

Decimation and interleaving operations in one-sided symbolic dynamics



William C. Abram^a, Jeffrey C. Lagarias^{b,*1}, Daniel J. Slonim^{c,*}

^a *USAA, 9800 Fredericksburg Road, San Antonio, TX 78288, USA*

^b *Department of Mathematics, University of Michigan, Ann Arbor, MI 48109-1043, USA*

^c *Department of Mathematics, Purdue University, West Lafayette, IN 47906, USA*

ARTICLE INFO

Article history:

Received 31 August 2019

Received in revised form 17 August 2020

Accepted 9 November 2020

Available online 14 January 2021

MSC:

primary 37B10

secondary 11B25, 18M65, 37B40

Keywords:

Symbolic dynamics

Entropy

Infinite words

Nonsymmetric operad

ABSTRACT

This paper studies subsets of one-sided shift spaces on a finite alphabet. Such subsets arise in symbolic dynamics, in fractal constructions, and in number theory. We study a family of decimation operations, which extract subsequences of symbol sequences in infinite arithmetic progressions, and show these operations are closed under composition. We also study a family of n -ary interleaving operations, one for each $n \geq 1$. Given subsets X_0, X_1, \dots, X_{n-1} of such a shift space, the n -ary interleaving operation produces a set whose elements combine individual elements x_i , one from each X_i , by interleaving their symbol sequences in arithmetic progressions ($\bmod n$). We determine algebraic relations between decimation and interleaving operations and the shift map. We study set-theoretic n -fold closure operations $X \mapsto X^{[n]}$, which interleave decimations of X of modulus level n . A set is n -factorizable if $X = X^{[n]}$. The n -fold interleaving operations are closed under composition and are idempotent. To each X we assign the set $\mathcal{N}(X)$ of all values $n \geq 1$ for which $X = X^{[n]}$. We characterize the possible sets $\mathcal{N}(X)$ as nonempty sets of positive integers that form a distributive lattice under the divisibility partial order and are downward closed under divisibility. We show that all sets of this type occur. We introduce a class of weakly

* Corresponding authors.

E-mail addresses: abramwcc@gmail.com (W.C. Abram), lagarias@umich.edu (J.C. Lagarias), dslonim@purdue.edu (D.J. Slonim).

¹ The research of the second author was supported by NSF grants DMS-1401224 and DMS-1701576, and a 2018 Simons Fellowship in Mathematics.

shift-stable sets and show that this class is closed under all decimation, interleaving, and shift operations. We study two notions of entropy for subsets of the full one-sided shift and show that they coincide for weakly shift-stable X , but can be different in general. We give a formula for entropy of interleavings of weakly shift-stable sets in terms of individual entropies.

© 2021 The Authors. Published by Elsevier Inc. This is an open access article under the CC BY license (<http://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Let \mathcal{A} be a finite alphabet of symbols, and suppose $|\mathcal{A}| \geq 2$. A basic object in one-sided symbolic dynamics is the full one-sided shift space $\mathcal{A}^{\mathbb{N}}$, which is the space of all one-sided infinite strings of symbols drawn from \mathcal{A} . Here $\mathbb{N} = \{0, 1, 2, \dots\}$ denotes the natural numbers, and $\mathbb{N}^+ = \mathbb{N} \setminus \{0\}$ denotes the positive integers. We view $\mathcal{A}^{\mathbb{N}} = \prod_{j \in \mathbb{N}} \mathcal{A}$ as a compact topological space carrying the product topology, with each copy of \mathcal{A} carrying the discrete topology; we call this topology of $\mathcal{A}^{\mathbb{N}}$ the *symbol topology*. The dynamics in one-sided symbolic dynamics is the action of the (*one-sided*) *shift map* $S : \mathcal{A}^{\mathbb{N}} \rightarrow \mathcal{A}^{\mathbb{N}}$ on individual symbol sequences $\mathbf{x} = a_0 a_1 a_2 a_3 \dots$ by

$$S(\mathbf{x}) := a_1 a_2 a_3 a_4 \dots \quad (1.1)$$

In contrast, two-sided symbolic dynamics (treated in Lind and Marcus [33]) uses the two-sided shift operator $S : \mathcal{A}^{\mathbb{Z}} \rightarrow \mathcal{A}^{\mathbb{Z}}$ with $S((a_i)_{i \in \mathbb{Z}}) = (b_i)_{i \in \mathbb{Z}}$ with $b_i = a_{i+1}$. It focuses on sets $X \subseteq \mathcal{A}^{\mathbb{Z}}$ that are invariant under the (two-sided) shift operator: $SX = X$. Such sets arise as discretizations of continuous dynamical systems such as geodesic flow, and led to the original formulation of symbolic dynamics by Morse and Hedlund [39]. In one-sided symbolic dynamics on subsets of $\mathcal{A}^{\mathbb{N}}$ the spaces X can encode initial conditions. Initial conditions can break shift-invariance, so it is natural to consider spaces that are stable under the shift: $SX \subseteq X$.

This paper studies the action of decimation and interleaving operations acting on sets X in the framework of symbolic dynamics and coding theory. Decimation operations are important in digital signal processing and coding theory, and interleaving operations form a kind of inverse operation to them, see (1.4).

- (1) At the level of individual symbol sequences, the *i*th decimation operation at level n , for $i \geq 0$ and $n \geq 1$, denoted $\psi_{i,n} : \mathcal{A}^{\mathbb{N}} \rightarrow \mathcal{A}^{\mathbb{N}}$, for an individual symbol sequence $\mathbf{x} = a_0 a_1 a_2 a_3 \dots$ is

$$\psi_{i,n}(\mathbf{x}) := a_i a_{i+n} a_{i+2n} a_{i+3n} \dots \quad (1.2)$$

This operation extracts symbol subsequences having indices in an arithmetic progression given by $i \pmod n$, starting at initial index i .

(2) The n -fold interleaving operation $\circledast_n : \mathcal{A}^{\mathbb{N}} \times \mathcal{A}^{\mathbb{N}} \times \cdots \times \mathcal{A}^{\mathbb{N}} \rightarrow \mathcal{A}^{\mathbb{N}}$ is an n -ary operation whose action on n individual symbol sequences $\mathbf{x}_i = a_{i,0}a_{i,1}a_{i,2}\cdots$ for $0 \leq i \leq n-1$ is defined by

$$(\mathbf{x}_0, \mathbf{x}_1, \dots, \mathbf{x}_{n-1}) \mapsto \mathbf{y} := (\circledast_n)_{i=0}^{n-1} \mathbf{x}_i = \mathbf{x}_0 \circledast \mathbf{x}_1 \circledast \cdots \circledast \mathbf{x}_{n-1} = b_0 b_1 b_2 \cdots \quad (1.3)$$

in which the output sequence $\mathbf{y} := b_0 b_1 b_2 \dots$ interleaves the symbols in arithmetic progressions of symbol indices $(\bmod n)$, so that

$$b_{i+jn} = a_{i,j} \quad \text{for } j \geq 0, 0 \leq i \leq n-1.$$

That is, the output \mathbf{y} has in its symbol positions $i \pmod n$ the symbols of \mathbf{x}_i given in order.

Decimation and interleaving operations defined pointwise extend by set union to define set-valued operations acting on arbitrary subsets X of $\mathcal{A}^{\mathbb{N}}$ (resp. of $(\mathcal{A}^{\mathbb{N}})^n$). For examples, see Sections 2.1 and 2.2.

All individual symbol sequences \mathbf{x} are constructible as n -fold interleavings of suitable decimations:

$$\mathbf{x} = (\circledast_n)_{i=0}^{n-1} \psi_{i,n}(\mathbf{x}) \quad \text{for } \mathbf{x} \in \mathcal{A}^{\mathbb{N}}, \quad (1.4)$$

see Section 4.1.

1.1. Summary

This paper treats two topics.

1.1.1. The first topic of this paper is the study of algebraic properties of decimation and interleaving operations under composition. The set of all decimation operations is closed under composition, and the decimation and shift actions are compatible in a sense we describe in Section 3. Decimation operations are closed under composition.

We define the n -fold interleaving closure $X^{[n]}$ of a set X in Section 2 as $X^{[n]} = (\circledast_n)_{i=0}^{n-1} \psi_{i,n}(X)$, an operation that combines both decimations and interleavings. We show the operation sending X to $X^{[n]}$ is a set-valued closure operation in the Moore sense, in particular $X \subseteq X^{[n]}$. A main result is that interleaving closure operations under composition satisfy

$$(X^{[m]})^{[n]} = (X^{[n]})^{[m]} = X^{[\text{lcm}(m,n)]}, \quad (1.5)$$

where $\text{lcm}(m, n)$ denotes the least common multiple of m and n . Thus these operations are closed under composition, commute under composition, and are idempotent.

We show X is closed under n -fold interleaving closure, meaning $X = X^{[n]}$, if and only if X factorizes as $X = (\circledast_n)_{j=0}^{n-1} X_j$ under the n -fold interleaving operation for some X_j . We study the allowable sets $M \subseteq \mathbb{N}^+$ for which there exists some set X that has $X = X^{[n]}$ if and only if $n \in M$. That is, letting $\mathcal{N}(X) = \{n : X = X^{[n]}\}$, we classify the sets $M \subseteq \mathbb{N}^+$ such that $M = \mathcal{N}(X)$ for some $X \in \mathcal{A}^{\mathbb{N}}$. We show that if finite, the set $\mathcal{N}(X)$ consists of the set of all divisors of an integer n_0 , and all such n_0 may occur. A new phenomenon is the existence of *infinitely factorizable* X , which necessarily have $X = X^{[n]}$ for all n in an infinite distributive sublattice of \mathbb{N}^+ under the divisibility partial order, downward closed under divisibility. We show all such infinite sublattices may occur for non-closed X , but if X is closed, we show the only allowed infinite sublattice is \mathbb{N}^+ .

There is an additional algebraic structure consisting of the collection of all operations obtained from combining interleaving operations of different arities under composition. These form a nonsymmetric operad in the category of sets, and we term it the *interleaving nonsymmetric operad*. We give a series of universal shuffle identities under composition satisfied by this operad. We discuss the operad formalism in Section 2.7 and in Appendix A.

1.1.2. The second topic of this paper is the study of symbolic dynamics aspects of decimation and interleaving operations. The shift operation acts compatibly with decimations and with n -fold interleaving, and we give commutation identities describing its action. The class of shift-invariant sets (those with $SX = X$) and the class of shift-stable sets (those with $SX \subseteq X$) are not preserved under interleaving. We introduce an enlarged class of sets better adapted to these operations.

A set $X \subseteq \mathcal{A}^{\mathbb{N}}$ is said to be *weakly shift-stable* if there are integers $k > j \geq 0$ such that $S^k X \subseteq S^j X$. The set X need not be a closed set in the symbol topology. We show the class of all weakly shift-stable sets, denoted $\mathcal{W}(\mathcal{A})$, is closed under the shift and under all decimation and interleaving operations, as is the subclass $\overline{\mathcal{W}}(\mathcal{A})$ of all closed sets in $\mathcal{W}(\mathcal{A})$.

The complexity of a set X can be measured using various notions of the entropy of X , which provide invariants that distinguish dynamical systems. The paper [2] studied two concepts of entropy for X , the *topological entropy* $H_{\text{top}}(X)$ and *path topological entropy* $H_p(X)$, which we term here *prefix topological entropy*. For general X one has $H_p(X) \leq H_{\text{top}}(X)$, and strict inequality may occur. We obtain an inequality relating the prefix topological entropy of an n -fold interleaving $X = (\circledast_n)_{i=0}^{n-1} X_i$ to that of its factors X_i :

$$H_p(X) \leq \frac{1}{n} \sum_{i=0}^{n-1} H_p(X_i), \quad (1.6)$$

and strict inequality may occur. A main result is that the class of weakly shift-stable sets $\mathcal{W}(\mathcal{A})$ has good properties for both entropies; the two entropies are equal and equality

holds in the interleaving inequality (1.6). In consequence, for weakly shift-stable sets $X = (\circledast_n)_{i=0}^{n-1} X_i$ we obtain a formula for topological entropy under interleaving:

$$H_{\text{top}}(X) = \frac{1}{n} \sum_{i=0}^{n-1} H_{\text{top}}(X_i).$$

1.1.3. Most results in this paper apply to general sets X , but for symbolic dynamics applications we are most interested in closed sets X in the product topology on $\mathcal{A}^{\mathbb{N}}$. These satisfy:

- (1) If X is a closed set, then all decimations $\psi_{i,n}(X)$ are closed sets for $i \geq 0$ and $n \geq 1$.
- (2) If X_0, X_1, \dots, X_{n-1} are closed sets, then their n -fold interleaving $X = (\circledast_n)_{i=0}^{n-1} X_i$ is a closed set.
- (3) Conversely, if X is a closed set and has an n -fold interleaving factorization $X = (\circledast_n)_{i=0}^{n-1} X_i$, then each X_i is a closed set.

The decimation, interleaving, and shift operations all commute with the topological closure operation $X \mapsto \overline{X}$. In consequence all n -fold interleaving closure operations commute with topological closure.

Detailed statements of results are made in Section 2. The main results concerning properties of n -fold interleaving closure operations of a set X are Theorems 2.10, 2.12 and 2.13. The main results concerning weakly shift-stable sets X are Theorems 2.15 and 2.20.

1.2. Background

This study was motivated by work on path sets initiated in [2]. Path sets are a class of closed sets in $\mathcal{A}^{\mathbb{N}}$ that forms a generalization of shifts of finite type and of sofic shifts in symbolic dynamics, and which also include sets not invariant under the shift map. Path sets are described by finite automata, and have an automata-theoretic characterization as the closed sets in $\mathcal{A}^{\mathbb{N}}$ that are the set of all infinite paths in some deterministic Büchi automaton. This class includes interesting sets arising in fractal constructions and in study of radix expansions in number theory (see [3], [4]) arising from a problem of Erdős ([20], [31]). The paper [2] considered decimation operations on path sets and showed that decimations of path sets are also path sets. The p -adic integers with the p -adic topology form a shift space with p -symbols, and interleaving operations on path sets arose in this context in [1].

The authors recently studied the action of interleaving operations on path sets, in [5]. Interleaving operations already lead to the breaking of shift-invariance even if all sets X_i used in the interleaving are shift-invariant. The paper [5] shows that the class $\mathcal{C}(\mathcal{A})$ of all path sets on a finite alphabet \mathcal{A} is closed under all interleaving operations.

This paper obtains results valid for general sets $X \subseteq \mathcal{A}^{\mathbb{N}}$, which provide perspective on results on path sets proved in [5]. The concept of weakly shift-stable closed sets $\overline{\mathcal{W}}(\mathcal{A})$ supplies a good generalization of the class $\mathcal{C}(\mathcal{A})$ of path sets to more general closed sets. The paper [5] shows that all path sets are weakly shift-invariant, which implies they are weakly shift-stable. In consequence, the entropy equalities of the present paper under weak shift-stability apply to interleaving of path sets. The present paper includes examples showing that various finiteness results given in [5] for path sets are not valid for general closed sets $X \subseteq \mathcal{A}^{\mathbb{N}}$; see Remark 7.3.

1.3. Related work

Decimation operations play an important role in sampling and interpolation operations in digital signal processing (“downsampling”), and in multi-scale analysis and wavelets (e.g., [16], [29]). Interleaving constructions have been used in coding theory as a method for improving the burst error correction capability of a code (cf. [48, Section 7.5]). They are also considered in formal language theory; see Krieger et al. ([30]). The analogue of n -fold interleaving for finite codes is referred to by coding theorists as *block interleaving of depth n* . Decimation and interleaving operators together have been considered both in cryptography and cryptanalysis (cf. Rueppel [45] and Cardell et al. [10]). Since methods of encoding and decoding can be viewed as dynamical processes, it is of interest to view these operations in a dynamical context.

1.3.1. There has been prior work on interleaving operations in the automata theory literature, typically for finite words. In 1974 Eilenberg [19, Chap. II.3, page 20] introduced a notion of *internal shuffle product* $A \coprod B$ of two recognizable sets (= regular languages) which corresponds to 2-fold interleaving. A more general notion is *alphabetic shuffle*. The shuffle product has been characterized in the context of finite automata by Duchamp et al. [18, Sect. 4]. In this paper we are considering such operations on infinite words, which differ in nature from the finite word case. For infinite words viewed in an automata-theoretic context, see Perrin and Pin [40]. We are not aware of prior work studying the algebraic structure of interleaving operations in this context.

1.3.2. Regarding dynamics, one-sided shift-stable sets have their dynamics partially classified by C^* -algebra invariants. The work of Cuntz and Krieger [15] and Cuntz [14] was seminal in attaching such invariants to topological Markov chains (= two-sided shifts of finite type). Carlsen ([11], [12]) attached C^* -algebras to one-sided subshifts and studied their properties. Shift-stable sets are studied in the context of partial isometry actions and C^* algebras attached to them by Dokuchaev and Exel [17]. See Exel [22] for related background. One may ask whether there are generalizations of these constructions to the class of weakly shift-stable sets introduced in this paper.

1.3.3. In the ongoing development of operad theory and n -categories, interleaving operations have recently played a role at a categorical level, see Leinster [32] and Cottrell

[13]. General references for operads are Markl, Shnider and Stasheff [35], and more recently Loday and Vallette [34] and Bremner and Dotsenko [9] for algebraic operads.

Acknowledgments. We thank the reviewers for helpful comments and references. We thank I. Kriz for a discussion on operads. Some work of W. Abram and D. Slonim was facilitated by the Hillsdale College LAUREATES program, done by D. Slonim under the supervision of W. Abram. Work of J. Lagarias was partially supported by NSF grants DMS-1401224 and DMS-1701576, and by a Simons Fellowship in Mathematics Award 555520 in 2018.

2. Results

We give formal definitions with examples, and then state results.

2.1. Decimation operations

Definition 2.1 (*Decimation operations*). Let \mathcal{A} be a finite alphabet of symbols.

(1) For individual sequences $\mathbf{x} \in \mathcal{A}^{\mathbb{N}}$ the *i-th decimation operation at level n*, denoted $\psi_{i,n} : \mathcal{A}^{\mathbb{N}} \rightarrow \mathcal{A}^{\mathbb{N}}$, for $i \geq 0$ is defined for $\mathbf{x} = a_0a_1a_2a_3\cdots$ by

$$\psi_{i,n}(\mathbf{x}) := a_i a_{i+n} a_{i+2n} a_{i+3n} \cdots.$$

This operation extracts symbol subsequences having indices in an arithmetic progression given by $i \pmod n$, which starts at initial index i . The *principal n-decimations* are those $\psi_{i,n}$ with $0 \leq i \leq n-1$.

(2) For sets $X \subseteq \mathcal{A}^{\mathbb{N}}$ the *i-th decimation at level n*, denoted $\psi_{i,n}(X)$, is the set union

$$\psi_{i,n}(X) := \{\psi_{i,n}(\mathbf{x}) : \mathbf{x} \in X\}. \quad (2.1)$$

Example 2.2. For the alphabet $\mathcal{A} = \{0, 1, 2, 3\}$ consider the sets²

$$X = \{\mathbf{x}_1 = (01)^\infty, \mathbf{x}_2 = (10)^\infty\}, \text{ and } Y = \{\mathbf{y}_1 = (323)^\infty, \mathbf{y}_2 = (332)^\infty\},$$

containing two periodic infinite words of period 2 and two periodic infinite words of period 3, respectively.

The principal 2-decimations of the elements of X are

$$\psi_{0,2}((01)^\infty) = 0^\infty, \psi_{1,2}((01)^\infty) = 1^\infty, \text{ and } \psi_{0,2}((10)^\infty) = 1^\infty, \psi_{1,2}((10)^\infty) = 0^\infty.$$

Thus $\psi_{0,2}(X) := \{0^\infty, 1^\infty\}$ and $\psi_{1,2}(X) = \{1^\infty, 0^\infty\} = \psi_{0,2}(X)$.

² Here $\mathbf{x}_1 = (01)^\infty = 010101\cdots$

The principal 2-decimations of the elements of Y are

$$\begin{aligned}\psi_{0,2}((323)^\infty) &= (332)^\infty, \psi_{1,2}((323)^\infty) = (233)^\infty, \quad \text{and} \\ \psi_{0,2}((332)^\infty) &= (323)^\infty, \psi_{1,2}((332)^\infty) = (332)^\infty.\end{aligned}$$

We obtain $\psi_{0,2}(Y) := \{(332)^\infty, (323)^\infty\} = Y$ and $\psi_{1,2}(Y) = \{(233)^\infty, (332)^\infty\} \neq Y$.

In Section 3 we show:

(1) The set of all decimation operations are closed under composition. For $X \subseteq \mathcal{A}^{\mathbb{N}}$,

$$\psi_{j,m} \circ \psi_{i,n}(X) = \psi_{i+jn,mn}(X).$$

This identity on subscripts matches an action of the $(ax + b)$ -group on \mathbb{Z} .

(2) The shift action is compatible with the decimation action: For $X \subseteq \mathcal{A}^{\mathbb{N}}$,

$$\psi_{i,n}(SX) = \psi_{i+1,n}(X)$$

and

$$S\psi_{i,n}(X) = \psi_{i,n}(S^n X).$$

2.2. Interleaving operations

Interleaving operations comprise an infinite collection of n -ary operations ($n \geq 1$), defined for arbitrary subsets X of the shift space $\mathcal{A}^{\mathbb{N}}$.

Definition 2.3 (*Interleaving operations*). Let \mathcal{A} be a finite alphabet of symbols.

(1) For individual sequences $\mathbf{x}_i = a_{i,0}a_{i,1}a_{i,2}\cdots \in \mathcal{A}^{\mathbb{N}}$, ($0 \leq i \leq n-1$), the n -fold interleaving operation $\circledast_n : \mathcal{A}^{\mathbb{N}} \times \mathcal{A}^{\mathbb{N}} \times \cdots \times \mathcal{A}^{\mathbb{N}} \rightarrow \mathcal{A}^{\mathbb{N}}$, denoted either $(\circledast_n)_{i=0}^{n-1} \mathbf{x}_i$ or $\mathbf{x}_0 \circledast \mathbf{x}_1 \circledast \cdots \circledast \mathbf{x}_{n-1}$, combines these sequences by

$$\begin{aligned}(\mathbf{x}_0, \mathbf{x}_1, \dots, \mathbf{x}_{n-1}) &\mapsto \mathbf{x}_0 \circledast \mathbf{x}_1 \circledast \cdots \circledast \mathbf{x}_n = \mathbf{y} \\ &:= (a_{0,0} a_{1,0} \cdots a_{n-1,0}) \circ (a_{0,1} a_{1,1} \cdots a_{n-1,1}) \circ (a_{0,2} \cdots,\end{aligned}$$

where \circ denotes concatenation of sequences. That is, $\mathbf{y} = b_0 b_1 b_2 \cdots$ with

$$b_{i+jn} = a_{i,j} \quad \text{for } 0 \leq i \leq n-1, \text{ and } j \geq 0,$$

so that the symbols of \mathbf{y} in symbol positions $i \pmod{n}$ are the symbols of \mathbf{x}_i , ($0 \leq i \leq n-1$).

(2) For sets $X_i \subseteq \mathcal{A}^{\mathbb{N}}$, $(0 \leq i \leq n-1)$, their n -fold interleaving, denoted $(\circledast_n)_{i=0}^{n-1} X_i$ or $X_0 \circledast X_1 \circledast X_2 \circledast \cdots \circledast X_{n-1}$, is defined by the set union:

$$(\circledast_n)_{i=0}^{n-1} X_i = \{\mathbf{x}_0 \circledast \mathbf{x}_1 \circledast \cdots \circledast \mathbf{x}_{n-1} : \mathbf{x}_i \in X_i \text{ for all } 0 \leq i \leq n-1\}.$$

A set $X = (\circledast_n)_{i=0}^{n-1} X_i$ is said to have an n -fold interleaving factorization. The sets X_i are called n -fold interleaving factors of X , or just interleaving factors. One can express n -fold interleavings in terms of principal decimations of level n as: $(\circledast_n)_{i=0}^{n-1} X_i = \{\mathbf{x} \in \mathcal{A}^{\mathbb{N}} : \psi_{i,n}(\mathbf{x}) \in X_i \text{ for all } 0 \leq i \leq n-1\}$; see Proposition 4.1.

Example 2.4. Continuing Example 2.2, the 2-fold interleaving of X with itself is

$$\begin{aligned} X \circledast X &= \{\mathbf{x}_1 \circledast \mathbf{x}_1, \mathbf{x}_1 \circledast \mathbf{x}_2, \mathbf{x}_2 \circledast \mathbf{x}_1, \mathbf{x}_2 \circledast \mathbf{x}_2\} \\ &= \{(0011)^\infty, (0110)^\infty, (1001)^\infty, (1100)^\infty\}. \end{aligned}$$

It contains four periodic words of period 4.

The 2-fold interleaving of Y with itself is

$$\begin{aligned} Y \circledast Y &= \{\mathbf{y}_1 \circledast \mathbf{y}_1, \mathbf{y}_1 \circledast \mathbf{y}_2, \mathbf{y}_2 \circledast \mathbf{y}_1, \mathbf{y}_2 \circledast \mathbf{y}_2\} \\ &= \{(332233)^\infty, (332332)^\infty, (333223)^\infty, (333322)^\infty\}. \end{aligned}$$

It contains four periodic words of period 6. The 2-fold interleavings of X and Y are

$$\begin{aligned} X \circledast Y &:= \{\mathbf{x}_1 \circledast \mathbf{y}_1, \mathbf{x}_1 \circledast \mathbf{y}_2, \mathbf{x}_2 \circledast \mathbf{y}_1, \mathbf{x}_2 \circledast \mathbf{y}_2\} \\ &= \{(031203130213)^\infty, (031302130312)^\infty, (130213031203)^\infty, (130312031302)^\infty\}. \\ Y \circledast X &:= \{\mathbf{y}_1 \circledast \mathbf{x}_1, \mathbf{y}_1 \circledast \mathbf{x}_2, \mathbf{y}_2 \circledast \mathbf{x}_1, \mathbf{y}_2 \circledast \mathbf{x}_2\} \\ &= \{(302130312031)^\infty, (312031302130)^\infty, (303120313021)^\infty, (313021303120)^\infty\}, \end{aligned}$$

Each of them contains four periodic words of period 12. We have $X \circledast Y \neq Y \circledast X$.

A basic relation between interleaving and decimation is an identity, valid at the pointwise level, stating that ordered n -fold decimations post-composed with n -fold interleaving give the identity map:

$$(\circledast_n)_{i=0}^{n-1} \psi_{i,n}(\mathbf{x}) = \mathbf{x} \quad \text{for } \mathbf{x} \in \mathcal{A}^{\mathbb{N}}. \quad (2.2)$$

For this reason we call the decimations $\psi_{i,n}$ for $0 \leq i \leq n-1$, the *principal decimations*. The remaining decimations $i \geq n$ may be obtained by applying the one-sided shift map to these decimation sets; see Proposition 3.2.

2.3. Interleaving closure operations

The interleaving operations together with principal decimations define a family of set-theoretic closure operations on general subsets $X \subseteq \mathcal{A}^{\mathbb{N}}$. These closure operations are a main focus of this paper.

Definition 2.5. The n -fold interleaving closure operation $X \mapsto X^{[n]}$ is defined for each $X \subseteq \mathcal{A}^{\mathbb{N}}$ by

$$X^{[n]} := (\circledast_n)_{i=0}^{n-1} \psi_{i,n}(X). \quad (2.3)$$

Example 2.6. For $X = \{(10)^\infty, (01)^\infty\}$, the 2-fold interleaving closure $X^{[2]} := \psi_{0,2}(X) \circledast \psi_{1,2}(X)$ is

$$X^{[2]} = \{0^\infty, (01)^\infty, (10)^\infty, 1^\infty\}.$$

We have $X \subsetneq X^{[2]}$.

Example 2.7 (Interleaving and n -fold interleaving closure). Let $\mathcal{A} = \{0, 1\}$ and let $X_0 \subset \mathcal{A}^{\mathbb{N}}$ be the *one-sided Fibonacci shift* consisting of all words that do not contain the pattern 11 in two consecutive digits. Let $X_1 = \mathcal{A}^{\mathbb{N}}$ be the full shift. Then:

- (1) $X_0 \circledast X_1 \subset \mathcal{A}^{\mathbb{N}}$ consists of all words that do not contain a 1 in digits i and $i + 2$ for any i even. That is, there can be no 1's in consecutive even digits, but there are no other restrictions on the word. Here X_0 and X_1 are each invariant under the shift operator, i.e., $S(X_i) = X_i$, but $X_0 \circledast X_1$ is not shift-invariant.
- (2) Interleaving any number of copies of X_1 gives X_1 . That is, $(\circledast_n)_{i=0}^{n-1} X_1 = X_1$ for $n \geq 1$.
- (3) The n -fold interleaving closure of X_0 is X_1 for all $n \geq 2$, that is, $X_0^{[n]} = X_1 = \mathcal{A}^{\mathbb{N}}$. This holds because $\psi_{i,n}(X_0) = X_1$ for all $i \geq 0$ when $n \geq 2$.
- (4) Likewise, $X_1^{[n]} = X_1$ for $n \geq 1$. So X_1 has n -fold interleavings for all $n \geq 1$.

In Section 4.1 we show the existence of an n -fold interleaving factorization of a set X corresponds to its invariance under n -fold interleaving closure, and in that case its interleaving factors are its principal decimations.

Theorem 2.8 (Decimations and interleaving factorizations).

- (1) A subset X of $\mathcal{A}^{\mathbb{N}}$ has an n -fold interleaving factorization $X = X_0 \circledast X_1 \circledast \cdots \circledast X_{n-1}$ if and only if $X = X^{[n]}$.
- (2) If $X = X_0 \circledast X_1 \circledast \cdots \circledast X_{n-1}$ has an n -fold interleaving factorization, then its ordered set of n -fold interleaving factors is unique, given by its principal decimations

$$X_i = \psi_{i,n}(X) \quad \text{for } 0 \leq i \leq n - 1.$$

Regarding (2), there typically are many sets Y such that $\psi_{i,n}(Y) = \psi_{i,n}(X)$ for $0 \leq i \leq n-1$, and we show X contains every such set Y in Theorem 4.2.

In Section 4.2 we justify the name n -fold interleaving closure by showing that $X \mapsto X^{[n]}$ is a set-theoretic closure operation, as formalized in Grätzer [26, Chap. I, Sect. 3.12, Defn. 26], and $X^{[n]}$ is characterized as the maximal set Z having the property that $\psi_{i,n}(Z) = \psi_{i,n}(X)$ for $0 \leq i \leq n-1$.

In Section 4.3 we establish universal algebraic identities relating certain compositions of n -fold interleavings for different n .

Proposition 2.9 (*Interleaving shuffle identities*). *For each $m, n \geq 2$ and arbitrary sets $\{X_i : 0 \leq i \leq mn-1\}$ contained in the one-sided shift $\mathcal{A}^{\mathbb{N}}$, one has the identity of sets*

$$(\circledast_n)_{i=0}^{n-1} ((\circledast_m)_{j=0}^{m-1} X_{i+jn}) = (\circledast_{mn})_{k=0}^{mn-1} X_k. \quad (2.4)$$

These identities are termed *shuffle identities* because the n -fold interleaving operation acts like a shuffling of n decks of cards together, taking the top cards in a particular order from each of the n decks, where the cards correspond to positions of symbols in the expansion.

In Section 4.4 we establish a main result determining the action of composition of interleaving closure operations. The shuffle identities play a crucial role in proving this result.

Theorem 2.10 (*Composition of interleaving closures*). *For all $m, n \geq 1$, and all $X \subseteq \mathcal{A}^{\mathbb{N}}$,*

$$(X^{[m]})^{[n]} = (X^{[n]})^{[m]} = X^{[\text{lcm}(m, n)]}, \quad (2.5)$$

where $\text{lcm}(m, n)$ denotes the least common multiple of m and n .

In Section 4.5 we show interleaving commutes with intersection:

$$\bigcap_{j=0}^{m-1} ((\circledast_n)_{i=0}^{n-1} X_{jn+i}) = (\circledast_n)_{i=0}^{n-1} \left(\bigcap_{j=0}^{m-1} X_{jn+i} \right).$$

In Section 4.6 we determine the action of the shift map on n -fold interleavings and interleaving closures. In particular we show that

$$SX^{[n]} = (SX)^{[n]}.$$

In Section 4.7 we show that the topological closure operation commutes with both decimation and interleaving operations. In particular it commutes under composition with n -fold interleaving closure:

$$\overline{X}^{[n]} = \overline{X^{[n]}}.$$

Thus if X is a closed then its n -fold interleaving closure $X^{[n]}$ is closed.

2.4. Structure of interleaving factorizations

We study the possible structure of the set of all interleaving factorizations of a fixed set $X \subseteq \mathcal{A}^{\mathbb{N}}$.

Definition 2.11. Let X in $\mathcal{A}^{\mathbb{N}}$ be a fixed set, with \mathcal{A} a finite alphabet.

(1) The *interleaving closure set* $\mathcal{N}(X) \subseteq \mathbb{N}_+$ of X is the set of integers

$$\mathcal{N}(X) := \{n : n \geq 1 \text{ and } X = X^{[n]}\}.$$

(2) The *interleaving factor set* $\mathfrak{F}(X)$ consists of all n -ary interleaving factors, $X_{i,n}$, for all $n \in \mathcal{N}(X)$, i.e.

$$\mathfrak{F}(X) = \{\psi_{i,n}(X) : n \in \mathcal{N}(X), 0 \leq i \leq n-1\}$$

(3) The (*full*) *decimation set* $\mathfrak{D}(X)$ consists of all decimations of X .

$$\mathfrak{D}(X) = \{\psi_{i,n}(X) : i \geq 0, n \geq 1\}.$$

The *principal decimation set* $\mathfrak{D}_{\text{prin}}(X)$ consists of all principal decimations

$$\mathfrak{D}_{\text{prin}}(X) := \{\psi_{i,n}(X) : n \geq 1, 0 \leq i \leq n-1\}.$$

The interleaving factor set is a subset of the set of all principal decimations: $\mathfrak{F}(X) \subseteq \mathfrak{D}_{\text{prin}}(X)$. We always have $X \in \mathfrak{F}(X)$ and $1 \in \mathcal{N}(X)$.

An important feature of factorizations is that some X are *infinitely factorizable* in the sense that they have n -fold interleaving factorizations for infinitely many n , i.e. $\mathcal{N}(X)$ is infinite. The full one-sided shift $X = \mathcal{A}^{\mathbb{N}}$ on the alphabet \mathcal{A} is an example; it has n -fold factorizations for all $n \geq 1$, and $\mathcal{N}(\mathcal{A}^{\mathbb{N}}) = \mathbb{N}^+$, while its interleaving factor set $\mathfrak{F}(\mathcal{A}^{\mathbb{N}}) = \{\mathcal{A}^{\mathbb{N}}\}$ contains one element. We term all the remaining ones *finitely factorizable*. There exist closed sets X having infinite $\mathcal{N}(X)$ and having an infinite interleaving factor set $\mathfrak{F}(X)$, see Example 6.5.

Theorem 2.12 (Structure of interleaving closure sets). Let $\mathcal{N}(X) = \{n \geq 1 : X = X^{[n]}\}$. Then $\mathcal{N}(X)$ is nonempty and has the following properties.

(1) If $n \in \mathcal{N}(X)$ and d divides n , then $d \in \mathcal{N}(X)$.

(2) If $m, n \in \mathcal{N}(X)$ then their least common multiple $\text{lcm}(m, n) \in \mathcal{N}(X)$.

Conversely, if a subset $N \subseteq \mathbb{N}^+$ is nonempty and has properties (1) and (2), then there exists $X \subseteq \mathcal{A}^{\mathbb{N}}$ with $N = \mathcal{N}(X)$.

This result is proved separately in the direct and converse directions as Theorem 5.1 and Theorem 5.3, respectively. A nonempty structure N having properties (1), (2) is abstractly characterized as any nonempty subset of \mathbb{N}^+ that is a sublattice under the divisibility partial order, which is also downward closed under divisibility, see 5.1 (3). The notion of lattice here is that of G. Birkhoff, see Grätzer [26].

In Section 5.3 we also treat *self-interleaving factorizations*, which are interleaving factorizations in which all factors are identical. For a general set X we define the *self-interleaving closure set*

$$\mathcal{N}_{\text{self}}(X) := \{n \in \mathbb{N} : X = (\otimes_n)_{i=0}^{n-1} Y \text{ for some } Y \subseteq \mathcal{A}^{\mathbb{N}}\}$$

as the set of n such that X has an n -fold self-interleaving factorization. We show that the sets $\mathcal{N}_{\text{self}}(X)$ may have exactly the same allowed forms as the sets $\mathcal{N}(X)$ in Theorem 2.12; however for individual X the set of values $\mathcal{N}_{\text{self}}(X)$ can be strictly smaller than $\mathcal{N}(X)$.

In Section 6 we study infinitely factorizable sets X in the special case that X is a closed set.

Theorem 2.13 (*Classification of infinitely factorizable closed X*). *For a closed set $X \subseteq \mathcal{A}^{\mathbb{N}}$, where \mathcal{A} is a finite alphabet, the following properties are equivalent.*

- (i) X is infinitely factorizable; i.e., $\mathcal{N}(X)$ is an infinite set.
- (ii) X has an n -fold interleaving factorization for all $n \geq 1$; i.e. $\mathcal{N}(X) = \mathbb{N}^+$.
- (iii) For each $k \geq 0$ there are nonempty subsets $\mathcal{A}_k \subseteq \mathcal{A}$ such that $X = \prod_{k=0}^{\infty} \mathcal{A}_k$ is a countable product of finite sets with the product topology.

In view of Theorem 2.12, the assumption that X is closed is necessary for these three equivalences to hold. The important restriction for closed sets X is that if they are infinitely factorizable then $\mathcal{N}(X) = \mathbb{N}^+$.

In Section 7 we study an iterated interleaving factorization process for a closed set X . If X is infinitely factorizable, we “freeze” it. If it is finitely factorizable, we decompose it to its maximal factorization, and then repeat the process on each of these factors. We show by example that this factorization process can go to infinite depth.

2.5. Shift-stability and weak shift-stability

We consider several classes of sets X having different transformation properties under the shift action.

Definition 2.14 (*Shift-invariance, shift-stability, weak shift-stability*).

- (1) A set $X \subseteq \mathcal{A}^{\mathbb{N}}$ is *shift-invariant* if $SX = X$.
- (2) A set X is *shift-stable* if $SX \subseteq X$.
- (3) A set X is *weakly shift-invariant* if there are $k > j \geq 0$ such that $S^k X = S^j X$.
- (4) A set X is *weakly shift-stable* if there are $k > j \geq 0$ such that $S^k X \subseteq S^j X$.

These definitions do not require the set X to be closed in the symbol topology.

In Section 8 we show consequences of these properties. We show that for shift-invariant sets, all interleaving factorizations are self-interleaving factorizations; that is, if X is shift-invariant, then $\mathcal{N}(X) = \mathcal{N}_{\text{self}}(X)$. We show that closed shift-stable sets have a forbidden blocks characterization paralleling the two-sided shift case. Example 8.5 constructs a closed set X giving an infinite, strictly descending chain of sets under iteration of the shift map.

An important property introduced here is weak shift-stability. The usefulness of this property is that the class $\mathcal{W}(\mathcal{A})$ of all weakly shift-stable sets on a finite alphabet \mathcal{A} is closed under all decimation, interleaving and shift operations. This is not the case for properties (1)-(3) above.

Theorem 2.15. *Let \mathcal{A} be finite alphabet and let $X \subseteq \mathcal{A}^{\mathbb{N}}$ be a general set.*

- (1) *If X is weakly shift-stable, then all decimations $\psi_{j,n}(X)$ for $j \geq 0$, $n \geq 1$ are weakly shift-stable.*
- (2) *If X_0, X_1, \dots, X_{n-1} are weakly shift-stable, then their n -fold interleaving $Y := (\circledast_n)_{i=0}^{n-1} X_i$ is weakly shift-stable.*
- (3) *If X is weakly shift-stable, then its n -fold interleaving closure $X^{[n]}$ is weakly shift-stable for each $n \geq 1$.*

A parallel result holds for the class $\overline{\mathcal{W}}(\mathcal{A})$ of all closed weakly shift-stable sets on the finite alphabet \mathcal{A} . This latter class of sets includes the path sets studied in [2], as shown in [5].

2.6. Entropy of interleavings

In Section 9 we study two notions of entropy for general sets X , topological entropy and prefix entropy.

Definition 2.16 (*Topological entropy*). The *topological entropy* $H_{\text{top}}(X)$ is given by

$$H_{\text{top}}(X) := \limsup_{k \rightarrow \infty} \frac{1}{k} \log N_k(X)$$

where $N_k(X)$ counts the number of distinct blocks of length k to be found across all words $\mathbf{x} \in X$.

The topological entropy is defined here as a limsup, however the limit always exists, as a consequence of a submultiplicativity property of block counting functions $N_k(X)$, which is $N_{k_1+k_2}(X) \leq N_{k_1}(X)N_{k_2}(X)$, see [6, Property 8]. Here \log denotes the natural logarithm; in information theory \log_2 is used instead.

We next consider prefix entropy.

Definition 2.17 (*Prefix entropy and stable prefix entropy*).

(1) The *prefix entropy* (or *path topological entropy*) $H_p(X)$ of a general set X is defined by

$$H_p(X) := \limsup_{k \rightarrow \infty} \frac{1}{k} \log N_k^I(X), \quad (2.6)$$

where $N_k^I(X)$ counts the number of distinct prefix blocks $b_0 b_1 \cdots b_{k-1}$ of length k found across all words $\mathbf{x} \in X$.

(2) The limit in (2.6) does not always exist, and we say that X has *stable prefix entropy* if the limit does exist:

$$H_p(X) := \lim_{k \rightarrow \infty} \frac{1}{k} \log N_k^I(X), \quad (2.7)$$

The prefix entropy was introduced in [2] under the name *path topological entropy* for a class of sets called *path sets*. In that paper symbol sequences were labels attached to paths of edges in a directed labeled graph. Prefix blocks were termed *initial blocks* (for path sets) because they represented the initial steps along a path in a directed labeled graph defining the path set. Since $N_k^I(X) \leq N_k(X)$ we always have $H_p(X) \leq H_{\text{top}}(X)$, and strict inequality may hold.

In Section 9.2 we show the shift map preserves both entropies. Decimation operations need not preserve entropy, and Section 9.3 gives inequalities such entropies must satisfy. In Section 9.4 we establish an inequality for prefix entropy of interleavings of general sets.

Theorem 2.18 (*Prefix entropy bound under interleaving*). *Let X_0, X_1, \dots, X_{n-1} be arbitrary subsets of $\mathcal{A}^{\mathbb{N}}$. The prefix entropy of the set $X = X_0 \circledast X_1 \circledast \cdots \circledast X_{n-1}$ is bounded above by the arithmetic mean of the prefix entropies of X_0, \dots, X_{n-1} . That is:*

$$H_p(X) \leq \frac{1}{n} \sum_{i=0}^{n-1} H_p(X_i). \quad (2.8)$$

Example 9.6 shows that strict inequality in (2.8) may occur.

In Section 9.5 we show that the assumption of stable prefix entropy for each of the sets X_0, X_1, \dots, X_{n-1} implies equality in this formula, and that the n -fold interleaving $X = X_0 \circledast \cdots \circledast X_{n-1}$ itself has stable prefix entropy.

Theorem 2.19 (*Stable prefix entropy interleaving formula*). *If each of the sets X_0, X_1, \dots, X_{n-1} has stable prefix entropy, then the n -fold interleaving $X = X_0 \circledast X_1 \circledast \cdots \circledast X_{n-1}$ also has stable prefix entropy. In this case*

$$H_p(X) = \frac{1}{n} \sum_{i=0}^{n-1} H_p(X_i). \quad (2.9)$$

In contrast to this result for interleaving, decimations of a set X having stable prefix entropy need not have stable prefix entropy; see Remark 9.7.

We also deduce in Section 9.5 that all weakly shift-stable sets X have good entropy properties.

Theorem 2.20 (*Weak shift-stability implies stable prefix entropy*). *If X is weakly shift-stable, then X has stable prefix entropy, and in addition $H_p(X) = H_{\text{top}}(X)$. Consequently the n -fold interleaving $X = X_0 \circledast X_1 \circledast \cdots \circledast X_{n-1}$ of weakly-shift stable sets X_i has*

$$H_{\text{top}}(X) = \frac{1}{n} \sum_{i=0}^{n-1} H_{\text{top}}(X_i). \quad (2.10)$$

Finally, we observe that since all decimations of weakly shift-stable sets are weakly shift-stable, they will have stable prefix entropy.

2.7. Composition of interleavings and operad structure

In Section 7 we consider factorizations of a set X under iterated composition of interleavings. We give examples of sets X having iterated factorizations going to infinite depth. This behavior differs from interleaving restricted to the class of all path sets on the finite alphabet \mathcal{A} , as we show in [5] that the iterated factorization of any path set terminates at some finite depth.

Abstractly, the family of operations obtained under iterated composition using interleaving operations of all arities determines a *non-symmetric operad* (also called a *non- Σ operad*) in the sense of May [38]; see also Markl et al. [35, Part I, Sect. 1.3] and Markl [36, Sect. 1]. Non-symmetric operads arise in many combinatorial constructions, see work of Giraudo [24], [25]. Iterated interleaving operations satisfy nontrivial universal identities under composition, examples being the shuffle identities given in Theorem 2.9. These identities show that certain nested compositions of interleaving operations give equivalent operations. However most nestings of compositions yield distinct operations. In particular, interleaving operations do not satisfy the associative law when acting on collections of subsets X of $\mathcal{A}^{\mathbb{N}}$. For instance, the 3-ary operations $X_0 \circledast X_1 \circledast X_2$ and $X_0 \circledast (X_1 \circledast X_2)$ and $(X_0 \circledast X_1) \circledast X_2$ are all distinct.

Operads in general are characterized as (universal) algebraic objects satisfying a given set of universal identities. We shall consider the *interleaving non-symmetric operad* to be the non-symmetric operad whose universal identities are all the identities satisfied on the collection of all sets $X \subseteq \mathcal{A}^{\mathbb{N}}$ with alphabet size $|\mathcal{A}| = 2$. These universal identities include the shuffle identities in Theorem 2.9. This set of identities may be a generating set for all universal identities for this operad; we leave it as an open question to determine a generating set.

In Appendix A we provide details checking the operad structure associated to interleaving.

2.8. Contents of paper

The contents of the remainder of the paper are as follows:

Section 3 relates decimation operations and shows these operations are closed under composition and under the shift operator.

Section 4 studies interleaving operations and the interleaving closure operation $X \rightarrow X^{[n]}$ for general sets $X \subseteq \mathcal{A}^{\mathbb{N}}$, proving Theorem 2.8 and the shuffle identities.

Section 5 establishes divisibility properties of n -fold factorizations of a closed set X .

Section 6 classifies infinitely factorizable closed sets X . These sets have more restricted factorizations than non-closed sets.

Section 7 studies iterated interleaving factorizations of closed sets X . It shows by example that such iterated factorizations can continue to infinite depth.

Section 8 studies shift-stability and weak shift-stability of sets $X \subseteq \mathcal{A}^{\mathbb{N}}$. It gives a forbidden-blocks characterization of shift-stable closed sets. It shows that the class of weakly shift-stable sets is closed under all decimation and interleaving operations.

Section 9 defines and discusses topological entropy and prefix (topological) entropy, proving Theorems 2.18 through 2.20.

Section 10 discusses further directions for research.

Appendix A studies an operad structure generated by interleaving operations.

3. Decimations of arbitrary subsets of $\mathcal{A}^{\mathbb{N}}$

This section studies decimations and interleaving for subsets $X \subseteq \mathcal{A}^{\mathbb{N}}$. All results in this section apply to arbitrary subsets X of $\mathcal{A}^{\mathbb{N}}$.

3.1. Compositions of decimations

The set of all decimation operators is closed under composition of operators. This composition action is a representation of the discrete $ax + b$ semigroup given by the nonnegative integer matrices $\begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix}$ with $a \geq 1$ and $b \geq 0$.

Proposition 3.1 (*Composition of decimations*). *Let $X \subseteq \mathcal{A}^{\mathbb{N}}$ be an arbitrary set. For all $j, k \geq 0$ and $m, n \geq 1$ we have*

$$\psi_{j,m} \circ \psi_{k,n}(X) := \psi_{j,m}(\psi_{k,n}(X)) = \psi_{jn+k,mn}(X). \quad (3.1)$$

Proof. The result is verified separately for each element $\mathbf{x} = x_0x_1x_2\cdots \in X$. We set $\mathbf{y} := \psi_{k,n}(\mathbf{x}) = x_kx_{k+n}x_{k+2n}x_{k+3n}\cdots$ where $\mathbf{y} = y_0y_1y_2\cdots$ has $y_j = x_{k+jn}$. Now

$$\psi_{j,m} \circ \psi_{k,n} = \psi_{j,m}(\mathbf{y}) = y_jy_{j+m}y_{j+2m}y_{j+3m}\cdots$$

giving

$$y_j y_{j+m} y_{j+2m} y_{j+3m} \cdots = x_{k+jn} x_{k+jn+mn} x_{k+jn+2mn} = \psi_{jn+k, mn}(\mathbf{x}),$$

as asserted. \square

3.2. Decimations and the shift

The decimation operations also transform nicely under the one-sided shift $S(a_0 a_1 a_2 \dots) = a_1 a_2 a_3 \dots$.

Proposition 3.2 (*Shift of decimations*). *Let $X \subseteq \mathcal{A}^{\mathbb{N}}$ be an arbitrary set.*

(1) *For all $j \geq 0$ and $m \geq 1$, the one-sided shift S acts as*

$$\psi_{j, m}(SX) = \psi_{j+1, m}(X). \quad (3.2)$$

(2) *In addition*

$$S(\psi_{j, m}(X)) = \psi_{j+m, m}(X) = \psi_{j, m}(S^m X). \quad (3.3)$$

Proof. (1) For a single element $\mathbf{x} \in X$, (3.2) is equivalent to the assertion

$$\begin{aligned} \psi_{j, m}(S\mathbf{x}) &= \psi_{j, m}(S(x_0 x_1 x_2 \cdots)) = \psi_{j, m}(x_1 x_2 x_3 \cdots) \\ &= x_{j+1} x_{m+(j+1)} x_{2m+(j+1)} \cdots = \psi_{j+1, m}(\mathbf{x}). \end{aligned}$$

(2) For $\mathbf{x} \in X$ we have

$$S(\psi_{j, m}(\mathbf{x})) = S(x_j x_{j+m} x_{j+2m} \cdots) = x_{j+m} x_{j+2m} \cdots = \psi_{j+m, m}(\mathbf{x}) = \psi_{j, m}(S^m \mathbf{x}),$$

where the last equality used (1) iterated m times. \square

4. Interleaving for arbitrary subsets of $\mathcal{A}^{\mathbb{N}}$

4.1. Interleaving and decimation

Interleaving operations can be characterized in terms of the principal decimations of their output. The criterion (2) below could be used as an alternate definition of n -fold interleaving of sets.

Proposition 4.1 (*Decimation characterization of interleavings*).

(1) *Every $\mathbf{x} \in \mathcal{A}^{\mathbb{N}}$ has an n -fold interleaving factorization $\mathbf{x} = (\circledast_n)_{i=0}^{n-1} \mathbf{x}_i$ for all $n \geq 1$. This factorization is unique, with $\mathbf{x}_i = \psi_{i, n}(\mathbf{x})$ ($0 \leq i \leq n-1$), so that*

$$\mathbf{x} = \psi_{0, n}(\mathbf{x}) \circledast \psi_{1, n}(\mathbf{x}) \circledast \cdots \circledast \psi_{n-1, n}(\mathbf{x}) = (\circledast_n)_{i=0}^{n-1} \psi_{i, n}(\mathbf{x}). \quad (4.1)$$

(2) If $X \subseteq \mathcal{A}^{\mathbb{N}}$ has an n -fold interleaving factorization $X = (\circledast_n)_{i=0}^{n-1} X_i$, then

$$X = \{\mathbf{x} \in \mathcal{A}^{\mathbb{N}} : \psi_{i,n}(\mathbf{x}) \in X_i \quad \text{for all } 0 \leq i \leq n-1\}. \quad (4.2)$$

This factorization is unique with $X_i = \psi_{i,n}(X)$ ($0 \leq i \leq n-1$), so that

$$X = \psi_{0,n}(X) \circledast \psi_{1,n}(X) \circledast \cdots \circledast \psi_{n-1,n}(X) = (\circledast_n)_{i=0}^{n-1} \psi_{i,n}(X). \quad (4.3)$$

Proof. The identity (4.1) is immediate from the definition of interleaving product, checking it symbol by symbol. This n -fold interleaving factorization of \mathbf{x} is unique because if $\mathbf{x} = (\circledast_n)_{i=0}^{n-1} \mathbf{x}_i$, then the $(i + kn)$ th symbol of \mathbf{x} is by definition the k th symbol of \mathbf{x}_i , so that each symbol of \mathbf{x}_i is determined by a symbol of \mathbf{x} .

(2) Let $X = X_0 \circledast X_1 \circledast \cdots \circledast X_{n-1}$. By definition

$$\begin{aligned} X &= \{\mathbf{x} \in \mathcal{A}^{\mathbb{N}} : \mathbf{x} = (\circledast_n)_{i=0}^{n-1} \mathbf{x}_i, \text{ with } \mathbf{x}_i \in X_i \text{ for all } 0 \leq i \leq n-1\} \\ &= \{\mathbf{x} \in \mathcal{A}^{\mathbb{N}} : \psi_{i,n}(\mathbf{x}) = \mathbf{x}_i, \text{ with } \mathbf{x}_i \in X_i \text{ for all } 0 \leq i \leq n-1\} \\ &= \{\mathbf{x} \in \mathcal{A}^{\mathbb{N}} : \psi_{i,n}(\mathbf{x}) \in X_i \text{ for all } 0 \leq i \leq n-1\}, \end{aligned}$$

which is (4.2); we used (1) to deduce the second equality.

To show (4.3), it suffices to show $\psi_{i,n}(X) = X_i$. We have $\psi_{i,n}(X) \subseteq X_i$ by (4.2). To show the map is onto, for any \mathbf{x}_i we can pick arbitrary $\mathbf{x}_j \in X_j$ for $j \neq i$ and then (1) implies that $\mathbf{x} := (\circledast_n)_{j=0}^{n-1} \mathbf{x}_j \in Z$ has $\psi_{i,n}(\mathbf{x}) = \mathbf{x}_i$, as required. \square

We deduce Theorem 2.8 from the proposition.

Proof of Theorem 2.8. (1) We are to show X has an interleaving factorization if and only if $X = X^{[n]}$. Suppose $X = X^{[n]}$. By definition $X^{[n]} = \psi_{0,n}(X) \circledast \cdots \circledast \psi_{n-1,n}(X)$ has an interleaving factorization, so X does too. Conversely if $X = X_0 \circledast X_1 \circledast \cdots \circledast X_{n-1}$ is an interleaving factorization then by Proposition 4.1 (2) $X_i = \psi_{i,n}(X)$ whence $X^{[n]} = X_0 \circledast X_1 \circledast \cdots \circledast X_{n-1} = X$.

(2) This is Proposition 4.1 (2). \square

4.2. n -fold interleaving closure operations

We show that the family of closure operations $X \rightarrow X^{[n]}$ on sets $X \subseteq \mathcal{A}^{\mathbb{N}}$ commutes with topological closure, and the equality $X = X^{[n]}$ corresponds to X having an n -fold interleaving factorization.

The following result shows this operation is a closure operation in the set-theoretic sense.

Theorem 4.2 (*Properties of n -fold interleaving closure*). *The n -fold interleaving closure operation $X^{[n]}$ of sets $X \subseteq \mathcal{A}^{\mathbb{N}}$ has the following properties:*

(1) (Projection property) *The n -fold interleaving closure $X^{[n]}$ is characterized by the property that it is the maximal set Z such that its principal decimations at level n satisfy*

$$\psi_{i,n}(Z) = \psi_{i,n}(X) \quad \text{for } 0 \leq i \leq n-1. \quad (4.4)$$

(2) (Extension property) *Any set $X \subseteq \mathcal{A}^{\mathbb{N}}$ satisfies*

$$X \subseteq X^{[n]}. \quad (4.5)$$

(3) (Idempotent property) *The operation $X \mapsto X^{[n]}$ is idempotent; i.e., $(X^{[n]})^{[n]} = X^{[n]}$ for all X .*

(4) (Isotone property) *If $X \subseteq Y$ then $X^{[n]} \subseteq Y^{[n]}$.*

Remark 4.3 (*Set theory closure property*). Properties (2), (3), and (4) comprise the axioms of a *Moore closure* property (see Schechter [46, Sec. 4.1-4.12]). These axioms are known to be equivalent to the property of being closed under arbitrary intersections. The n -fold interleaving closure operation does not satisfy all of Kuratowski's axioms defining the closed sets of a topology; it does not satisfy the set union property $(X \cup Y)^{[n]} = X^{[n]} \cup Y^{[n]}$. It does satisfy the inclusion

$$X^{[n]} \cup Y^{[n]} \subseteq (X \cup Y)^{[n]}. \quad (4.6)$$

As an example showing the inclusion can be strict, take $X = X^{[2]} = \{0^\infty\}$, $Y = Y^{[2]} = \{1^\infty\}$. Then $X^{[2]} \cup Y^{[2]} \subsetneq (X \cup Y)^{[2]} = \{0^\infty, 1^\infty, (01)^\infty, (10)^\infty\}$. Relations between the interleaving closure operations and topological closure in $\mathcal{A}^{\mathbb{N}}$ are given in Section 4.7.

Proof. (1) If a collection of sets each have property (4.4) then so does their union, and X has property (4.4), so there exists a maximal set Z with property (4.4). By definition

$$X^{[n]} := \psi_{0,n}(X) \circledast \psi_{1,n}(X) \circledast \cdots \circledast \psi_{n-1,n}(X)$$

Then by Proposition 4.1(2),

$$X^{[n]} = \{\mathbf{z} \in \mathcal{A}^{\mathbb{N}} : \psi_{i,n}(\mathbf{z}) \in \psi_{i,n}(X) \text{ for all } 0 \leq i \leq n-1\} \quad (4.7)$$

The statement $\psi_{i,n}(Z) = \psi_{i,n}(X)$ means that $\psi_{i,n}(\mathbf{z}) \in \psi_{i,n}(X)$ for all $\mathbf{z} \in Z$. From (4.7), one sees that $Z = X^{[n]}$ is precisely the maximal set such that (4.4) holds for all $0 \leq i \leq n-1$.

(2) It follows from (1). Alternatively, by Proposition 4.1(1) given $\mathbf{x} \in X$ we have

$$\mathbf{x} = \psi_{0,n}(\mathbf{x}) \circledast \psi_{1,n}(\mathbf{x}) \circledast \cdots \circledast \psi_{n-1,n}(\mathbf{x}) \in \psi_{0,n}(X) \circledast \psi_{1,n}(X) \circledast \cdots \circledast \psi_{n-1,n}(X),$$

which certifies $\mathbf{x} \in X^{[n]}$, proving (4.5).

(3) Idempotence follows from (1) and (2): By (1) $X^{[n]}$ is the maximal set having $\psi_{i,n}(X^{[n]}) \subseteq \psi_{i,n}(X)$ holds for $0 \leq i \leq n-1$. Now by (2) $(X^{[n]})^{[n]}$ contains $X^{[n]}$. But $\psi_{i,n}((X^{[n]})^{[n]}) \subseteq \psi_{i,n}(X^{[n]}) \subseteq \psi_{i,n}(X)$ for $0 \leq i \leq n-1$, so it is also maximal, so $(X^{[n]})^{[n]} = X^{[n]}$.

(4) Suppose that $X \subseteq Y$. Using the projection property (2) for X and Y separately shows

$$\begin{aligned}\psi_{i,n}(Y^{[n]} \cup X^{[n]}) &= \psi_{i,n}(Y^{[n]}) \cup \psi_{i,n}(X^{[n]}) = \psi_{i,n}(Y) \cup \psi_{i,n}(X) \\ &= \psi_{i,n}(Y) = \psi_{i,n}(Y^{[n]}) \quad 0 \leq i \leq n-1.\end{aligned}$$

The projection property now gives $Y^{[n]} \cup X^{[n]} \subseteq Y^{[n]}$, whence $X^{[n]} \subseteq Y^{[n]}$. \square

4.3. Shuffle identities for interleaving operators

The family of interleaving operations satisfy universal algebraic identities under particular compositions of operations, acting on general subsets of $\mathcal{A}^{\mathbb{N}}$. We now prove Proposition 2.9, which asserts

$$(\circledast_n)_{i=0}^{n-1} ((\circledast_m)_{j=0}^{m-1} X_{i+jn}) = (\circledast_{mn})_{k=0}^{mn-1} X_k. \quad (4.8)$$

One reads the interleaving of interleavings on the left side of (4.8) as

$$\begin{aligned}(X_0 \circledast X_n \circledast \cdots \circledast X_{(m-1)n}) \circledast (X_1 \circledast X_{n+1} \circledast \cdots \circledast X_{(m-1)n+1}) \circledast \cdots \\ \cdots \circledast (X_{n-1} \circledast X_{2n-1} \circledast \cdots \circledast X_{mn-1}),\end{aligned}$$

with parentheses indicating composition of m -fold interleavings given as input to an n -fold interleaving. The right side of (4.8) is an mn -fold interleaving,

$$X_0 \circledast X_1 \circledast X_2 \circledast \cdots \circledast X_{n-1} \circledast X_n \circledast X_{n+1} \circledast \cdots \circledast \cdots \circledast X_{(m-1)n+n-2} \circledast X_{(m-1)n+n-1}, \quad (4.9)$$

with factors taken in linear order.

Proof of Proposition 2.9. Using Proposition 4.1(2) we obtain

$$\begin{aligned}(\circledast_n)_{i=0}^{n-1} ((\circledast_m)_{j=0}^{m-1} X_{i+jn}) \\ &= \{\mathbf{x} \in \mathcal{A}^{\mathbb{N}} : \psi_{i,n}(\mathbf{x}) \in (\circledast_m)_{j=0}^{m-1} X_{i+jn} \text{ for all } 0 \leq i \leq n-1\} \\ &= \{\mathbf{x} \in \mathcal{A}^{\mathbb{N}} : \psi_{j,m}(\psi_{i,n}(\mathbf{x})) \in X_{i+jn} \text{ for all } 0 \leq j \leq n-1, 0 \leq i \leq n-1\} \\ &= \{\mathbf{x} \in \mathcal{A}^{\mathbb{N}} : \psi_{i+jn,mn}(\mathbf{x}) \in X_{i+jn} \text{ for all } 0 \leq j \leq n-1, 0 \leq i \leq n-1\} \\ &= (\circledast_{mn})_{k=0}^{mn-1} X_k.\end{aligned}$$

Proposition 4.1(2) gives the first, second and fourth equality and Proposition 3.1 the third equality. \square

Shuffle identities are useful in studying self-interleavings of sets X .

Definition 4.4. Give $X \subseteq \mathcal{A}^{\mathbb{N}}$ let $X^{(\circledast n)}$ denote the n -fold self-interleaving defined by

$$X^{(\circledast n)} := (\circledast_n)_{i=0}^{n-1} X = X \circledast X \circledast \cdots \circledast X \quad (n \text{ factors in product}).$$

The special case of self-interleaving under composition satisfies identities similar to that of exponentiation, a consequence of the shuffle identities.

Proposition 4.5 (*Composition of self-interleavings*). *For any natural numbers $m, n \geq 1$, and any subset X of $\mathcal{A}^{\mathbb{N}}$, the following set-theoretic identity holds for n -fold, m -fold and mn -fold self-interleaving:*

$$(X^{(\circledast n)})^{(\circledast m)} = (X^{(\circledast m)})^{(\circledast n)} = X^{(\circledast mn)}. \quad (4.10)$$

Proof. In Theorem 2.9 choose all $X_k = X$ for $0 \leq k \leq mn - 1$ and obtain $(X^{(\circledast m)})^{(\circledast n)} = X^{(\circledast mn)}$. Then interchange m and n . \square

4.4. Composition identities for interleaving closure operations

We prove Proposition 2.10 determining the composition of self-interleaving closure operations: $(X^{[m]})^{[n]} = (X^{[n]})^{[m]} = X^{[\text{lcm}(m, n)]}$.

We first establish a preliminary result giving formulas and inclusions for compositions of interleaving closure operations.

Proposition 4.6 (*Composition formulas*). (1) For all $m, n \geq 1$, and all $X \subseteq \mathcal{A}^{\mathbb{N}}$,

$$(X^{[m]})^{[n]} = (\circledast_n)_{i=0}^{n-1} \psi_{i,n}(X^{[m]}). \quad (4.11)$$

(2) For all $m, n \geq 1$, and all $X \subseteq \mathcal{A}^{\mathbb{N}}$,

$$X^{[mn]} = (\circledast_n)_{i=0}^{n-1} (\psi_{i,n}(X)^{[m]}). \quad (4.12)$$

(3) For all $m, n \geq 1$

$$X^{[m]} \subseteq X^{[mn]}. \quad (4.13)$$

(4) If $\text{gcd}(m, n) = 1$ then

$$(X^{[m]})^{[n]} = (X^{[n]})^{[m]} = X^{[mn]}$$

Proof. (1) This assertion is the definition of the n -fold interleaving closure of $X^{[m]}$.

(2) We set $X_k := \psi_{k,mn}(X)$ for $0 \leq k \leq mn - 1$ in the shuffle identity (2.4), obtaining

$$X^{[mn]} = (\circledast_n)_{i=0}^{n-1} ((\circledast_m)_{j=0}^{m-1} \psi_{i+jn,mn}(X))$$

The right side of this equation contains terms $Z_i := (\circledast_m)_{j=0}^{m-1} \psi_{i+jn,mn}(X)$, and we must show $Z_i = \psi_{i,n}(X)^{[m]}$. We have

$$\begin{aligned} \psi_{i,n}(X)^{[m]} &:= (\psi_{0,m} \circ \psi_{i,n}(X)) \circledast (\psi_{1,m} \circ \psi_{i,n}(X)) \circledast \cdots \circledast (\psi_{m-1,m} \circ \psi_{i,n}(X)) \\ &= \psi_{i,mn}(X) \circledast \psi_{i+n,mn}(X) \circledast \cdots \circledast \psi_{i+(m-1)n,mn}(X) = Z_i, \end{aligned}$$

as required.

(3) We have $X^{[m]} \subseteq (X^{[m]})^{[n]}$ by the extension property of n -fold interleaving. We claim that

$$(X^{[m]})^{[n]} \subseteq X^{[mn]}. \quad (4.14)$$

To prove the claim, comparing the now proved (4.11) and (4.12), it suffices to show

$$\psi_{i,n}(X^{[m]}) \subseteq \psi_{i,n}(X)^{[m]} \quad \text{for } 0 \leq i \leq n - 1. \quad (4.15)$$

For fixed i , the right side of this inclusion is an m -fold interleaving

$$\psi_{i,n}(X)^{[m]} = (\psi_{0,m} \circ \psi_{i,n}(X)) \circledast (\psi_{1,m} \circ \psi_{i,n}(X)) \circledast \cdots \circledast (\psi_{m-1,m} \circ \psi_{i,n}(X))$$

The composition rule for decimations (Proposition 3.1) shows that

$$\psi_{i,n}(X)^{[m]} = \psi_{i,mn}(X) \circledast \psi_{i+n,mn}(X) \circledast \cdots \circledast \psi_{i+(m-1)n,mn}(X). \quad (4.16)$$

To evaluate the left side of the inclusion (4.15), suppose $\mathbf{x} = \psi_{i,n}(\mathbf{z}) \in \psi_{i,n}(X^{[m]})$ with $\mathbf{z} \in X^{[m]}$. Now by Proposition 4.1 (1), \mathbf{x} has an m -fold interleaving factorization

$$\mathbf{x} = (\circledast_m)_{j=0}^{m-1} \mathbf{w}_j = \mathbf{w}_0 \circledast \mathbf{w}_1 \circledast \cdots \circledast \mathbf{w}_{m-1},$$

where

$$\mathbf{w}_j = \psi_{j,m}(\mathbf{x}) = \psi_{j,m}(\psi_{i,n}(\mathbf{z})) = \psi_{i+jn,mn}(\mathbf{z}).$$

Therefore

$$\mathbf{x} = \psi_{i,n}(\mathbf{z}) = (\circledast_m)_{j=0}^{m-1} \psi_{i+jn,mn}(\mathbf{z}) = \psi_{i,mn}(\mathbf{z}) \circledast \psi_{i+n,mn}(\mathbf{z}) \circledast \cdots \circledast \psi_{i+(m-1)n,mn}(\mathbf{z}). \quad (4.17)$$

We are to show $\mathbf{x} \in \psi_{i,n}(X)^{[m]}$. It suffices to show

$$\psi_{i+jn,mn}(\mathbf{z}) \in \psi_{i+jn,mn}(X) \quad \text{for } 0 \leq j \leq m-1, \quad (4.18)$$

since (4.17) then asserts $\mathbf{x} \in (\circledast_m)_{j=0}^{m-1} \psi_{i+jn,mn}(X)$ whence (4.16) shows $\mathbf{x} \in \psi_{i,n}(X)^{[m]}$.

To show (4.18), any $\mathbf{z} \in X^{[m]}$ has, for $0 \leq k \leq m-1$,

$$\psi_{k,m}(\mathbf{z}) \in \psi_{k,m}(X^{[m]}) = \psi_{k,m}(X),$$

where the equality of sets holds by definition of m -fold interleaving. Thus there exists some $\tilde{\mathbf{z}}_k \in X$ with $\psi_{k,m}(\mathbf{z}) = \psi_{k,m}(\tilde{\mathbf{z}}_k)$. Now for $0 \leq i \leq n-1, 0 \leq j \leq m-1$, there exist unique (k, ℓ) satisfying

$$i+jn = k + \ell m, \quad (4.19)$$

with $0 \leq k \leq m-1, 0 \leq \ell \leq n-1$. Here $k = k(i, j)$ is determined by $k \equiv i+jn \pmod{m}$. We have

$$\begin{aligned} \psi_{i+jn,mn}(\mathbf{z}) &= \psi_{k+\ell m,mn}(\mathbf{z}) = \psi_{\ell,n}(\psi_{k,m}(\mathbf{z})) \\ &= \psi_{\ell,n}(\psi_{k,m}(\tilde{\mathbf{z}}_k)) = \psi_{k+\ell m,mn}(\tilde{\mathbf{z}}_k) \\ &= \psi_{i+jn,mn}(\tilde{\mathbf{z}}_k) \in \psi_{i+jn,mn}(X), \end{aligned}$$

showing (4.18).

(4) It suffices to show $(X^{[m]})^{[n]} = X^{[mn]}$ if $\gcd(m, n) = 1$; interchanging m and n then gives the other case. The proof of (3) showed that $(X^{[m]})^{[n]} \subseteq X^{[mn]}$ holds (with no gcd restriction), so it suffices to show the reverse inclusion $X^{[mn]} \subseteq (X^{[m]})^{[n]}$. By the already proved (4.11) and (4.12) this assertion is

$$X^{[mn]} = (\circledast_n)_{i=0}^{n-1} (\psi_{i,n}(X)^{[m]}) \subseteq (\circledast_n)_{i=0}^{n-1} (\psi_{i,n}(X^{[m]})) = (X^{[m]})^{[n]}. \quad (4.20)$$

It therefore suffices to prove the individual set inclusions

$$\psi_{i,n}(X)^{[m]} \subseteq \psi_{i,n}(X^{[m]}) \quad \text{for } 0 \leq i \leq n-1, \quad (4.21)$$

hold when $\gcd(m, n) = 1$.

Now suppose we are given an arbitrary $\mathbf{x} \in \psi_{i,n}(X)^{[m]}$. We wish to show $\mathbf{x} \in \psi_{i,n}(X^{[m]})$. To begin, \mathbf{x} has an m -fold interleaving factorization

$$\mathbf{x} = (\circledast_m)_{j=0}^{m-1} \psi_{j,m}(\mathbf{x}_j),$$

in which each $\mathbf{x}_j = \psi_{i,n}(\mathbf{z}_j) \in \psi_{i,n}(X)$ with $\mathbf{z}_j \in X$. Thus we have

$$\psi_{j,m}(\mathbf{x}_j) = \psi_{j,m}(\psi_{i,n}(\mathbf{z}_j)) = \psi_{i+jn,mn}(\mathbf{z}_j). \quad (4.22)$$

As in (3) there are (k, ℓ) with

$$\psi_{i+jn,mn}(\mathbf{z}_j) = \psi_{k+\ell m,mn}(\mathbf{z}_j) = \psi_{\ell,n}(\psi_{k,m}(\mathbf{z}_j)).$$

Here, for fixed i , the value $k = k(i, j)$ is given by $k \equiv i + jn \pmod{m}$. The values $k(i, j)$ are all distinct as j ranges from 0 to $m - 1$ with i fixed, because $\gcd(m, n) = 1$. It follows that the inverse map $j = j(i, k)$ is well defined. By definition of m -fold interleaving closure, there will exist a value $\mathbf{z} \in X^{[m]}$ having

$$\psi_{k,m}(\mathbf{z}) = \psi_{k,m}(\mathbf{z}_j) \quad \text{for } 0 \leq k \leq m - 1, \quad (4.23)$$

with $\mathbf{z}_j \in X$ and $j = j(i, k)$ runs over all $0 \leq j \leq m - 1$ as k varies.

We claim that $\psi_{i,n}(\mathbf{z}) = \mathbf{x}$. We have

$$\begin{aligned} \psi_{i,n}(\mathbf{z}) &= (\circledast_m)_{j=0}^{m-1} \psi_{i+jn,mn}(\mathbf{z}) && \text{by (4.17)} \\ &= (\circledast_m)_{j=0}^{m-1} \psi_{k(i,j)+\ell(i,j)m,mn}(\mathbf{z}) && \text{by (4.19)} \\ &= (\circledast_m)_{j=0}^{m-1} \psi_{\ell(i,j),n}(\psi_{k(i,j),m}(\mathbf{z})) \\ &= (\circledast_m)_{j=0}^{m-1} \psi_{\ell(i,j),n}(\psi_{k(i,j),m}(\mathbf{z}_j)), && \text{by (4.23).} \end{aligned}$$

Now we simplify and obtain

$$\begin{aligned} \psi_{i,n}(\mathbf{z}) &= (\circledast_m)_{j=0}^{m-1} \psi_{k(i,j)+\ell(i,j)m,mn}(\mathbf{z}_j) \\ &= (\circledast_m)_{j=0}^{m-1} \psi_{i+jn,mn}(\mathbf{z}_j) = (\circledast_m)_{j=0}^{m-1} \psi_{j,m}(\mathbf{x}_j) && \text{by (4.22)} \\ &= \mathbf{x}, \end{aligned}$$

so $\mathbf{x} \in \psi_{i,n}(X^{[m]})$. \square

We now prove the Theorem 2.10 formulas for composition of interleaving closures.

Proof of Theorem 2.10. It suffices to prove $(X^{[m]})^{[n]} = X^{[\text{lcm}(m,n)]}$, because its right side is symmetric in m and n ; we may then exchange m and n to establish $(X^{[n]})^{[m]} = X^{[\text{lcm}(m,n)]}$. We have already proven $(X^{[m]})^{[n]} = X^{[mn]}$ for the case $\gcd(m, n) = 1$ in Proposition 4.6.

For general n, m we let $d = \gcd(m, n)$, the greatest common divisor. One can always find e, f with $d = ef$ such that $e|m$ and $f|n$ and $\gcd(\frac{m}{e}, \frac{n}{f}) = 1$. To see this, let $d = \prod_p p^{e(p,d)}$ denote the prime factorization of d ; then the choice $e = \prod_{p^{e(p,d)} \mid m} p^{e(p,d)}$ and $f = \prod_{p^{e(p,d)}+1 \mid m} p^{e(p,d)}$ will work. Note that if $p^{e(p,d)+1} \mid m$, then necessarily $p^{e(p,d)} \mid n$, so that $f \mid n$. By construction, $e|m$, $ef = d$, and $\gcd(\frac{m}{e}, \frac{n}{f}) = 1$.

We then have

$$X^{[\text{lcm}(m,n)]} = X^{[mn/ef]} = (X^{[m/e]})^{[n/f]} \subseteq (X^{[m/e]})^{[n]} \subseteq (X^{[m]})^{[n]}.$$

Reading from left to right the second equality comes from Proposition 4.6 (4), the first inclusion follows from Proposition 4.6(3), and the final inclusion follows from the isotone property (4) in Theorem 4.2.

It remains to show that

$$(X^{[m]})^{[n]} \subseteq X^{[\text{lcm}(m,n)]}.$$

Now let $d = \gcd(m, n)$, so that $\ell = \text{lcm}(m, n) = \frac{mn}{d}$. By Proposition 4.6(1) we have $(X^{[m]})^{[n]} = (\circledast_n)_{i=0}^{n-1} \psi_{i,n}(X^{[m]})$ (without any gcd restriction).

Now consider $\mathbf{x} = \mathbf{x}_0 \circledast \mathbf{x}_1 \circledast \cdots \circledast \mathbf{x}_{n-1} \in (X^{[m]})^{[n]}$, and write $\mathbf{x} = b_0 b_1 b_2 \cdots$. Here for $0 \leq i \leq n-1$,

$$\mathbf{x}_i := \psi_{i,n}(\mathbf{x}) = b_i b_{i+n} b_{i+2n} b_{i+3n} \cdots.$$

We are to show that $\mathbf{x} \in X^{[\text{lcm}(m,n)]}$. To begin, we have

$$\mathbf{x}_i = \psi_{i,n}(\mathbf{z}_{i,0} \circledast \mathbf{z}_{i,1} \circledast \cdots \circledast \mathbf{z}_{i,m-1}) \in \psi_{i,n}(X^{[m]}),$$

where each $\mathbf{z}_{i,j} \in \psi_{j,m}(X)$ for $0 \leq j \leq m-1$, so that

$$\mathbf{z}_{i,j} = \psi_{j,m}(\mathbf{w}_{i,j}) \quad \text{with} \quad \mathbf{w}_{i,j} \in X.$$

Because $\gcd(m, n) = d$, the application of $\psi_{i,n}(\cdot)$ to $\mathbf{z}_i = (\circledast_m)_{j=0}^{m-1} \mathbf{z}_{i,j} \in X^{[m]}$ only hits those words $\mathbf{z}_{i,j}$ having subscripts j falling in $\frac{m}{d}$ different residue classes $(\bmod m)$, and it visits each such class exactly d times, as j varies over $0 \leq j \leq m-1$. These $\frac{m}{d}$ classes $(\bmod m)$ comprise distinct residue classes $(\bmod \frac{m}{d})$, again because $\gcd(m, n) = d$. These classes are exactly $i + jn \pmod{\frac{m}{d}}$ for $0 \leq j \leq \frac{m}{d} - 1$. We can therefore rewrite $\mathbf{x}_i = \mathbf{y}_{i,0} \circledast \mathbf{y}_{i,1} \circledast \cdots \circledast \mathbf{y}_{i,\frac{m}{d}-1}$ with $\mathbf{y}_{i,j} = b_{i+jn} b_{i+jn+mn/d} b_{i+jn+2mn/d} \cdots$ for $0 \leq j \leq \frac{m}{d} - 1$. We have $\text{lcm}(m, n) = \frac{mn}{d}$ different elements $\mathbf{y}_{i,j} \in \psi_{k,\frac{m}{d}}(X)$. The key point is that for $k = i + jn$ we have

$$\mathbf{y}_{i,j} = \psi_{i+jn \pmod{m/d}, m/d}(\mathbf{w}_{i+jn}) \in \psi_{k, \frac{m}{d}}(X) \quad \text{for} \quad 0 \leq i \leq n-1, \quad 0 \leq j \leq \frac{m}{d} - 1.$$

Here $k = i + jn$ varies over the interval $0 \leq k \leq \frac{mn}{d} - 1$. Consequently,

$$\mathbf{x} = (\circledast_n)_{i=0}^{n-1} \mathbf{x}_i = (\circledast_n)_{i=0}^{n-1} \left((\circledast_{m/d})_{j=0}^{m/d-1} \mathbf{y}_{i,j} \right) = (\circledast_{\frac{mn}{d}})_{k=0}^{mn/d-1} \psi_{k, \frac{mn}{d}}(\mathbf{w}_k),$$

where the last equality uses the shuffle identity (2.4). We also find that $k = i + jn$ runs through the residue classes $(\bmod mn/d)$ in the correct order. We conclude that $\mathbf{x} \in X^{[mn/d]} = X^{[\text{lcm}(m,n)]}$, establishing the desired inclusion. \square

4.5. Interleaving commutes with set intersection

Interleaving also behaves well with respect to intersection.

Proposition 4.7 (*Interleaving commutes with intersection*). *For $m, n \geq 2$ and subsets $X_0, X_1, \dots, X_{mn-1}$ of $\mathcal{A}^{\mathbb{N}}$, the following set-theoretic identity holds:*

$$\bigcap_{j=0}^{m-1} ((\circledast_n)_{i=0}^{n-1} X_{jn+i}) = (\circledast_n)_{i=0}^{n-1} \left(\bigcap_{j=0}^{m-1} X_{jn+i} \right). \quad (4.24)$$

Proof. By Proposition 4.1 (2), we have $\mathbf{x} \in Z_j := (\circledast_n)_{i=0}^{n-1} X_{jn+i}$ if and only if $\psi_i(\mathbf{x}) \in X_{jn+i}$ for $0 \leq i \leq n-1$. Consequently:

$$\begin{aligned} \mathbf{x} \in \bigcap_{j=0}^{m-1} ((\circledast_n)_{i=0}^{n-1} X_{jn+i}) &\Leftrightarrow \psi_i(\mathbf{x}) \in X_{jn+i} \quad \text{for } 0 \leq i \leq n-1, 0 \leq j \leq m-1 \\ &\Leftrightarrow \psi_i(\mathbf{x}) \in \bigcap_{j=0}^{m-1} X_{jn+i} \quad \text{for } 0 \leq i \leq n-1 \\ &\Leftrightarrow \mathbf{x} \in (\circledast_n)_{i=0}^{n-1} \left(\bigcap_{j=0}^{m-1} X_{jn+i} \right), \end{aligned}$$

verifying (4.24). \square

Corollary 4.8. *Let $X, Y \subseteq \mathcal{A}^{\mathbb{N}}$. Then their n -fold interleaving closures satisfy*

$$X^{[n]} \cap Y^{[n]} = Z^{[n]} \quad (4.25)$$

where $Z := (\circledast_n)_{i=0}^{n-1} (\psi_{i,n}(X) \cap \psi_{i,n}(Y)) = Z^{[n]}$.

Proof. In Proposition 4.7 take $m = 2$ and $n \geq 2$ and choose $X_i = \psi_{i,n}(X)$ and $X_{n+i} = \psi_{i,n}(Y)$ for $0 \leq i \leq n-1$. The left side of (4.24) is $X^{[n]} \cap Y^{[n]}$ and the right side is Z . Here $Z = Z^{[n]}$ holds because Z is defined as an n -fold interleaving of $\psi_{i,n}(Z) := \psi_{i,n}(X) \cap \psi_{i,n}(Y)$ by construction. (In general $\psi_{i,n}(X \cap Y) \subseteq \psi_{i,n}(X) \cap \psi_{i,n}(Y)$, so that $(X \cap Y)^{[n]} \subseteq Z^{[n]}$, and strict inequality can hold.) \square

Remark 4.9 (*Intersection of general interleaving closures*). For intersection of two interleaving closures of different arities of a single set X we have, for all $m, n \geq 1$,

$$X^{[\gcd(m,n)]} \subseteq X^{[m]} \cap X^{[n]}. \quad (4.26)$$

Equality always holds trivially when $m = n$, but need not hold when $m \neq n$. As an example, for $m = 2, n = 3$ take $X = \{\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3\} = \{(010100)^\infty, (111111)^\infty, (110111)^\infty\}$.

Then $(01)^\infty$ is contained in both $X^{[2]}$ via the 2-fold interleaving $\psi_{0,2}(\mathbf{x}_1) \circledast \psi_{1,2}(\mathbf{x}_2)$, and $X^{[3]}$ via the 3-fold interleaving $\psi_{0,3}(\mathbf{x}_1) \circledast \psi_{1,3}(\mathbf{x}_1) \circledast \psi_{2,3}(\mathbf{x}_3)$. We conclude $X \subsetneq X^{[2]} \cap X^{[3]}$. Note this example is closed and weakly shift-stable, having $S^6X = X$.

4.6. Shift action on interleavings

The one-sided shift map acts as

$$S(a_0a_1a_2a_3\cdots) = a_1a_2a_3a_4\cdots.$$

We show the one-sided shift S action preserves the property of having an n -fold interleaving factorization. Suppose that X has an n -fold interleaving factorization $X = X_0 \circledast X_1 \circledast \cdots \circledast X_{n-2} \circledast X_{n-1}$.

(1) The one-sided shift map S acts by

$$S(X) = X_1 \circledast X_2 \circledast \cdots \circledast X_{n-1} \circledast S(X_0). \quad (4.27)$$

Consequently

$$S^n(X) = S(X_0) \circledast S(X_1) \circledast \cdots \circledast S(X_{n-2}) \circledast S(X_{n-1}). \quad (4.28)$$

(2) All iterates $S^k(X)$ possess n -fold interleaving factorizations

$$S^k(X) = \psi_{k,n}(X) \circledast \psi_{k+1,n}(X) \circledast \cdots \circledast \psi_{k+n-1,n}(X).$$

Proof. (1), (2). It suffices to prove (4.27). The other assertion in (1) and assertion (2) then follow easily by induction on $k \geq 1$.

To begin, for all infinite words $\mathbf{x} \in \mathcal{A}^\mathbb{N}$ we have

$$\psi_{j,n}(S\mathbf{x}) = \psi_{j+1,n}(\mathbf{x}) \quad \text{for all } j \geq 0. \quad (4.29)$$

By Theorem 2.8(2) we have $X_i = \psi_{i,n}(X)$ for $0 \leq i \leq n-1$. We set $X_n = \psi_{n,n}(X)$. By Proposition 3.2 (2),

$$\psi_{n,n}(X) = \psi_{0,n}(S^n X) = S\psi_{0,n}(X) = S(X_0). \quad (4.30)$$

We assert $S(X) = X_1 \circledast X_2 \circledast \cdots \circledast X_{n-1} \circledast S(X_0)$. We have the inclusion

$$S(X) \subseteq (\circledast_n)_{i=0}^{n-1} \psi_{i,n}(S(X)) = (\circledast_n)_{i=0}^{n-1} \psi_{i+1,n}(X) = (\circledast_n)_{i=1}^n X_i.$$

To show the opposite inclusion

$$X_1 \circledast X_2 \circledast \cdots \circledast X_{n-1} \circledast S(X_0) \subseteq SX,$$

let $\mathbf{y} = \mathbf{y}_1 \circledast \mathbf{y}_2 \circledast \cdots \circledast \mathbf{y}_n \in X_1 \circledast X_2 \circledast \cdots \circledast X_n$; then $\mathbf{y}_i \in X_i$ for $1 \leq i \leq n$. For $\mathbf{y}_n \in X_n$ by definition there exists $\mathbf{x} \in X$ such that $\psi_{0,n}(\mathbf{x}) = x_0 \circ \mathbf{y}_n \in X_0$, for some x_0 , where $x_0 \circ \mathbf{y}_n$ denotes the concatenation of the letter x_0 and the infinite word \mathbf{y}_n . By the n -fold factorization hypothesis on X one may choose this \mathbf{x} so that also $\psi_{i,n}(\mathbf{x}) = \mathbf{y}_i$ holds for $1 \leq i \leq n-1$. Now one checks using (4.29) that

$$\psi_{i,n}(S(\mathbf{x})) = \mathbf{y}_{i+1} \quad \text{for } 0 \leq i \leq n-1. \quad \square$$

Proposition 4.11 (*Shift map and n -fold interleaving closure*). *The shift map commutes with n -fold interleaving closure. For each $n \geq 1$, and a general set $X \subseteq \mathcal{A}^{\mathbb{N}}$, there holds*

$$S(X^{[n]}) = (SX)^{[n]}. \quad (4.31)$$

Proof. By definition the n -fold interleaving closure $X^{[n]}$ has an n -fold interleaving factorization. We have

$$\begin{aligned} S(X^{[n]}) &= S(\psi_{0,n}(X) \circledast \psi_{1,n}(X) \circledast \cdots \circledast \psi_{n-2,n}(X) \circledast \psi_{n-1,n}(X)) \\ &= \psi_{1,n}(X) \circledast \psi_{2,n}(X) \circledast \cdots \circledast \psi_{n-1,n}(X) \circledast S\psi_{0,n}(X) \\ &= \psi_{1,n}(X) \circledast \psi_{2,n}(X) \circledast \cdots \circledast \psi_{n-1,n}(X) \circledast \psi_{n,n}(X) = (SX)^{[n]}. \end{aligned}$$

Here the second equality comes from Proposition 4.10 (1), the third comes from (4.30), and the fourth comes from the definition of interleaving closure and the fact that by Proposition 3.2 (1), $\psi_{i,n}(X) = \psi_{i-1,n}(SX)$, $i = 1, \dots, n$. \square

4.7. Topological closure

Decimation and interleaving operations and the shift operation all commute with topological closure in $\mathcal{A}^{\mathbb{N}}$.

Theorem 4.12. *Given a subset X of $\mathcal{A}^{\mathbb{N}}$, let \overline{X} denote its topological closure in the shift topology (product topology) in $\mathcal{A}^{\mathbb{N}}$.*

(1) *For each $n \geq 1$ and $j \geq 1$,*

$$\psi_{j,n}(\overline{X}) = \overline{\psi_{j,n}(X)}.$$

In particular if X is a closed set in $\mathcal{A}^{\mathbb{N}}$ then each decimation $X_{j,n} = \psi_{j,n}(X)$ is a closed set.

(2) *For $X_0, X_1, \dots, X_{n-1} \subseteq \mathcal{A}^{\mathbb{N}}$, there holds*

$$(\circledast_n)_{j=0}^{n-1} \overline{X}_j = \overline{(\circledast_n)_{j=0}^{n-1} X_j}.$$

In particular the n -fold interleaving of closed sets is a closed set.

(3) The n -fold interleaving closure operation commutes with the closure operation on the product topology on $\mathcal{A}^{\mathbb{N}}$,

$$(\overline{X})^{[n]} = \overline{X^{[n]}}.$$

(4) The shift operator commutes with topological closure,

$$S\overline{X} = \overline{SX}.$$

Proof. (1) Given $\mathbf{y} \in \psi_{j,n}(\overline{X})$, there is a symbol sequence $\mathbf{x} = x_0x_1x_2 \dots \in \overline{X}$ such that $\psi_{j,n}(\mathbf{x}) = \mathbf{y}$. Then there is a sequence (of symbol sequences) $(\mathbf{x}_k)_{k \geq 1}$, with each $\mathbf{x}_k = x_{0,k}x_{1,k}x_{2,k} \dots \in X$, converging to \mathbf{x} (Convergence is defined by eventual stability of each symbol $x_{\ell,k}$ as $k \rightarrow \infty$, with $x_{\ell,k} = x_{\ell}$ for all sufficiently large k). It is easy to see that if $\mathbf{x}_k \rightarrow \mathbf{x}$, then necessarily $\psi_{j,n}(\mathbf{x}_k) \rightarrow \psi_{j,n}(\mathbf{x}) = \mathbf{y}$, with each $\psi_{j,n}(\mathbf{x}_k)$ in $\psi_{j,n}(X)$, so that $\mathbf{y} \in \overline{\psi_{j,n}(X)}$. Thus, $\psi_{j,n}(\overline{X}) \subseteq \overline{\psi_{j,n}(X)}$. On the other hand, let $\mathbf{y} \in \overline{\psi_{j,n}(X)}$. Then there is a sequence $(\mathbf{y}_k)_{k \geq 1}$ in $\psi_{j,n}(X)$ converging to \mathbf{y} . So there is a sequence $(\mathbf{x}_k)_{k \geq 1}$ in X , with each $\psi_{j,n}(\mathbf{x}_k) = \mathbf{y}_k$. Since closed sets are compact in $\mathcal{A}^{\mathbb{N}}$, there exists a convergent subsequence $(\mathbf{x}_{k_i})_{i \geq 1}$ of the \mathbf{x}_k , having limit $\mathbf{x} \in \overline{X}$. Then $\psi_{j,n}(\mathbf{x}_{k_i}) \rightarrow \psi_{j,n}(\mathbf{x})$ as $i \rightarrow \infty$, but we also have $\psi_{j,n}(\mathbf{x}_{k_i}) = \mathbf{y}_{k_i} \rightarrow \mathbf{y}$. Hence $\mathbf{y} = \psi_{j,n}(\mathbf{x}) \in \psi_{j,n}(\overline{X})$. Thus $\overline{\psi_{j,n}(X)} \subseteq \psi_{j,n}(\overline{X})$, so equality holds.

(2) Let $\mathbf{x} \in (\circledast_n)_{j=0}^{n-1} \overline{X}_j$. Then for each $1 \leq j \leq n$, $\psi_{i,n}(\mathbf{x}) \in \overline{X}_j$, and so there is a sequence $(\mathbf{x}_{j,k})_{k \geq 1}$ in X_j converging to each $\psi_{j,n}(\mathbf{x})$. Since there are only n of these sequences, the convergence is uniform across all of them, and so $((\circledast_n)_{j=0}^{n-1} \mathbf{x}_{j,k})_{k \geq 1}$ converges to $(\circledast_n)_{j=0}^{n-1} \psi_{j,n}(\mathbf{x}) = \mathbf{x}$. But each of the $(\circledast_n)_{j=0}^{n-1} \mathbf{x}_{j,k}$ is in $(\circledast_n)_{j=0}^{n-1} X_j$. Hence $\mathbf{x} \in \overline{(\circledast_n)_{j=0}^{n-1} X_j}$. This gives us $(\circledast_n)_{j=0}^{n-1} \overline{X}_j \subseteq \overline{(\circledast_n)_{j=0}^{n-1} X_j}$. For the opposite inclusion, let $\mathbf{x} \in \overline{(\circledast_n)_{j=0}^{n-1} X_j}$. Then there is a sequence $(\mathbf{x}_k)_{k \geq 1}$ in $(\circledast_n)_{j=0}^{n-1} X_j$ converging to \mathbf{x} . Each \mathbf{x}_k therefore has $\psi_{j,n}(\mathbf{x}_k) \in X_j$ for $0 \leq j \leq n-1$. By compactness of \overline{X}_0 , there must be a subsequence of the k along which $\psi_{0,n}(\mathbf{x}_k)$ converges to some $\mathbf{y}_0 \in \overline{X}_0$, a subsequence of this subsequence along which $\psi_{1,n}(\mathbf{x}_k)$ converges to some $\mathbf{y}_1 \in \overline{X}_1$, and so on. We ultimately obtain a subsequence along which $\psi_{j,n}(\mathbf{x}_k)$ converges to some $\mathbf{y}_j \in \overline{X}_j$ for all $0 \leq j \leq n-1$. Along this subsequence, $\mathbf{x}_k = (\circledast_n)_{j=0}^{n-1} \psi_{j,n}(\mathbf{x}_k)$ converges to $(\circledast_n)_{j=0}^{n-1} \mathbf{y}_j$. Since \mathbf{x}_k converges to \mathbf{x} , we have $\mathbf{x} = (\circledast_n)_{j=0}^{n-1} \mathbf{y}_j \in (\circledast_n)_{j=0}^{n-1} \overline{X}_j$. Hence $\overline{(\circledast_n)_{j=0}^{n-1} X_j} \subseteq \overline{(\circledast_n)_{j=0}^{n-1} \overline{X}_j}$, and equality holds.

(3) This follows from the first two parts and the definition of the n -fold interleaving closure operation.

(4) Given $\mathbf{y} \in S\overline{X}$, we have $\mathbf{y} = S\mathbf{x}$ for some $\mathbf{x} \in \overline{X}$, and there is a sequence $(\mathbf{x}_k)_{k \geq 1}$ in X converging to \mathbf{x} . Then the sequence $\mathbf{y}_k := S\mathbf{x}_k \in SX$ converges to \mathbf{y} , so $\mathbf{y} \in \overline{SX}$, and we have $S\overline{X} \subseteq \overline{SX}$. Take now $\mathbf{y} \in \overline{SX}$, and $\mathbf{y}_k \in SX$ converging to \mathbf{y} . By definition of SX there exists $\mathbf{x}_k \in X$ with $S\mathbf{x}_k = \mathbf{y}_k$. Since the alphabet \mathcal{A} is finite, infinitely many of the \mathbf{x}_k have a fixed letter a_0 as initial symbol. These define a subsequence $(\mathbf{x}_{k_i})_{i \geq 1}$ that converges to a limit word $\mathbf{x} \in \overline{X}$, and necessarily $S\mathbf{x} = \mathbf{y}$. Thus $\overline{SX} \subseteq S\overline{X}$. \square

5. Interleaving factorizations and divisibility

We classify the possible values of n in n -fold interleaving factorizations for different n of arbitrary subsets $X \subseteq \mathcal{A}^{\mathbb{N}}$.

5.1. Divisibility for interleaving factorizations

Theorem 5.1 (*Divisibility structure for interleaving factorizations*). *For a set X let $\mathcal{N}(X) = \{n : X = X^{[n]}\}$.*

(1) *If $n \in \mathcal{N}(X)$ and d divides n , then $d \in \mathcal{N}(X)$.*

(2) *If $m, n \in \mathcal{N}(X)$ then their least common multiple $\text{lcm}(m, n) \in \mathcal{N}(X)$.*

(3) *The interleaving closure set $\mathcal{N}(X)$ of X has the structure of a distributive lattice with respect to the divisibility partial order, being closed under the join operation (least common multiple lcm), and the meet operation (greatest common divisor (gcd)). It is downward closed under divisibility, and contains the minimal element 1.*

Proof of Theorem 5.1. (1) If $n \in \mathcal{N}(X)$ then $X = X^{[n]}$. Suppose d divides n , so $n = de$. Now $X \subseteq X^{[d]}$ by the extension property of Theorem 4.2. However $X^{[d]} \subseteq X^{[de]} = X^{[n]}$ by Proposition 4.6 (3). Since $X^{[n]} = X$ we conclude $X^{[d]} = X$, so $d \in \mathcal{N}(X)$.

(2) Suppose $m, n \in \mathcal{N}(X)$, so that $X = X^{[m]}$ and $X = X^{[n]}$. Then

$$X = X^{[n]} = (X^{[m]})^{[n]} = X^{[\text{lcm}(m, n)]}$$

where, reading from the left, the second equality substituted $X^{[m]}$ for X and the last equality is Theorem 2.10. Thus $\text{lcm}(m, n) \in \mathcal{N}(X)$.

(3) The set $\mathcal{N}(X)$ is downward closed under divisibility by (1). If $m, n \in \mathcal{N}(X)$ then $\text{gcd}(m, n) \in \mathcal{N}(X)$ since it divides m . It is closed under the join operation lcm by (2). Thus $\mathcal{N}(X)$ is a sublattice of the distributive lattice of integers \mathbb{N}_+ under divisibility. It always has minimal element 1. \square

A corollary of part (2) says that interleaving factors of infinitely factorizable sets are infinitely factorizable.

Corollary 5.2. *Let X be infinitely factorizable. Then every interleaving factor of X is also infinitely factorizable.*

Proof. Suppose X is infinitely factorizable, and $X = (\circledast_n)_{i=0}^{n-1} X_i$. We show that X_i is infinitely factorizable for each $0 \leq i \leq n - 1$. Since X has an m -fold interleaving factorization for infinitely many m , Theorem 2.12 (2) implies that X has an $\text{lcm}(m, n)$ -fold interleaving factorization for infinitely many m . Thus, X has an ne -fold interleaving factorization for infinitely many e . Moreover, for each such e , if $X = (\circledast_{ne})_{k=0}^{ne-1}$,

then the shuffle identities of Theorem 2.9, combined with uniqueness of n -fold interleaving factorizations, imply that each X_i has the e -fold interleaving factorization $X_i = (\circledast_e)_{j=0}^{e-1} Y_{i+jn}$. \square

5.2. Structure of interleaving factorizations

Theorem 5.3 (*Converse divisibility structure for interleaving factorizations*). *Let $N \subseteq \mathbb{N}^+$ be a nonempty set with the following properties:*

- (1) *If $n \in N$ and d divides n , then $d \in N$.*
- (2) *If $m, n \in N$, then $\text{lcm}(m, n) \in N$.*

If the alphabet \mathcal{A} has at least two letters, then $N = \mathcal{N}(X)$ for some $X \subseteq \mathcal{A}^{\mathbb{N}}$.

Proof. Given a set N satisfying (1), (2) we construct a set \tilde{X} on $\mathcal{A} = \{0, 1\}$ with $\mathcal{N}(\tilde{X}) = N$. Enumerate the elements of N as n_1, n_2, \dots . Let $\ell_1 = n_1$, and for $i > 1$, let $\ell_i = \text{lcm}(n_1, \dots, n_i)$. Notice for $i \leq j$, that $\ell_j = \text{lcm}(\ell_i, \ell_j)$, hence for any set $X \subseteq \mathcal{A}^{\mathbb{N}}$ we have $X^{[\ell_i]} \subseteq (X^{[\ell_i]})^{[\ell_j]} = X^{[\text{lcm}(\ell_i, \ell_j)]} = X^{[\ell_j]}$, using Theorem 2.10. Thus, $(X^{[\ell_j]})_j$ is an increasing sequence of sets.

Choose $X = \{0^\infty, 1^\infty\}$. Notice that for any $n \in \mathbb{N}$, $X^{[n]}$ is precisely the set of all sequences in \mathcal{A} that are periodic with period dividing n . Now set $\tilde{X} := \lim_{j \rightarrow \infty} X^{[\ell_j]} = \bigcup_{j=1}^{\infty} X^{[\ell_j]}$, so that \tilde{X} is the set of sequences in \mathcal{A} that are periodic and have a period $p \in N$ (since N is precisely the set $\{n : n|\ell_j \text{ for some } j \geq 1\}$).

Claim. $N = \mathcal{N}(\tilde{X})$.

(1) We show that if $n \in N$, then $\tilde{X}^{[n]} = \tilde{X}$. We already know $\tilde{X} \subseteq \tilde{X}^{[n]}$. Let $\mathbf{x} \in \tilde{X}^{[n]}$. Then $\mathbf{x} = (\circledast_n)_{i=0}^{n-1} \mathbf{x}_i$ for $\mathbf{x}_1, \dots, \mathbf{x}_n \in \tilde{X}$. Since there are finitely many of these \mathbf{x}_i , there is an ℓ_j large enough that $\mathbf{x}_1, \dots, \mathbf{x}_n \in X^{[\ell_j]}$. Choose ℓ_j with j large enough that $n|\ell_j$. Then $\text{lcm}(n, \ell_j) = \ell_j$, so $X^{[\ell_j]}$ is closed under n -fold interleaving, and thus $\mathbf{x} \in X^{[\ell_j]} \subseteq \tilde{X}$. Hence $\tilde{X}^{[n]} = \tilde{X}$, and so $n \in \mathcal{N}(\tilde{X})$.

(2) We show that if $n \notin N$, then $\tilde{X}^{[n]} \neq \tilde{X}$. Since $X \subseteq \tilde{X}$, we have $X^{[n]} \subseteq \tilde{X}^{[n]}$ by the extension property in Theorem 4.2. Let \mathbf{x} be any sequence in \mathcal{A} that is periodic with period n . Then $\mathbf{x} \in X^{[n]}$, and so $\mathbf{x} \in \tilde{X}^{[n]}$. However, for any ℓ_j we have $\ell_j \in N$ by the structure of N , and since M is closed under divisibility, $n \notin N$ implies n does not divide ℓ_j ; hence $\mathbf{x} \notin X^{[\ell_j]}$. Since this is the case for all ℓ_j , $\mathbf{x} \notin \tilde{X}$, and so $n \notin \mathcal{N}(\tilde{X})$. \square

Remark 5.4. The sets \tilde{X} constructed in the proof of Theorem 5.3 are all shift-invariant: $S\tilde{X} = \tilde{X}$. To show this, we note that a word \mathbf{x} on alphabet $\mathcal{A} = \{0, 1\}$ is in \tilde{X} if and only if it is fully periodic with a minimal period p belonging to $N \subseteq \mathbb{N}^+$, since N is downward closed under divisibility. The word $S\mathbf{x}$ is also periodic with the same period, so $S\mathbf{x} \in \tilde{X}$, hence $S\tilde{X} \subseteq \tilde{X}$. Since $S^p\mathbf{x} = \mathbf{x}$, we have $\mathbf{y} = S^{p-1}\mathbf{x}$ is periodic with the same period, so $\mathbf{y} \in \tilde{X}$, and $S\mathbf{y} = S^p\mathbf{x} = \mathbf{x} \in S\tilde{X}$. It follows that $S\tilde{X} = \tilde{X}$.

5.3. Divisibility for self-interleaving factorizations

Definition 5.5. An n -fold interleaving factorization $X = (\circledast_n)_{i=0}^{n-1} X_{i,n}$ is *self-interleaving* (or n -fold *self-interleaving*), if all factors are identical, i.e. $X_{i,n} = X_{0,n}$ holds for $1 \leq i \leq n-1$. We sometimes write $Z_n := X_{0,n}$ for the unique factor in this case.

There exist many sets X for which every interleaving factorization is a self-interleaving. We will show later, in Proposition 8.2, that if X is shift-invariant, then $X = X^{[n]}$ implies, letting $X_{i,n} := \psi_{i,n}(X)$, that $X_{0,n} = X_{i,n}$ holds for all $i \geq 1$. In addition there exist examples with X having an n -fold self-interleaving, so that $X_{0,n} = X_{i,n}$ for $0 \leq i \leq n-1$, but with $X_{0,n} \neq X_{i,n}$ for all $i \geq n$; see Example 5.7. The latter sets X can have a mixture of self-interleaving factorizations and non-self interleaving factorizations.

We show that the set of values of n for which a given X has an n -self-interleaving has divisibility properties parallel to those described in Theorem 2.12.

Theorem 5.6 (Structure of self-interleaving closure sets). *Let $\mathcal{N}_{\text{self}}(X) = \{n \geq 1 : X = (\circledast_n)_{i=0}^{n-1} Z_n \text{ for some } Z_n \subseteq \mathcal{A}^{\mathbb{N}}\}$. Then $\mathcal{N}_{\text{self}}(X)$ is nonempty and has the following properties.*

- (1) *If $n \in \mathcal{N}_{\text{self}}(X)$ and d divides n , then $d \in \mathcal{N}_{\text{self}}(X)$.*
- (2) *If $m, n \in \mathcal{N}_{\text{self}}(X)$ then their least common multiple $\text{lcm}(m, n) \in \mathcal{N}_{\text{self}}(X)$.*

Conversely, if a subset $N \subseteq \mathbb{N}^+$ is nonempty and has properties (1) and (2), then there exists $X \subseteq \mathcal{A}^{\mathbb{N}}$ with $N = \mathcal{N}(X)$.

Proof. (1) If d divides n we have $n = de$ and now $X = (\circledast_n)_{k=0}^{de-1} Z_n$ and $Z_n = \psi_{k,de}(X)$ for $0 \leq k \leq de-1$. By the shuffle product identities in Theorem 2.9,

$$X = (\circledast_d)_{i=0}^{d-1} ((\circledast_e)_{j=0}^{e-1} (X_{jd+i})) = (\circledast_d)_{i=0}^{d-1} ((\circledast_e)_{j=0}^{e-1} Z_n).$$

We deduce $X = (\circledast_d)_{i=0}^{d-1} Z_d$ where $Z_d = (\circledast_e)_{j=0}^{e-1} Z_n$, so X has a d -fold self-interleaving.

(2) Suppose that X has both an n -fold and an m -fold self-interleaving factorization. We wish to show it has an $\text{lcm}(m, n)$ -fold self-interleaving factorization. Let $d = \text{gcd}(m, n)$, and recall that there exist e, f with $e|m, f|n$ having $d = ef$ and $\text{gcd}(\frac{m}{e}, \frac{n}{f}) = 1$ (shown in the proof of Theorem 2.10). By (1) the set of self-interleaving factorizations is downward closed under divisibility, so that it has an $\frac{m}{e}$ -fold self-interleaving factorization and an $\frac{n}{f}$ -fold self-interleaving factorization, and now $\text{lcm}(\frac{m}{e}, \frac{n}{f}) = \frac{mn}{ef} = \frac{mn}{d} = \text{lcm}(m, n)$. We have therefore reduced proving (2) to proving it in the special case where $\text{gcd}(m, n) = 1$, with $\text{lcm}(m, n) = mn$.

In this case we are given that X has an m -fold and an n -fold self-interleaving factorization. We now have $\text{gcd}(m, n) = 1$ so by Theorem 2.12 we have an mn -fold interleaving factorization $X = (\circledast_{mn})_{k=0}^{mn-1} X_{k,mn}$. We wish to show it is self-interleaving, i.e. that

$$X_{k_1,mn} = X_{k_2,mn} \quad \text{for } 0 \leq k_1 < k_2 \leq mn-1. \quad (5.1)$$

We assert that for each $0 \leq i \leq n - 1$,

$$X_{j_1+im,mn} = X_{j_2+im,mn} \quad \text{for } 0 \leq j_1 < j_2 \leq m - 1. \quad (5.2)$$

To see this, note that by the shuffle identities in Theorem 2.9,

$$(\circledast_{mn})_{k=0}^{mn-1} X_{k,mn} = (\circledast_m)_{j=0}^{m-1} \left((\circledast_n)_{i=0}^{n-1} X_{j+im,mn} \right).$$

Since m -fold factorizations are unique, the right-hand side is a self-interleaving factorization, so for all $0 \leq j_1 < j_2 \leq m - 1$, $(\circledast_n)_{i=0}^{n-1} X_{j_1+im,mn} = (\circledast_n)_{i=0}^{n-1} X_{j_2+im,mn}$. This implies, again by uniqueness, that $X_{j_1+im,mn} = X_{j_2+im,mn}$ for all $0 \leq i \leq n - 1$.

Similarly, using the shuffle identity with the n -fold interleaving on the outside and the m -fold interleaving on the inside, we obtain for $0 \leq i_1 < i_2 \leq n - 1$ that for each $0 \leq j \leq m - 1$,

$$X_{i_1+jn,mn} = X_{i_2+jn,mn} \quad \text{for } 0 \leq i_1 < i_2 \leq n - 1. \quad (5.3)$$

Now we assert that when $\gcd(m, n) = 1$ that (5.2) and (5.3) imply (5.1). For each $0 \leq i \leq n - 1$, (5.2) implies the equality of all $X_{k,mn}$ for k within blocks $B_i = \{j + im : 0 \leq j \leq m - 1\}$, but (5.2) says nothing about equalities across different blocks B_i . On the other hand, for fixed $0 \leq j \leq m - 1$, (5.3) implies the equality of all $X_{k,mn}$ for k within blocks $C_j = \{k = i + jn : 0 \leq i \leq n - 1\}$. Now let $0 \leq k \leq mn - 2$. If k and $k + 1$ are not in the same block B_i , then $k + 1 \equiv 0 \pmod{m}$. Similarly, if k and $k + 1$ are not in the same block C_j , then $k + 1 \equiv 0 \pmod{m}$. Now the condition $\gcd(m, n) = 1$ implies that, since $0 \leq k \leq mn - 2$, $k + 1$ cannot be equal to 0 modulo m and n at the same time. Therefore, k and $k + 1$ are both in one of the blocks B_i or C_j , and $X_{k,mn} = X_{k+1,mn}$. It follows that all the $X_{k,mn}$ are equal as k ranges from 0 to $mn - 1$, so the factorization $X = (\circledast_{mn})_{k=0}^{mn-1}$ is a self-interleaving.

For the converse, it remains to show that if a subset $N \subseteq \mathbb{N}^+$ is nonempty and has properties (1) and (2), then there exists $X \subseteq \mathcal{A}^{\mathbb{N}}$ with $N = \mathcal{N}_{self}(X)$. For this, we use the fact that the sequences \tilde{X} constructed in Theorem 5.3, that achieve $N = \mathcal{N}(\tilde{X})$ are shift-invariant, see Remark 5.4. Now Proposition 8.2 (which will be proved in Section 8) asserts that any shift-invariant X has the property that all of its interleaving factorizations will be self-interleaving factorizations. Thus, $\mathcal{N}(\tilde{X}) = \mathcal{N}_{self}(\tilde{X})$. We have already shown in the proof of Theorem 5.3 that $\mathcal{N}(\tilde{X}) = N$. \square

Example 5.7. For a general set X , the set of n giving a self-interleaving factorization can be a strict subset of all interleaving factorizations of X . Let $\mathcal{A} = \{0, 1\}$, and take $X = \{00\{0, 1\}^{\mathbb{N}}\}$ (i.e., all infinite words beginning with 00). Set $X_{j,n} = \psi_{j,n}(X)$.

We show X has an n -fold interleaving factorization for all $n \geq 1$, so $\mathcal{N}(X) = \mathbb{N}_+$. In contrast we show $\mathcal{N}_{self} = \{1, 2\}$ is finite. For $n = 1$ and $n = 2$ the factorization is self-interleaving with $X_{0,2} = X_{1,2} = \{0\{0, 1\}^{\mathbb{N}}\}$. (Note that for $j \geq 2$ one has $X_{j,2} =$

$\{0, 1\}^{\mathbb{N}}$.) For $n \geq 3$ it has the interleaving factorization $X_{0,n} = X_{1,n} = \{0\{0, 1\}^{\mathbb{N}}\}$, while $X_{j,n} = \{0, 1\}^{\mathbb{N}}$ is the full shift for all $j \geq 2$, so that it is not self-interleaving.

6. Infinitely factorizable closed subsets of $\mathcal{A}^{\mathbb{N}}$

Definition 6.1. A subset $X \subseteq \mathcal{A}^{\mathbb{N}}$ is *infinitely factorizable* (under interleaving) if it has an n -fold interleaving factorization

$$X = X^{[n]} = \psi_{0,n}(X) \circledast \psi_{1,n}(X) \circledast \cdots \circledast \psi_{n-1,n}(X)$$

for infinitely many $n \geq 1$.

6.1. Characterization of infinitely factorizable closed sets

We now characterize infinitely factorizable closed sets X by the properties given in Theorem 2.13. Property (iii) shows there are uncountably many different infinitely factorizable closed sets when the alphabet size $|\mathcal{A}| \geq 2$.

Proof of Theorem 2.13. We prove $(iii) \Rightarrow (ii) \Rightarrow (i) \Rightarrow (iii)$.

$(iii) \Rightarrow (ii)$. Suppose property (iii) holds, and let $n \geq 1$. Then, using Proposition 4.1(2), we have, writing $\mathbf{x} = x_0 x_1 x_2 \cdots$,

$$\begin{aligned} X &= \{\mathbf{x} \in \mathcal{A}^{\mathbb{N}} : x_k \in \mathcal{A}_k \text{ for all } k \geq 0\} \\ &= \{\mathbf{x} \in \mathcal{A}^{\mathbb{N}} : x_{j+kn} \in \mathcal{A}_{j+kn} \text{ for all } k \geq 0, 0 \leq j \leq n-1\} \\ &= \{\mathbf{x} \in \mathcal{A}^{\mathbb{N}} : \psi_{j,n}(\mathbf{x}) \in \prod_{k=0}^{\infty} \mathcal{A}_{j+kn} \text{ for all } 0 \leq j \leq n-1\} \\ &= (\circledast_n)_{j=0}^{n-1} \prod_{k=0}^{\infty} \mathcal{A}_{j+kn}, \end{aligned}$$

which is an n -fold interleaving factorization.

$(ii) \Rightarrow (i)$. Immediate.

$(i) \Rightarrow (iii)$. We prove the contrapositive. Suppose property (iii) does not hold for X , we are to show property (i) does not hold. Let \mathcal{A}_k denote the letters that occur in the k th position of some word in X ; it is a finite nonempty subset of the (finite) alphabet \mathcal{A} . If for each $k \geq 0, \ell \geq 1$ all letter patterns in positions k through $k + \ell$ in $\mathcal{A}_k \times \mathcal{A}_{k+1} \times \cdots \times \mathcal{A}_{k+\ell}$ may occur in X , then by the assumption X is closed, we would have $X = \prod_{k=0}^{\infty} \mathcal{A}_k$ which has property (iii), contradicting our assumption. Therefore there must exist some finite $k \geq 0, \ell \geq 1$ and a finite set of consecutive $\mathcal{A}_k, \mathcal{A}_{k+1}, \mathcal{A}_{k+2}, \dots, \mathcal{A}_{k+\ell}$ such that there is a block $a_k a_{k+1} \cdots a_{k+\ell}$ with each $a_{k+i} \in \mathcal{A}_{k+i}$ for $0 \leq i \leq \ell$ that does not occur in positions k through $k + \ell$ in any element of X . We call this situation a (k, ℓ) -missing-configuration.

If property (i) were to hold for X , then there would exist some $n \geq k + \ell + 1$ such that X has an n -fold interleaving factorization

$$X = \psi_{0,n}(X) \circledast \psi_{1,n}(X) \circledast \cdots \circledast \psi_{n-1,n}(X).$$

Each word $\mathbf{x} \in X$ has symbol x_{k+i} in position $k + i$ lying as the first symbol in a word in the n -decimation set $\psi_{k+i,n}(X)$. We can find an infinite word, call it $\mathbf{w}(k+i) \in X$ that has the symbol $a_i \in \mathcal{A}$ in position $k + i$ for each $0 \leq i \leq \ell$ (by definition of \mathcal{A}_{k+i}). For all remaining positions, $0 \leq j \leq n - 1$, with $j \notin \{k, k + 1, \dots, k + \ell\}$ we pick a word $\mathbf{w}(j) \in X$ arbitrarily.

Now the symbol sequence $\mathbf{w} := \circledast_{j=0}^{n-1} \psi_{j,n}(\mathbf{w}(j)) \in \psi_{0,n}(X) \circledast \psi_{1,n}(X) \circledast \cdots \circledast \psi_{n-1,n}(X)$ belongs to X , but it contains the forbidden block $a_k a_{k+1} \cdots a_{k+\ell}$ in positions k through $k + \ell$, showing that $\mathbf{w} \notin X$, the desired contradiction. \square

Remark 6.2. An important finiteness feature of the proof of Theorem 2.13 is that it shows that the existence of a (k, ℓ) -missing-configuration certifies that X has no n -fold interleaving factorization with $n \geq k + \ell + 1$ when X is closed.

The following example shows the hypothesis of X being a closed set is necessary in the statement of Theorem 2.13.

Example 6.3 (*Non-closed infinitely factorizable sets*). Let X be the countable subset of $\mathcal{A}^{\mathbb{N}}$ consisting of all infinite sequences having a finite number of 1's. Then X is infinitely factorizable, and all decimations $\psi_{j,n}(X) = X$ are copies of itself. It is not a closed set; its closure in $\mathcal{A}^{\mathbb{N}}$ is the full one-sided shift. It satisfies properties (i) and (ii) of Theorem 2.13 but fails to satisfy property (iii). (The set X can be viewed as the set of terminating binary expansions of all nonnegative dyadic rationals $\frac{k}{2^m}$.)

The construction of Theorem 5.3 produces infinitely factorizable X having $\mathcal{N}(X) \subsetneq \mathbb{N}^+$. Such sets satisfy property (i), and do not satisfy properties (ii), (iii) of Theorem 2.13.

6.2. Consequences of infinite factorizability

Corollary 6.4. *Let X be an infinitely factorizable closed subset of $\mathcal{A}^{\mathbb{N}}$. Then its factor set $\mathfrak{F}(X)$ consists of all decimations $\psi_{j,n}(X)$ for $n \geq 1$ and $0 \leq j \leq n - 1$. Each decimated set $\psi_{j,n}(X)$ is also infinitely factorizable.*

Proof. By property (ii) of Theorem 2.13 X is factorizable for each $n \geq 1$, and its n -fold factors are $\psi_{j,n}(X)$ for $0 \leq j \leq n - 1$. Now the property (iii) is preserved under decimations of all orders, hence all $\psi_{j,n}(X)$ must be infinitely factorizable. \square

Example 6.5 (*Infinitely factorizable closed subsets X of $\mathcal{A}^{\mathbb{N}}$ having all decimations $\psi_{j,n}(X)$ distinct*). For $\mathcal{A} = \{0, 1\}$ define $\mathcal{A}_k \subset \mathcal{A}$ for $0 \leq k < \infty$ as follows. Let $\mathcal{A}_k = \{0\}$ for all indices $k \in \mathcal{A}$ with

$$A := \{k \geq 0 : 0 \leq \{k\sqrt{2}\} < \frac{1}{2}\} \quad \text{where} \quad \{x\} = x - \lfloor x \rfloor.$$

(No special properties other than irrationality of $\sqrt{2}$ are used.) This set of indices is aperiodic (and has natural density $\frac{1}{2}$, using Weyl's equidistribution theorem). Set $\mathcal{A}_k = \{0, 1\}$ for all other integers $k \notin A$, which is also an aperiodic set of natural density $\frac{1}{2}$.

Set $X = \prod_{k=0}^{\infty} \mathcal{A}_k$. By Theorem 2.13, property (iii), it is a closed set and is infinitely factorizable, i.e., $\mathcal{N}(X) = \mathbb{N}_+$. Each decimation $\psi_{j,n}(X)$ is also an infinite product space of the same kind whose set of indices k that have reduced alphabet $\{0\}$ is exactly

$$A(j, n) := \{k \geq 0 : 0 \leq \{(nk + j)\sqrt{2}\} < \frac{1}{2}\}.$$

Each $\psi_{j,n}(X)$ is closed and infinitely factorizable. Consider now two distinct decimations $\psi_{j,n}(X)$ and $\psi_{\ell,m}(X)$, where we may suppose $1 \leq n \leq m$ and $0 \leq j, \ell < \infty$, with $j \neq \ell$ if $n = m$. To show distinctness we must show $A(j, n) \neq A(\ell, m)$. We use the well known fact that for each $n \geq 1$ the sequence of fractional parts $x_k = \{k(n\sqrt{2})\}$ ($k \geq 1$) is dense modulo 1. (In fact, since $n\sqrt{2}$ is irrational, Weyl's theorem implies that the sequence x_k is uniformly distributed modulo 1.) The argument has two cases.

Case 1. $n = m$. We write $x_k := \{(kn + j)\sqrt{2}\}$, and $y_k := \{(kn + \ell)\sqrt{2}\}$, where $j \neq \ell$. Now $y_k = \{x_k + \theta\}$ for all k , where $\theta = \{(\ell - j)\sqrt{2}\}$. Because $\sqrt{2}$ is irrational, $\theta \in (0, 1)$; hence there must be an open interval $(a, b) \subset [0, \frac{1}{2})$ such that $(a + \theta, b + \theta) \subset (\frac{1}{2}, 1]$. Since x_k takes values dense in $(0, 1)$, we will have infinitely many k with $x_k \in (a, b)$, and thus with $y_k \in (a + \theta, b + \theta)$. Therefore, there are infinitely many k with $x_k \in [0, \frac{1}{2})$ and $y_k \in (\frac{1}{2}, 1]$. For these k , $\mathcal{A}_{kn+j} = \{0\}$, while $\mathcal{A}_{kn+\ell} = \{0, 1\}$, so all sequences in $\psi_{j,n}(X)$ must have k th symbol 0, while $\psi_{n,\ell}(X)$ has sequences with k th symbol taking both values 0 or 1 (i.e., $k \in A(j, n)$ but $k \notin A(\ell, n)$ for these k). Thus $\psi_{j,n}(X) \neq \psi_{\ell,n}(X)$.

Case 2. $n < m$. We write $x_k := \{(nk + j)\sqrt{2}\}$ and $y_k := \{(mk + \ell)\sqrt{2}\}$. A calculation shows that $y_k = \{\frac{m}{n}x_k + \theta\}$, where $\theta = \{(\ell - \frac{jm}{n})\sqrt{2}\}$. Again, $\theta \in (0, 1)$. There is an open interval $(c, d) \subset (\frac{1}{2}, 1]$ such that $(c - \theta, d - \theta) \subset (0, \frac{1}{2})$. Letting $(a, b) = \frac{n}{m}(c - \theta, d - \theta)$, we see that if $x_k \in (a, b)$, then $y_k \in (c, d)$. Again, by positive density of x_k , this happens infinitely often, and so there are infinitely many k with $x_k \in [0, \frac{1}{2})$ and $y_k \in (\frac{1}{2}, 1]$. We conclude as in Case 1 that $\psi_{j,n}(X) \neq \psi_{\ell,m}(X)$.

We conclude that the interleaving factor set $\mathfrak{F}(X)$ consists of all principal decimations, and they are all distinct. Therefore $\mathfrak{F}(X)$ is infinite.

Example 6.6. (A closed X with an infinite factor set $\mathfrak{F}(X)$) The set X constructed in Example 6.5 has infinitely many distinct decimations so its decimation set $\mathfrak{D}(X)$ and its principal decimation set $\mathfrak{D}_{prin}(X)$ are infinite. In addition all principal decimations are interleaving factors, so that its factor set $\mathfrak{F}(X)$ is also infinite.

Corollary 6.7. *The set $\mathcal{Y}(\mathcal{A})$ of all infinitely factorizable closed subsets $X \subseteq \mathcal{A}^{\mathbb{N}}$ is closed under n -fold interleaving operations of all $n \geq 1$. That is, if $X_0, X_1, \dots, X_{n-1} \in \mathcal{Y}(\mathcal{A})$, then $(\circledast_n)_{i=0}^{n-1} X_i = X_0 \circledast X_1 \circledast \dots \circledast X_{n-1} \in \mathcal{Y}(\mathcal{A})$.*

Proof. The corollary follows using the characterization of membership in $\mathcal{Y}(\mathcal{A})$ by property (iii) of Theorem 2.13. Property (iii) is inherited under n -fold interleaving of sets X_i that have it. \square

7. Iterated interleaving factorizations of general closed subsets of $\mathcal{A}^{\mathbb{N}}$

We consider iterated interleaving factorizations for general sets $X \subseteq \mathcal{A}^{\mathbb{N}}$. If a set X factors as $X = X_0 \circledast \cdots \circledast X_{n-1}$, it is possible that one or more of the factors X_j can itself be factored. However, unlike with factorizations of positive integers, for example, the further factors that appear at lower levels may not be interleaving factors of the original set X . We therefore name them *iterated interleaving factors*. We define an *iterated interleaving factorization* as follows: The iterated interleaving factorization of depth 0 of a set X is the equation $X = X$ (or the right hand side of such an equation). An iterated interleaving factorization of depth 1 is a single n -fold factorization $X = (Y_0 \circledast Y_1 \circledast \cdots \circledast Y_{n-1})$ (with parentheses). The Y_i are iterated interleaving factors of depth 1. An *iterated interleaving factorization of depth k* is obtained recursively from an iterated interleaving factorization of depth $k-1$, with one or more finitely factorizable sets Y on the right hand side of depth k being replaced by interleaving factorizations $Y = (Y_0 \circledast Y_1 \circledast \cdots \circledast Y_{n-1})$ (with parentheses), for $n \geq 2$ (allowing different n for different Y). The new added internal factors on the right are assigned depth $k+1$; they are inside a nested set of $k+1$ parentheses.

7.1. Iterated interleaving factorization trees

An iterated interleaving factorization can be visually represented by a rooted tree, as pictured in Fig. 7.1 below. It has root node X , leaf nodes corresponding to the factors in the iterated interleaving factorization, and internal nodes corresponding to intermediate factors.

In our definition of iterated interleaving factorizations, each step is a finite factorization. If an iterated interleaving factor Y at level k has n -fold interleaving factorizations for multiple values of n , it is natural to choose the n -fold factorization with the largest n because this factorization refines all the other possible factorizations of Y , by the divisibility properties of $\mathcal{N}(X)$ from Theorem 2.12.

How should one treat infinitely factorizable factors? We will adopt the convention in this factorization process that we “freeze” any infinitely factorizable factors encountered, and do not further factorize them. We do this for two reasons. First, for infinitely factorizable Y , no natural choice of n exists for a n -factorization at the next level. Secondly, all interleaving factors of infinitely factorizable sets are also infinitely factorizable by Corollary 5.2, so the factorization process would necessarily proceed forever if we did not freeze any infinitely factorizable factors.

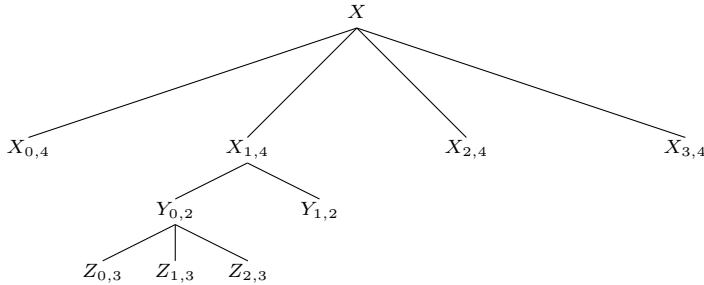


Fig. 7.1. Iterated interleaving tree for $X = (X_{0,4} \circledast ((Z_{0,3} \circledast Z_{1,3} \circledast Z_{2,3}) \circledast Y_{1,2}) \circledast X_{2,4} \circledast X_{3,4})$, an iterated interleaving factorization of depth 3.

This raises the question: If one factorizes only finitely factorizable sets, will the iterated interleaving factorization process always terminate at a finite depth? We show below that the answer is: there are closed X where the iteration process can go on forever.

7.2. Arbitrary depth factorizations

We show, by construction, that there exist closed sets X having iterated interleaving factorizations of all depths $k \geq 1$, with all factors at all depths being finitely factorizable. (Thus the “freezing” property is never needed.)

Theorem 7.1 (*Infinite depth interleaving factorizations*). *There exist uncountably many closed sets $Z_I \subseteq \mathcal{A}^{\mathbb{N}}$ with $\mathcal{A} = \{0, 1\}$, indexed by $I \in \mathcal{A}^{\mathbb{N}}$, that possess iterated interleaving factorizations of every depth $k \geq 1$. They each have a unique iterated interleaving factorization of depth k , for all $k \geq 1$. Each Z_I has an interleaving factor set $\mathfrak{F}(Z_I)$ containing at most three elements. There exist such I for which the principal decimation set $\mathfrak{D}_{\text{prin}}(Z_I)$ is infinite.*

Proof. Let X_0 and X_1 be two distinct closed sets in $\mathcal{A}^{\mathbb{N}}$ having trivial interleaving set $\mathcal{N}(X_0) = \mathcal{N}(X_1) = \{1\}$. For definiteness consider $X_0 = X_F$ the *Fibonacci shift*, consisting of all words which do not have two consecutive 1’s, and $X_2 = X_{\text{AF}}$ the *anti-Fibonacci shift*, which consists of all one-sided infinite words which do not contain two consecutive 0’s. Example 2.7 showed X_F has no n -fold interleaving factorizations for $n \geq 2$, and the proof applies to X_{AF} . Given an index set $I = i_0 i_1 i_2 \cdots \in \mathcal{A}^{\mathbb{N}}$, we define a set

$$Z_I = \{\mathbf{z} \in \mathcal{A}^{\mathbb{N}} : \psi_{2^r-1, 2^{r+1}}(\mathbf{z}) \in X_{i_r} \quad \text{for } r \geq 0\}. \quad (7.1)$$

Let $\mathbf{z} = z_0 z_1 z_2 \cdots$. The decimations determine the values of z_i for subscripts in arithmetic progressions. We represent an arithmetic progression as $\text{AP}(a; d) = \{n \geq 0 : n \equiv a \pmod{d}\}$. Then the values \mathbf{z}_i for $i \in \text{AP}(2^r - 1; 2^{r+1})$ are restricted by $\psi_{2^r-1, 2^{r+1}}(\mathbf{z}) \in X_{i_r}$. We first show that Z_I is well-defined.

Claim 1. *The set of arithmetic progressions $\text{AP}(2^r - 1; 2^{r+1})$ for $r \geq 0$ form a partition of \mathbb{N} .*

We show by induction on $r \geq 0$ that $N_m := \sqcup_{r=0}^m \text{AP}(2^r - 1; 2^{r+1}) = \mathbb{N} \setminus \text{AP}(2^{r+1} - 1; 2^{r+1})$, a disjoint union. The base case $r = 0$ asserts $\text{AP}(0; 2) = \mathbb{N} \setminus \text{AP}(1; 2)$. The induction step uses $\text{AP}(2^{m+1} - 1; 2^{m+1}) = \text{AP}(2^{m+1} - 1; 2^{m+2}) \sqcup \text{AP}(2^{m+2} - 1; 2^{m+2})$. Finally, the set N_m contains the interval $[0, 2^m - 2]$, so the infinite set union covers \mathbb{N} , proving Claim 1.

Claim 2. *If $I \neq J$ then $Z_I \neq Z_J$.*

If $I \neq J$ then some $i_r \neq j_r$. Then $\psi_{2^r-1, 2^{r+1}}(Z_I) = X_{i_r}$ and $\psi_{2^r-1, 2^{r+1}}(Z_J) = X_{j_r}$ which are distinct since $X_1 \neq X_2$. Thus $Z_I \neq Z_J$, proving Claim 2.

Claim 3. *Each Z_I is a closed set in $\mathcal{A}^{\mathbb{N}}$.*

It suffices to show each convergent subsequence of elements of Z_I has a limit in Z_I . Convergence in $\mathcal{A}^{\mathbb{N}}$ is pointwise on each index separately. Suppose $\mathbf{x}_k \rightarrow \mathbf{y}$ in $\mathcal{A}^{\mathbb{N}}$ ($k \in \mathbb{N}$) as $k \rightarrow \infty$ with each $\mathbf{x}_k \in Z_I$. We then have $\psi_{2^r-1, 2^{r+1}}(\mathbf{x}_k) \rightarrow \psi_{2^r-1, 2^{r+1}}(\mathbf{y})$ in $\mathcal{A}^{\mathbb{N}}$. For each $r \geq 0$ we have $\psi_{2^r-1, 2^{r+1}}(\mathbf{x}_k) \in X_{i_r}$, hence $\psi_{2^r-1, 2^{r+1}}(\mathbf{x}_k) \rightarrow \psi_{2^r-1, 2^{r+1}}(\mathbf{y}) \in X_{i_r}$, since X_{i_r} is a closed set. The property $\psi_{2^r-1, 2^{r+1}}(\mathbf{y}) \in X_{i_r}$ for all $r \geq 0$ certifies that $\mathbf{y} \in Z_I$, proving Claim 3.

Claim 4. *Each Z_I has a 2-fold interleaving factorization*

$$Z_I = X_{i_0} \circledast Z_{SI},$$

where $SI = i_1 i_2 i_3 \dots$ denotes the one-sided shift of $I \in \mathcal{A}^{\mathbb{N}}$.

Using Proposition 3.1 we find

$$\psi_{2^r-1, 2^{r+1}}(\mathbf{z}) = \psi_{0,2} \circ \underbrace{\psi_{1,2} \circ \dots \circ \psi_{1,2}}_{r \text{ times}}(\mathbf{z}),$$

and one proves it by induction on $r \geq 0$. Letting $\mathbf{w} = \psi_{1,2}(\mathbf{z})$, we have for $r \geq 1$

$$\psi_{2^r-1, 2^{r+1}}(\mathbf{z}) = \psi_{0,2} \circ \underbrace{\psi_{1,2} \circ \dots \circ \psi_{1,2}}_{r-1 \text{ times}}(\mathbf{w}) = \psi_{2^{r-1}-1, 2^r}(\mathbf{w}). \quad (7.2)$$

By definition

$$Z_{SI} = \{\mathbf{w} \in \mathcal{A}^{\mathbb{N}} : \psi_{2^r-1, 2^{r+1}}(\mathbf{w}) \in X_{i_{r+1}} \text{ for } r \geq 0\}.$$

Now we have, using (7.2),

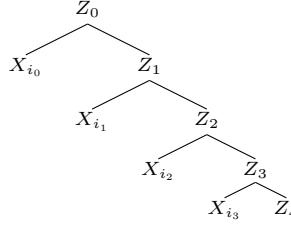


Fig. 7.2. Iterated interleaving tree for $Z_0 = (X_{i_0} \circledast (X_{i_1} \circledast (X_{i_2} \circledast (X_{i_3} \circledast Z_4))))$.

$$\begin{aligned} Z_I &= \{\mathbf{z} \in \mathcal{A}^{\mathbb{N}}; \psi_{0,2}(\mathbf{z}) \in X_{i_0} \text{ and } \mathbf{w} = \psi_{1,2}(\mathbf{z}) \text{ has } \psi_{2r-1,2r+1}(\mathbf{w}) \in X_{i_{r+1}} \text{ for } r \geq 1\} \\ &= \{\mathbf{z} \in \mathcal{A}^{\mathbb{N}} : \psi_{0,2}(\mathbf{z}) \in X_{i_0} \text{ and } \psi_{1,2}(\mathbf{z}) \in Z_{SI}\} = X_{i_0} \circledast Z_{SI}, \end{aligned}$$

proving Claim 4.

At this point we obtain an iterated interleaving factorization for Z_I to arbitrary depth $k \geq 1$, by iterating the factorization given in Claim 4. This can be done since one factor is again of the form Z_I (with a different I). Given I , using the notation $Z_0 := Z_I$ and $Z_k := Z_{S^k I}$ we have the depth k factorization

$$Z_0 = X_{i_0} \circledast (X_{i_1} \circledast (\cdots (X_{i_{k-2}} \circledast (X_{i_{k-1}} \circledast Z_k)) \cdots)).$$

Fig. 7.2 shows a tree corresponding to such an iterated factorization after the fourth level of factoring.

The remaining part of the proof will show this factorization tree is unique at every level k . Finally a suitable choice of I will lead to Z_I having infinitely many different principal decimations.

Claim 5. *The interleaving closure set $\mathcal{N}(Z_I) = \{1, 2\}$ with associated factor set $\mathfrak{F}(Z_I) = \{Z_I, X_{i_0}, Z_{SI}\}$.*

It suffices to show that Z_I has no n -fold interleavings with $n \geq 3$, in view of Claim 4. We argue by contradiction. Given an n -fold interleaving for $n \geq 3$, by Theorem 2.12(2), it would also have an $\text{lcm}(2, n)$ -fold interleaving, and we set $2m := \text{lcm}(2, n)$ with $m \geq 2$. A shuffle identity from Proposition 2.9 gives

$$Z_I = (\circledast_{2m})_{j=0}^{2m-1} X_{i,2m} = \left((\circledast_m)_{i=0}^{m-1} X_{2i,2m} \right) \circledast \left((\circledast_m)_{i=0}^{m-1} X_{2i+1,2m} \right).$$

Since 2-fold interleaving factorizations are unique, and $Z_I = X_{i_0} \circledast Z_{SI}$, we must have

$$X_{i_0} = (\circledast_m)_{i=0}^{m-1} X_{2i,2m}.$$

This contradicts the fact that X_0 and X_1 have no nontrivial interleaving factorizations, proving Claim 5.

Claim 6. For $k \geq 1$, each Z_I has a unique iterated interleaving factorization of depth k , whose iterated interleaving factors are X_{I_r} for $0 \leq r \leq k-1$ and $Z_{S^k}(I)$.

This claim follows by induction on $k \geq 1$, the base case being the factorization in Claim 4. For the induction step from k to $k+1$, all but one of the leaves of the tree (iterated interleaving factors) are of form X_i , which have no non-trivial interleaving factors, and the remaining factor Z_J , with $J = S^k I$, which has only a 2-fold interleaving factorization $Z_{S^k I} = X_{i_k} \circledast Z_{S^{k+1}(I)}$. By updating the list of iterated interleaving factors we complete the induction step. This proves Claim 6.

Claim 7. If I is strongly aperiodic, meaning that all its shifts $S^k I$ for $k \geq 0$ are distinct, then all the decimations of Z_I of form $\psi_{2r-1,2r+1}(Z_I)$ for $r \geq 0$ are distinct. In particular, the principal decimation set $\mathfrak{D}_{\text{prin}}(Z_I)$ of Z_I is an infinite set.

We have $\psi_{2r-1,2r+1}(Z_I) = Z_{S^r I}$. By Claim 2 distinct S^I give distinct $Z_{S^r I}$. The strongly aperiodic assumption then makes all $\psi_{2r-1,2r+1}(Z_I)$ distinct. They are principal decimations, so $\mathfrak{D}_{\text{prin}}(Z_I)$ is infinite. This proves Claim 7. \square

Example 7.2 (A closed set with an infinite principal decimation set but a finite factor set). Theorem 7.1 exhibited Z_I that have infinitely many distinct principal decimations; $\mathfrak{D}_{\text{prin}}(Z_I) \subseteq \mathfrak{D}(Z_I)$. However Claim 5 showed the factor set $\mathfrak{F}(Z_I)$ is always finite.

Remark 7.3. The sets Z_I in Example 7.2 exhibit the failure of two finiteness properties possessed by all path sets studied in [5]. First, interleaving factorizations of path sets \mathcal{P} always halt at finite depth (under the freezing convention), while Z_I never does. Second, path sets \mathcal{P} always have finitely many different decimations, i.e. $\mathfrak{D}(\mathcal{P})$ is finite, while this example does not. Example 6.6 gave another example having infinitely many different decimations.

8. Shift-stable and weakly shift-stable sets

Classical symbolic dynamics is concerned with properties of sets $X \subseteq \mathcal{A}^{\mathbb{N}}$ invariant under the shift operator. The class of such sets is not preserved under decimation or interleaving operations. We study two weaker notions of sets X compatible with the shift operation—*shift-stable sets* and *weakly shift-stable sets*—with better properties. Shift-stable sets naturally arise in one-sided dynamics that encode initial conditions, and we show they are closed under all decimations, but not closed under interleaving operations. The wider class of weakly shift-stable sets is closed under all decimation and interleaving operations.

8.1. Shift-stable sets

Recall from Definition 2.14 that a general set $X \subseteq \mathcal{A}^{\mathbb{N}}$ is *shift-stable* if $SX \subseteq X$, and it is *shift-invariant* if $SX = X$. These definitions allow non-closed sets. Shift-stability is a strictly weaker condition than shift-invariance; see Example 8.5 below.

Shift-stable and shift-invariant sets satisfy the following closure properties under decimation and interleaving closure operations:

Theorem 8.1. *Let \mathcal{A} be finite alphabet and let $X \subseteq \mathcal{A}^{\mathbb{N}}$ be a general set (not necessarily closed).*

- (1) *If X is shift-stable (resp. shift-invariant), then all decimations $\psi_{j,n}(X)$ for $j \geq 0$, $n \geq 1$ are shift stable (resp. shift-invariant).*
- (2) *If X is shift-stable (resp. shift-invariant) then all n -fold interleaving closures $X^{[n]}$ with $n \geq 1$ are shift-stable (resp. shift-invariant).*

Proof. (1) Shift-stability of X implies $S^m X \subseteq S^{m-1} X$ whence $S^m X \subseteq X$ for all $m \geq 0$. Now Proposition 3.2 gives

$$S\psi_{j,n}(X) = \psi_{j,n}(S^n X) \subseteq \psi_{j,n}(X).$$

If X is shift invariant, then $S^m X = X$ for all $m \geq 0$ and equality holds.

- (2) If X is shift stable, then we have, by Proposition 4.10, Proposition 3.2, and (1):

$$\begin{aligned} SX^{[n]} &= S(\psi_{0,n}(X) \circledast \psi_{1,n}(X) \circledast \cdots \circledast \psi_{n-1,n}(X)) \\ &= \psi_{1,n}(X) \circledast \psi_{2,n}(X) \circledast \cdots \circledast \psi_{n,n}(X) \\ &= \psi_{0,n}(SX) \circledast \psi_{1,n}(SX) \circledast \cdots \circledast \psi_{n-1,n}(SX) \\ &\subseteq \psi_{0,n}(X) \circledast \psi_{1,n}(X) \circledast \cdots \circledast \psi_{n-1,n}(X) = X^{[n]}. \end{aligned}$$

If X is shift invariant, then all steps hold with equality, as required. \square

The shift-invariant property restricts the form of interleaving factorizations.

Proposition 8.2 (*Shift invariance implies self-interleaving*). *If a general set $X \subseteq \mathcal{A}^{\mathbb{N}}$ is shift-invariant, then all of its interleaving factorizations will be self-interleaving factorizations.*

Proof. We have for each $n \geq 1$, that for $j \geq 0$

$$\psi_{j+1,n}(X) = \psi_{j,n}(SX) = \psi_{j,n}(X)$$

with the leftmost equality generally true by Proposition 3.1 (2) and the second equality from shift invariance. We now have

$$\psi_{j,n}(X) = \psi_{0,n}(X) \quad \text{for } j \geq 0.$$

But by Theorem 2.8 any n -fold interleaving $X = (\circledast_n)_{i=0}^{n-1} X_{i,n}$ has $X_{i,n} = \psi_{i,n}(X)$, hence it is a self-interleaving with $Z_n = \psi_{0,n}(X)$. \square

8.2. Closed shift-stable sets

An important feature of closed shift-stable sets is that they are characterized by forbidden blocks, paralleling the definition of two-sided shift spaces in [33, Sec. 1.2]. Let \mathcal{A}^* denote the set of all finite words in the alphabet \mathcal{A} , including the empty word. A *block* in an infinite word $\mathbf{x} = a_0a_1a_2\cdots$ is a finite sequence of consecutive symbols $a_k a_{k+1} \cdots a_{k+\ell}$.

Proposition 8.3 (*Forbidden block characterization of shift-stability*). *The following statements about a set $X \subseteq \mathcal{A}^{\mathbb{N}}$ are equivalent:*

- (1) X is closed and shift-stable, i.e. X is closed and $SX \subseteq X$.
- (2) X is the set of all infinite words avoiding a (finite or infinite) set $\mathcal{B}^\perp \subseteq \mathcal{A}^*$ of forbidden blocks.

Remark 8.4. An analogous result holds in two-sided symbolic dynamics for subsets of $\mathcal{A}^{\mathbb{Z}}$, ([33, Theorem 6.1.21]), where shift-stability is replaced by shift invariance, proved with a similar argument. The difference between shift-stability and shift-invariance is discussed in Example 8.7.

Proof. (2) \Rightarrow (1). The set X is closed, since any limit word in the sequence topology will not contain any forbidden block. Now SX is a closed set of infinite words, which do not contain any of the forbidden blocks. It follows that $SX \subseteq X$.

(1) \Rightarrow (2). The hypothesis $SX \subseteq X$ implies $S^k X \subseteq S^{k-1} X \subseteq X$ for all $k \geq 1$ by induction on k . We let $\mathcal{B}^\perp(X) \subseteq \mathcal{A}^*$ denote all the finite words that do not appear anywhere in any word in X . Let Y denote the set of all infinite words that avoid any block in $\mathcal{B}^\perp(X)$. By definition $X \subseteq Y$. To complete the proof we show the reverse inclusion $Y \subseteq X$. Let $\mathbf{y} = b_0b_1b_2\cdots \in Y$. By hypothesis the initial word $b_0b_1\cdots b_k \in Y$ does not contain any element of $\mathcal{B}^\perp(X)$, so it must occur as a block inside some word $\mathbf{x} = a_0a_1a_2\cdots \in X$, for if it did not this would contradict maximality of $\mathcal{B}^\perp(X)$. Say it is positions $a_ja_{j+1}\cdots a_{j+k} = b_0b_1\cdots b_k$. Now $\mathbf{y}_k := S^j \mathbf{x} = .b_0b_1\cdots b_k a_{k+1}\cdots \in S^k X \subseteq X$. We now have a sequence $\{\mathbf{y}_k : k \geq 0\}$ with $\mathbf{y}_k \in X$ that converges in the sequence topology to $\mathbf{y} \in Y$. Since X is closed, we deduce $\mathbf{y} \in X$ as required. \square

We give examples of allowed behavior and of non-behavior of closed shift-stable sets.

Example 8.5. There exists a shift-stable closed set X which yields an infinite strictly descending chain of inclusions under application of the shift; i.e.:

$$X \supsetneq SX \supsetneq S^2X \supsetneq S^3X \supsetneq \dots.$$

To construct X , define for each $k \geq 4$ the set $X_k := (0^k 1)^k \{000, 111\}^{\mathbb{N}}$. That is, X_k has a fixed finite prefix $(0^k 1)^k$ of length $k(k+1)$ followed by a full 2-block shift

$$Y = \{000, 111\}^{\mathbb{N}}.$$

Note that $S^3Y = Y$. We now set

$$X := \bigcup_{k=4}^{\infty} \left(\bigcup_{n=0}^{\infty} S^n X_k \right).$$

The set X is shift-stable, since

$$SX = \bigcup_{k=4}^{\infty} \left(\bigcup_{n=1}^{\infty} S^n X_k \right) \subseteq X.$$

Every element of X is an (eroded) finite prefix followed by a member of Y , SY , or S^2Y . The set X is closed because the only limit point obtainable in $\mathcal{A}^{\mathbb{N}}$ from repeated shifts of blocks in the finite prefixes alone is the vector 0^{∞} , which already belongs to Y .

To show all inclusions are strict, we note for $0 \leq j \leq 3$ the set $S^j X$ contains the word $0^{4-j} 1 (0^4 1)^3 (000)^{\infty}$, which is not contained in any $S^m X$ for $m \geq j+1$. For $j \geq 4$ each set $S^j X$ contains the word $1 (0^j 1)^{j-1} (000)^{\infty}$, which is not contained in any $S^m X$ for $m \geq j+1$.

Example 8.6 (*Shift-stability is not always preserved under interleavings*). The one-sided Fibonacci shift X_F having 11 as a forbidden block and the one-sided anti-Fibonacci shift X_{AF} having 00 as a forbidden block are both closed, shift-invariant sets. We show their 2-fold interleaving $Y = X_{AF} \circledast X_F$ is not shift-stable. Indeed X_{AF} allows the initial block 0110, and X_F allows the initial block 010, whence $X_{AF} \circledast X_F$ allows the initial block 0011100, so SY contains the initial block 011100. If $SY \subseteq Y$, then there is a $\mathbf{y} = \mathbf{y}_1 \circledast \mathbf{y}_2 \in Y$ with initial block 011100. But this means $\mathbf{y}_2 \in X_F$ has initial block 110, which is a forbidden block of the Fibonacci shift, a contradiction showing that $SY \not\subseteq Y$. (We do have $S^2Y = Y$.)

Example 8.7 (*One-sided shifts*). The notion of *one-sided shift* X defined by Lind and Marcus [33, Sect. 12.8] consists of those sets $X \subseteq \mathcal{A}^{\mathbb{N}}$ that are the restriction to positions $k \geq 0$ of all sequences in a two-sided shift X_{\pm} described by forbidden blocks. One-sided shifts X are necessarily closed and shift-invariant: $SX = X$, so they form a strict subclass of closed shift-stable X .

The difference between one-sided shifts and closed shift-stable sets is visible at the level of *minimal forbidden blocks*, which are forbidden blocks that do not contain any other forbidden block as a strict sub-block. For a one-sided shift-stable set X we let $\mathcal{B}_{\min}^{\perp}(X)$

denote its minimal forbidden block set. For a two-sided shift X_{\pm} we let $\mathcal{B}_{\min, \pm}^{\perp}(X_{\pm})$ denote its minimal forbidden block set. Now consider the closed set $Y = \{001^{\infty}, 01^{\infty}, 1^{\infty}\}$ which has $SY = \{01^{\infty}, 1^{\infty}\} \subset X$, so is shift-stable but not shift-invariant. Here $S^2Y = \{1^{\infty}\}$ is shift-invariant. It is easy to check that $\mathcal{B}_{\min}^{\perp}(Y) = \{1001, 101, 000\}$. The two-sided shift Y^{\pm} determined by this set of forbidden blocks is $Y^{\pm} = \{1^{\mathbb{Z}}\} \in \mathcal{A}^{\mathbb{Z}}$, because any bi-infinite word that contains a 0 must also contain one of the patterns 101, 1001, 000 and so is excluded. However Y_{\pm} has minimal forbidden block set $\mathcal{B}_{\min, \pm}^{\perp}(Y_{\pm}) = \{0\}$ viewed as a two-sided shift. The one-sided shift \tilde{Y} determined from Y_{\pm} , using the Lind and Marcus prescription has $\tilde{Y} = S^2Y = \{1^{\infty}\}$. The shift-stable sets Y and SY cannot be obtained by the Lind and Marcus prescription; their minimal forbidden block sets are not minimal forbidden block sets of any two-sided shift.

8.3. Weakly shift-stable sets

The notion of *weak shift-stability* provides a large class of sets $X \subseteq \mathcal{A}^{\mathbb{N}}$ which respect the shift operator and are closed under all decimation and interleaving operations. This class of sets includes all path sets studied in [2]; see [5].

Definition 8.8. A general set $X \subseteq \mathcal{A}^{\mathbb{N}}$ is *weakly shift-stable* if there are $\ell > k \geq 0$ such that $S^{\ell}X \subseteq S^kX$. We call $p = \ell - k$ an *eventual period* for this shift semi-stable set.

The notion of *eventual period* of X reflects the inclusion

$$S^{\ell+j}X = S^{(k+j)+p}X \subseteq S^{k+j}X \quad \text{for all } j \geq 0.$$

Theorem 2.15 shows that the class $\mathcal{W}(\mathcal{A})$ of all weakly shift-stable sets is closed under all decimation and interleaving operations:

Proof of Theorem 2.15. (1) Weak shift-stability $S^{\ell}X \subseteq S^kX$ gives $S^{\ell+j}X \subseteq S^{k+j}X$ for all $j \geq 0$. Setting $p = \ell - k$, we deduce for $m \geq k$ that

$$S^{m+jp}(X) \subseteq S^mX \quad \text{whenever } j \geq 1. \tag{8.1}$$

By Proposition 3.2 we have, for $j \geq 0$, $n \geq 1$,

$$S^{\ell p}\psi_{j,n}(X) = \psi_{j+\ell p n, n}(X) = \psi_{j,n}(S^{\ell p n}X) \subseteq \psi_{j,n}(S^{k p n}X) = S^{k p}\psi_{j,n}(X),$$

the inclusion holding because $S^{\ell p n}(X) \subseteq S^{k p n}(X)$ by (8.1), since the difference of iterations is a multiple of p and $k p n \geq k$.

(2) Let X_j be weakly shift-stable with parameters (ℓ_j, k_j) , for $0 \leq j \leq n-1$, and $p_j = \ell_j - k_j$. We assert that $Y = (\circledast_n)_{i=0}^{n-1} X_i$ is weakly shift-stable with an eventual period $p = p_0 p_1 \cdots p_{n-1}$. Indeed, setting $k = \max_j(k_j)$ and $\ell = k + 1$, we have, using Proposition 4.10:

$$\begin{aligned}
S^{\ell p n} Y &= S^{\ell p n} (X_0 \circledast X_1 \circledast \cdots \circledast X_{n-1}) \\
&= (S^{\ell p} X_0) \circledast (S^{\ell p} X_1) \circledast \cdots \circledast (S^{\ell p} X_{n-1}) \\
&\subseteq (S^{k p} X_0) \circledast (S^{k p} X_1) \circledast \cdots \circledast (S^{k p} X_{n-1}) = S^{k p n} Y.
\end{aligned}$$

The third line above used the inclusions $S^{\ell p} X_i \subseteq S^{k p} X_i$ for $0 \leq i \leq n-1$, which follow from (8.1), since $k \geq k_i$, and p_i divides p .

(3) It follows from (1) and (2) using the definition $X^{[n]} = (\circledast_n)_{i=0}^{n-1} \psi_{i,n}(X)$. \square

Remark 8.9. Path sets, studied in [2], are closed subsets of $\mathcal{A}^{\mathbb{N}}$ describable as infinite paths in graphs of finite automata. Such sets are not always shift-stable. In [5] it is shown they are always weakly shift-invariant, so they are weakly shift-stable.

9. Entropy of interleavings for general sets

We study two notions of entropy for general sets $X \subseteq \mathcal{A}^{\mathbb{N}}$, topological entropy $H(X)$ and prefix entropy $H_p(X)$, defined for all sets X , and we also study a notion of stable prefix entropy which only certain sets X possess.

9.1. Topological entropy and prefix entropy

We recall two notions of topological entropy for general sets $X \subseteq \mathcal{A}^{\mathbb{N}}$, following the paper [2], given in Definition 2.16 and Definition 2.17(1).

(1) The *topological entropy* of X is

$$H_{\text{top}}(X) := \limsup_{k \rightarrow \infty} \frac{1}{k} \log N_k(X),$$

where $N_k(X)$ counts the number of distinct blocks of length k to be found across all words $\mathbf{x} \in X$. It is defined as a limsup, but the limit always exists.

(2) The *prefix entropy* (or *path topological entropy*) of X is

$$H_p(X) := \limsup_{k \rightarrow \infty} \frac{1}{k} \log N_k^I(X),$$

where $N_k^I(X)$ counts the number of distinct prefix blocks $b_0 b_1 \cdots b_{k-1}$ of length k found across all words $\mathbf{x} \in X$.

As remarked in Section 2.6, for $H_{\text{top}}(X)$ the limsup is always a limit. However the limsup is needed in the definition of prefix entropy, as shown by the next example.

Example 9.1 (*The limit of $\frac{1}{k} \log N_k^I(X)$ may not exist*). Take $X_0 = \prod_{j=0}^{\infty} \mathcal{A}_j$ where $\mathcal{A}_j = \{0\}$ for $0 \leq j \leq 3$, and for $m \geq 1$,

(i) $\mathcal{A}_j = \{0\}$ for $2^{2m} \leq j \leq 2^{2m+1} - 1$

(ii) $\mathcal{A}_j = \{0, 1\}$ for $2^{2m+1} \leq j \leq 2^{2m+2} - 1$.

Then X_0 is a closed subset of $\mathcal{A}^{\mathbb{N}}$ having values $\frac{1}{k} \log N_k^I(X_0)$ that oscillate between $\frac{1}{3} \log 2$ and $\frac{2}{3} \log 2$ infinitely often as $k \rightarrow \infty$, with minima at $k = 2^{2m+1}$ and maxima at $k = 2^{2m+2}$. Here the \limsup gives $H_p(X) = \frac{2}{3} \log 2$. On the other hand, property (ii) implies $N_k(X_0) = 2^k$ so $H_{\text{top}}(X_0) = \log 2$.

Example 9.1 shows, first, that $H_p(X)$ cannot in general be defined as a limit, and second, that $H_p(X)$ and $H_{\text{top}}(X)$ need not be equal.

Proposition 9.2. *For general sets $X \subseteq \mathcal{A}^{\mathbb{N}}$, the following hold.*

(1) *Let \overline{X} denote the closure of X in the symbol topology on $\mathcal{A}^{\mathbb{N}}$. One has $H_{\text{top}}(X) = H_{\text{top}}(\overline{X})$ and $H_p(X) = H_p(\overline{X})$.*

(2) *One has*

$$H_p(X) \leq H_{\text{top}}(X) \leq \log |\mathcal{A}|.$$

Proof. (1) The definitions of $H_{\text{top}}(X)$ and $H_p(X)$ depend only on finite symbol sequences (resp. finite initial symbol sequences) that occur in X . However all infinite words in $\overline{X} \setminus X$ have all finite symbol sequences (resp. finite initial symbol sequences) occurring for some word in X .

(2) The bounds follow from $N_k^I(X) \leq N_k(X) \leq |\mathcal{A}|^k$. \square

Example 9.3 (*Strict inequality $H_p(X) < H_{\text{top}}(X)$ may occur for general X*). Let $\mathcal{A} = \{0, 1\}$, and let the closed set X consist of all words which, for $m \geq 1$,

- (i) have symbol 0 in each position $2^m \leq k \leq 2^{m+1} - m$,
- (ii) allow arbitrary symbols $\{0, 1\}$ in positions $2^{m+1} - (m - 1) \leq k \leq 2^{m+1} - 1$.

Then $N_k = 2^k$ for all $k \geq 1$, because (ii) gives arbitrarily long blocks of the full shift, whence $H_{\text{top}}(X) = \log 2$.

On the other hand, for a given symbol position k there are at most $(\log_2 k)^2$ symbol positions of type (ii), so we obtain $N_k^I(X) \leq 2^{(\log_2 k)^2}$. It follows that $H_p(X) = 0$.

9.2. Entropy and the shift operator

The shift operator preserves both entropies $H_{\text{top}}(X)$ and $H_p(X)$.

Proposition 9.4. *For general sets $X \subseteq \mathcal{A}^{\mathbb{N}}$ on a finite alphabet \mathcal{A} the following hold.*

(1) *The shift operator S preserves topological entropy:*

$$H_{\text{top}}(SX) = H_{\text{top}}(X).$$

(2) The shift operator S preserves prefix entropy:

$$H_p(SX) = H_p(X).$$

Proof. (1) We have, for a finite alphabet,

$$N_k(X) \geq N_k(SX) \geq \frac{1}{|\mathcal{A}|} N_{k+1}(X),$$

since there are at most $|\mathcal{A}|$ choices for a letter that is dropped. Using a limsup definition for $H_{\text{top}}(X)$ (although the limit always exists) we have

$$H_{\text{top}}(SX) = \limsup_{k \rightarrow \infty} \frac{1}{k} \log N_k(SX) \leq \limsup_{k \rightarrow \infty} \frac{1}{k} \log N_k(X) = H_{\text{top}}(X).$$

On the other hand,

$$\begin{aligned} H_{\text{top}}(SX) &= \limsup_{k \rightarrow \infty} \frac{1}{k} \log N_k(SX) \\ &\geq \limsup_{k \rightarrow \infty} \left(\frac{1}{k} \log N_{k+1}(X) - \frac{1}{k} \log |\mathcal{A}| \right) \\ &= \limsup_{k \rightarrow \infty} \frac{1}{k+1} \log N_{k+1}(X) = H_{\text{top}}(X). \end{aligned}$$

(2) For a finite alphabet \mathcal{A} we have

$$N_{k+1}^I(X) \geq N_k^I(SX) \geq \frac{1}{|\mathcal{A}|} N_{k+1}^I(X). \quad (9.1)$$

The result $H_p(SX) = H_p(X)$ is proved similarly to (1). \square

9.3. Entropy and decimations

Entropies may change under decimation, subject to the following inequalities.

Proposition 9.5. *For general sets $X \subseteq \mathcal{A}^{\mathbb{N}}$ on a finite alphabet \mathcal{A} the following hold for all $n \geq 1$ and all $i \geq 0$:*

$$0 \leq H_{\text{top}}(\psi_{i,n}(X)) \leq \min(nH_{\text{top}}(X), \log |\mathcal{A}|)$$

and

$$0 \leq H_p(\psi_{i,n}(X)) \leq \min(nH_p(X), \log |\mathcal{A}|).$$

All equalities can be attained.

Proof. The lower bounds are trivial, and the upper bounds $\log |\mathcal{A}|$ are trivial. For the upper bounds, the symbols of any block of size k of $\psi_{i,n}(X)$ are contained (in successive positions with index $i \pmod{n}$) inside a block of length nk of X , with the first symbol aligned; hence $N_k(\psi_{i,n}(X)) \leq N_{nk}(X)$. We have

$$\begin{aligned} H_{\text{top}}(\psi_{i,n}(X)) &= \limsup_{k \rightarrow \infty} \frac{1}{k} \log N_k(\psi_{i,n}(X)) \\ &\leq \limsup_{k \rightarrow \infty} \frac{1}{k} \log N_{nk}(X) \leq n \left(\limsup_{k \rightarrow \infty} \frac{1}{k} \log N_k(X) \right) = nH_{\text{top}}(X). \end{aligned}$$

For the corresponding prefix entropy upper bound we use the bound $N_k^I(\psi_{i,n}(X)) \leq |\mathcal{A}|^i N_{nk}^I(X)$, obtained by containment of a prefix of length k in $\psi_{i,n}(X)$ inside a prefix of X of length $nk + i$.

To show the bounds are attained, take the interleaved set $X = (\circledast_n)_{i=0}^{n-1} X_i$ where $X_0 = \mathcal{A}^{\mathbb{N}}$ and each $X_i = \{0^\infty\}$ for $1 \leq i \leq n-1$. We have $H_{\text{top}}(X) = H_p(X) = \frac{1}{n} \log |\mathcal{A}|$ (by counting blocks). For the upper bound we have $H_{\text{top}}(\psi_{0,n}(X)) = H_p(\psi_{0,n}(X)) = \log |\mathcal{A}|$. For the lower bound $H_{\text{top}}(\psi_{1,n}(X)) = H_p(\psi_{1,n}(X)) = 0$. \square

9.4. Prefix entropy upper bound for interleaving

We prove Theorem 2.18, which is a general upper bound for the prefix entropy of an n -fold interleaving in terms of the prefix entropies of its factors.

Proof of Theorem 2.18. By definition for $X = X_0 \circledast \cdots \circledast X_{n-1}$,

$$H_p(X) = \limsup_{k \rightarrow \infty} \frac{1}{k} \log \left(N_k^I(X_0 \circledast \cdots \circledast X_{n-1}) \right), \quad (9.2)$$

where $N_k^I(X)$ is the number of distinct initial blocks of length k occurring in the symbol sequences of X . Now we partition into subsequences $\{nk + j : k \geq 0\}$ for $0 \leq j \leq n-1$ to obtain:

$$H_p(X_0 \circledast \cdots \circledast X_{n-1}) = \max_{0 \leq j \leq n-1} \limsup_{k \rightarrow \infty} \frac{1}{nk + j} \log \left(N_{nk+j}^I(X_0 \circledast \cdots \circledast X_{n-1}) \right).$$

Call the terms on the right side

$$H_{p,j}(X) := \limsup_{k \rightarrow \infty} \frac{1}{nk + j} \log \left(N_{nk+j}^I(X_0 \circledast \cdots \circledast X_{n-1}) \right)$$

for $0 \leq j \leq n-1$. The number of distinct initial $(nk + j)$ -blocks in $X_0 \circledast \cdots \circledast X_{n-1}$ is simply the product of the number of distinct initial $(k+1)$ -blocks in each of X_0, X_1, \dots, X_{j-1} and of the distinct initial k -blocks in $X_j, X_{j+1}, \dots, X_{n-1}$. Thus we obtain, for a fixed j , $0 \leq j \leq n-1$,

$$\begin{aligned}
H_{p,j}(X) &= \limsup_{k \rightarrow \infty} \frac{1}{nk + j} \log \left(N_{nk+j}^I(X_0 \circledast \cdots \circledast X_{n-1}) \right) \\
&= \limsup_{k \rightarrow \infty} \frac{1}{nk + j} \log \left(\prod_{i=0}^{j-1} N_{k+1}^I(X_i) \cdot \prod_{i=j}^{n-1} N_k^I(X_i) \right) \\
&= \limsup_{k \rightarrow \infty} \frac{1}{nk + j} \left(\sum_{i=1}^{j-1} \log N_{k+1}^I(X_i) + \sum_{i=j}^{n-1} \log N_k^I(X_i) \right)
\end{aligned}$$

By (9.1), which applies to general sets $X \subseteq \mathcal{A}^{\mathbb{N}}$, each $\log N_{k+1}^I(X_i)$ differs from $\log N_k^I(X_i)$ by no more than $\log |\mathcal{A}|$. Since the entire sum is divided by $nk + j$, this difference does not affect the limsup, so:

$$\begin{aligned}
H_{p,j}(X) &= \limsup_{k \rightarrow \infty} \frac{1}{nk + j} \sum_{i=0}^{n-1} \log N_k^I(X_i) = \frac{1}{n} \limsup_{k \rightarrow \infty} \frac{1}{k} \sum_{i=0}^{n-1} \log N_k^I(X_i) \\
&\leq \frac{1}{n} \sum_{i=0}^{n-1} \limsup_{k \rightarrow \infty} \frac{1}{k} \log N_k^I(X_i) = \frac{1}{n} \sum_{i=0}^{n-1} H_p(X_i).
\end{aligned}$$

Thus, all the $H_{p,j}(X)$ are bounded above by $\frac{1}{n} \sum_{i=0}^{n-1} H_p(X_i)$. It follows that $H_p(X) = \max_{0 \leq j \leq n-1} H_{p,j}(X)$ obeys the same bound. \square

Example 9.6 (*Strict inequality may hold in Theorem 2.18*). We start with the closed set X_0 with alphabet $\mathcal{A} = \{0, 1\}$ defined in Example 9.1. Let a second closed set X_1 consist of all words that allow $\{0\}$ in index positions where X_0 allows $\{0, 1\}$, and allow $\{0, 1\}$ in all index positions where X_0 allows only $\{0\}$; i.e., $X_1 = \prod_{j=0}^{\infty} \mathcal{A}'_j$ where $\mathcal{A}'_j = \{0, 1\}$ for $0 \leq j \leq 3$, and for $m \geq 1$,

- (i) $\mathcal{A}'_j = \{0, 1\}$ for $2^{2m} \leq j \leq 2^{2m+1} - 1$
- (ii) $\mathcal{A}'_j = \{0\}$ for $2^{2m+1} \leq j \leq 2^{2m+2} - 1$.

Then $\mathcal{B}_k(X_1) = \{0, 1\}^k$ for all $k \geq 1$, since (ii) has arbitrarily long blocks of the full shift, whence $H_{\text{top}}(X) = \log 2$. We have $H_p(X_0) = H_p(X_1) = \frac{2}{3} \log 2$, by the same calculation as in Example 9.1. We assert that the interleaved set $X := X_0 \circledast X_1$ has

$$H_p(X) = \frac{1}{2} \log 2 < \frac{1}{2} (H_p(X_0) + H_p(X_1)) = \frac{2}{3} \log 2.$$

To compute $H_p(X)$, note that in each pair of consecutive symbol positions $(2j, 2j+1)$, the words in X have one symbol frozen to be 0 and the other symbol free to be chosen in $\{0, 1\}$, where the frozen symbol is the symbol in position $2j$ for $2^{2m} \leq j < 2^{2m+1}$ and is the symbol in position $2j+1$ for $2^{2m+1} \leq j < 2^{2m+2}$. Thus $2^{k/2-1} \leq N_k^I(X) \leq 2^{k/2+1}$ for all $k \geq 0$, whence $H_p(X) = \lim_{k \rightarrow \infty} \frac{1}{k} \log N_k^I(X) = \frac{1}{2} \log 2$.

9.5. Stable prefix entropy and interleaving entropy equality

We study the concept of stable prefix entropy and show its consequences for the behavior of entropy under interleaving. Recall from Definition 2.17 (2) that a set $X \subseteq \mathcal{A}^{\mathbb{N}}$ has *stable prefix entropy*, if the prefix entropy can be defined as a limit. That is, the following limit exists:

$$H_p(X) := \lim_{k \rightarrow \infty} \frac{1}{k} \log N_k^I(X).$$

Recall that Theorem 2.19 asserts that stable prefix entropy is preserved under interleaving, and that stable prefix entropy of all the interleaving factors implies equality in the prefix entropy formula of Theorem 2.18.

Proof of Theorem 2.19. Let $X = (\circledast_n)_{i=0}^{n-1} X_i$. The inequality $H_p(X) \leq \frac{1}{n} \sum_{i=0}^{n-1} H_p(X_i)$ in Theorem 2.18 arose in interchanging a finite sum with a \limsup . Using the stable prefix hypothesis for each X_i , we obtain a matching lower bound.

By definition $H_p(X) := \limsup_{k \rightarrow \infty} \frac{1}{k} \log N_k^I(X)$. Let $H'_p(X) := \liminf_{k \rightarrow \infty} \frac{1}{k} N_k(X)$. It suffices to show that $H'_p(X) \geq \frac{1}{n} \sum_{i=0}^{n-1} H_p(X_i)$ to conclude that $H'_p(X) = H_p(X)$ has a limit which is the desired value $\frac{1}{n} \sum_{i=0}^{n-1} H_p(X_i)$.

Partitioning into subsequences $\{nk + j : k \geq 0\}$ for $0 \leq j \leq n - 1$ as in the proof of Theorem 2.18, we get:

$$H'_p(X) = \min_{0 \leq j \leq n-1} \left(\liminf_{k \rightarrow \infty} \frac{1}{nk + j} \log \left(N_{nk+j}^I(X_0 \circledast \cdots \circledast X_{n-1}) \right) \right).$$

Call the right side values $H'_{p,j}(X)$. We have

$$\begin{aligned} H'_{p,j}(X) &\geq \frac{1}{n} \liminf_{k \rightarrow \infty} \left(\sum_{i=0}^{n-1} \frac{1}{k} \log N_k^I(X_i) \right) \\ &\geq \frac{1}{n} \sum_{i=0}^{n-1} \liminf_{k \rightarrow \infty} \frac{1}{k} \log N_k^I(X_i) \\ &= \frac{1}{n} \sum_{i=0}^{n-1} \lim_{k \rightarrow \infty} \frac{1}{k} \log N_k^I(X_i) = \frac{1}{n} \sum_{i=0}^{n-1} H_p(X_i), \end{aligned}$$

where stable prefix entropy was used in the last line. We conclude $H'_p(X) \geq \frac{1}{n} \sum_{i=0}^{n-1} H_p(X_i)$. \square

Example 9.7 (*Stable prefix entropy is not always preserved under decimation*). The set $X = X_0 \circledast X_1$ of Example 9.6 has stable prefix entropy, but $X_0 = \psi_{0,2}(X)$ does not, as shown in Example 9.1. The set $X_1 = \psi_{1,2}(X)$ does not have stable prefix entropy by a similar analysis.

Recall that Theorem 2.20 asserts weak shift-stability of X implies both stable prefix entropy of X and equality of the two notions of entropy, $H_p(X)$ and $H_{\text{top}}(X)$.

Proof of Theorem 2.20. For any set X we have $N_m^I(X) \leq N_m(X)$. By hypothesis, $S^\ell X \subseteq S^k X$ for some $\ell \geq k \geq 0$. Since $X \subseteq Y$ implies $S(X) \subseteq S(Y)$, an easy induction argument shows that $S^{\ell+j} X \subseteq S^{k+j} X$ holds for all $j \geq 0$. Since any block of length m in X , starting in any position n , is an initial block of $S^n(X)$, we may conclude that it is an initial block of $S^{\ell'}(X)$, for some $\ell' \leq \ell$. Consequently all such blocks are counted among the initial blocks of $X, SX, \dots, S^{\ell-1}(X)$ of length m . To each such block one can associate an initial block of length $m+\ell$ of X which contains the given block in positions ℓ' through $\ell' + m - 1$. Any initial block of length $m+\ell$ can be counted this way at most $\ell + 1$ times, one for each prefix $\ell' \leq \ell$, so we obtain the upper bound

$$N_m(X) \leq (\ell + 1)N_{m+\ell}^I(X).$$

We then obtain the bounds

$$N_m^I(X) \leq N_m(X) \leq (\ell + 1)|\mathcal{A}|^\ell N_m^I(X),$$

since $N_{m+\ell}^I(X) \leq |\mathcal{A}|^\ell N_m^I(X)$. It follows that

$$\log N_m^I(X) \leq \log N_m(X) \leq \log N_m^I(X) + C,$$

for an absolute constant C . Thus

$$\lim_{m \rightarrow \infty} \frac{1}{m} (\log N_m^I(X) - \log N_m(X)) = 0.$$

Since the limit $\lim_{m \rightarrow \infty} \frac{1}{m} \log N_m(X)$ exists for topological entropy, it must also exist for prefix entropy, showing stability. Moreover, since the limits are the same, $H_p(X) = H_{\text{top}}(X)$. Finally, since weak shift-stability is preserved under n -fold interleaving, the entropy equation (2.10) for topological entropy follows from Theorem 2.19. \square

10. Concluding remarks

10.1. General interleaving operations

Iterated interleaving factorizations are a special case of factorizations of closed sets $X \subseteq \mathcal{A}^{\mathbb{N}}$ into a product of closed sets obtained by projections onto subsets of indices $I_j \subseteq \mathbb{N}$, where the index sets $\{I_j : 0 \leq j \leq n-1\}$ form a partition of \mathbb{N} . Iterated interleaving factorizations project onto a partition of \mathbb{N} in which each I_j is a complete arithmetic progression in \mathbb{N} .

Exact covering systems are partitions of \mathbb{N} into finite sets of disjoint complete arithmetic progressions (of various moduli). They have been extensively studied; see [21],

[42] and [43] for surveys. There are interesting necessary and sufficient conditions for a finite set of complete arithmetic progressions to be an exact cover of \mathbb{N} , starting with Fraenkel [23]; see also Beebe [7] and Porubský and Schónheim [44]. The exact covers determined by iterated interleaving are the set of *natural exact covering systems* introduced by Porubský [41], who credits the construction to an unpublished paper of Znam. It is known that not all exact covers can be obtained by iterated interleaving constructions. An example due to Znam (cf. Guy [28, Problem F14]) is:

$$\begin{aligned} & \{0 \pmod{6}; 1 \pmod{10}; 2 \pmod{15}; \\ & 3, 4, 5, 7 - 10, 13 - 16, 19, 20, 22, 23, 25 - 29 \pmod{30}\}. \end{aligned}$$

This set of arithmetic progressions has $\gcd(6, 10, 15) = 1$, while any iterated interleaving factorization with an initial n -fold interleaving necessarily has all arithmetic progressions in any refinement having periods divisible by n . The natural exact covering systems play a special role in the reversion (inversion under composition) of the Möbius function power series, see Goulden et al. [27].

One can introduce more general interleaving operations, which might include arbitrary exact covering systems. For a set $X \subseteq \mathcal{A}^{\mathbb{N}}$, one can ask which decimations $\psi_{j,n}(X)$ have the property that X can be written as a topological product $\psi_{j,n}(X) \times Y$, where Y is the projection of X onto the set I of all indices having $i \neq j \pmod{n}$? Call such a decimation $\psi_{j,n}(X)$ with this property a *generalized factor* of X . Can one characterize the possible sets of all generalized factors of X , as X varies?

10.2. Iterated interleaving closure operations

One may ask for a given set X , what are the set of all interleaving closures of it: $\{X^{[n]} : n \geq 1\}$. We can define a filtered limit as $n \rightarrow \infty$ as follows. Letting p_k denote the k th prime in increasing order, we can define

$$X^{[\infty]} := \lim_{n_k = (p_1 p_2 \cdots p_k)^k \rightarrow \infty} X^{[n_k]},$$

where the limit exists since $X^{[n_k]} \subseteq X^{[n_{k+1}]}$ by Proposition 4.6(3), and for each n one has n divides n_k for all sufficiently large k . The set $X^{[\infty]}$ will be infinitely factorizable. What can one say about the possible forms of $X^{[\infty]}$?

10.3. Characterizing closed weakly shift-stable sets

Is there a characterization of closed weakly shift-stable sets $X \subseteq \mathcal{A}^{\mathbb{N}}$ having a parallel with the characterization by forbidden blocks of closed shift-stable sets given in Proposition 8.3?

Appendix A. Interleaving operad

Operads were systematically developed by Boardman and Vogt [8] and May [37] and as a vehicle to study iterated loop spaces in stable homotopy theory. More recently, operads have been used by researchers in homological algebra, category theory, algebraic geometry, and mathematical physics; see [47] for a brief introduction. Interleaving operations determine a certain kind of operad, giving an application of the operad concept to symbolic dynamics. In this Appendix we only define operads over the category of sets, although they can be defined over any symmetric monoidal category.

Non-symmetric operads (as in [34], [25]) are a weak version of operads which do not require equivariance under actions of symmetric groups on factors. They provide a convenient framework to keep track of properties of an infinite family of n -ary operations under iterated composition.

Definition A.1. A *non-symmetric operad* (or *plain operad*) $\underline{\mathcal{Q}}$ consists of a set $\underline{\mathcal{Q}}(n)$ for each natural number n satisfying the following conditions:

(a) (composition) for all positive integers n, k_1, \dots, k_n , there is a composition function

$$\circ : \underline{\mathcal{Q}}(n) \times \underline{\mathcal{Q}}(k_1) \times \dots \times \underline{\mathcal{Q}}(k_n) \rightarrow \underline{\mathcal{Q}}(k_1 + \dots + k_n),$$

written as $(f, f_1, \dots, f_n) \mapsto f \circ (f_1, \dots, f_n)$ for elements $f \in \underline{\mathcal{Q}}(n)$ and $f_i \in \underline{\mathcal{Q}}(k_i)$;

(b) (identity) there is an element $1 \in \underline{\mathcal{Q}}(1)$, called the *identity*, such that

$$f \circ (1, \dots, 1) = f = 1 \circ f$$

for all f ;

(c) (associativity) there holds

$$\begin{aligned} f \circ (f_1 \circ (f_{1,1}, \dots, f_{1,k_1}), f_n \circ (f_{n,1}, \dots, f_{n,k_n})) &= \\ &= (f \circ (f_1, \dots, f_n)) \circ (f_{1,1}, \dots, f_{1,k_1}, \dots, f_{n,1}, \dots, f_{n,k_n}) \end{aligned}$$

for all $f \in \underline{\mathcal{Q}}(n)$, $f_i \in \underline{\mathcal{Q}}(k_i)$ and $f_{i,j}$.

For a non-symmetric operad $\underline{\mathcal{Q}}$, we think of the elements of $\underline{\mathcal{Q}}(n)$ as n -ary operations. An *operad* is a non-symmetric operad that also possesses a right-action of the symmetric group Σ_n on the set of operations of arity n for each n , satisfying an equivariance condition, as described in the definition below.

Following [35], we use an underline to denote non-symmetric operads $\underline{\mathcal{Q}}$ and remove the underline for (symmetric) operads \mathcal{O} .

Definition A.2. An *operad* (or *symmetric operad*) \mathcal{O} is a non-symmetric operad together with a right action of the symmetric group Σ_n on each $\mathcal{O}(n)$ satisfying the following

equivariance conditions for each $\sigma \in \Sigma_n$, $\tau_i \in \Sigma_{k_i}$, $f \in \mathcal{O}(n)$, and $f_i \in \mathcal{O}(k_i)$ for $1 \leq i \leq n$:

- (A) $(f \cdot \sigma) \circ (f_1, \dots, f_n) = (f \circ (f_1, \dots, f_n)) \cdot \sigma$;
- (B) $f \circ (f_1 \cdot \tau_1, \dots, f_n \cdot \tau_n) = (f \circ (f_1, \dots, f_n)) \cdot (\tau_1, \dots, \tau_n)$.

Here the action of σ on the right-half of (A) is defined as the action of the permutation $\tilde{\sigma} \in \sigma_{k_1+\dots+k_n}$ that permutes consecutive blocks of length k_1, \dots, k_n , respectively, according to the permutation σ .

We let $\mathcal{S}(\mathcal{A})$ denote any class of subsets of $\mathcal{A}^{\mathbb{N}}$ that is closed under all decimation and interleaving operations, combining n sets in $\mathcal{S}(\mathcal{A})$ in any order in any n -fold interleaving. Examples of such classes include the collection $\mathcal{W}(\mathcal{A})$ of all weakly shift-stable sets (Theorem 2.15), the sub-collection $\overline{\mathcal{W}}(\mathcal{A})$ of all closed weakly shift-stable sets (since the property of being closed is preserved under all decimation and interleaving operations), and the class $\mathcal{C}(\mathcal{A})$ of path sets studied in [2], which is shown to satisfy weak shift-stability in [5].

We first construct a non-symmetric operad $\underline{\mathcal{I}}$ such that each element of $\underline{\mathcal{I}}(n)$ is an n -ary operation acting on $\mathcal{S}(\mathcal{A}) \times \mathcal{S}(\mathcal{A}) \times \dots \times \mathcal{S}(\mathcal{A})$ (n times). Although the non-symmetric operad $\underline{\mathcal{I}}$ will be built up from the n -fold interleaving operations, the resulting set $\underline{\mathcal{I}}(n)$ of operations at level n will contain many more operations. For notational convenience, let \circledast_n denote the n -fold interleaving operation on $\mathcal{S}(\mathcal{A})$. We let $\underline{\mathcal{I}}(1) = \{\circledast_1\}$, where of course $\circledast_1 = id_{\mathcal{S}(\mathcal{A})}$ is the trivial “1-fold interleaving”. Also let $\underline{\mathcal{I}}(2) = \{\circledast_2\}$. However, it will not be sufficient for $\underline{\mathcal{I}}(3)$ to be a singleton set. Rather,

$$\underline{\mathcal{I}}(3) = \{\circledast_3, \circledast_2 \circ (\circledast_1, \circledast_2), \circledast_2 \circ (\circledast_2, \circledast_1)\},$$

where, for instance,

$$[\circledast_2 \circ (\circledast_1, \circledast_2)](X_1, X_2, X_3) = X_1 \circledast (X_2 \circledast X_3)$$

for general sets $X_1, X_2, X_3 \in \mathcal{S}(\mathcal{A})$. $\underline{\mathcal{I}}(n)$ for $n > 3$ is defined analogously, so as to satisfy the composition condition of Definition A.1. It is easy to see that \circledast_1 serves as an identity for $\underline{\mathcal{I}}$ with respect to the various compositions, as in (b). Since the compositions of $\underline{\mathcal{I}}$ are genuine function composition, associativity in $\underline{\mathcal{I}}$ follows from the associativity of function composition. Therefore, $\underline{\mathcal{I}}$ is a non-symmetric operad. We call $\underline{\mathcal{I}}$ the *interleaving non-symmetric operad*, and refer to operations from $\underline{\mathcal{I}}$ as *compound interleaving operations*.

The non-symmetric operad $\underline{\mathcal{I}}$ can be upgraded to a symmetric operad by adding a right action of the symmetric group permuting the interleaving factors. This requires adding additional n -ary operations for each n . In particular, for $\sigma \in \Sigma_n$ and an operation $f \in \mathcal{I}(n)$, we need to admit the operation $f \cdot \sigma$ where $(f \cdot \sigma)(X_1, \dots, X_n) = f(X_{\sigma(1)}, \dots, X_{\sigma(n)})$. Note that, like the interleaving operations themselves, this is also a

function $\mathcal{S}(\mathcal{A}) \times \cdots \times \mathcal{S}(\mathcal{A}) \rightarrow \mathcal{S}(\mathcal{A})$, given by a (possibly compound) interleaving of some permutation of the input sets. Denote by $\mathcal{I}(n)$ the set of n -ary operations expanded to include the operations $f \cdot \sigma$ defined above, which permute the inputs prior to any (compound) interleaving. Note that we can think of an element $f \in \underline{\mathcal{I}}(n)$ as corresponding to $f \cdot \epsilon \in \mathcal{I}(n)$, where $\epsilon \in \Sigma_n$ is the identity element. We can then extend the compositions for the $\underline{\mathcal{I}}(k)$ to

$$\circ : \mathcal{I}(n) \times \mathcal{I}(k_1) \times \cdots \times \mathcal{I}(k_n) \rightarrow \mathcal{I}(k_1 + \cdots + k_n),$$

by genuine function composition. Then it is natural to define a right action of Σ_n on $\mathcal{I}(n)$ by $(f \cdot \sigma) \cdot \tau = f \cdot (\sigma\tau)$ for $f \cdot \sigma \in \mathcal{I}(n)$ and $\tau \in \Sigma_n$. Note that the equivariance conditions (A) and (B) of Definition A.2 apply generally to an action permuting the inputs of genuine functions with respect to genuine composition. Thus, since the n -ary operations in $\mathcal{I}(n)$ are genuine functions on sets and the compositions are function composition, these conditions hold. We call the resulting (symmetric) operad the *interleaving symmetric operad* and denote it by \mathcal{I} .

Proposition A.3. *Let \mathcal{I} be the interleaving symmetric operad acting on a collection of sets $\mathcal{S}(\mathcal{A})$ closed under all decimation and interleaving operations. Then for any $f \in \mathcal{I}(n)$ and any sets $X_0, \dots, X_{n-1} \in \mathcal{S}(\mathcal{A})$, we have also $f(X_0, \dots, X_{n-1}) \in \mathcal{S}(\mathcal{A})$.*

Proof. Every $f \in \mathcal{I}(n)$ is just a composition of interleavings of various n -arities, where possibly the input sets have their order permuted. Since $\mathcal{S}(\mathcal{A})$ is closed under the interleaving operations, it follows that it is closed under all composition operations from \mathcal{I} . \square

Generally, we recall below the notion of an algebra over an operad. We will see that the descriptions given above for the nonsymmetric operad $\underline{\mathcal{I}}$ and the (symmetric) operad \mathcal{I} were really given in terms of certain algebras over those operads. This approach has helped to keep the exposition concretely rooted in the examples of interest, but differs from the more typical, categorical exposition.

The following definition matches [35, Definition 1.20], restricted to operads in the category of sets. For a set X , let $\mathcal{E}nd_X(n)$ denote the set of all functions $X^n \rightarrow X$, and let $\mathcal{E}nd_X = \bigcup_{n=1}^{\infty} \mathcal{E}nd_X(n)$. Then $\mathcal{E}nd_X$ has the structure of an operad, and is called the *Endomorphism Operad* (of sets); see [35, Definition 1.7].

Definition A.4. Let \mathcal{O} be an operad in the category of sets, and let X be a set. An \mathcal{O} -algebra structure on X is a morphism of operads $\alpha_X : \mathcal{O} \rightarrow \mathcal{E}nd_X$, that is, a family of Σ_n -equivariant morphisms $\alpha_X(n) : \mathcal{O}(n) \rightarrow \mathcal{E}nd_X(n)$, $n \geq 1$, compatible with the identity, composition, and equivariance structures of \mathcal{O} and $\mathcal{E}nd_X$.

If we omit the equivariance structure from the above definition, then we get the notion of an *algebra over a nonsymmetric operad*.

Example A.5 (*Algebras over interleaving nonsymmetric operad $\underline{\mathcal{I}}$*). The sets $\mathcal{W}(\mathcal{A})$ of all weakly shift-stable sets on the finite alphabet \mathcal{A} , $\overline{\mathcal{W}}(\mathcal{A})$ of all closed weakly shift-stable sets on \mathcal{A} , and $\mathcal{C}(\mathcal{A})$ of path sets on \mathcal{A} are all algebras over the interleaving nonsymmetric operad $\underline{\mathcal{I}}$. If the set $\mathcal{S}(\mathcal{A})$ is any of these sets, and for any $n \in \mathbb{N}$, the maps $\alpha_{\mathcal{S}(\mathcal{A})}$ of Definition A.4 are built up from

$$\alpha_{\mathcal{S}(\mathcal{A})}(n)(\circledast_n)[(X_0, \dots, X_{n-1})] := (\circledast_n)_{j=0}^{n-1} X_j = X_0 \circledast X_1 \circledast \dots \circledast X_{n-1}$$

by function composition, where $(X_0, \dots, X_{n-1}) \in \mathcal{S}(\mathcal{A})^n$.

References

- [1] W.C. Abram, A. Bolshakov, J.C. Lagarias, Intersections of multiplicative translates of 3-adic Cantor sets II: two infinite families, *Exp. Math.* 26 (2017) 468–489.
- [2] W.C. Abram, J.C. Lagarias, Path sets in one-sided symbolic dynamics, *Adv. Appl. Math.* 56 (2014) 109–134.
- [3] W.C. Abram, J.C. Lagarias, p -Adic path set fractals and arithmetic, *J. Fractal Geom.* 1 (2014) 45–81.
- [4] W.C. Abram, J.C. Lagarias, Intersections of multiplicative translates of 3-adic Cantor sets, *J. Fractal Geom.* 1 (2014) 349–390.
- [5] W.C. Abram, J.C. Lagarias, D.J. Slonim, Interleaving of path sets, eprint: arXiv:2101.02441.
- [6] R. Adler, A.G. Konheim, M.H. McAndrew, Topological entropy, *Trans. Am. Math. Soc.* 114 (1965) 309–319.
- [7] J. Beebee, Bernoulli numbers and exact covering systems, *Am. Math. Mon.* 99 (1992) 946–948.
- [8] J.M. Boardman, R.M. Vogt, Homotopy Invariant Algebraic Structures on Topological Spaces, *Lecture Notes in Math.*, vol. 347, Springer, Berlin, 1973.
- [9] M.R. Bremner, V. Dotsenko, *Algebraic Operads: An Algorithmic Companion*, CRC Press, Boca Raton, FL, 2014.
- [10] S.D. Cardell, A. Fuster-Sabatier, A.H. Ranea, Linearity in decimation-based generators: an improved cryptanalysis of the shrinking generator, *Open Math.* 16 (2018) 646–655.
- [11] T.M. Carlsen, Cuntz-Pimsner C^* -algebras associated with subshifts, *Int. J. Math.* 9 (2008) 47–70.
- [12] T.M. Carlsen, An introduction to the C^* -algebra of a one-sided shift space, in: *Operator Algebras and Dynamics*, in: *Springer Proc. Math. Stat.*, vol. 58, Springer, Heidelberg, 2013, pp. 63–88.
- [13] T. Cottrell, A study of Penon weak n -categories, part 1. Monad interleaving, *Cah. Topol. Géom. Différ. Catég.* 59 (2018) 197–259.
- [14] J. Cuntz, A class of C^* -algebras and topological Markov chains II. Reducible chains and the Ext-function for C^* -algebras, *Invent. Math.* 63 (1981) 25–40.
- [15] J. Cuntz, W. Krieger, A class of C^* -algebras and topological Markov chains, *Invent. Math.* 56 (1980) 251–268.
- [16] I. Daubechies, *Ten Lectures on Wavelets*, CBMS-NSF Regional Conf. Ser. in Appl. Math., vol. 61, SIAM, Philadelphia, PA, 1992.
- [17] M. Dokuchaev, R. Exel, Partial actions and subshifts, *J. Funct. Anal.* 272 (2017) 5038–5106.
- [18] G. Duchamp, M. Flouret, É. Laugerotte, J.G. Luque, Direct and dual laws for automata with multiplicities, *Theor. Comput. Sci.* 267 (2001) 105–120.
- [19] S. Eilenberg, *Automata, Languages and Machines*, Volume A, Pure and Applied Mathematics, vol. 59A, Academic Press, New York, 1974.
- [20] P. Erdős, Some unconventional problems in number theory, *Math. Mag.* 52 (1979) 67–70.
- [21] P. Erdős, R.L. Graham, *Old and New Problems and Results in Combinatorial Number Theory*, Monographie de L’Enseignement Mathématique, vol. 28, Univ. Genéve, 1980.
- [22] R. Exel, *Partial Dynamical Systems, Fell Bundles and Applications*, Math. Surveys Monogr., vol. 224, Amer. Math. Soc., Providence, RI, 2017.
- [23] A. Fraenkel, A characterization of exactly covering congruences, *Discrete Math.* 4 (1973) 359–366.
- [24] S. Giraudo, *Operads in algebraic combinatorics*, Habilitation 2017, Université Paris-Est Marne-la-Vallée, 388 pages. eprint: arXiv:1712.03782.

- [25] S. Giraudo, Nonsymmetric Operads in Combinatorics, Springer, Cham, 2018.
- [26] G. Grätzer, Lattice Theory: Foundation, Birkhäuser, Berlin, 2011.
- [27] I.P. Goulden, A. Granville, L.B. Richmond, J. Shallit, Natural exact covering systems and the reversion of the Möbius series, *Ramanujan J.* 50 (2019) 211–235.
- [28] R.K. Guy, Unsolved Problems in Number Theory, third edition, Springer-Verlag, New York, 2004.
- [29] Zhiqing Hui, J. Baccou, J. Liandrat, On the coupling of decimation operator with subdivision schemes for multi-scale analysis, in: Mathematical Methods for Curves and Surfaces, in: Lecture Notes in Computer Science, vol. 10521, Springer, Cham, 2017, pp. 162–185.
- [30] D. Krieger, A. Miller, N. Rampersad, B. Ravikumar, J.O. Shallit, Decimations of languages and state complexity, *Theor. Comput. Sci.* 410 (2009) 2401–2409.
- [31] J.C. Lagarias, Ternary expansions of powers of 2, *J. Lond. Math. Soc.* 79 (2009) 562–588.
- [32] T. Leinster, Higher Operads, Higher Categories, London Math. Soc. Lecture Note Series, vol. 298, Cambridge University Press, Cambridge, 2004.
- [33] D. Lind, B. Marcus, An Introduction to Symbolic Dynamics and Coding, Cambridge University Press, New York, 1995. (Reprinted 1999 with corrections.).
- [34] Jean-Louis Loday, Bruno Vallette, Algebraic Operads, Grundlehren der Mathematischen Wissenschaften, vol. 346, Springer-Verlag, New York, 2012.
- [35] M. Markl, S. Shnider, J. Stasheff, Operads in Algebra, Topology and Physics, Math. Surveys Monogr., vol. 96, American Mathematical Society, Providence, RI, 2002.
- [36] M. Markl, Operads and PROPS, in: Handbook of Algebra, vol. 5, Elsevier/North Holland, Amsterdam, 2008, pp. 87–140.
- [37] J.P. May, The Geometry of Iterated Loop Spaces, Springer Lecture Notes in Mathematics, vol. 271, Springer, 1972.
- [38] J.P. May, Operads, algebras and modules, in: Operads: Proceedings of Renaissance Conferences, Hartford, CT/Luminy, 1995, in: Contemp. Math., vol. 202, Amer. Math. Soc., Providence, RI, 1997, pp. 15–31.
- [39] M. Morse, G.A. Hedlund, Symbolic dynamics, *Am. J. Math.* 60 (1938) 815–866.
- [40] D. Perrin, J-E. Pin, Infinite Words: Automata, Semigroups, Logic and Games, Elsevier, Dordrecht, 2004.
- [41] S. Porubský, Natural exactly covering systems of congruences, *Czechoslov. Math. J.* 24 (1974) 598–606.
- [42] S. Porubský, Results and problem on covering systems of residue classes, *Mitt. Math., Semin. Giessen* 150 (1981) 1–85.
- [43] S. Porubský, J. Schönheim, Covering systems of Paul Erdős. Past, present and future, in: Paul Erdős and His Mathematics I, Budapest, 1999, J. Bolyai Math. Soc., Budapest, 2002, pp. 581–627.
- [44] S. Porubský, J. Schönheim, Old and new necessary and sufficient conditions on (a_i, m_i) in order that $n \equiv a_i \pmod{m_i}$ be a covering system, *Math. Slovaca* 53 (2003) 341–349.
- [45] R.A. Rueppel, Analysis and Design of Stream Ciphers, Springer-Verlag, Berlin, 1986.
- [46] E. Schechter, Handbook of Analysis and Its Foundations, Academic Press, New York, 1996, Elsevier, Dordrecht, 1997.
- [47] J. Stasheff, What is an operad?, *Not. Am. Math. Soc.* 51 (2004) 630–631.
- [48] S.A. Vanstone, P. van Oorschot, An Introduction to Error Correcting Codes with Applications, Kluwer Academic Publishers, Boston, 1989.