, we will use the conjugate norm l_{p^*}, where the numbers p and p^* are related, as usual, by the equality

$$\frac{1}{p} + \frac{1}{p^*} = 1,$$

assuming $p^*= 1$ if $p=\infty$, and $p^*=\infty$ if $p= 1$. Therefore, we further suppose that the range of variation of the numbers p and p^* is the closed interval $[1,\infty]$, and the numbers are related by the conditions above.

Further we use the well-known Hölder's inequality (see [5])

$$|a^T b| \le \|a\|_p \|b\|_{p^*} \tag{6}$$

that is true for any two vectors $a=(a_1, a_2, \ldots, a_n)^T \in \mathbf{R}^n$ and $b=(b_1, b_2, \ldots, b_n)^T \in \mathbf{R}^n$ and for any $p \in [1,\infty]$.

Perturbation of the elements of the matrix C is imposed by adding matrices C' of $\mathbf{R}^{m\times n}$. Thus, the perturbed problem $Z^m(C + C')$ has the form

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

and the set of its $(I_1, I_2, ..., I_s)$-efficient solutions is denoted by $G^m(C+C', I_1, I_2, \ldots, I_s)$. For an arbitrary number $\varepsilon> 0$, we define the set of perturbing matrices

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

with rows $C'_i,\ i \in N_m$.

Following [6, 7], the *stability radius* of the ILP problem $Z^m(C, I_1, I_2, \ldots, I_s)$, $m \in \mathbf{N}$, (called T_3-stability radius in the terminology of [8, 9]) is the number

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

where

$$\Xi = \left\{ \varepsilon > 0 :\ \forall C' \in \Omega_{pq}(\varepsilon) \quad (G^m(C + C') \subseteq G^m(C)) \right\}.$$

Thus, the stability radius of the problem $Z^m(C)$ determines the limit level of perturbations of the elements of the matrix C that no new optima appear in the perturbed problem $Z^m(C+C')$. For any $C' \in \Omega_{pq}(\varepsilon)$ and $\varepsilon> 0$, it is obvious that $G^m(C+C') \subseteq G^m(C)$ if $G^m(C) = \mathrm{X}$. Therefore, the problem $Z^m(C)$ with $\bar{G}^m(C) = G^m(C)\backslash X \neq \emptyset$ is called *non-trivial*.

3 Main result

Given the multicriteria non-trivial ILP problem $Z^m(C, I_1, I_2, \ldots, I_s)$, $m \in \mathbf{N}$ considered, for any $p, q \in [1,\infty]$ and $s \in N_m$ we define:

$$\varphi_s^m(p) = \min_{k\in N_s} \min_{x\notin G^m(C)} \max_{x'\in P(x,C_{I_k})} \min_{i\in I_k} \frac{C_i(x-x')}{\|x-x'\|_{p^*}},$$

$$\psi_s^m(p,q) = n^{\frac{1}{p}} \min_{k\in N_s} \min_{x\notin G^m(C)} \max_{x'\in P(x,C_{I_k})} \min_{i\in I_k} \frac{C_i(x-x')}{\|x-x'\|_1} |I_k|^{\frac{1}{q}},$$

$$\gamma_s(p,q) = \min\{\|C_{I_k}\|_{pq} : \ k \in N_s\},$$

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

where

$$P(x, C_{I_k}) = P(C_{I_k}) \cap X(x, C_{I_k}).$$

It is obvious that $\varphi_s^m(p) \geq 0$ and $\psi_s^m(p,q) \geq 0$.

We are now ready to formulate the main result.

Theorem 1. *For any $m \in \boldsymbol{N}$, $p, q \in [1,\infty]$ and $s \in N_m$, the stability radius of the multicriteria non-trivial ILP problem $Z^m(C, I_1, I_2, \ldots, I_s)$ has the following lower and upper bounds:*

$$\varphi_s^m(p) \leq \rho_s^m(p,q) \leq \gamma_s(p,q). \tag{7}$$

If the problem is Boolean i.e. $Z^m(C) = Z_B^m(C)$, then

$$\varphi_s^m(p) \leq \rho_s^m(p,q) \leq \min\{\psi_s^m(p,q), \ \sigma^m(p)\}. \tag{8}$$

Proof. The scheme of the proof is the following. We start with proving bounds for integer case, i.e. for $Z^m(C)$. Afterwards, we prove bounds for Boolean case, i.e. for $Z_B^m(C)$.

Firstly, we prove that $\varphi_s^m(p) \leq \rho_s^m(p,q)$. We assume $\varphi_s^m(p) > 0$ otherwise the inequality is evident. We chose an arbitrary perturbing matrix $C' \in \mathbf{R}^{m\times n}$ with rows C_i', $i \in N_m$ such that the matrix C' belongs to $\Omega_{pq}(\varphi_s^m(p))$. Then according to the definition of $\varphi_s^m(p)$ and due to (4), for any $k \in N_s$ and $x \notin G^m(C)$ there exists a solution $x^0 \in P(x, C_{I_k})$ such that

$$\frac{C_i(x-x^0)}{\|x-x^0\|_{p^*}} \geq \varphi^m(p) \geq \|C'\|_{pq} \geq \|C_i'\|_p, \ i \in I_k.$$

Using Hölder's inequality (6) we get

$$(C_i + C_i')(x-x^0) \geq C_i(x-x^0) - \|C_i'\|_p \|x-x^0\|_{p^*} > 0.$$

This directly implies that $x \notin P(C_{I_k} + C_i')$ for any $k \in N_s$, i.e. due to lemma 1

$$x \notin G^m(C + C').$$

Summarizing, any non-efficient solution of $Z^m(C)$ remains so in any perturbed problem $Z^m(C+C')$. Hence, we have $G^m(C+C') \subseteq G^m(C)$ for any perturbing matrix $C' \in \Omega_{pq}(\varphi_s^m(p))$, i.e $\rho_s^m(p,q) \geq \varphi_s^m(p)$.

Secondly, we prove that $\rho_s^m(p,q) \leq \gamma_s(p,q)$. In order to do this, it suffices to show that for any $k \in N_s$ the inequality $\rho_s^m(p,q) \leq \|C_{I_k}\|_{pq}$. Assuming $k \in N_s$ and $\varepsilon > \|C_{I_k}\|_{pq}$, we consider a perturbing matrix $C^0 = (C^0_{I_1}, C^0_{I_2}, \ldots, C^0_{I_s})^T$ with components

$$C^0_{I_i} = \begin{cases} -C_{I_i} & \text{if } i = k; \\ \mathbf{0}^{|I_i| \times n} & \text{if } i \in N_s \backslash \{k\}, \end{cases}$$

where $\mathbf{0}^{|I_i| \times n}$ is zero matrix of dimension $|I_i| \times n$. Then we obtain

$$\|C^0\|_{pq} = \|C^0_{I_k}\|_{pq} = \|C_{I_k}\|_{pq},\ C^0 \in \Omega_{pq}(\varepsilon),$$

and

$$P(C_{I_k} + C^0_{I_k}) = G^m(C + C^0) = X \not\subseteq G^m(C).$$

Summarizing, we get

$$\forall k \in N_s \ \ \forall \varepsilon > \|C_{I_k}\|_{pq} \ \ \exists C^0 \in \Omega_{pq}(\varepsilon) \ \ (G^m(C + C^0) \not\subseteq G^m(C)),$$

i.e. the stability radius cannot be larger than any of numbers $\|C_{I_k}\|_{pq}$, $k \in N_s$, and hence

$$\rho_s^m(p,q) \leq \gamma_s(p,q) = \min\{\|C_{I_k}\|_{pq} :\ k \in N_s\}.$$

Now we prove bounds for the Boolean problem $Z_B^m(C)$.

The inequality $\varphi_s^m(p) \leq \rho_s^m(p,q)$ has been proven above for $Z^m(C)$, so the same lower bound is valid for the Boolean problem $Z_B^m(C)$.

Now we continue with showing correctness of the upper bound for the stability radius $\rho_s^m(p,q)$ of the Boolean problem $Z_B^m(C)$. Firstly, we prove that $\rho_s^m(p,q) \leq \psi_s^m(p,q)$. According to the definition of $\psi_s^m(p,q)$, there exist $r \in N_s$ and $x^0 \notin G^m(C)$ such that for any $x \in P(x^0, C_{I_r})$ one can find an index $l = l(x) \in I_r$ satisfying the condition

$$n^{\frac{1}{p}} |I_r|^{\frac{1}{q}} C_l(x^0 - x) \leq \psi_s^m(p,q) \|x^0 - x\|_1. \tag{9}$$

Assuming $\varepsilon > \psi_s^m(p,q)$, we consider a perturbing matrix $C^0 = [c^0_{ij}] \in \mathbf{R}^{m \times n}$ with rows $C^0_i \in \mathbf{R}^n$, $i \in N_m$ and elements c^0_{ij} defined as:

$$c^0_{ij} = \begin{cases} -\delta & \text{if } i \in I_r,\ x^0_j = 1, \\ \delta & \text{if } i \in I_r,\ x^0_j = 0, \\ 0 & \text{if } (i,j) \notin I_r \times N_n, \end{cases}$$

where δ satisfies the condition below

$$\psi_s^m(p,q) < \delta n^{\frac{1}{p}} |I_r|^{\frac{1}{q}} < \varepsilon. \tag{10}$$

So, using (5) we continue

$$\|C^0_i\|_p = \delta n^{\frac{1}{p}},\ i \in I_r,$$

$$\|C^0_{I_r}\|_{pq} = \delta n^{\frac{1}{p}} |I_r|^{\frac{1}{q}} < \varepsilon,$$
$$C^0 \in \Omega_{pq}(\varepsilon),$$
$$C^0_i(x^0 - x) = -\delta \|x^0 - x\|_1 < 0,\ i \in I_r. \tag{11}$$

Using (9) and (10), for any solution $x \in P(x^0, C_{I_r})$ the inequalities hold

$$(C_l + C^0_l)(x^0 - x) \le (\psi^m_s(p,q)(n^{\frac{1}{p}}|I_r|^{\frac{1}{q}})^{-1} - \delta)\|x^0 - x\|_1 < 0,$$

i.e. the following formula holds:

$$\forall x \in P(x^0, C_{I_r})\ \ (x \notin X(x^0, C_{I_r} + C^0_{I_r})) \tag{12}$$

If $X(x^0, C_{I_r} + C^0_{I_r}) = \emptyset$, then $x^0 \in G^m(C + C^0)$. Assume $X(x^0, C_{I_r} + C^0_{I_r}) \neq \emptyset$. Then due to the property of external stability of the Pareto set $P(C_{I_r} + C^0_{I_r})$ (see e.g. [10]) there exists a solution $x^* \in P(x^0, C_{I_r} + C^0_{I_r})$, and hence $x^* \in G^m(C + C^0)$.

Further, by contradiction we prove that $x^* \notin P(C_{I_r})$. Suppose $x^* \in P(C_{I_r})$. Then due to (12) we have

$$x^* \in P(C_{I_r}) \backslash P(x^0, C_{I_r}).$$

Therefore, either the equality

$$C_{I_r} x^* = C_{I_r} x^0$$

holds or the inequalities

$$C_{I_r} x^* \le C_{I_r} x^0$$

do not hold. In the first case, due to (11) we derive

$$(C_i + C^0_i)(x^0 - x^*) < 0,\ i \in I_r.$$

In the second case, the exists an index $h \in I_r$ such that

$$C_h x^* > C_h x^0.$$

Now again due to (11) we derive

$$(C_h + C^0_h)(x^0 - x^*) < 0.$$

Thus, in both cases we get contradiction to the inclusion

$$x^* \in P(x^0, C_{I_r} + C^0_{I_r}).$$

Summarizing, for any $\varepsilon > \psi^m_s(p,q)$ we guarantee the existence of the perturbing matrix $C^0 \in \Omega_{pq}(\varepsilon)$ such that there exists a solution (x^0 or x^*) preserving non-efficiency in the perturbed problem $Z^m(C + C^0)$. So, the following formula is valid:

$$\forall \varepsilon > \psi^m_s(p,q)\ \exists C^0 \in \Omega_{pq}(\varepsilon)\ (G^m(C + C^0) \not\subseteq G^m(C)).$$

Hence, we conclude that $\rho^m_s(p,q) \le \psi^m_s(p,q)$.

Secondly and finally, we prove that $\rho_s^m(p,q) \leq \sigma^m(p)$. Let $x^0 \notin G^m(C)$, and let indices $l \in N_m$ and $k \in N_s$ be such that

$$\sigma^m(p) = \|C_l\|_p,\ l \in I_k. \tag{13}$$

Setting $\varepsilon > \sigma^m(p)$, we introduce δ such that

$$0 < \delta n^{\frac{1}{p}} < \varepsilon - \sigma^m(p). \tag{14}$$

Further, we consider a vector $\eta = (\eta_1, \eta_2, \ldots, \eta_n)$ with

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

Then we derive

$$\|\eta\|_p = \delta n^{\frac{1}{p}}. \tag{15}$$

Notice that for any $x \in X \backslash \{x^0\}$ the inequality

$$\eta(x^0 - x) = -\delta \|x^0 - x\|_1 < 0 \tag{16}$$

holds. The rows $C_i^0 \in \mathbf{R}^n$, $i \in N_m$ of the perturbing matrix $C^0 \in \mathbf{R}^{m \times n}$ are defined as:

$$C_i^0 = \begin{cases} \eta - C_i & \text{if } i = l \\ 0^{(n)} & \text{if } i \in N_m \setminus \{l\}, \end{cases}$$

where $0^{(n)} = (0, 0, \ldots, 0) \in \mathbf{R}^n$. Then taking into account (16), we get

$$C_l^0(x^0 - x) = (\eta - C_l)(x^0 - x) = -\delta \|x^0 - x\| - C_l(x^0 - x).$$

Using equalities (13) and inequalities (14) as well as equality (15), we yield

$$\|C^0\|_{pq} = \|C_l^0\|_p = \|\eta - C_l\|_p \leq \|\eta\|_p + \|C_l\|_p = \delta n^{\frac{1}{p}} + \sigma^m(p) < \varepsilon.$$

Therefore, for any vector $x \in X \backslash \{x^0\}$ we have

$$(C_l + C_l^0)(x^0 - x) = -\delta \|x^0 - x\|_1 < 0,$$

i.e. $x \notin X(x^0, C_{I_k} + C_{I_k}^0)$, where $C^0 \in \Omega_{pq}(\varepsilon)$. Since $x^0 \notin X(x^0, C_{I_k} + C_{I_k}^0)$, then $X(x^0, C_{I_k} + C_{I_k}^0) = \emptyset$. The last implies $x^0 \in P^m(C_{I_k} + C_{I_k}^0)$, and according to formula (3) we obtain

$$x^0 \in G^m(C + C^0).$$

Taking into consideration that $x^0 \notin G^m(C)$, we conclude $\rho_s^m(p,q) \leq \varepsilon$ for any $\varepsilon > \sigma^m(p)$. Therefore, $\rho_s^m(p,q) \leq \sigma^m(p)$.

Finally, summarizing all the facts proven above, we conclude that the theorem has now been proven. □

4 Corollaries

From theorem 1 we get the following known results.

Corollary 1. *[11] For any $m \in \boldsymbol{N}$, $p, q \in [1, \infty]$, the stability radius of the multicriteria non-trivial Boolean problem $Z_B^m(C, N_m)$, $C \in \mathbf{R}^{m \times n}$ of finding the Pareto set $P^m(C)$ has the following bounds:*

$$\varphi_1^m(p) \le \rho_1^m(p, q) \le \min\{n^{\frac{1}{p}} m^{\frac{1}{q}} \varphi_1^m(\infty), \sigma^m(p)\},$$

where

$$\varphi_1^m(p) = \min_{x \notin P^m(C)} \max_{x' \in P(x,C)} \min_{i \in N_m} \frac{C_i(x - x')}{\|x - x'\|_{p^*}},$$

$$P(x, C) = P^m(C) \cap X(x, C),$$

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

Corollary 2. *[12] For any $m \in \boldsymbol{N}$, $p, q \in [1, \infty]$, the stability radius of the multicriteria non-trivial Boolean problem $Z_B^m, (C, \{1\}, \{2\}, \dots \{m\})$, $C \in \mathbf{R}^{m \times n}$ consisting in finding the extreme set $E^m(C)$ has the following lower and upper bounds:*

$$0 < \varphi_m^m(p) \le \rho_m^m(p, q) \le \min\{n^{\frac{1}{p}} \varphi_m^m(\infty), \sigma^m(p)\},$$

where

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

$$E(x, C_i) = E^m(C) \cap X(x, C_i),$$

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

Notice also that $\varphi_m^m(p) > 0$, since it is obvious that the following formula is true:

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

indicating the fact that $\rho_m^m(p, q) > 0$.

Corollary 3. *If every Pareto set $P(C_{I_k})$, $k \in N_s$ in the multicriteria non-trivial ILP problem $Z^m(C, I_1, I_2, \dots, I_s)$ consists of unique solution $x^{(k)}$, then*

$$\rho_s^m(p, q) = \min_{k \in N_s} \min_{x \in X \setminus \{x^{(k)}\}} \min_{i \in I_k} \frac{C_i(x - x^{(k)})}{\|x - x^{(k)}\|_{p^*}}. \tag{17}$$

Proof. Let Θ denote the right-hand side of (17). According to the definition of Θ, there exist $\hat{x} \in X \setminus \{x^{(k)}\}$, $r \in N_s$, and $l \in I_r$ such that the following equality holds:

$$C_l(\hat{x} - x^{(r)}) = \Theta \|\hat{x} - x^{(r)}\|_{p^*}. \tag{18}$$

Notice that here $\Theta > 0$. Set $\varepsilon > \Theta$ and a number γ satisfying

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

According to formula (17), there exists a vector $a \in \mathbf{R}^n$ such that

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

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

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:

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

Then we have

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

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

$$C_l^0(\hat{x} - x^{(r)}) = -\gamma\|\hat{x} - x^{(r)}\|_{p^*}.$$

From the above using inequality (18) we deduce

$$(C_l + C_l^0)(\hat{x} - x^{(r)}) = C_l(\hat{x} - x^{(r)}) - \gamma\|\hat{x} - x^{(r)})\|_{p^*} =$$

$$(\Theta - \gamma)\|\hat{x} - x^{(r)}\|_{p^*} < 0.$$

Summing up, we have that for any $\varepsilon > \Theta$ there exists the perturbing matrix $C^0 \in \Omega_{pq}(\varepsilon)$ such that one can specify $\hat{x} \neq x^{(k)}$ such that there exists $r \in N_s$ satisfying the condition $\hat{x} \in P(C_{I_r} + C_{I_r}^0)$, i.e. $\hat{x} \in G^m(C + C^0)$. This implies that $G^m(C + C^0) \not\subseteq G^m(C)$. Hence $\rho_s^m(p, q) < \varepsilon$ for any number $\varepsilon > \Theta$, i.e. $\rho_s^m(p, q) \leq \Theta$. Taking into consideration the main result of theorem 1, we conclude that $\rho_s^m(p, q) = \Theta$. □

Corollary 4. *For any $m \in \boldsymbol{N}$ and $s \in N_n$, the stability radius of the multicriteria non-trivial Boolean problem $Z_B^m(C, I_1, I_2, \ldots, I_s)$ is expressed by formula:*

$$\rho_s^m(\infty, \infty) = \varphi_s^m(\infty) = \psi_s^m(\infty, \infty) =$$

$$\min_{k\in N_s} \min_{x\notin G^m(C)} \max_{x'\in P(x, C_{I_k})} \min_{i\in I_k} \frac{C_i(x - x')}{\|x - x'\|_1}.$$

When $s = 1$, the result was first mentioned in [6].

References

[1] V. Emelichev, Y. Nikulin, "Post-optimal analysis for multicriteria integer linear programming problem of finding extreme solutions", *Proceedings of the Fifth Russian Finnish Symposium on Discrete Mathematics*, Yaroslav-the-Wise Novgorod State University, pp. 42–58, 2019.

[2] V. Emelichev, Y. Nikulin, "Post-optimal analysis for multicriteria integer linear programming problem with parametric optimality", *Control and Cybernetics*, vol. 49, no.2, pp. 163–179, 2020.

[3] V. Pareto. *Manuel D'economie Politique*. Paris: V. Giard & E. Briere, 1909.

[4] K. Miettinen. *Nonlinear Multiobjective Optimization*. Boston: Kluwer, 1999.

[5] G. Hardy, J. Littlewood, G. Polya. *Inequalities*. Cambridge: Cambridge University Press, 1988.

[6] V. Emelichev, E. Girlich, Y. Nikulin, D. Podkopaev, "Stability and regularization of vector problem of integer linear programming", *Optimization*, vol. 51, no. 4, pp. 645–676, 2002.

[7] V. Emelichev, V. Kotov, K. Kuzmin, T. Lebedeva, N. Semenova, T. Sergienko, "Stability in the combinatorial vector optimization problems", *Journal Automation and Information Sciences*, vol. 26, no. 2, pp. 27–41, 2004.

[8] I. Sergienko, V. Shilo. *Discrete Optimization Problems. Problems, methods, research.* Kiev: Naukova dumka, 2003.

[9] T. Lebedeva, T. Sergienko, "Different types of stability of vector integer optimization problem: general approach", *Cybernetics and Systems Analysis*, vol. 44, no. 3, pp. 429–433, 2008.

[10] V. Podinovskii, V. Noghin. *Pareto-Optimal Solutions of Multicriteria Problems*. Moscow: Fizmatlit., 2007.

[11] V. Emelichev, K. Kuzmin, V. Mychkov, "Estimates of stability radius of multicriteria Boolean problem with Hölder metrics in parameter spaces", *Bulletin of the Academy of Sciences of Moldova. Mathematics*, vol. 78, pp. 74–81, 2015.

[12] V. Emelichev, Y. Nikulin, "Post-optimal analysis for multicriteria integer linear programming problem of finding extremum solutions", *Control and Cybernetics*, vol. 47, no. 3, pp. 225–238, 2018.

Rationality Conditions in Dynamic Multicriteria Games

Anna Rettieva*

Institute of Applied Mathematical Research
Karelian Research Center of RAS
11 Pushkinskaya str., Petrozavodsk, 185910, Russia
Saint Petersburg State University
7/9 Universitetskaya nab., Saint Petersburg, 199034, Russia
annaret@krc.karelia.ru

Abstract

We consider a dynamic, discrete-time, game model where the players use a common resource and have different criteria to optimize. To construct a multicriteria Nash equilibrium the bargaining solution is adopted. To design a multicriteria cooperative equilibrium, a modified bargaining scheme that guarantees the fulfillment of rationality conditions is applied. The concept of dynamic stability is adopted for dynamic multicriteria games. To stabilize the multicriteria cooperative solution a time-consistent payoff distribution procedure is constructed. The conditions for rational behavior are defined for dynamic multicriteria games. To illustrate presented approaches a bi-criteria resource management problem is investigated.

Keywords: dynamic games, multicriteria games, Nash bargaining solution, ratonal behavior.

1 Introduction

Game-theoretic models that take into account the presence of several objective functions of participants [7] are closer to reality. Players often seek to achieve several goals simultaneously, which can be incomparable. The multicriteria approach helps to determine an optimal behavior in such situations. The methods of static multicriteria games are not applicable to the dynamic statements. Hence, in the series of papers [4, 5, 6], new approaches to obtain players' optimal behavior in dynamic multicriteria games were suggested.

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

We consider a dynamic, discrete-time, game model where the players use a common resource and have different criteria to optimize. To construct a multicriteria Nash equilibrium the bargaining solution is adopted. To design a multicriteria cooperative equilibrium, a modified bargaining scheme [5] that guarantees the fulfillment of rationality conditions is applied. To stabilize the multicriteria cooperative solution a time-consistent payoff distribution procedure [6] is constructed. The conditions for rational behavior, namely irrational-behavior-proofness condition [8] and each step rational behavior condition [1, 2] are defined for dynamic multicriteria games. To illustrate the presented approaches, a dynamic bi-criteria resource management problem with many players 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 resource 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 exploitation rate 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 modified bargaining approach [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 determine the cooperative behavior applying the modified bargaining solution that combines compromise programming and the Nash bargaining scheme. The status quo points are the noncooperative payoffs obtained by the players using the multicriteria Nash equilibrium strategies u_t^N:

$$\begin{gathered} (J_1^{1c}(u_t^c) - J_1^{1N}(u_t^N)) \cdot \dots \cdot (V_1^{kc}(u_t^c) - J_1^{kN}(u_t^N)) + \dots \\ + (V_n^{1c}(u_t^c) - J_n^{1N}(u_t^N)) \cdot \dots \cdot (V_n^{kc}(u_t^c) - J_n^{kN}(u_t^N)) = \\ = (\sum_{t=0}^{m} \delta^t g_1^1(u_t^c) - J_1^{1N}(u_t^N)) \cdot \dots \cdot (\sum_{t=0}^{m} \delta^t g_1^k(u_t^c) - J_1^{kN}(u_t^N)) + \dots \end{gathered}$$

$$+(\sum_{t=0}^{m}\delta^t g_n^1(u_t^c)-J_n^{1N}(u_t^N))\cdot\ldots\cdot(\sum_{t=0}^{m}\delta^t g_n^k(u_t^c-J_n^{kN}(u_t^N))\to\max_{u_t^c}. \tag{3}$$

It was shown [5] that this solution concept guarantees the rationality of cooperative behavior as the cooperative payoffs of the players are greater than or equal to the multicriteria Nash payoffs.

3 Rationality Conditions

The players' cooperative payoffs for the whole game can be calculated as

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

where $u_t^c=(u_{1t}^c,\ldots,u_{nt}^c)$ are the cooperative strategies determined in (3).

Similarly we determine the cooperative payoffs $J_i^c(t)$, $i\in N$, for every subgame started from the state x_t^c at a time t.

To stabilize the cooperative solution in multicriteria dynamic games we adopt the time-consistent payoff distribution procedure [3, 6]. The main idea of this scheme is to distribute the cooperative gain along the game path to guarantee that the players do not have any incentives to deviate from the cooperation agreement.

Definition 1. A vector $\beta(t)=(\beta_1(t),\ldots,\beta_n(t))$, where

$$\beta_1(t)=\begin{pmatrix}\beta_1^1(t)\\ \ldots\\ \beta_1^k(t)\end{pmatrix},\ldots,\beta_n(t)=\begin{pmatrix}\beta_n^1(t)\\ \ldots\\ \beta_n^k(t)\end{pmatrix}$$

is a payoff distribution procedure (PDP) for the dynamic multicriteria game (1), (2), if

$$J_i^c(0)=\sum_{t=0}^{m}\delta^t\beta_i(t),\ \ i\in N.$$

Definition 2. A vector $\beta(t)=(\beta_1(t),\ldots,\beta_n(t))$ is a time-consistent [3, 6] PDP for dynamic multicriteria game (1), (2), if for every $t\geq 0$

$$J_i^c(0)=\sum_{\tau=0}^{t}\delta^\tau\beta_i(\tau)+\delta^{t+1}J_i^c(t+1),\ \ i\in N.$$

Theorem 1. *A vector $\beta(t)=(\beta_1(t),\ldots,\beta_n(t))$, where*

$$\beta_i(t)=J_i^c(t)-\delta J_i^c(t+1),\ \ i\in N, \tag{4}$$

is a time-consistent payoff distribution procedure for dynamic multicriteria game (1), (2).

The conditions for rational behavior, namely irrational-behavior-proofness condition [8] and each step rational behavior condition [1, 2] are defined for dynamic multicriteria games.

Definition 3. The multicriteria cooperative solution $J^c(t) = (J_1^c(t), \ldots, J_n^c(t))$ satisfies the irrational-behavior-proofness condition if

$$\sum_{\tau=0}^{t} \delta^\tau \beta_i(\tau) + \delta^{t+1} J_i^N(t+1) \geq J_i^N(0) \tag{5}$$

for all $t \geq 0$, where $\beta(t) = (\beta_1(t), \ldots, \beta_n(t))$ – time-consistent PDP (4) and $J_i^N(t)$ is the noncooperative payoff of player i, $i \in N$.

If this condition is satisfied, then each player is irrational-behavior-proof because irrational actions that break the cooperative agreement will not bring his payoff below the initial noncooperative payoff.

Definition 4. The multicriteria cooperative solution $J^c(t) = (J_1^c(t), \ldots, J_n^c(t))$ satisfies each step rational behavior condition if

$$\beta_i(t) + \delta J_i^N(t+1) \geq J_i^N(t) \tag{6}$$

for all $t \geq 0$, where $\beta(t) = (\beta_1(t), \ldots, \beta_n(t))$ – time-consistent PDP (4) and $J_i^N(t)$ is the noncooperative payoff of player i, $i \in N$.

The proposed condition offers an incentive to each player to maintain cooperation because at every step she gains more from cooperation than from noncooperative behavior.

To illustrate the presented approaches, a dynamic bi-criteria bioresource management problem with many players is investigated.

References

[1] Mazalov, V.V., Rettieva, A.N.: Incentive conditions for rational behavior in discrete-time bioresource management problem. Dokl. Math. 81, 399–402 (2010)

[2] Mazalov, V.V., Rettieva, A.N.: Cooperation maintenance in fishery problems. Fishery Management. Nova Science Publishers, 151–198 (2012)

[3] Petrosjan, L.A.: Stable solutions of differential games with many participants. Viestn. Leningr. Univ. 19, 46–52 (1977)

[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 asymmetric players. J. Glob. Optim. (2020)

[6] Rettieva, A.: Rational behavior in dynamic multicriteria games. Mathematics 8, 1485 (2020)

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

[8] Yeung, D.W.K.: An irrational-behavior-proof condition in cooperative differential games. Int. Game Theory Rev. 8, 739–74 (2006).

Minimal subshifts with a language pivot property

Ville Salo

vosalo@utu.fi

Abstract

We construct an infinite binary minimal subshift whose words of length n form a connected subset of the Hamming graph for each n. We show that Sturmian subshifts (even up to conjugacy) do not give such an example, but that they are a near miss. We also discuss some stronger connectivity notions for (languages of) subshifts.

1 Background

We paraphrase a question M. Hochman asked in the conference Current Trends in Dynamical Systems and the Mathematical Legacy of Rufus Bowen, organized in Vancouver in 2017. This question (and many more) can be found on the website of the conference [1].

Question 1.1. *Does there exist an infinite minimal subshift X such that for some k and all n, the set of words of length n in X is connected in the kth power of the Hamming graph? Is such X necessarily topologically mixing?*

We give two solutions: In Section 4, for $k = 1$, we construct such a minimal subshift with the inductive word-building method.[1] In Section 3, for $k = 2$, we prove Sturmian subshifts are an example. This arose in discussions with Nishant Chandgotia, who gave an independent (but basically equivalent) proof of this latter result in [4]. We also show that Sturmian subshifts do not give $k = 1$ even up to conjugacy. We do not solve the second question of Hochman for $k = 1$.

Hochman's motivation for this question comes from the rigidity theory of dynamical systems: the question is meant as a subshift analog of the question of whether every rigid ergodic system has a rigid minimal topological model, which is still open. The existence of (not necessarily minimal) rigid topological models was shown in [5]. See the website of [1] for more information.

We find that the study of possible shapes of the language of a minimal subshift is interesting enough in its own right, and outline some possible directions where this study could be continued.

[1] See [6] for an early use of such a method for constructing subshifts. Contemporary applications of the method are probably too many to list.

2 Conventions

An *alphabet* is a finite set Σ of *symbols*. A *(formal) language* (over Σ) is a subset of Σ^*, where Σ^* is the set of all (possibly empty) words. We write ϵ for the empty word. Words over Σ form a free monoid with basis Σ and identity element ϵ. The monoid operation is concatenation, and is written as $u \cdot v$ or simply uv.

The *Hamming distance* $H(u, v)$ between two words of the same length $u, v \in \Sigma^k$ is $|\{i \mid u_i \neq v_i\}|$. The *Hamming graph (of words of length k over alphabet Σ)* has vertices Σ^k and edges (u, v) for all $u, v \in \Sigma^k$ having Hamming distance $H(u, v) = 1$. We say a set of words $W \subset \Sigma^n$ is *connected* if it induces a connected subgraph of the Hamming graph. The *kth power* of an undirected graph represented by its Boolean incidence matrix M is $\bigvee_{\ell \leq k} M^\ell$, so the kth power of the Hamming has edges (u, v) where $H(u, v) \leq k$. Question 1.1 asks about the connectedness of the graph induced by the words of length n in the kth power of the Hamming graph.

The set $\Sigma^{\mathbb{Z}}$ with the product topology and the action of the shift map $\sigma(x)_i = x_{i+1}$ is called the *full shift*, and $x \in \Sigma^{\mathbb{Z}}$ is a *configuration*. A *subshift* is a closed shift-invariant set $X \subset \Sigma^{\mathbb{Z}}$, and we write $\mathcal{L}(X) \subset \Sigma^*$ for its *language* (set of words that appear in its configurations) and $\mathcal{L}_n(X) = \mathcal{L}(X) \cap \Sigma^n$. We say X is *language-connected* if for every n the language $\mathcal{L}_n(X)$ is connected. A subshift is *minimal* if it has no nontrivial subshifts, equivalently every word in the language appears as a subword of every long enough word in the language. A subshift X is *topologically mixing* if for any two words u, v in the language of X, there exists n such that

$$m \geq n \implies \exists w : |w| = m \wedge uwv \in \mathcal{L}(X).$$

A subshift X is *Sturmian* if $|\mathcal{L}_n(X)| = n + 1$ for all $n \in \mathbb{N}$.

If $L \subset \Sigma^*$ is a language which is *extendable* in the sense that

$$w \in L \implies \exists u, v : |u|, |v| > 0 \wedge uwv \in L,$$

then we write $\mathcal{L}^{-1}(L)$ for the subshift $X \subset \Sigma^{\mathbb{Z}}$ whose language is the closure of L under taking subwords, that is,

$$\mathcal{L}(X) = \{w \in \Sigma^* \mid \exists u, v : uwv \in L\}$$

We use the usual semiring structure for languages, in particular $L \cdot K = \{u \cdot v \mid u \in L, v \in K\}$. We also use the Kleene star operation for $A \subset \Sigma^*$:

$$A^* = \{w_1 w_2 \cdots w_k \mid k \geq 0, \forall i \in \{1, \ldots, k\} : w_i \in A\}.$$

A *recoding*, or *topological conjugacy*, is a homeomorphism $\phi : X \to Y$ between two subshifts which commutes with the shift maps. The existence of a topological conjugacy is an equivalence relation, and this is usually taken to be the natural notion of isomorphism between two subshifts. A topological conjugacy always has a *radius* $r \in \mathbb{N}$, meaning the symbol $\phi(x)_i$ only depends on the word $x_{[i-r,i+r]}$.

3 Sturmian subshifts

It turns out that for Sturmian subshifts (which are minimal and not topologically mixing), the subshift has a connected language when two changes are allowed at once, and we can even make the two changes next to each other.

Definition 3.1. *The* k-change graph *of a language* $L \subset \Sigma^n$ *has nodes* L *and edge* (u, v) *whenever*

$$u = wu'w', v = wv'w'$$

where $u, u' \in \Sigma^{k'}$ *for some* $k' \leq k$ *and* $w, w' \in \Sigma^*$.

Such k-changes are sometimes referred to as *pivoting*. We show that the 2-change graph of $\mathcal{L}_n(X)$ is connected for all n for a Sturmian X, which clearly implies that $\mathcal{L}_n(X)$ induces a connected subgraph in the second power of the Hamming graph of words of length n. It is well-known that Sturmian subshifts are not topologically mixing, therefore they completely solve Question 1.1 (as stated).

Theorem 3.2. *Let* X *be a Sturmian subshift. Then for every* $n \geq 2$*, the* 2*-change graph of* $\mathcal{L}_n(X)$ *is connected.*

Proof. Configurations in a Sturmian subshift can be characterized with cutting sequences [8], i.e. for a Sturmian subshift there exists an irrational slope $\alpha > 0$ such that words of length n in the language of the subshift are obtained by starting a line that contains no elements of $\mathbb{Z}^2$ from some point on

$$A = ([0, 1] \times \{0\}) \cup (\{0\} \times [0, 1]),$$

following it until it crosses n horizontal or vertical lines of the grid, and writing 1 whenever the line crosses a horizontal line and 0 whenever it crosses a vertical line. The resulting word is the associated *cutting sequence*. We think of the line as crossing the horizontal or vertical line of A that it begins on by an infinitesimal amount, giving on the first symbol of u, and similarly the line on which it ends is crossed infinitesimally, giving the last symbol. This is illustrated in Figure 1.

Thus if $u, v \in \mathcal{L}_n(X)$ and X is Sturmian, then both u and v have corresponding finite line segments that start on some points $x_a, x_b \in A$ and end on some horizontal or vertical line of the grid.

Now slide x_a towards x_b along A and have the path cross exactly n lines at all times. The cutting sequence does not change as long as the line does not hit an element of $\mathbb{Z}^2$, though one may visualize the 1-labels as moving around (following the intersection points) in Figure 1. There are finitely many points where the line would hit an element of $\mathbb{Z}^2$, and we jump over them. By the irrationality of α, a line of that slope cannot hit two lattice points at once, so we see that when a central point of the line hits an element of $\mathbb{Z}^2$, we will only change 01 to 10 or vice versa in the cutting sequence (the 1 jumps over the 0).

When we move from the horizontal piece $[0, 1] \times \{0\}$ of A to the vertical piece $\{0\} \times [0, 1]$ or vice versa, we only flip the initial symbol of the cutting sequence. When the

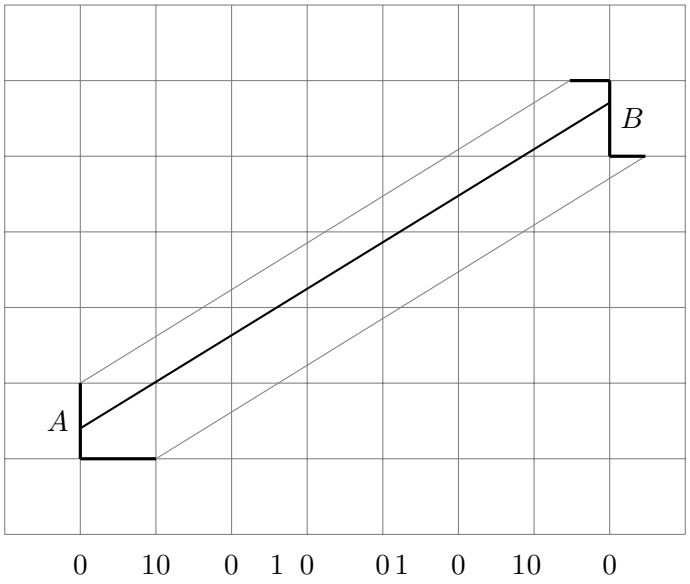

Figure 1: A cutting sequence in the language of the Fibonacci subshift; $\alpha = \phi^{-1}$ (the inverse golden ratio), $n = 12$. The set A is highlighted on the bottom left corner, and $B = ([4\phi, 7] \times \{5\}) \cup (\{7\} \times [4, 5]) \cup ([7, 4\phi + 1] \times \{4\})$ is also highlighted. Sliding the starting point on A (and the endpoint on B) gives all words of length n.

endpoint of the line crosses an integer point (which happens exactly twice), either only the last symbol changes or the last two symbols change. In each case, the change corresponds to an edge in the 2-change graph. □

We do not know whether it is possible to somehow turn a Sturmian subshift into a language-connected minimal subshift. However, at least a simple recoding does not work.

Theorem 3.3. *Let $Y \subset \Sigma^{\mathbb{Z}}$ be topologically conjugate to a Sturmian subshift. Then there do not exist configurations $x', y' \in Y$ such that x' and y' differ in exactly one position. In particular, Y is not language-connected.*

Proof. For the "In particular" claim, if Y is language-connected, then the 1-change graph of $\mathcal{L}_n(Y)$ is connected for all n. Since Y has at least two configurations, an easy compactness argment shows there exist configurations x', y' which differ in exactly one position.

Suppose now that such a pair (x', y') exists, say $x'_0 = a \neq b = y'_0$. Suppose now that Y is topologically conjugate to a Sturmian subshift X. It is clear from the characterization by cutting sequences and the minimality of irrational rotations that a Sturmian subshift has a unique asymptotic pair (x, y), corresponding to a crossing of a lattice point. Up to shifting we have $x_{[0,1]} = 01$, $y_{[0,1]} = 10$ and the configurations agree in other positions.

The pair (x', y') must correspond to this unique asymptotic pair in X, say $\phi(x) = x', \phi(y) = y'$.

We argue as in the previous proof, but it is now helpful to consider cutting sequences which extend r symbols below and left of the starting point, and $n + r$ steps above and right, where r is the radius of the topological conjugacy $\phi : X \to Y$. We can take the cutting sequences to be functions $[-r, n+r-1] \to \Sigma$. Again, we move the starting point of the line on $([0, 1] \times \{0\}) \cup (\{0\} \times [0, 1])$, but now we move it in only one direction, first left, then upward. At the corner point $(0, 1)$, we turn to the left and continue on $(-1, 0) \times \{1\}$. Extending this, one can visualize the starting point as following a zig-zag path moving alternately upward and to the left. The transition where the starting point starts moving left amounts to changing the subword of length 2 at coordinates $\{0, 1\}$ from to 10 to 01 in the associated cutting sequence.

Now, observe that as we move the starting point around a full zig-zag, the cutting sequence of length $n+2r$ around the starting point only changes by rewriting 01s to 10s (some of these rewrites being degenerate, i.e. touching only one symbol on the boundary). Now extend these words to configurations in an arbitrary way, apply ϕ to this sequence of words and take the subwords at $[0, n - 1]$.

We claim that, inside $[0, n - 1]$, each of the changes modifies at most one symbol in the ϕ-images, and in fact turns it from b to a. To see this, observe that due to the way the cutting sequence is defined, whenever a change from 01 to 10 happens, this change is surrounded by a suffix of the word $x_{(-\infty,-1]} = y_{(-\infty,-1]}$ and a prefix of the word $x_{[2,\infty)}$. The claim then folows from the facts that $\phi(x) = x'$ and $\phi(y) = y'$ and ϕ has radius r.

Now, since we can reach any cutting sequence of length $n + 2r$ from any other one by moving along the zig-zag path, and ϕ is surjective, we in particular obtain that we can reach any word of length n in Y from any other one, by only changing symbols a to symbols b. This is of course impossible, and contradicts our assumption that there is an asymptotic pair in Y with only one difference. □

4 Language-connected example

Theorem 4.1. *There exists a language-connected minimal subshift.*

Proof. Let $\Sigma = \{0, 1\}$. Let $w_{0,0} = 01$ and $w_{0,1} = 11$, $W_0 = \{w_{0,0}, w_{0,1}\}$, $\ell_0 = 2$, $n_0 = 2$.

Assuming W_i has been defined, define

$$L_{i,k,g} = (W_i\{\epsilon, 0, \dots, 0^g\})^{k-1}W_i.$$

Note that $L_{i,k,0} = W_i^k$. If w is a word over this language and we have fixed such a decomposition into the defining form, then we call the maximal words 0^a (more precisely, the positions of such words) separating words in W_i *gaps*, and refer to the words taken from W_i as the *W_i-words* of w. There may be multiple decompositions of a word of $L_{i,k,g}$, but we usually work with, and consistently modify, a fixed such decomposition. This should not cause confusion.

For each i, we build by induction a set of n_i words $W_i = \{w_{i,j} \mid j \in \{0, \dots, n_i - 1\}\} \subset \Sigma^{\ell_i}$ with the following properties:

- $H(w_{i,j}, w_{i,j+1}) = 1$ for all $j \in \{0, \ldots, n_i - 2\}$.
- $H(w_{i,0}0, 0w_{i,n_i-1}) = 1$.
- Every word in W_i has every word of $L_{i-1,2,0}$ as a subword.
- Every word $w_{i,j}$ with $0 \leq j \leq n_i - 1$ is in $L_{i-1,k,1} \cdot \{\epsilon, 0\}$ for the same k, and $w_{i,0} \in L_{i-1,k,1}$.

The first two items mean, intuitively, that W_i forms a cycle under Hamming distance, except that going around the cycle once has a cocyclic effect of moving the word to the left by one step. This is where the connectedness of the language will come from. The third item will be important in the proof of minimality. The importance of the fourth condition is that it prevents the accumulation of zeroes when we perform the inductive construction.

Suppose these properties hold for i. We build W_{i+1} as follows: First, pick

$$w_{i+1,0} = w_{i,0} \cdot 0u \cdot w_{i,0}$$

where u is any sufficiently generic word in $L_{i,k,0} = W_i^k$ for large enough k. More precisely, it is sufficient that $u = w_{i,h_0} w_{i,h_1} \cdots w_{i,h_{k-1}}$ satisfies that for all $j, j' \in \{0, \ldots, n_i - 1\}$ there exist $|n' - n| \geq 2$ such that $h_n = j, h_{n+1} = j'$ and $h_{n'} = j, h_{n'+1} = j'$.

Consider the decomposition $w_{i+1,0} = w_{i,0} \cdot 0u \cdot w_{i,0}$, and rewrite the central

$$0u = 0w_{i,h_0} w_{i,h_1} \cdots w_{i,h_{k-1}}$$

(where $w_{i,h_j} \in W_i$ for all $j \in \{0, \ldots, k-1\}$) successively into

$$0w_{i,h_0+1} w_{i,h_1} \cdots w_{i,h_{k-1}}$$

$$0w_{i,h_0+2} w_{i,h_1} \cdots w_{i,h_{k-1}}$$

$$\cdots$$

$$0w_{i,n_i-1} w_{i,h_1} \cdots w_{i,h_{k-1}}$$

$$w_{i,0}0w_{i,h_1} \cdots w_{i,h_{k-1}}$$

$$w_{i,1}0w_{i,h_1} \cdots w_{i,h_{k-1}}$$

$$\cdots$$

$$w_{i,h_0}0w_{i,h_1} \cdots w_{i,h_{k-1}}$$

and continue by similarly rotating the word w_{i,h_1} 'around W_i' to move it to the left in n rewriting steps, then w_{i,h_2} and so on until $0u$ has been changed to $u0$. This rewriting is done between the two occurrences of $w_{i,0}$ (the prefix and suffix of the initial word $w_{i+1,0}$). Collecting the words we see during this rewriting process into a list, we have defined $w_{i+1,j}$ for $j \in \{0, 1, \ldots, n_i k\}$.

Next, consider the decomposition $w_{i+1,n_i k} = w_{i,0} \cdot u \cdot 0 w_{i,0}$ and rewrite the prefix $w_{i,0}$ into w_{i,n_i-1} in $n_i - 1$ steps. Then rewrite the final word $0w_{i,0}$ into $w_{i,0}0$ in n_i steps. Letting $n_{i+1} = n_i(k+2)$, we have defined $w_{i+1,j}$ for all $j \in \{0, 1, \ldots, n_{i+1} - 1\}$, and the final word is $w_{i+1,n_{i+1}-1} = w_{i,n_i-1} u w_{i,0} 0$.

By construction (and induction) we have $H(w_{i+1,j}, w_{i+1,j+1}) = 1$ for all $j \in \{0, \ldots, n_{i+1}-2\}$. We have $H(w_{i+1,0}0, 0w_{i+1,n_{i+1}-1}) = 1$ because

$$H(w_{i,0}0uw_{i,0} \cdot 0, 0 \cdot w_{i,n_i-1}uw_{i,0}0) = H(w_{i,0}0, 0w_{i,n_i-1}) = 1$$

by induction.

Every word in W_{i+1} has every word in $L_{i,2,0}$ as a subword because u has at least two copies of each such word, and at any time during the construction of the words $w_{i+1,j}$ we are modifying only one W_i-subword of u (and the rest have only been shifted, as they have been fully cycled through). We have that every word $w_{i+1,j}$ with $0 \leq j < n_{i+1} - 1$ is in $L_{i,k,1} \cdot \{\epsilon, 0\}$ directly by construction. Similarly have $w_{i+1,0} \in L_{i,k,1}$ by construction.

This concludes the construction of the sets W_i, and the proof of the inductive properties listed above.

Next, we prove by induction a property which we call Property A:[2] for any i and $m \geq i+1$, we have $W_m \subset L_{i,k,2} \cdot \{\epsilon, 0\}$ for some k, and further $w_{m,0} \in L_{i,k,2}$. For $m = i+1$ this is direct from the last condition in the list of properties already proved, because $L_{i,k,1} \subset L_{i,k,2}$. Now suppose the assumptions hold for m. Then when building the words in the next stage, note that we always have a decomposition into a concatenation of words in W_m with either ϵ or 0 between them. The words in W_m have a decomposition into W_i-words and ϵ, 0 or 00 between them by induction. Thus, we immediately see that every word $w \in W_{m+1}$ has a decomposition into W_i-words and (a priori) gaps ϵ, 0, 00 or 000 between them. To show property A, we need to consider this decomposition in more detail and show that 000 does not appear, the gap at the end is of length at most one, and there is no gap at the end of the decomposition if $w = w_{m+1,0}$.

First, any gap in the decomposition of w which occurs inside the decomposition of a W_m-word is, by induction, of length at most 2. Any gap properly inside w and between two W_m-words has length at most 2 since the W_i-decomposition of a word in W_m begins with a word of W_i and ends in a gap of length at most 1.

If $w \neq w_{m+1,n_{m+1}-1}$, then the gap at the end of w in its W_i-decomposition is precisely as long as the gap in the last W_m-word, since the W_m-decomposition of w does not end in 0. Thus in these cases the gap at the end is of length at most one by induction. In $w_{m+1,n_{m+1}-1}$ the gap is one longer than the gap after the last W_i-word in the decomposition of $w_{m,0}$. By induction, the gap is of length 1 in this case. We have shown that $w \in L_{i,k,2} \cdot \{\epsilon, 0\}$ for all $w \in W_{m+1}$. Finally, in the decomposition of $w_{m+1,0}$, the last word is $w_{m,0}$, and thus by induction there is no gap in the W_i-decomposition. This shows $w_{m+1,0} \in L_{i,k,2}$, concluding the proof of Property A.

We define our subshift to be $X = \mathcal{L}^{-1}(\bigcup_i W_i)$, where we note that by construction the language $\bigcup_i W_i$ is extendable. Note that for any i, the subshift X is contained in

[2]The letter A stands for "no accumulAtion of zeroes".

the SFT $X_i = \mathcal{L}^{-1}((W_i\{\epsilon, 0, 00\})^*)$ by property A. Note also that it is nonempty since $W_0 \neq \emptyset$ and since $L \subset \mathcal{L}(\mathcal{L}^{-1}(L))$ for an extendable language L.

We claim that X is minimal. To see this, let w occur in some configuration in X. Then w is a subword of some $w_{i,j}$ by definition. Observe that $w_{i,j}$ is a subword of every word in W_{i+1}. Since $X \subset X_{i+1}$, actually every configuration in X contains $w_{i,j}$ with bounded gaps, thus w also.

To see that X is language-connected, it is enough to show that for arbitrarily large n, the language $\mathcal{L}_n(X)$ is connected, as paths between shorter words are obtained as projections of paths between arbitrary extensions into longer words. Let $n = n_i$ for any i and consider any word $w \in \mathcal{L}_n(X)$.

We first show that there is a path from w to some word in W_i. To see this, observe that by the definition of X, w appears as a subword of some W_m. Thus, it appears as a subword of the u-part of $w_{m+1,0} \in W_{m+1}$, at distance at least ℓ_m from the boundaries of u (since u contains at least two copies of each word in $L_{m,2,0}$; see the definition of W_{m+1}). The path from $w_{m+1,0}$ to $w_{m+1,n_{m+1}-1}$ gives a path from $0u$ to $u0$ by projection.

Consider now the splitting of $w_{m+1,0}$ into a word of $L_{i,k,2} \cdot (\epsilon, 0)$ given by property A. In this splitting, w appears between some two W_i-words in the u-part of $w_{m+1,0}$. Thus is it a subword of u which is contained in some $v0^a v'$ for some $v, v' \in W_i$ and $a \in \{0, 1, 2\}$. Suppose this subword begins in coordinate c, that is, $w = (v0^a v')_{[c,c+n-1]}$. If w is not the suffix of $v0^a v'$, then the path from $0u$ to $u0$ restricts to a path from w to $(v0^a v')_{[c+1,c+n]}$, then from $(v0^a v')_{[c+1,c+n]}$ to $(v0^a v')_{[c+2,c+n+1]}$, and so on, and finally we connect w to $v' \in W_i$.

The set W_i is connected by construction, so we have shown that the language is connected. □

In the construction, we have more or less complete freedom in the choice of u, and it is easy to add some additional nice properties, in particular the subshift can be made uniquely ergodic, to have positive entropy or to have zero entropy. However, we do not know whether we can control the topological mixing property.

5 How connected can the language be?

One can come up with infinitely many interesting (and perhaps also some non-interesting) questions by restricting to subshifts X with some dynamical property, and asking what the sets $\mathcal{L}_n(X)$ can look like, as subgraphs of the Hamming graph, a power of it, or the k-change graph. Here, we restrict to minimal X and notions of connectibity, and state three questions related to the connectivity of these finite graphs.

5.1 Higher connectedness

One standard notion for higher connectedness of graphs is the following: a graph is *ℓ-vertex-connected* if it has more than ℓ vertices and it stays connected even if ℓ vertices are removed.

Question 5.1. *Does there exist an infinite minimal subshift X such that*

$$\exists k : \forall \ell : \exists n_0 : \forall n \geq n_0 :$$
$$\mathcal{L}_n(X) \text{ is } \ell\text{-vertex-connected in the } k\text{th power of the Hamming graph.}$$

5.2 A combinatorial notion of contractibility

We suggest a notion of "contractibility" that strengthens connectedness (and holds in the full shift), inspired by the intuition that in both our main construction and Sturmian subshifts, connectedness is based on the words forming some type of cycle.

Definition 5.2. *If $\delta \in \mathbb{N}$ and $\Delta : \mathbb{N} \to \mathbb{N}$, we say a metric space (M, d) is (δ, Δ)-contractible if there exists a finite sequence of functions $f_0, f_1, \ldots, f_\ell : M \to M$ such that f_0 is the identity map and $|f_\ell(M)| = 1$, and for all applicable i and $x, y \in M$ we have $d(f_i(x), f_{i+1}(x)) \leq \delta$, and $\forall k \in \mathbb{N} : d(x, y) \leq k \implies d(f_i(x), f_i(y)) \leq \Delta(k)$.*

Definition 5.3. *Let $\mathcal{M} = (M_n, d_n)_{n \in \mathcal{D}}$ be a net of metric spaces, where $\mathcal{D}$ is a directed set. We say $\mathcal{M}$ is* (δ, Δ)-contractible *if there exists $n_0 \in \mathcal{D}$ such that for all $n \geq n_0$, M_n is δ-contractible. We say it is* contractible *if it is (δ, Δ)-contractible for some δ.*

Question 5.4. *Is there a minimal infinite subshift X such that $(\mathcal{L}_n(X), H)_{n \in \mathbb{N}}$ is contractible?*

Here, H is the Hamming distance (for any word length). Combinatorially, this means the following: for each large enough n (and then for any n by possibly changing δ and Δ), there is a sequence of functions $f_1, f_2, ..., f_\ell \in \mathcal{L}_n(X)^{\mathcal{L}_n(X)}$ where f_1 is the identity function and f_ℓ a constant function, between adjacent functions the image of no word changes in more than δ coordinates, and two words that differ in k coordinates in $\mathcal{L}_n(X)$ differ in at most $\Delta(k)$ coordinates in their f_i-images. Paths in the kth power of the Hamming graph are mapped to paths in the $\Delta(k)$th power of the Hamming graph, so since the $d(f_i(x), f_{i+1}(x)) \leq \delta$ condition in the definition of contractibility means that the δth power of the Hamming graph is connected, one cannot trivially "cheat" the last condition for $k = \delta$. Making a requirement for all k seems more natural, however (one could imagine that the words form a path for $\delta = 1$ but a circle for $\delta = 2$, for example).

It seems that the natural cycle in the 2-change graph of a Sturmian subshift (see the proof of Theorem 3.3) is always an induced cycle in the second power of the Hamming graph. This would mean that Sturmian subshifts at least do not give an example of contractibility with $\delta = 2$, and we suspect that they are not contractible for any δ.

It might be natural to require the conditions to be "compatible" for different n, i.e. that the sequence f_i somehow "projects" to one on shorter words. We have not explored how feasible this is. The following section suggests another way to link contractibility at different lengths.

For any n and any set of words $W \subset \Sigma^n$, the largest subshift $X \subset \Sigma^{\mathbb{Z}}$ such that $\mathcal{L}_n(X) \cap W = \emptyset$ is called a *subshift of finite type*. A *mixing sofic shift* is a subshift which is the image of a topologically mixing subshift of finite type under a continuous shift-commuting function (possibly over a different alphabet). See [7] for the basic theory.

Proposition 5.5. *If X is a mixing sofic shift, then $(\mathcal{L}_n(X), H)_{n\in\mathbb{N}}$ is contractible.*

Proof. We can take $n_0 = 0$. If X is a full shift, one can take $\delta = 1$ and simply flip the coordinates one by one to a fixed symbol $a \in \Sigma$, from left to right. For a general mixing sofic shift one can similarly pick a word w_n of length n for each n and for each fixed n, flip coordinates one by one to those of w_n, but one needs to write down a mixing segment of some bounded length s between the segments that have been changed, and ones that have not. This leads to (δ, Δ)-contractibility with $\delta = s + 1$ and $\Delta(k) = k + s$. □

More generally, one may wonder what can be said about the structure of languages of minimal subshifts as induced subgraphs of powers of the Hamming graph (or the k-change graph), when they are not "contractible". For instance, given that there is a reasonably natural contractibility notion for our graph sequences (the one defined above), presumably there is a natural way to discuss coarse structures of sequences of metric spaces more generally, though we do not aware of a framework where this directly fits.

5.3 Homotopy types in global topologies

The *Besicovitch pseudometric* on a subshift X is defined by

$$d_B(x, y) = \limsup_n \frac{H(x_{[-n,n]}, y_{[-n,n]})}{2n + 1},$$

and the *Weyl pseudometric* by

$$d_B(x, y) = \limsup_n \sup_i \frac{H(x_{[i-n,i+n]}, y_{[i-n,i+n]})}{2n + 1}.$$

Each of these can be used to topologize a subshifts. These pseudometrics arise from the study of almost periodic functions [2], see e.g [3] for a symbolic dynamical take.

Proposition 5.6. *Every Sturmian subshift is path-connected in the Besicovitch and Weyl topologies.*

Proof. Consider again the characterization by cutting sequences as in Theorem 3.2 and Theorem 3.3. Let us now associate to each starting point on the set A a full configuration, by continuing the line infinitely in both directions. We can also associate configurations to lines that hit a lattice point, by making an arbitrary choice of which side the line bypasses the point ("move it by an infinitesimal amount"). This choice changes the point by Besicovitch/Weyl distance zero, thus the map from A to the metric identification of the subshift is well-defined and surjective. It is easy to see that the map to the subshift is in fact continuous, thus the subshift is path-connected as a continuous image of the circle. □

It is less obvious whether the subshift constructed in Theorem 4.1 is path-connected in these topologies.

Question 5.7. *What can be said about the homotopy equivalence classes of minimal subshifts in these topologies? Is there a minimal subshift that is simply connected (or contractible) in the Besicovitch (resp. Weyl) topology?*

We suspect that every Sturmian subshift is homeomorphic to a circle in both topologies, thus would not be simply connected (or contractible). We note that, by a simple argument, a minimal subshift with at least two configurations is never homeomorphic to a single point in the Besicovitch (resp. Weyl) topology, thus cannot be trivially contractible. It is easy to show that the full shift is contractible in both topologies, see [9] for a proof, and more information on homotopy equivalence of sofic shifts in the Besicovitch topology.

Acknowledgements

We thank Nishant Chandgotia for discussions and comments.

References

[1] Current Trends in Dynamical Systems and the Mathematical Legacy of Rufus Bowen. `https://www.pims.math.ca/scientific-event/170730-ctdsmlrb-0`. Accessed: 2018-10-16.

[2] Abram Samoilovitch Besicovitch and Abram Samoilovitch Besicovitch. *Almost periodic functions*, volume 4. Dover New York, 1954.

[3] Gianpiero Cattaneo, Enrico Formenti, Luciano Margara, and Jacques Mazoyer. A shift-invariant metric on $S^{\mathbb{Z}}$ inducing a non-trivial topology. In *Mathematical foundations of computer science 1997 (Bratislava)*, volume 1295 of *Lecture Notes in Comput. Sci.*, pages 179–188. Springer, Berlin, 1997.

[4] Nishant Chandgotia. A short note on the pivot property. *https://nishantchandgotia.github.io/Research_files/Notes_files/Pivot.pdf*, 2018.

[5] Sebastián Donoso and Song Shao. Uniformly rigid models for rigid actions. *arXiv preprint arXiv:1508.03366*, 2015.

[6] Frank Hahn and Yitzhak Katznelson. On the entropy of uniquely ergodic transformations. *Transactions of the American Mathematical Society*, 126(2):335–360, 1967.

[7] Douglas Lind and Brian Marcus. *An introduction to symbolic dynamics and coding*. Cambridge University Press, Cambridge, 1995.

[8] M. Lothaire. *Algebraic combinatorics on words*, volume 90 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, 2002.

[9] Ville Salo and Ilkka Törmä. Geometry and Dynamics of the Besicovitch and Weyl Spaces. *ArXiv e-prints*, April 2012.

Double domination in graphs revisited

Nasrin Soltankhah and Babak Samadi*

Department of Mathematics, Faculty of Mathematical Sciences, Alzahra University,
Tehran, Iran
soltan@alzahra.ac.ir
b.samadi@alzahra.ac.ir

Abstract

For any graph G of order n with degree sequence $d_1 \geq \cdots \geq d_n$, we define the double Slater number $s\ell_{\times 2}(G)$ as the smallest integer t such that $t+d_1+\cdots+d_{t-e} \geq 2n-p$ in which e and p are the number of end-vertices and penultimate vertices of G, respectively. We show that $\gamma_{\times 2}(G) \geq s\ell_{\times 2}(G)$, where $\gamma_{\times 2}(G)$ is the well-known double domination number of a graph G with no isolated vertices. We prove that the problem of deciding whether the equality holds for a given graph is NP-complete even when restricted to 4-partite graphs. Finally, some lower and upper bounds on the double domination number in this paper improve the previous ones in the literature.

Keywords: Double domination number, double Slater number, NP-complete, tree.
MSC 2010: 05C69.

1 Introduction and preliminaries

Throughout this paper, we consider G as a finite simple graph with vertex set $V(G)$ and edge set $E(G)$. We use [16] as a reference for terminology and notation which are not explicitly defined here. The *open neighborhood* of a vertex v is denoted by $N(v)$, and its *closed neighborhood* is $N[v] = N(v) \cup \{v\}$. We denote the *degree* of vertex v by $deg(v)$, and let $deg_S(v) = |N(v) \cap S|$ in which $S \subseteq V(G)$. The *minimum* and *maximum degrees* of G are denoted by $\delta(G)$ and $\Delta(G)$, respectively. An *end-vertex* is a vertex of degree one and a *penultimate vertex* is a vertex adjacent to an end-vertex (they are called *leaf* and *support vertex* in the case of trees). Given the subsets $A, B \subseteq V(G)$, by $[A, B]$ we mean the set of all edges with one end point in A and the other in B. The *corona* of two graphs G_1 and G_2 is the graph $G_1 \circ G_2$ formed from one copy of G_1 and $|V(G_1)|$

*Speaker

copies of G_2 where the ith vertex of G_1 is adjacent to every vertex in the ith copy of G_2. Finally, for a given set $S \subseteq V(G)$, by $G[S]$ we represent the subgraph induced by S in G.

A set $S \subseteq V(G)$ is a *dominating set* if each vertex in $V(G)\setminus S$ has at least one neighbor in S. The *domination number* $\gamma(G)$ is the minimum cardinality of a dominating set in G. For more information about domination and its related parameters the reader can consult [10] and [11].

Slater [15] showed that the domination number of a graph of order n with non-increasing degree sequence $d_1 \geq \cdots \geq d_n$ can be bound from below by the smallest integer t such that t added to the sum of the first t terms of the above-mentioned sequence is at least n. This parameter was first called the *Slater number* and denoted by $s\ell(G)$ in [4]. This parameter and its properties have been investigated in [6] and [7].

A vertex subset S of a graph G is said a *double dominating set*, adrreviated DDS, if $|N[v]\cap S| \geq 2$ for each vertex v of G. The *double domination number* $\gamma_{\times 2}(G)$ of the graph G is the minimum cardinality of a DDS in G. A DDS in G of the minimum cardinality is called a $\gamma_{\times 2}(G)$-*set*. This parameter was introduced by Harary and Haynes in [9].

For a given graph G of order n with e end-vertices, p penultimate vertices and non-increasing degree sequence $d_1 \geq \cdots \geq d_n$, we define the *double Slater number* $s\ell_{\times 2}(G)$ as follows:

$$s\ell_{\times 2}(G) = \min\{t \mid t + d_1 + \cdots + d_{t-e} \geq 2n - p\}.$$

This paper is organized as follows. We first present some properties of the Slater number $s\ell_{\times 2}(G)$ of graphs G. In particular, we observe that $s\ell_{\times 2}(G)$ is a lower bound on $\gamma_{\times 2}(G)$ for all graphs with no isolated vertices. We than prove that the problem of characterizing the extremal graphs for this inequality is NP-hard (even for 4-partite graphs) despite that fact that $s\ell_{\times 2}(G)$ can be computed in linear-time. Some bounds on the double domination number in this paper improve the main results in [3] and [8]. We also give a much shorter proof for the upper bound $\gamma_{\times 2}(T) \leq (2n + \ell + s)/3$ for a non-trivial tree T of order n with ℓ leaves and s support vertices ([2]) with characterization of the extremal trees for this inequality.

Note that for some other domination parameters, lower bounds similar to the double Slater number can be obtained. The reader can consult [1], [5] and [7] for more information about them.

2 Preliminary properties of double Slater number

In this section, we give some results on $\gamma_{\times 2}(G)$ and $s\ell_{\times 2}(G)$ and discuss their relationship for general graphs G. For any graph G of order n with $\delta(G) \geq 2$, we have

$$\gamma_{\times 2}(G) \geq s\ell_{\times 2}(G) = \min\{t \mid t + d_1 + \cdots + d_t \geq 2n\}. \tag{1}$$

In spite of the fact that the lower bound given in (1) and its proof are simple, the family of graphs for which the equality holds cannot be characterized in polynomial-time (even if we restrict the problem to some special families of graphs) unless P=NP. We will prove this in Theorem 3.1.

In the next two propositions we discuss some properties of the double Slater number.

Proposition 2.1. *Let G be a graph of order n with minimum degree $\delta \geq 2$ and maximum degree Δ. Then,*

$$\lceil \frac{2n}{1+\Delta} \rceil \leq s\ell_{\times 2}(G) \leq \lceil \frac{2n}{1+\delta} \rceil.$$

As an immediate consequence of Theorem 2.1, we have $s\ell_{\times 2}(G) = \lceil 2n/(1+r) \rceil$ for any r-regular graph G.

Proposition 2.2. *Let G be a graph of order n and size m with minimum degree $\delta \geq 2$. The following statements hold.*

(i) $1 \leq s\ell_{\times 2}(G) - s\ell(G) \leq \lceil n/(\delta+1) \rceil$. *There bounds are sharp.*

(ii) $2 \leq s\ell_{\times 2}(G) \leq n$. *Moreover,* $s\ell_{\times 2}(G) = 2$ *if and only if G has at least two vertices of degree $n-1$, and* $s\ell_{\times 2}(G) = n$ *if and only if* $m \leq \lfloor (n+\delta)/2 \rfloor$.

(iii) $s\ell_{\times 2}(G) = 2n/(1+\Delta)$ *if and only if* $2n \equiv 0 \pmod{1+\Delta}$ *and* $d_{2n/(1+\Delta)} = \Delta$.

3 Complexity results

Note that the non-increasing degree sequence of a graph G of order n can be made in linear-time by the counting sort algorithm. Therefore sum of the first t degrees, and hence $s\ell_{\times 2}(G)$, can be computed in linear-time. In spite of this fact, the following theorem shows that the problem of determining whether the lower bound (1) holds with equality for a given graph G is NP-complete even if we restrict our attention to some special families of graphs.

Theorem 3.1. *The problem of deciding whether $\gamma_{\times 2}(G) = s\ell_{\times 2}(G)$ for a given graph G is NP-complete even when restricted to 4-partite graphs.*

4 Bounding the double domination number

Let H be a bipartite graph with partite sets X and Y such that every vertex in X has degree two. We make a matching M whose edges join some vertices in Y which have neighbors in X. We also join at least one end-vertex to the vertices in Y which are not saturated by M. Let G be the constructed graph and let Ω be the family of such graphs G (see Figure 1 in the case of a tree T).

Theorem 4.1. *Let G be a graph of order n and size m with no isolated vertices. Let e and p be the number of end-vertices and penultimate vertices in G, respectively. Then,*

$$\gamma_{\times 2}(G) \geq \frac{4n - 2m + e - p}{3}.$$

Furthermore, the equality holds if and only if $G \in \Omega$.

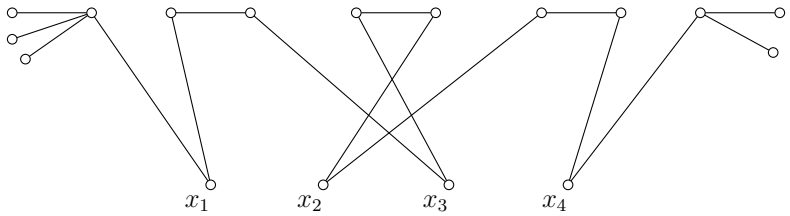

Figure 1: A tree $T \in \Omega$ with $X = \{x_1, x_2, x_3, x_4\}$ and $|M| = 3$.

Note that Theorem 4.4 implies the lower bound given in Theorem 4.1. In spite of this, we proved it by a different method so as to give the characterization of graphs attaining the lower bound.

As an immediate consequence of Theorem 4.1 for trees we have the following result of Chellali in 2006.

Theorem 4.2. ([3]) *If T is a nontrivial tree of order n with ℓ leaves and s support vertices, then $\gamma_{\times 2}(T) \geq (2n + \ell - s + 2)/3$.*

Note that the whole of paper [3] is devoted to the bound given in Theorem 4.2 and a constructive characterization of all trees attaining it.

In order to characterize all trees for which the equality holds in the bound given in Theorem 4.2, it suffices to restrict the family Ω to trees. Let us denote the resulting family by Ω'. In what follows, we describe a typical member of Ω'. We begin with a copies of P_2 and s copies of stars T_i with partite sets X_i and Y_i such that $|X_i| = 1$. We then add $r = a + s - 1$ new vertices and join any any of them to precisely two vertices in the P_2-copies and X_i's such that all vertices of P_2-copies are incident with at least one of them. Note that $m = a + \sum_i |Y_i| + 2r = n - 1$ guarantees that the resulting graph is a tree (see Figure 1 for $(a, s, |Y_1|, |Y_2|) = (3, 2, 3, 2)$).

Hajian and Jafari Rad in 2019 generalized Theorem 4.2 to connected graphs as follows. Note that they used the words "leaf" and "support vertex" instead of "end-vertex" and "penultimate vertex", respectively.

Theorem 4.3. ([8]) *If G is a connected graph of order $n \geq 2$ with $k \geq 0$ cycles, e end-vertices and p penultimate vertices, then $\gamma_{\times 2}(G) \geq (2n + e - p + 2)/3 - 2k/3$.*

They also characterized the family of all graphs achieving the equality in the above bound by extending the characterization given in [3].

Let G be a graph of size m given in Theorem 4.3 and let T be a spanning tree of it. Clearly, all end-vertices and penultimate vertices of G belong to $V(T)$. Let k' be the number of edges of G which are not in T. So, $m = n - 1 + k'$. It is well-known that for such an edge xy, $T + xy$ contains a unique cycle C_{xy} containing xy. Moreover, for any two such edges xy and $x'y'$, $C_{xy} = C_{x'y'}$ implies that $xy = x'y'$. This shows that $xy \longrightarrow C_{xy}$ is a one-to-one function. Therefore, $k' \leq k$. We then have

$$\frac{4n - 2m + e - p}{3} = \frac{2n + e - p + 2}{3} - \frac{2k'}{3} \geq \frac{2n + e - p + 2}{3} - \frac{2k}{3}.$$

In fact, Theorem 4.1 is an improvement of Theorem 4.3.

Theorem 4.4. *For any graph G of order n and size m with e end-vertices, p penultimate vertices and $\delta(G) \geq 1$,*

$$\gamma_{\times 2}(G) \geq s\ell_{\times 2}(G) \geq (4n - 2m + e - p)/3.$$

Furthermore, $s\ell_{\times 2}(T) = (4n - 2m + e - p)/3$ if and only if $n + m + e - p \equiv 0 \pmod 3$ and one of the following conditions hold:
(i) If $\delta(G) \geq 2$, then $d_q = 2$, where $q = (4n - 2m + 3)/3$.
(ii) If $\delta(G) = 1$, then $\big(n = 2m - e + p\big)$ or $\big(n < 2m - e + p$ and $d_q = 2$, where $q = (4n - 2m - 2e - p + 3)/3\big)$.

Remark 4.5. Note that the gap between $s\ell_{\times 2}(T)$ and $(2n+\ell-s+2)/3$ can be arbitrarily large in the case of nontrivial trees T of order n with ℓ leaves and s support vertices. In fact, we claim that for any integer $b \geq 1$, there exists a tree T for which $s\ell_{\times 2}(T) - (2n + \ell - s + 2)/3 = b$. To see this, consider $T = P_{6b+4} \circ K_1$. Then $n = 12b + 8$ and $\ell = s = 6b + 4$. Then, $(2n + \ell - s + 2)/3 = 8b + 6$. On the other hand,

$$9b+6+d_1+\cdots+d_{9b+6-\ell} = 9b+6+d_1+\cdots+d_{3b+2} = 9b+6+3(3b+2) = 18b+12 = 2n-s$$

shows that $s\ell_{\times 2}(T) = 9b + 6 = (2n + \ell - s + 2)/3 + b$, as desired.

The following theorem was proved by Blidia et al. in 2006.

Theorem 4.6. ([2]) *For any tree T of order $n \geq 2$ with ℓ leaves and s support vertices, $\gamma_{\times 2}(T) \leq (2n + \ell + s)/3$.*

They also gave a characterization of the trees attaining the upper bound.

In what follows, we give a much shorter proof for this bound and its extremal trees. To do so, we introduce some notations. Let T be a tree and let $L(T)$ and $S(T)$ be the sets of its leaves and support vertices, respectively. Suppose that T' is a tree as a component of the forest $F = T - (L(T) \cup S(T))$. Let v, as a root, be a leaf of T'. Label each vertex of T' with its distance from v (mod 3). We set $A_i(T') = \{u \mid d(u, v) \equiv i \pmod 3\}$, for $0 \leq i \leq 2$. Note that $\{L(T), S(T)\} \cup \{A_0(T'), A_1(T'), A_2(T')\}_{T'}$ is a partition of $V(T)$ (although some $A_i(T')$ may be empty). Finally, we set $A_i(T) = \cup_{T'} A_i(T')$ for $0 \leq i \leq 2$. Let Γ be the family of all trees T satisfying:

(a) $|A_0(T')| = |A_1(T')| = |A_2(T')|$ for each T', and

(b) for each $u \in A_1(T)$, $deg(u) = 2$ and it does not have any neighbor in support vertices.

Theorem 4.7. *Let T be a tree of order $n \geq 2$ with ℓ leaves and s support vertices. Then, $\gamma_{\times 2}(T) \leq (2n + \ell + s)/3$. Moreover, the equality holds if and only if $T \in \Gamma$.*

For the sake of convenience, we let Π be the family of trees attaining the lower bound given in Theorem 4.4, that is, the family of nontrivial trees T of order n with ℓ leaves and s support vertices for which "$n = \ell - s + 2$" or "$n > \ell - s + 2$ and $d_q = 2$ in which $q = (2n - 2\ell - s + 5)/3$".

Corollary 4.8. *For any tree T of order $n \geq 2$ with s support vertices,*

$$\gamma_{\times 2}(T) - s\ell_{\times 2}(T) \leq 2(s-1)/3$$

with equality if and only if $T \in \Pi \cap \Gamma$.

A *double outer-independent dominating set* (DOIDS) of G is a double dominating set D in G such that $V(G) \setminus D$ is independent. Moreover, the *double outer-independent domination number* $\gamma_d^{oi}(G)$ of G is the smallest possible cardinality taken over all DOIDSs of G. This graph parameter was introduced in [13] and investigated in several papers, for example [12] and [14]. Clearly, $\gamma_{\times 2}(G) \leq \gamma_d^{oi}(G)$ for any graph G with no isolated vertices. Krzywkowski in [12] proved the same upper bound for the double outer-independent domination number of a non-trivial tree T of order n with ℓ leaves and s support vertices, that is, $\gamma_d^{oi}(T) \leq (2n+\ell+s)/3$. Notice that the DDS D constructed in the proof of Theorem 4.7 has the property that $V(T) \setminus D$ is independent. Therefore, D is a DOIDS of T and so $\gamma_d^{oi}(T) \leq |D| \leq (2n+\ell+s)/3$. Indeed, the proof of Theorem 4.7 is much shorter than that of [12] as well.

References

[1] D. Amos, J. Asplund, B. Brimkov and R. Davila, *The Slater and sub-k-domination number of a graph with applications to domination and k-domination*, Discuss. Math. Graph Theory, **40** (2020), 209–225.

[2] M. Blidia, M. Chellali, T.W. Haynes and M.A. Henning, *Independent and double domination in trees*, Utilitas Math. **70** (2006), 159–173.

[3] M. Chellali, *A note on the double domination number in trees*, AKCE J. Graphs. Combin. **3** (2006), 147–150.

[4] W.J. Desormeaux, T.W. Haynes and M.A. Henning, *Improved bounds on the domination number of a tree*, Discrete Appl. Math. **177** (2014), 88–94.

[5] W.J. Desormeaux and M.A. Henning, *A new lower bound on the total domination number of a tree*, Ars Combin. **138** (2018), 305–322.

[6] M. Gentner, M.A. Henning and D. Rautenbach, *Smallest domination number and largest independence number of graphs and forests with given degree sequence*, J Graph Theory, **88** (2018), 131–145.

[7] M. Gentner and D. Rautenbach, *Some comments on the Slater number*, Discrete Math. **340** (2017), 1497–1502.

[8] M. Hajian and N. Jafari Rad, *A new lower bound on the double domination number of a graph*, Discrete Appl. Math. **254** (2019), 280–282.

[9] F. Harary and T.W. Haynes, *Double Domination in Graphs*, Ars Combin. **55** (2000), 201–213.

[10] T.W. Haynes, S.T. Hedetniemi and M.A. Henning (editors), Topics in Domination in Graphs, Switzerland: Springer International Publishing, 2020.

[11] T.W. Haynes, S.T. Hedetniemi and P.J. Slater, Fundamentals of Domination in Graphs, New York, Marcel Dekker, 1998.

[12] M. Krzywkowski, *An upper bound for the double outer-independent domination number of a tree*, Georgian Math. J. **22** (2015), 105–109.

[13] M. Krzywkowski, *Double outer-independent domination in graphs*, Ars Combin. **134** (2017), 193–207.

[14] D.A. Mojdeh, I. Peterin, B. Samadi and I.G. Yero, *On three outer-independent domination related parameters in graphs*, Discrete Appl. Math. **294** (2021), 115–124.

[15] P.J. Slater, *Locating dominating sets and locating-dominating sets*, in: Graph Theory, Combinatorics, and Applications, in: Proc. 7th Quadrennial Int. Conf. Theory Applic. Graphs, **2** (1995), 1073–1079.

[16] D.B. West, Introduction to Graph Theory (Second Edition), Prentice Hall, USA, 2001.

Generically Nilpotent Cellular Automata

Ilkka Törmä*

Department of Mathematics and Statistics
University of Turku, Finland
iatorm@utu.fi

Abstract

We study the generic limit sets of one-dimensional cellular automata, which intuitively capture their asymptotic dynamics while discarding transient phenomena. As our main results, we characterize the automata whose generic limit set is a singleton, and show that this class is Σ_2^0-complete. We also prove that given a CA whose generic limit set is guaranteed to be a singleton, the sole configuration it contains cannot be algorithmically determined.

1 Introduction

A one-dimensional cellular automaton (CA for short) is a dynamical system whose phase space consists of bi-infinite sequences $x \in A^{\mathbb{Z}}$, where A is a finite alphabet. Every CA $f : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ is defined by a local rule that is applied to every coordinate simultaneously. We consider cellular automata as topological dynamical systems. In general, they are neither injective nor surjective, and *attractors* play an important role in the study of their dynamics. The maximal attractor of a dynamical system is its *limit set*, or the set of points that have infinitely long chains of preimages. Limit sets of cellular automata have been studied since the 80s, see e.g. [4, 17].

Attractors in general, and the limit set in particular, reflect the long-term dynamics of a system. There are related notions that correspond more strongly to the intuition of discarding transient phenomena. For a CA f and shift-invariant probability measure μ on $A^{\mathbb{Z}}$, the *μ-limit set* of f, defined by Kůrka and Maass in [15], is obtained by forbidding every word $w \in A^*$ with $\lim_{n\to\infty} f^n\mu([w]_0) = 0$. It corresponds to observations whose probability of occurrence does not tend to 0 with time, when the initial condition is drawn from μ. The *generic limit set*, defined by Milnor in [18], is the smallest closed subset of X that attracts a comeager, or topologically large, subset of X. Intuitively, it represents the eventual fate of all initial conditions save for a negligible set of "pathological" cases. The generic limit set contains the μ-limit set for sufficiently well-behaved measures μ,

*Research supported by Magnus Ehrnrooth Foundation.

and it is contained in the limit set. Generic limit sets of cellular automata were first studied in [8] from the dynamical point of view, and in [22, 6] from the computational perspective.

In this article we study the problem of determining when the generic limit set of a CA is trivial, that is, a singleton set containing a uniform configuration $a^{\mathbb{Z}}$ for some $a \in A$. We call such CA *generically nilpotent*. The name comes from the classical result that a CA f is nilpotent (satisfies $|f^k(A^{\mathbb{Z}})| = 1$ for some $k \in \mathbb{N}$) if and only if its limit set is such a singleton set [4, Theorem 3.5]. Nilpotency is an important property of cellular automata, and several variants of it exist in the literature. Determining whether a given CA is nilpotent is Σ^0_1-complete [12], and the analogous problem for μ-limit sets, when μ is a Bernoulli measure with full support, is Π^0_3-complete [1, Proposition 5.6]. We also mention *asymptotic nilpotency*, which is the property that $\lim_{n\to\infty} f^n(x) = a^{\mathbb{Z}}$ for all $x \in A^{\mathbb{Z}}$, and *unique ergodicity*, which is equivalent to $\lim_{n\to\infty} \frac{1}{n} \left|\left\{0 \leq k < n \;\middle|\; f^k(x)_0 = a\right\}\right| = 1$ for all $x \in A^{\mathbb{Z}}$ when a is a quiescent state of f. It was proved in [9], and generalized in [19, 20], that asymptotic nilpotency is equivalent to nilpotency. On the other hand, [21, Proposition 48] shows that unique ergodicity is Π^0_2-complete.

We show that the class of generically nilpotent cellular automata is Σ^0_2-complete. We also prove that even if a given CA is known to be generically nilpotent, its generic limit set cannot be determined algorithmically. Our proofs are based on a combinatorial characterization of generic nilpotency that we give in Section 3, and the walls-and-counters technique introduced in [5] for constructing cellular automata with specific asymptotic behaviors.

2 Preliminaries

2.1 Definitions

Let A be a finite alphabet, whose elements are often called *states*. The one-dimensional *full shift* is the set $A^{\mathbb{Z}}$ of two-way infinite sequences over A, called *configurations*, equipped with the prodiscrete topology. The topology is generated by the *cylinder sets* $[w]_i = \left\{x \in A^{\mathbb{Z}} \;\middle|\; x|_{[i,i+|w|)} = w\right\}$ for $w \in A^*$ and $i \in \mathbb{Z}$, which are nonempty and clopen. For a set of words $L \subset A^*$ of equal lengths, we denote $[L]_i = \bigcup_{w\in L}[w]_i$. For $a \in A$, the all-a configuration is denoted $a^{\mathbb{Z}}$, and such configurations are called *uniform*.

The *left shift* $\sigma : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ is the homeomorphism defined by $\sigma(x)_i = x_{i+1}$. A *subshift* is a topologically closed set $X \subset A^{\mathbb{Z}}$ satisfying $\sigma(X) = X$. Alternatively, subshifts can be defined by *forbidden words*: there is a set $F \subset A^*$ such that $X = A^{\mathbb{Z}} \setminus \bigcup_{w\in F}\bigcup_{i\in\mathbb{Z}}[w]_i$ is exactly the set configurations where none of the words in F occur at any position. For $n \in \mathbb{N}$, let $\mathcal{L}_n(X) = \left\{x|_{[0,n)} \;\middle|\; x \in X\right\}$ be the set of length-n words occurring in configurations of X. The *language* of X is $\mathcal{L}(X) = \bigcup_{n\in\mathbb{N}} \mathcal{L}_n(X)$. A standard reference for one-dimensional symbolic dynamics is [16].

A (one-dimensional) *cellular automaton*, or CA, on $A^{\mathbb{Z}}$ is a continuous function $f : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ that commutes with the shift: $f \circ \sigma = \sigma \circ f$. By the Curtis-Hedlund-Lyndon theorem [10], CA are also characterized by having a finite *neighborhood* $N \subset \mathbb{Z}$ and a

local rule $F : A^N \to A$ with $f(x)_i = F(\sigma^i(x)|_N)$ for all $x \in A^{\mathbb{Z}}$ and $i \in \mathbb{Z}$. If $N \subset [-r, r]$, then r is a *radius* for f. A state $a \in A$ is *quiescent* for f if $f(a^{\mathbb{Z}}) = a^{\mathbb{Z}}$. See [13] for a survey on one- and multidimensional CA.

A *topological dynamical system*, or TDS, is a pair (X, T) where X is a compact metric space and $T : X \to X$ is continuous. If $X \subset A^{\mathbb{Z}}$ is a subshift and f is a CA on $A^{\mathbb{Z}}$, then $(X, \sigma|_X)$ and $(A^{\mathbb{Z}}, f)$ are examples of topological dynamical systems.

The *limit set* of a TDS (X, T) is $\Omega(T) = \bigcap_{n\in\mathbb{N}} T^n(X)$. The *asymptotic set* $\omega_T(x)$ of a point $x \in X$ is the set of limit points of the forward orbit $(T^n(x))_{n\in\mathbb{N}}$. The *realm of attraction* of $K \subset X$ is $\mathfrak{D}_T(K) = \{x \in X \mid \omega_T(x) \subset K\}$. The *generic limit set* $\tilde{\omega}(T)$ of (X, T) is the intersection of all closed subsets $K \subset X$ such that $\mathfrak{D}_T(K)$ is comeager in X. Generic limit sets were first defined in [18].

Let μ be a Borel probability measure on $A^{\mathbb{Z}}$ and $f : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ a CA. We can apply f to μ and obtain a new probability measure $f\mu$ defined by $(f\mu)(X) = \mu(f^{-1}(X))$ for each Borel set $X \subset A^{\mathbb{Z}}$. We say μ is *shift-invariant* if $\sigma\mu = \mu$. The μ-limit set $\Omega_\mu(f) \subset A^{\mathbb{Z}}$ of f with respect to a shift-invariant measure μ is the subshift obtained by forbidding each word $w \in A^*$ with $\lim_{n\to\infty} f^n\mu([w]_0) = 0$. The μ-limit set was first defined in [15].

The *support* of a measure μ is the unique smallest closed set $K \subset A^{\mathbb{Z}}$ with $\mu(K) = 1$. If $K = A^{\mathbb{Z}}$, we say μ has *full support*. The *Bernoulli measure* corresponding to a distribution $p : A \to [0, 1]$ with $\sum_{a\in A} p(a) = 1$ is the unique Borel probability measure μ_p on $A^{\mathbb{Z}}$ with $\mu_p([w]_i) = \prod_{j=0}^{|w|-1} p(w_j)$ for all cylinder sets $[w]_i$. It has full support iff $p(a) > 0$ for all $a \in A$.

We say that a CA f is *nilpotent* if $|\Omega(f)| = 1$, *generically nilpotent* if $|\tilde{\omega}(f)| = 1$, and *μ-nilpotent* for a measure μ if $|\Omega_\mu(f)| = 1$. In each case the unique configuration must be uniform. In other words, f is generically nilpotent if there exists $a \in A^{\mathbb{Z}}$ and a comeager set $U \subset A^{\mathbb{Z}}$ such that $\lim_{n\to\infty} f^n(x) = a^{\mathbb{Z}}$ for all $x \in U$. It is μ-nilpotent if $\lim_{n\to\infty} f^n\mu([b]_0) = 0$ for all $b \in A \setminus \{a\}$. An alternative (and the more common) definition of nilpotency is that there exists $n \in \mathbb{N}$ such that $f^n(A^{\mathbb{Z}})$ is a singleton [4].

2.2 Auxiliary results

We list some properties of generic limit sets of cellular automata that are not evident from the definition. The following is Proposition 4.10 from [8].

Lemma 1. *Let f be a CA on $A^{\mathbb{Z}}$. Then $\tilde{\omega}(f)$ is a nonempty f-invariant subshift.*

The following two results are from [22]. The first is a combinatorial characterization of the language of the generic limit set, and the second is a tool for proving structural properties of generic limit sets.

Lemma 2. *Let f be a CA on $A^{\mathbb{Z}}$. A word $s \in A^*$ occurs in $\tilde{\omega}(f)$ if and only if there exists a cylinder set $[v]_i$ such that for all $u, w \in A^*$ there exist infinitely many $t \in \mathbb{N}$ with $f^t([uvw]_{i-|u|}) \cap [s]_0 \neq \emptyset$.*

We say that the word v, or the set $[v]_i$, *enables* s for f.

Lemma 3. *Let f be a CA on $A^{\mathbb{Z}}$, let $n \in \mathbb{N}$, and let $[v]_i \subset A^{\mathbb{Z}}$ be a cylinder set. Then there exists a cylinder set $[w]_j \subset [v]_i$ and $T \in \mathbb{N}$ such that for all $t \geq T$ we have $f^t([w]_j) \subset [\mathcal{L}_n(\tilde{\omega}(f))]_0$.*

Words w with the above property are called *$\tilde{\omega}(f)$-forcing*. The lemma states that every word can be extended into a forcing one.

3 Dynamics of generically nilpotent automata

Example 5.13 of [8] shows that there exist simple non-nilpotent cellular automata that are generically nilpotent. In particular, nilpotency and generic nilpotency are not equivalent conditions. We prove this fact for completeness, and to illustrate the use of Lemma 2. Recall that $a \in A$ is a *spreading state* for a CA f if the local rule $F : A^N \to A$ satisfies $F(P) = a$ whenever $P_i = a$ for some $i \in N$.

Example 4 (Example 5.13 in [8])**.** *Let $A = \{0, 1\}$ and let $f : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ be the two-neighbor minimum CA, defined by $f(x)_i = \min(x_i, x_{i+1})$. The limit set $\Omega(f)$ contains exactly the configurations where none of the words 10^n1 for $n \geq 0$ occur. In particular, $\Omega(f)$ is infinite since it contains the configurations ${}^{\infty}0.1^n0^{\infty}$ for all $n \geq 0$, and f is not nilpotent.*

Let then $s \in \mathcal{L}(\tilde{\omega}(f))$ be any word occurring in the generic limit set, and let $[v]_i$ enable it as per Lemma 2. We may assume $i + |v| \geq |s|$ by extending v if necessary. Choose $u = \epsilon$ (the empty word), $w = 0$ and $t > i + |v|$ such that $[uvw]_{i-|u|} \cap f^{-t}([s]_0)$ contains at least one configuration x. Since $x_{i+|v|} = 0$ and 0 is a spreading state, we have $f^n(x)_j = 0$ for all $n \geq 0$ and $i+|v|-n \leq j \leq i+|v|$. In particular, $s = f^t(x)|_{[0,|s|)} = 0^{|s|}$. Since $\tilde{\omega}(f)$ is a nonempty subshift, it must equal $\{0^{\mathbb{Z}}\}$.

In [12], Kari proved that the set of nilpotent CA is Σ^0_1-complete, even within the set of CA with neighborhood $\{0, 1\}$ and a spreading state. By [3, Remark 1], every CA with a spreading state is μ-nilpotent for every full-support Bernoulli measure μ. Hence nilpotent CA are Σ^0_1-complete among μ-nilpotent CA. With the same proof as Example 4 we can show that every CA with neighborhood $\{0, 1\}$ and a spreading state is generically nilpotent. Hence nilpotent CA are Σ^0_1-complete among generically nilpotent CA as well.

From Proposition 6.2 and Corollary 6.5 of [8] we deduce that the μ-limit set $\Omega_\mu(f)$ is contained in the generic limit set $\tilde{\omega}(f)$ whenever μ has full support and is σ-ergodic. In particular, this holds when μ is a full-support Bernoulli measure, and then generic nilpotency implies μ-nilpotency. A simple example shows that the two properties are distinct.

Example 5 (Example 5.13 in [8])**.** *Let $A = \{0, 1\}$ and define $f : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ by $f(x)_i = \min(x_{i+1}, x_{i+2})$. We claim that f is μ-nilpotent for every full-support Bernoulli measure μ on $A^{\mathbb{Z}}$, but not generically nilpotent. For the first claim, we note that $f^{-n}([1]_0) = [1^{n+1}]_n$ for all $n \geq 0$, and then $f^{-n}\mu([1]_0) = \mu([1]_0)^{n+1} \to 0$ as $n \to \infty$. Hence $1 \notin \mathcal{L}(\Omega_\mu(f))$, implying $\Omega_\mu(f) = \{0^{\mathbb{Z}}\}$. Note that this is essentially the argument that*

a spreading state implies μ-nilpotency. On the other hand, we have $1 \in \mathcal{L}(\tilde{\omega}(f))$ since the empty word enables it with $i = 0$: for all words $u, w \in A^*$ and $t \geq |w|$, there exists a configuration $x \in [uw]_{-|u|}$ with $x_j = 1$ for all $t \leq j \leq 2t$, which implies $f^t(x)_0 = 1$. This also shows that a spreading state alone does not guarantee generic nilpotency.

In general, the limit set and the μ-limit set are invariant under compositions by shifts, that is, $\Omega(f \circ \sigma) = \Omega(f)$ and $\Omega_\mu(f \circ \sigma) = \Omega_\mu(f)$ always hold. The generic limit sets of f and $f \circ \sigma$ may be distinct. This phenomenon was studied in detail in [8].

We now present a combinatorial characterization of generic nilpotency.

Lemma 6. *Let f be a CA with radius $r \geq 0$ on $A^{\mathbb{Z}}$, and let $a \in A$. Then $\tilde{\omega}(f) = \{a^{\mathbb{Z}}\}$ if and only if there exists a cylinder set $[w]_i$ and $T \in \mathbb{N}$ such that*

- *for all $t \geq T$ we have $f^t([w]_i) \subset [a^r]_0$, and*
- *for all $n \in \mathbb{N}$ we have $f^{T+|A|^n}([w]_i \cap [w]_{i+r+n}) \subset [a^n]_r$.*

The first condition in particular implies that w can be extended into a *blocking word* for f, meaning a word $v \in A^*$ with some $j \in \mathbb{Z}$ that satisfies $\left|\left\{ f^t(x)|_{[0,r)} \;\middle|\; x \in [v]_j \right\}\right| = 1$ for all $t \in \mathbb{N}$. The intuition for the second condition is that if we "trap" an interval of cells between two occurrences of w that force its borders to consist of a-states, then the deterministic dynamics of f will enter a loop on this interval. The loop must be a fixed point in which every cell contains an a-state, for otherwise some non-a states would be found in the generic limit set.

Proof. Suppose that $\tilde{\omega}(f) = \{a^{\mathbb{Z}}\}$. By Lemma 3 applied to the empty word $v = \epsilon$ and $n = r$, there exists $T \in \mathbb{N}$ and a cylinder set $[w]_i$ such that $f^t([w]_i) \subset [a^r]_0$ for all $t \geq T$. This is precisely the first claim.

For the second claim, fix $n \in \mathbb{N}$ and an arbitrary configuration $x \in [w]_i \cap [w]_{i+r+n}$. Denote $K := \max(n + r(T + 2), |i| + |w| + n + r)$ and $v = x|_{[-K,K]}$. Then we have $[v]_{-K} \subset [w]_i \cap [w]_{i+r+n}$. By the definition of $[w]_i$, this implies

$$f^t([v]_{-K}) \subset [a^r]_0 \cap [a^r]_{n+r} \tag{1}$$

for all $t \geq T$. Furthermore, since r is a radius for f, we have

$$f^T(y)|_{[0,n+2r)} = f^T(x)|_{[0,n+2r)} \tag{2}$$

for every $y \in [v]_{-K}$.

We now prove by induction that for each $t \geq T$, the word $f^t(y)|_{[0,n+2r)} \in A^{n+2r}$ is independent of the choice of $y \in [v]_{-K}$. For $t = T$ this follows from (2). Suppose then that the claim holds for some $t \geq T$. For each $r \leq \ell < n + r$ we have $f^{t+1}(y)_\ell = F(f^t(y)_{\ell-r}, \ldots, f^t(y)_{\ell+r})$, where F is the local function of f. The right hand side is independent of y by the induction hypothesis. For $0 \leq \ell < r$ and $n + r \leq \ell < n + 2r$, we have $f^{t+1}(y)_\ell = a$ by (1). These are clearly independent of y.

The above argument also shows that the sequence $s' := (f^t(x)|_{[r,n+r)})_{t \geq T}$ of length-n words is eventually periodic, and the length of its pre-periodic part is less than $|A|^n$.

Namely, each $s'(t+1)$ is determined from $s'(t)$ by the local rule F and (1). The number of distinct words $s'(t) \in A^n$ for $t \geq T$ is at most $|A|^n$, and once a repetition occurs, the rest of the sequence is periodic.

Again by Lemma 3, there exists a cylinder set $C \subset [v]_{-K}$ and $T' \geq T$ with $f^t(C) \subset [a^n]_r$ for all $t \geq T'$. Let $y \in C$. Then $s'(T') = f^{T'}(y)|_{[r,n+r)} = a^n$, so that the periodic part of the sequence s' is $(a^n, a^n, \ldots)$. Since $s'(T + |A|^n)$ is in the periodic part, we have $f^{T+|A|^n}(x)|_{[r,n+r)} = a^n$. The configuration $x \in [w]_i \cap [w]_{i+r+n}$ was arbitrary, so the second condition holds.

For the converse direction, suppose that there are $[w]_i$ and T that satisfy the two properties. Let $s \in \mathcal{L}(\tilde{\omega}(f))$ be arbitrary, and let $[v]_j$ enable it as per Lemma 2. Then for all large enough $n \in \mathbb{N}$, there exist infinitely many $t \in \mathbb{N}$ with $f^t([w]_{i-n} \cap [u]_j \cap [w]_{i+n}) \cap [s]_0 = \emptyset$. But for each $n \geq r$ we have $f^{T+|A|^{2n-r}}([w]_{i-n} \cap [w]_{i+n}) \subset [a^{2n-r}]_{r-n}$ by assumption, which implies $s \in a^*$. Because $\tilde{\omega}(f)$ is a nonempty subshift of $A^{\mathbb{Z}}$, we must have $\tilde{\omega}(f) = \{a^{\mathbb{Z}}\}$. □

4 Construction with walls and counters

4.1 Overview

Our remaining results rely heavily on the type of construction introduced in [5] and used to prove various realization results in the measure-theoretic setting [2, 1, 11]. We present a "prototypical" version of the construction in this section.

The idea is to have a designated *initializer state* that can only be present in an initial configuration. In one step, it turns into a somewhat persistent *wall state*. These walls divide a configuration into *segments*. We can achieve a high level of control over the contents of the segments by ensuring that each pair of initializers starts a process that formats the segment between them, in particular removing all walls that are not properly initialized. When the segments are formatted, we allow them to host simulated computations, and communicate and merge with their neighbors; new walls are never created after the first time step. In applications, we guarantee that in a typical configuration, every wall and auxiliary state will eventually disappear, so the only patterns visible in the generic limit set are those that occur inside the properly formatted segments.

Figure 1 illustrates the roles of the various signals used in the construction. Figure 2 depicts the creation of walls and formatted segments from a typical initial configuration. The figures and the following presentation are based on [1, Section 3.2], which the reader may consult for more details. The only major difference is that in our version, wall states are created directly by initializers instead of colliding counter signals, as this simplifies some parts of the proofs. The article [11] contains a variant in which wall states are likewise created by initializers, but the formatting process is more complex.

4.2 The construction

We define a radius-1 CA f on an alphabet A that realizes the prototypical segment construction. The alphabet A consists of the *initializer state* `I`, the *wall state* `W`, the

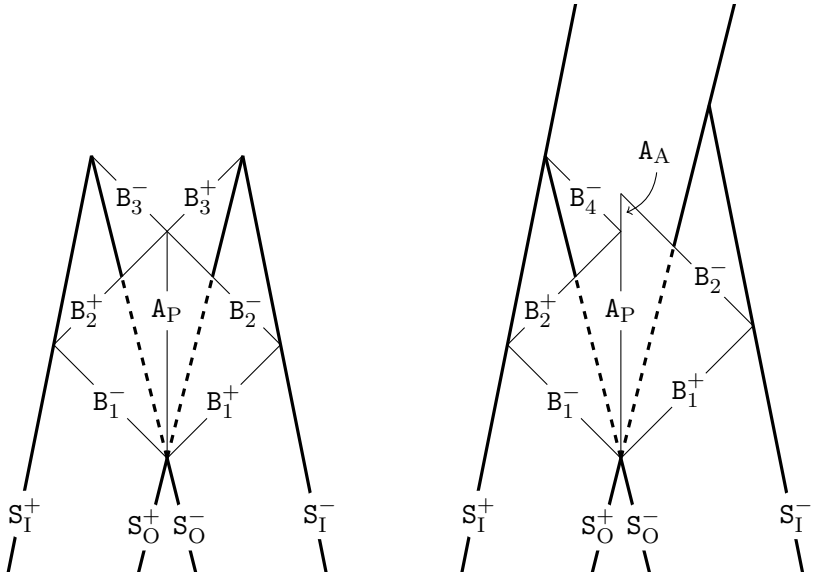

Figure 1: Comparing the values of two counters, of equal values on the left and unequal values on the right. The counter with the smaller value survives.

empty state $\mathtt{E}$, as well as states that encode *signals* of various speeds. When we say that a cell $i \in \mathbb{Z}$ of a configuration $x \in A^{\mathbb{Z}}$ is *erased* by f, we mean that its next state is the empty state: $f(x)_i = \mathtt{E}$. Initializers cannot be created by f, and every initializer will immediately turn into a wall, which is the only way a wall can be created. A wall that originates from an initializer is called *properly initialized*.

Every initializer also emits four signals: *left and right inner signals* $\mathtt{S}_\mathrm{I}^\pm$, which move at speeds $\pm 1/5$, and *left and right outer signals* $\mathtt{S}_\mathrm{O}^\pm$, which move at speeds $\pm 1/4$. The outer signals can be either *open* or *closed*, and they start as closed. Open signals are presesented by dashed lines in Figure 1. A pair of inner and outer signals moving in the same direction, with the outer signal being the leading one, is called a *counter*. The idea is that the distance between the signals encodes the common age of the counter in unary. A counter can appear to be older than the initial configuration, but not younger, since the signal pairs are only created by initializers and an inner signal cannot cross an outer one.

A closed outer signal erases all data it encounters, except for a closed outer signal of the opposite direction. When two closed outer signals meet, they become open, pass through each other, and emit three new signals: *left and right bouncing signals* $\mathtt{B}_i^\pm$ of speeds ± 1, and a stationary *passive anchor signal* $\mathtt{A}_\mathrm{P}$. The bouncing signals come in a few different flavors ($i = 1, 2, 3, 4$), but all of them erase all data they encounter apart from inner and outer borders and the few special cases described below. The collision of two closed outer signals first produces bouncing signals $\mathtt{B}_1^\pm$, which erase all data except an outer signal, which erases them, or an inner signal, which causes them to "bounce

back" and become $\mathtt{B}_2^{\mp}$, moving in the opposite direction.

The signals $\mathtt{B}_2^{\pm}$ can pass through an open outer signal, and together with other outer signals, they are the only signals able to do so. When this happens, the open signal becomes closed.

When two signals $\mathtt{B}_2^{\pm}$ encounter a passive anchor signal simultaneously, the latter is erased, and two new signals $\mathtt{B}_3^{\pm}$ are emitted. When a signal $\mathtt{B}_3^{\pm}$ collides with a closed outer signal $\mathtt{S}_{\mathrm{O}}^{\pm}$ of the same orientation and an inner signal $\mathtt{S}_{\mathrm{I}}^{\mp}$ of the opposite orientation, all three are erased. In the case that the signal $\mathtt{B}_3^{\pm}$ is produced by the collision of two equal counters, the three signals will collide simultaneously (see the left half of Figure 1).

When a signal $\mathtt{B}_2^{\pm}$ encounters a passive anchor signal without its symmetrical counterpart, a signal $\mathtt{B}_4^{\mp}$ is emitted in the opposite direction and the anchor becomes an *active anchor signal* $\mathtt{A}_{\mathrm{A}}$. When a signal $\mathtt{B}_4^{\pm}$ encounters a closed outer signal of the same orientation, both are erased, but an inner signal of the opposite orientation arriving at the same position is not. If $\mathtt{B}_4^{\pm}$ is produced by the collision of unequal counters, such a three-way collision does occur (see the right half of Figure 1). The only event that can erase an outer signal is a collision with $\mathtt{B}_3^{\pm}$ or $\mathtt{B}_4^{\pm}$ as described above. When a signal $\mathtt{B}_2^{\pm}$ encounters $\mathtt{A}_{\mathrm{A}}$, both are erased.

The above scheme involves signals with fractional speeds, which can be implemented using additional states. For example, a right inner signal with speed $1/5$ is represented by five distinct states. They evolve cyclically and one of the transitions moves the signal by a single step. The bouncing signals also need to remember the phases of the fractional-speed signals they bounced from, which can likewise be implemented with a finite number of additional states.

The construction ensures that when two counters collide, if they have equal values then both are destroyed, and otherwise the one with smaller value survives. The initial configuration may contain "rogue" signals and walls that are not part of a counter or a comparison process, but these cannot interfere with properly initialized counters, as they will be erased by either outer signals or $\mathtt{B}_1^{\pm}$-signals. Thus f has the following property.

Lemma 7. *Let $x \in A^{\mathbb{Z}}$ be a configuration containing at least one initializer* $\mathtt{I}$*. For each $i \in \mathbb{Z}$ with $x_i = \mathtt{I}$, we have $f^n(x)_i = \mathtt{W}$ for all $n \geq 1$. For each $i \in \mathbb{Z}$ with $x_i \neq \mathtt{I}$, we have $f^n(x)_i = \mathtt{E}$ for all $n > 5d$, where $d = \min\{|i-j| \mid x_j = \mathtt{I}\}$.*

In a configuration, the space between two initializers or properly initialized walls is called a *segment*. Lemma 7 states that all segments will eventually consist of empty cells. See Figure 2.

In our applications, we simulate computations of Turing machines inside the segments. A simulated machine head is created to the right of each initializer (unless that cell also contains an $\mathtt{I}$), and the $\mathtt{E}$-states inside the segment are interpreted as blank tape cells. We do not give the details of this simulation since they are standard in the literature and unimportant for our constructions, except that we must guarantee that it takes at least $5k$ time steps for the simulated head to advance to the kth tape cell, for each $k \geq 1$. Otherwise it would catch the inner signal produced by the same initializer.

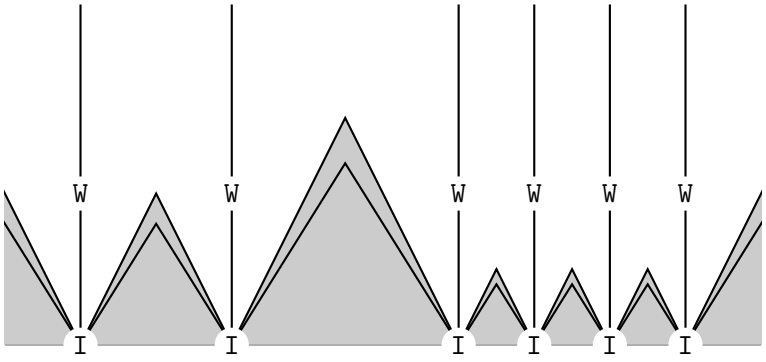

Figure 2: Creation of properly initialized walls. The white regions consist of E-states.

4.3 Application: finite generic limit sets

The walls-and-counters method was used in [1, Theorem 6.1] to construct a CA f such that for any full-support Bernoulli measure μ, the μ-limit set $\Omega_\mu(f)$ consists of exactly two unary configurations that f maps to each other. It was noted in [8, Example 5.18] that in this case $\tilde{\omega}(f) = \Omega_\mu(f)$ has the same property. In particular, the analogue of the classical result that $\Omega(f)$ is finite if and only if f is nilpotent (see e.g. [12]) is false for both generic limit sets and μ-limit sets.

We describe the construction for completeness. In fact, it can be easily generalized to obtain generic limit sets of any finite cardinality $1 \leq k < \infty$. The idea is to split the empty state $\mathtt{E}$ into k copies $\mathtt{E}_0, \ldots, \mathtt{E}_{k-1}$, and discard the wall states $\mathtt{W}$, so that the CA turns every initializer into $\mathtt{E}_1$ instead. Each $\mathtt{E}_i$ becomes $\mathtt{E}_{i+1 \bmod k}$ under an application of the CA. When an inner or outer signal moves to an adjacent cell or is destroyed, the cell that contained it becomes $\mathtt{E}_{i+1 \bmod k}$ if the neighboring cell in the opposite direction contained $\mathtt{E}_i$. Then for each configuration x that contains at least one initializer, for each cell $j \in \mathbb{Z}$ we have $f^t(x)_j = \mathtt{E}_{t \bmod k}$ for all large enough t. It follows that $\tilde{\omega}(f) = \{\mathtt{E}_0^{\mathbb{Z}}, \ldots, \mathtt{E}_{k-1}^{\mathbb{Z}}\}$.

In [8, Section 4.4] Djenaoui and Guillon studied dynamical systems with finite generic limit sets. Proposition 4.16 of that article states that if f is a CA with $|\tilde{\omega}(f)| < \infty$, then $\tilde{\omega}(f)$ consists of uniform configurations that f permutes cyclically. Hence the above construction realizes essentially all possible pairs $(\tilde{\omega}(f), f|_{\tilde{\omega}(f)})$, where f is a CA such that $\tilde{\omega}(f)$ is finite.

5 Main results

Theorem 8. *The class of generically nilpotent cellular automata is Σ_2^0-complete.*

Proof. The combinatorial condition of Lemma 6 is Σ_2^0 by form. Hence the set of generi-

cally nilpotent CA is Σ^0_2.

To show completeness, let $(M_k)_{k\in\mathbb{N}}$ be a Gödel numbering of Turing machines, and let $P = \{k \in \mathbb{N} \mid \exists w : M_k(w)\uparrow\}$ be the numbers of those machines that do not halt on every input. This set is Σ^0_2-complete. We many-one reduce P to the set of generically nilpotent cellular automata, showing that the latter is Σ^0_2-complete as well.

We modify the radius-1 cellular automaton $f : A \to A$ of Section 4. The high-level idea is the following. Each segment will host a simulated computation of the machine M_k on successive input words w, and the number of steps to be simulated depends on the length of the segment in such a way that $k \in P$ if and only if only finitely many lengths host a simulation that ends in a halting state. Whenever this happens, the segment invades a portion of its left neighbor, but in any case the eventual fate of all segments is to be filled with E-states and merge with their neighbors. The invasions are visible in the generic limit set if and only if $k \notin P$.

For each $k \in \mathbb{N}$, define a new alphabet $A_k = A \cup B_k$, where B_k is an auxiliary alphabet that contains additional states needed to simulate a Turing machine M'_k and a new state G. We define a CA $f_k : A_k^{\mathbb{Z}} \to A_k^{\mathbb{Z}}$ such that $\tilde{\omega}(f) = \{\mathtt{E}^{\mathbb{Z}}\}$ for the empty state $\mathtt{E} \in A$ if $k \in P$, and $\tilde{\omega}(f)$ is infinite if $k \notin P$.

The restriction $f_k|_{A^{\mathbb{Z}}}$ is exactly the walls-and-counters CA of Section 4. In addition, all signals of A erase all states of B_k they encounter, which ensures that a configuration with infinitely many initializers will give rise to infinitely many properly initialized walls with formatted segments in between.

Whenever f_k creates a wall, it starts a simulation of the machine M'_k on its right. This machine behaves as follows. First, it measures the width $n \in \mathbb{N}$ of the segment that hosts it. Then it simulates the machine M_k on inputs $w_0, w_1, w_2, \ldots$, where $(w_i)_{i\in\mathbb{N}}$ is the enumeration of all binary words by length and then lexicographically, for a total of n steps. If the final computation step of the simulation puts M_k into a halting state, we say the segment containing M'_k is *bad*. Otherwise it is *good*. We also define segments of length 0 to be good.

The new state $\mathtt{G} \in B_k$ is by default stationary. When M'_k has determined that its segment is good, it fills the segment with E-states, except for the leftmost and rightmost cells, where it places G-states. We extend the definition of good segments to include all segments containing G-states at both ends and E-states everywhere else. Whenever a wall has G-states or walls on both sides, the central wall and any adjacent G-states are immediately erased by f_k. This means that two or more neighboring good segments will merge into a larger good segment.

If M'_k determines that its segment is bad, the simulated head travels to its left end. It waits there until the cell at the other side of the wall contains a G-state, designating the neighboring segment as good. Then M'_k merges the two segments by erasing the wall and the G-state next to it, and travels n steps to the left of the position of the erased wall, or up to the left end of the combined segment, whichever is nearer, where n is the length of the original bad segment. Note that the interior of a good segment contains only E-states, so the head can travel through it undisturbed. Then the head travels to the right end of the combined segment, erasing all data from the combined segment as

it goes. It places a G-state next to the right wall and erases itself. This means that a bad segment will merge with a good segment to its left, and the combined segment then becomes good. In the process a simulated head of M'_k travels n cells deep into the good segment.

This concludes the definition of f_k. We note that f_k can be realized with radius $r = 2$.

Suppose that $k \in P$. Since there is an input on which M_k never halts, the set of lengths that result in bad segments is finite, so it has an upper bound $N \in \mathbb{N}$. We claim that the word $w = \mathtt{IE}^{N+3}\mathtt{I} \in B_k^{N+5}$ satisfies the conditions of Lemma 6 with $i = -2$ and some $T \in \mathbb{N}$. Consider a configuration $x \in [w]_{-2}$. The two I-states x_{-2} and x_{N+2} delimit a segment, which is properly formatted in $f_k^{5N}(x)$. After the simulated machine M'_k in this segment has finished its computation, it becomes good, since it is strictly longer than N cells. Let T be the time step at which this happens. Then $f^T(x)|_{[0,1]} = \mathtt{E}^2$, and we claim that $f^t(x)|_{[0,1]} = \mathtt{E}^2$ holds for all $t \geq T$.

For $t \geq T$, let $S_t \subset \mathbb{Z}$ be the segment of $f^t(x)$ containing the coordinate 0. If S_t merges with one or more good segments, the resulting segment S_{t+1} is also good, and the merging process does not involve the interior cells of S_t. If S_t merges with a bad segment to its right, then a simulated head of M'_k will travel some $n \leq N$ cells into S_t. Since the rightmost coordinate of S_t is initially $N+1$ and cannot decrease, the head will not reach the coordinate 1. This shows $f^t(x)|_{[0,1]} = \mathtt{E}^2$ for all $t \geq T$.

For the second condition of Lemma 6, take any $n \in \mathbb{N}$ and a configuration $x \in [w]_{-2} \cap [w]_{n-2}$. The word $x|_{[-2,n+N+3]}$ contains some number of I-states that divide it into segments. Each of those segments will eventually be properly formatted and become either good or bad. The first and last segments will become good. It follows that the segment of $f^t(x)$ containing the coordinate 0 will always be good, and it will merge with the segment to its right as soon as the latter becomes good or bad. Hence, for large enough t we will have $f^t(x)|_{[0,n+N+1]} = \mathtt{E}^{n+N+2}$, which implies the second condition of Lemma 6. Thus f_k is generically nilpotent.

Suppose now that $k \notin P$. Then there exist infinitely many lengths that result in bad segments. For each $n \geq 0$, denote $L_n = \{\mathtt{E}^n b \mid b \in B_k \setminus \{\mathtt{E}\}\} \subset B_k^{n+1}$. We show that $L_n \cap \mathcal{L}(\tilde{\omega}(f)) \neq \emptyset$ for all $n \geq 0$. More strongly, we show that some word in L_n is enabled by the empty word, using the terminology of Lemma 2, which is equivalent to the condition that for every cylinder set C there are infinitely many $t \in \mathbb{N}$ with $f^t(C) \cap [L_n]_0 \neq \emptyset$. This implies that $\tilde{\omega}(f_k)$ is an infinite subshift, so f_k is not generically nilpotent.

Let $[w]_i$ be a cylinder set. We may assume $i \leq 0$ and $|w| \geq |i| + n$ by extending w if necessary. Choose a number $N \geq |w| - n$ that results in a bad segment and consider the configuration $x = {}^{\infty}\mathtt{EII}.w\mathtt{IE}^N\mathtt{IE}^{\infty}$, where the dot denotes coordinate i, so that $x \in [w]_i$. We claim that if N is large enough, then $f_k^t(x) \in [L_n]_0$ for some $t > N$. As we have infinitely many choices for N, this implies that $f^t([w]_i) \cap [L_n]_0 \neq \emptyset$ for infinitely many t.

Every finite segment in x will eventually become either good or bad. The leftmost segment has length 0, and we have guaranteed that such segments are good. Therefore it will merge with its right neighbor once that segment has determined its goodness

status, and the combined segment will become good. In this way all segments in x will eventually merge into one.

Suppose N is so large that the rightmost segment becomes bad only after all the other segments have merged into a good segment. This requires more than N applications of f_k, since it takes at least N steps for the simulates head of M'_k to measure the length of the segment. Since we assumed $N \geq |w| - n$, the head of M'_k will travel to the left, and at some time step $t > N$ enter the coordinate n. Then $f_k^t(x)|_{[0,n]} \in L_n$, which is what we claimed. This shows that $\tilde{\omega}(f_k)$ is infinite. □

In [1], the authors consider the complexity of μ-nilpotent cellular automata also within specific subclasses. They prove that for a σ-ergodic measure μ with full support, μ-nilpotent CA are Π_1^0 within the class of CA with a *persistent state* (a state $a \in A$ with $f(x)_i = a$ whenever $x_i = a$), and Σ_2^0 within the class of CA with an equicontinuity point. The latter result is somewhat analogous to Theorem 8: as discussed after Lemma 6, every generically nilpotent CA admits a blocking word, and hence an equicontinuity point [14].

Delacourt proved in [6] that every nontrivial property of generic limit sets of cellular automata is undecidable. More strongly, they are Π_1^0-hard or Σ_1^0-hard. It was left open whether this complexity bound is tight, that is, whether there exist Π_1^0 properties of generic limit sets. We do not resolve this problem, but Theorem 8 shows that some properties are Σ_2^0-complete.

If $f : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ is a nilpotent CA, then $\Omega(f) = \{a^{\mathbb{Z}}\}$ for some $a \in A$. Determining the state a from the local rule of f is simple: it is the sole quiescent state of f. We show that it is impossible to algorithmically determine the generic limit set of a given generically nilpotent CA.

Theorem 9. *Given a finite alphabet A, distinct states $a, b \in A$, and a cellular automaton $f : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ that satisfies either $\tilde{\omega}(f) = \{a^{\mathbb{Z}}\}$ or $\tilde{\omega}(f) = \{b^{\mathbb{Z}}\}$, it is undecidable whether the first case holds.*

Proof. We reduce the halting problem of Turing machines on empty input to the problem in the theorem statement. Let M be a turing machine. We define a cellular automaton f_M as follows. As in the proof of Theorem 8, we modify the radius-1 CA $f : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ of Section 4 by extending the alphabet into $A_M := A \cup B_M$. The auxiliary alphabet B_M contains new states that are used to simulate a Turing machine M', as well as new states `G` and `H`. The state `G` plays a similar role as in the earlier proof, marking segments that are ready to merge with their neighbors. The state `H` spreads over `E`-states in both directions, but not over other states of A_M.

As a wall is created by an initializer, a simulated computation of M' is started on its right. This machine measures the length n of the segment containing it and simulates M on empty input for n steps. Then it writes `G`-states on the leftmost and rightmost cells of the segment. If M halted during the simulated computation, then M' writes an `H`-state somewhere in the interior of the segment. Then, regardless of whether M halted, M' erases itself. As before, if a wall is surrounded by walls or `G`-states, it erases itself and any adjacent `G`-states.

This concludes the definition of f_M. It can be implemented with radius $r = 2$.

We claim that $\tilde{\omega}(f_M) = \{\mathtt{H}^{\mathbb{Z}}\}$ if M halts on empty input, and $\tilde{\omega}(f_M) = \{\mathtt{E}^{\mathbb{Z}}\}$ if it does not. Suppose first that M halts after some N steps. We claim that the word $w = \mathtt{IE}^{N+4}\mathtt{I}$, $i = -2$ and $a = \mathtt{H}$ satisfy the two conditions of Lemma 6, showing that $\tilde{\omega}(f_M) = \{\mathtt{H}^{\mathbb{Z}}\}$.

For the first condition, let $x \in [w]_{-2}$ be arbitrary. The initializers at x_{-2} and x_{N+3} delimit a segment of length $N + 4$. In this segment, the machine M' is simulated, which in turn simulates M until it halts. Then it writes G-states at coordinates -1 and $N + 2$ and an H somewhere in between before erasing itself. The H will spread over the cells at coordinates $0, 1, \ldots, N + 1$. After this, their contents will never change, as the merging of segments only affects the cells adjacent to the walls. In particular, we have $f_M^t(x)|_{[0,1]} = \mathtt{H}^2$ for all large enough t, and thus the first condition holds.

For the second condition, take any $n \in \mathbb{N}$ and a configuration $x \in [w]_{-2} \cap [w]_{n-2}$. As in the proof of Theorem 8, the word $x|_{[-2,n+N+4]}$ contains some number of I-states that divide it into segments, which will eventually merge into one large segment. This segment contains at least one H, since the original leftmost segment has length $N + 4$. Hence $f_M^t(x)|_{[-2,n+N+4]} = \mathtt{H}^{n+N+6}$ for all large enough t, and the second condition holds.

Suppose then that M does not halt on empty input. We show that $w = \mathtt{IE}^4\mathtt{I}$, $i = -2$ and $a = \mathtt{E}$ satisfy the two conditions of Lemma 6, implying $\tilde{\omega}(f_M) = \{\mathtt{E}^{\mathbb{Z}}\}$. Let $x \in [w]_{-2}$ be arbitrary. The segment delimited by $x_{-2} = x_3 = \mathtt{I}$ will host a simulation of M', which simulates M for 4 steps and writes GEEG on its cells. In general, every properly formatted length-n segment in x will eventually be filled with E-states, except for the two bordermost cells. Merging two such segments preserves this property, and the walls-and-counters construction ensures that segments can only be modified by merging. Thus $f_M^t(x)|_{[0,1]} = \mathtt{E}^2$ for all large enough t, and the first condition holds.

The proof of the second condition is analogous to the case of M halting, except that no H-symbols are produced in any segments. □

6 Future work

In the proof of Theorem 9, we actually show that the problem of determining the generic limit set of a generically nilpotent CA is Σ_1^0-hard. By symmetry, it is also Π_1^0-hard. This implies that it is not complete for either class. It is Σ_2^0 by Lemma 6, but not Σ_2^0-complete for the same reason as above. We leave its exact complexity open.

In this article we have only considered one-dimensional cellular automata. The proof of Lemma 6 cannot be directly generalized to the multidimensional case, since it relies on the ability of blocking words to cut a one-dimensional configuration into two independently evolving halves. Thus, we do not know if our results hold for two- and higher-dimensional CA. A two-dimensional version of the walls-and-counters CA of Section 4 was presented in [7].

Finally, we have concentrated on generic limit sets consisting of a single configuration. Our results probably apply to CA with finite generic limit sets with mostly the same proofs, save for additional technical details.

References

[1] L. Boyer, M. Delacourt, V. Poupet, M. Sablik, and G. Theyssier. μ-limit sets of cellular automata from a computational complexity perspective. *J. Comput. System Sci.*, 81(8):1623–1647, 2015.

[2] Laurent Boyer, Martin Delacourt, and Mathieu Sablik. Construction of μ-limit sets. In Jarkko Kari, editor, *Second Symposium on Cellular Automata "Journées Automates Cellulaires", JAC 2010, Turku, Finland, December 15-17, 2010. Proceedings*, pages 76–87. Turku Center for Computer Science, 2010.

[3] Laurent Boyer, Victor Poupet, and Guillaume Theyssier. On the complexity of limit sets of cellular automata associated with probability measures. In *Mathematical Foundations of Computer Science 2006*, volume 4162 of *Lecture Notes in Comput. Sci.*, pages 190–201. Springer, Berlin, 2006.

[4] Karel Culik, II, Jan Pachl, and Sheng Yu. On the limit sets of cellular automata. *SIAM J. Comput.*, 18(4):831–842, 1989.

[5] M. Delacourt, V. Poupet, M. Sablik, and G. Theyssier. Directional dynamics along arbitrary curves in cellular automata. *Theoret. Comput. Sci.*, 412(30):3800–3821, 2011.

[6] Martin Delacourt. Rice's theorem for generic limit sets of cellular automata. In Alonso Castillo-Ramirez, Pierre Guillon, and Kévin Perrot, editors, *27th IFIP WG 1.5 International Workshop on Cellular Automata and Discrete Complex Systems (AUTOMATA 2021)*, volume 90 of *Open Access Series in Informatics (OASIcs)*, pages 6:1–6:12, Dagstuhl, Germany, 2021. Schloss Dagstuhl – Leibniz-Zentrum für Informatik.

[7] Martin Delacourt and Benjamin Hellouin de Ménibus. Construction of μ-limit sets of two-dimensional cellular automata. In Ernst W. Mayr and Nicolas Ollinger, editors, *32nd International Symposium on Theoretical Aspects of Computer Science (STACS 2015)*, volume 30 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 262–274, Dagstuhl, Germany, 2015. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik.

[8] Saliha Djenaoui and Pierre Guillon. The generic limit set of cellular automata. *J. Cellular Automata*, 14(5-6):435–477, 2019.

[9] Pierre Guillon and Gaétan Richard. Nilpotency and limit sets of cellular automata. In *Mathematical Foundations of Computer Science 2008*, volume 5162 of *Lecture Notes in Comput. Sci.*, pages 375–386. Springer, Berlin, 2008.

[10] G. A. Hedlund. Endomorphisms and automorphisms of the shift dynamical system. *Math. Systems Theory*, 3:320–375, 1969.

[11] Benjamin Hellouin de Menibus and Mathieu Sablik. Characterization of sets of limit measures of a cellular automaton iterated on a random configuration. *Ergodic Theory Dynam. Systems*, 38(2):601–650, 2018.

[12] Jarkko Kari. The nilpotency problem of one-dimensional cellular automata. *SIAM J. Comput.*, 21(3):571–586, 1992.

[13] Jarkko Kari. Theory of cellular automata: a survey. *Theoret. Comput. Sci.*, 334(1-3):3–33, 2005.

[14] Petr Kůrka. Languages, equicontinuity and attractors in cellular automata. *Ergodic Theory Dynam. Systems*, 17(2):417–433, 1997.

[15] Petr Kůrka and Alejandro Maass. Limit sets of cellular automata associated to probability measures. *J. Statist. Phys.*, 100(5-6):1031–1047, 2000.

[16] Douglas Lind and Brian Marcus. *An introduction to symbolic dynamics and coding.* Cambridge University Press, Cambridge, 1995.

[17] Alejandro Maass. On the sofic limit sets of cellular automata. *Ergodic Theory Dynam. Systems*, 15(4):663–684, 1995.

[18] John Milnor. On the concept of attractor. *Comm. Math. Phys.*, 99(2):177–195, 1985.

[19] Ville Salo. On nilpotency and asymptotic nilpotency of cellular automata. In Enrico Formenti, editor, *Proceedings 18th international workshop on Cellular Automata and Discrete Complex Systems and 3rd international symposium "Journées Automates Cellulaires", AUTOMATA & JAC 2012, La Marana, Corsica, September 19-21, 2012*, volume 90 of *EPTCS*, pages 86–96, 2012.

[20] Ville Salo and Ilkka Törmä. Nilpotent endomorphisms of expansive group actions. *Internat. J. Algebra Comput.*, 31(3):393–452, 2021.

[21] Ilkka Törmä. A uniquely ergodic cellular automaton. *J. Comput. System Sci.*, 81(2):415–442, 2015.

[22] Ilkka Törmä. Complexity of generic limit sets of cellular automata. In *Cellular Automata and Discrete Complex Systems*, volume 12286 of *Lecture Notes in Comput. Sci.*, pages 126–138. Springer, Cham, 2020.

Optimal functions with spectral constraints in hypercubes

Alexandr Valyuzhenich*[1]

[1]Sobolev Institute of Mathematics, Novosibirsk, Russia

Let $G = (V, E)$ be a graph with the adjacency matrix $A(G)$. The set of neighbors of a vertex x is denoted by $N(x)$. Suppose λ is an eigenvalue of the matrix $A(G)$. A function $f : V \longrightarrow \mathbb{R}$ is called a λ-*eigenfunction* of G if $f \not\equiv 0$ and the equality

$$\lambda \cdot f(x) = \sum_{y \in N(x)} f(y)$$

holds for any vertex $x \in V$. The *support* of a function $f : V \longrightarrow \mathbb{R}$ is the set $S(f) = \{x \in V \mid f(x) \neq 0\}$. There is the following interesting extremal problem for eigenfunctions of graphs.

Problem 1 *Let G be a graph and let λ be an eigenvalue of G. Find the minimum cardinality of the support of a λ-eigenfunction of G.*

Problem 1 is closely related to the intersection problem of two combinatorial objects and to the problem of finding the minimum cardinality of bitrades. Often such problems can be considered as Problem 1 for the corresponding graph and some eigenvalue with some additional discrete restrictions on the functions. For example, the results of Etzion and Vardy [4] on the intersection problem of two binary perfect codes are directly related to Problem 1 for the Hamming graph and eigenvalue -1; the results of Hwang [6] on combinatorial trades and the results of Cho [2, 3] on null designs are directly related to Problem 1 for the smallest eigenvalue of the Johnson and Grassmann graphs respectively. Problem 1 was first formulated by Krotov and Vorob'ev [14] in 2014 (they considered MS-problem for the Hamming graph). During the last six years, Problem 1 has been actively studied for various families of distance-regular graphs [1, 5, 8, 9, 10, 12, 13, 15] and Cayley graphs on the symmetric group [7]. In particular, Problem 1 is completely solved for all eigenvalues of the Hamming graph [12, 13] and asymptotically solved for all eigenvalues of the Johnson graph [15]. For more information on Problem 1 we refer the reader to a recent survey [11].

The *Hamming graph* $H(n, q)$ is defined as follows. Let $\Sigma_q = \{0, 1, \ldots, q-1\}$. The vertex set of $H(n, q)$ is Σ_q^n, and two vertices are adjacent if they differ in exactly one position. The Hamming graph $H(n, q)$ has $n + 1$ distinct eigenvalues $\lambda_i(n, q) = n(q -$

*graphkiper@mail.ru

$1) - q \cdot i$, where $0 \leq i \leq n$. Denote by $U_i(n,q)$ the $\lambda_i(n,q)$-eigenspace of $H(n,q)$. The direct sum of subspaces

$$U_i(n,q) \oplus U_{i+1}(n,q) \oplus \ldots \oplus U_j(n,q)$$

for $0 \leq i \leq j \leq n$ is denoted by $U_{[i,j]}(n,q)$. We say that a function $f \in U_{[i,j]}(n,q)$, where $f \not\equiv 0$, is *optimal* in the space $U_{[i,j]}(n,q)$ if $|S(f)| \leq |S(g)|$ for any function $g \in U_{[i,j]}(n,q)$, $g \not\equiv 0$.

In this talk we focus on the following generalization of Problem 1 for the Hamming graph.

Problem 2 *Let $n \geq 1$, $q \geq 2$ and $0 \leq i \leq j \leq n$. Find the minimum cardinality of the support of functions from the space $U_{[i,j]}(n,q)$.*

Problem 2 is completely solved for all $n \geq 1$ and $q \geq 2$ in [12, 13]. Moreover, in [13] a characterization of functions that are optimal in the space $U_{[i,j]}(n,q)$ was obtained for $q \geq 3$, $i + j \leq n$ and $q \geq 5$, $i = j$, $i > \frac{n}{2}$. In this work we characterize functions that are optimal in the space $U_{[i,j]}(n,q)$ for arbitrary n and $q = 2$.

References

[1] E. A. Bespalov, On the minimum supports of some eigenfunctions in the Doob graphs, Siberian Electronic Mathematical Reports 15 (2018) 258–266.

[2] S. Cho, Minimal null designs of subspace lattice over finite fields, Linear Algebra and Its Applications 282 (1998) 199–220.

[3] S. Cho, On the support size of null designs of finite ranked posets, Combinatorica 19(4) (1999) 589–595.

[4] T. Etzion, A. Vardy, Perfect binary codes: Constructions, properties and enumeration, IEEE Transactions on Information Theory 40(3) (1994) 754–763.

[5] S. Goryainov, V. Kabanov, L. Shalaginov, A. Valyuzhenich, On eigenfunctions and maximal cliques of Paley graphs of square order, Finite Fields and Their Applications 52 (2018) 361–369.

[6] H. L. Hwang, On the structure of (v,k,t) trades, Journal of Statistical Planning and Inference 13 (1986) 179–191.

[7] V. Kabanov, E. V. Konstantinova, L. Shalaginov, A. Valyuzhenich, Minimum supports of eigenfunctions with the second largest eigenvalue of the Star graph, The Electronic Journal of Combinatorics 27(2) (2020) #P2.14.

[8] D. S. Krotov, Trades in the combinatorial configurations, XII International Seminar Discrete Mathematics and its Applications, Moscow, 20–25 June 2016, 84–96 (in Russian).

[9] D. S. Krotov, I. Yu. Mogilnykh, V. N. Potapov, To the theory of q-ary Steiner and other-type trades, Discrete Mathematics 339(3) (2016) 1150–1157

[10] E. V. Sotnikova, Minimum supports of eigenfunctions in bilinear forms graphs, Siberian Electronic Mathematical Reports 16 (2019) 501–515.

[11] E. Sotnikova, A. Valyuzhenich, Minimum supports of eigenfunctions of graphs: a survey, February 2021, arXiv:2102.11142v1.

[12] A. Valyuzhenich, Eigenfunctions and minimum 1-perfect bitrades in the Hamming graph, Discrete Mathematics 344(3) (2021) 112228.

[13] A. Valyuzhenich, K. Vorob'ev, Minimum supports of functions on the Hamming graphs with spectral constraints, Discrete Mathematics 342(5) (2019) 1351–1360.

[14] 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 9(1) (2015) 141–146, translated from Discrete Analysis and Operations Research 21(6) (2014) 3–10.

[15] K. Vorob'ev, I. Mogilnykh, A. Valyuzhenich, Minimum supports of eigenfunctions of Johnson graphs, Discrete Mathematics 341(8) (2018) 2151–2158.

Hosoya palindromicity for trees

Konstantin Vorob'ev[1], Alexandr Grebennikov[2], and Dmitry Badulin[3]

[1]Sobolev Institute of Mathematics, Russia, vorobev@math.nsc.ru
[2]St. Petersburg State University, Russia, sagresash@yandex.ru
[3]Moscow State University, Russia, badulind@bk.ru

Abstract

Let G be a connected graph, then its Hosoya polynomial is defined as

$$H(G,x) = \sum_{k=0}^{D} d_k x^k,$$

where D is the diameter of G and d_k is the number of such pairs of vertices in G, that the graph distance between them equals k. The first coefficient d_0 coincides with the number of vertices of G.

A graph G with diameter D is H-palindromic if the equality $d_k = d_{D-k}$ holds for all $k = 0, 1, \ldots, \lceil \frac{D}{2} \rceil$. The value

$$Z(G) = \sum_{k=0}^{\lfloor \frac{D}{2} \rfloor} |d_k - d_{D-k}|$$

is called a distance to H-palindromicity of a graph G.

Caporossi, Dobrynin, Gutman and Hansen showed [2] that there are only five H-palindromic trees among all trees on $3 \leq n \leq 27$ vertices. Two of them have diameter 6 and three others have 8. Based on computer experiments with trees with odd diameter they stated the following conjectures (see also [1]).

Conjecture 1. *For all trees with $n > 4$ vertices and odd diameter the distance to palindromicity is at least $\lceil \frac{n}{2} \rceil$.*

Conjecture 2. *There are no H-palindromic tress with odd diameter.*

In this work we provide a short proof for the first and, as a consequence, for the second Conjecture. Moreover, we prove the following theorem.

Theorem 1. *There is an infinite number of H-palindromic trees of diameter* 6.

This research project was started during the Summer Research Program for Undergraduates 2021 organized by the Laboratory of Combinatorial and Geometric Structures at MIPT. This program was funded by the Russian Federation Government (Grant number 075-15-2019-1926).

References

[1] Dobrynin A.A., Entringer R., Gutman I., *Wiener Index of Trees: Theory and Applications*, Acta Applicandae Mathematicae, **66** (2001), 211–249.

[2] Caporossi G., Dobrynin A.A., Gutman I., Hansen P., *Trees with palindromic Hosoya polynomials*, Graph Theory Notes of New York, **37** (1999), 10–16.

Turku Centre for Computer Science
TUCS Lecture Notes

1. **Ralph-Johan Back och Joakim von Wright**, Matematik med lite logik: Strukturerade härledningar I gymnasiematematiken
2. **Ralph-Johan Back och Joakim von Wright**, Matematik med lite logik: En kort kurs i talteori
3. **Ralph-Johan Back och Joakim von Wright**, Matematik med lite logik: Studentexamen i lång matematik, våren 2003
4. **Ralph-Johan Back ja Joakim von Wright**, Matematiikkaa logiikan avulla: Rakenteiset päättelyketjut lukiomatematiikassa
5. **Ralph-Johan Back ja Joakim von Wright**, Matematiikkaa logiikan avulla: Lyhyt lukuteorian kurssi
6. **Ralph-Johan Back ja Joakim von Wright**, Matematiikkaa logiikan avulla: Pitkän matematiikan ylioppilaskoe, kevät 2003
7. **Ralph-Johan Back och Joakim von Wright**, Matematik med lite logik: Introduktion till strukturerade härledningar
8. **Ralph-Johan Back och Joakim von Wright**, Matematik med lite logik: Logik för strukturerade härledningar
9. **Ralph-Johan Back och Joakim von Wright**, Matematik med lite logik: Strukturerade härledningar som allmänt bevisformat
10. **Ralph-Johan Back ja Joakim von Wright**, Matematiikkaa logiikan avulla: Johdatus rakenteisiin päättelyketjuihin
11. **Ralph-Johan Back ja Joakim von Wright**, Matematiikkaa logiikan avulla: Logiikka ja rakenteiset päättelyketjut
12. **Ralph-Johan Back ja Joakim von Wright**, Matematiikkaa logiikan avulla: Rakenteiset päättelyketjut yleisenä todistusmuotona
13. **Jarkko Kari (Editor)**, Proceedings of JAC 2010 – journées Automates Cellulaires
14. **Mike Stannet, Danuta Makowiec, Anna T. Lawniczak and Bruno N. Di Stefano**, Proceedings of the Satellite Workshops of UC 2011
15. **Timo Leino (Editor)**, Proceedings of the IRIS 2011 Conference
16. **Hongxiu Li (Editor)**, Studies on Inequalities in Information Society – Proceedings of the Conference, Well-Being in the Information Society. WIS 2012
17. **Vesa Halava, Juhani Karhumäki and Yuri Matiyasevich (Editors)**, RuFiDiM II, Proceedings of the Second Russian Finnish Symposium on Discrete Mathematics 2012
18. **Michael Butler, Stefan Hallerstede and Marina Waldén (Editors)**, Proceedings of the 4th Rodin User and Development Workshop
19. **Hongxiu Li and Jonna Järveläinen (Editors)**, Effective, Agile and Trusted eServices Co-Creation – Proceedings of the 15th International Conference on Electronic Commerce ICEC 2013
20. **Juhani Karhumäki, Markus Whiteland and Luca Zamboni (Editors)**, Local Proceedings of WORDS 2013
21. **Juha-Pekka Soininen, Sergey Balandin, Johan Lilius, Petri Liuha and Tullio Salmon Cinotti (Editors)**, Proceedings of the Open International M3 Semantic Interoperability Workshop
22. **Lutz M. Wegner**, Sorting – The Turku Lectures
23. **Kai K. Kimppa, Diane Whitehouse, Tiina Kuusela and Jackie Phahlamohlaka (Editors)**, Human Choice and Computers – HCC11, Work-in-Progress Proceedings
24. **Jarkko Kari, Ilkka Törmä and Michal Szabados (Eds.)**, 21st International Workshop on Cellular Automata and Discrete Complex Systems – Exploratory Papers of AUTOMATA 2015
25. **Juhani Karhumäki and Aleksi Saarela (Editors)**, Proceedings of the Finnish Mathematical Days 2016
26. **Juhani Karhumäki, Aleksi Saarela and Yuri Matiyasevichin (Eds.)**, Proceedings of the Fourth Russian Finnish Symposium on Discrete Mathematics

27. **Maria Waldén (Editor)**, Proceedings of the 29th Nordic Workshop on Programming Theory
28. **Hongxiu Li, Reima Suomi, Ágústa Pálsdóttir, Roland Trill and Hamed Ahmadinia (Editors)**, Proceedings of the Seventh International Conference on Well-Being In the Information Society: Fighting Inequalities (WIS 2018)
29. **Jouni Smed, Tomi "bgt" Suovuo, Natasha Trygg and Petter Skult**, Lecture Notes on Interactive Storytelling
30. **Mika Hirvensalo and Abuzer Yakaryilmaz (Editors)**, Proceedings of Workshop on Quantum Computing and Quantum Information
31. **Anni Hakanen, Vesa Halava, Pyry Herva, Jarkko Kari, Tero Laihonen, Ion Petre, and Aleksi Saarela (Editors)**, Proceedings on the Sixth Russian-Finnish Symposium on Discrete Mathematics

https://tucs.fi

ISBN 978-952-12-4113-0
ISSN 1797-8831