

FORWARD LIMIT SETS OF SEMIGROUPS OF SUBSTITUTIONS
AND
ARITHMETIC PROGRESSIONS IN AUTOMATIC SEQUENCES

by
Ibai Aedo Goñi

Under the supervision of
Uwe Grimm, Ian Short, Neil Mañibo, and Reem Yassawi

A thesis submitted for the degree of
Doctor of Philosophy in Mathematics



March 2023

DECLARATION OF AUTHORSHIP

This thesis is the author's own work. It has material from joint collaboration with other researchers, as detailed below. It has not been submitted for another qualification to the Open University or to any other university or institution.

- (i) Most of the material in Chapter 2, which gives background mathematics for the remainder of the thesis, has been expounded by the author based on a conveniently cited literature review.
- (ii) Most of the material in Chapter 3 is part of the author's joint work with Uwe Grimm, Yaushi Nagai and Petra Staynova, and has been published in *Theoretical Computer Science* [2].
- (iii) Most of the material in Chapter 4 is part of the author's joint work with Uwe Grimm, Neil Mañibo, Yaushi Nagai and Petra Staynova. A preprint of this work can be found on arXiv [1]. Section 4.4.3 is the author's own work and can only be found in this thesis.
- (iv) Most of the material in Chapter 5 is part of the author's joint work with Uwe Grimm and Ian Short. A preprint of this work can be found on arXiv [3]. Section 5.4.1.1 and Theorem 5.6.6 are the author's own work and can only be found in this thesis.
- (v) The material in Chapter 6 is the author's own work.
- (vi) The author presented part of his research at the conference *4th BYMAT – Bringing Young Mathematicians Together* and plans to submit a paper to *La Matematica, Official Journal of the Association for Women in Mathematics* for an special issue related to the topics discussed at the conference. The author plans to do this with parts of Chapters 5 and 6, which will be conveniently extended.
- (vii) The material in Appendix A is the author's own work.
- (viii) All examples in this thesis are the author's own elaboration, unless otherwise stated. All figures in this thesis are the author's own creation.

Ibai Aedo Goñi
March 2023

ACKNOWLEDGMENTS

I feel very much fortunate in having Uwe Grimm, Ian Short and Neil Mañibo as my supervisors. This thesis would not have been possible without their invaluable guidance and support, and their friendly advice and encouragement.

Ian, I will always be extremely grateful to you and Uwe for the opportunity you gave me to start this PhD with you and the trust you placed in me. It has been the most beautiful intellectual adventure I have ever been involved in. Neil, when Uwe died, you were, along with Ian, a formidable support. But above all, you are a friend who came into my life at just the right time. You all gave me, among many other things, a taste for good mathematics.

I would like to thank Yasushi Nagai and Petra Stainova too, research collaborators and friends. Uwe was our main linking vertex, but when he died it became clear that the graph was a complete graph, and ever since the remaining edges got strengthened and new edges arose.

I would also like to mention the people of the Department of Mathematics and Statistics of The Open University. In the atmosphere you create I feel at home, part of a big family. I enjoyed very much the informal discussions about mathematics and other things, the lunch breaks, and the side activities we had from time to time.

I do not want to forget the people of the Faculty of Mathematics in Bielefeld for the pleasant stay I had with them. I found an active research environment that I had missed during the Covid times, which made my brief stay a great experience.

Finally, I want to thank my family for many things, which I will summarise as the love I receive from them.

When I was to start the PhD, I thought it was going to be a great experience. Now that I am to finish it, I can say that, despite the difficult times, the journey has been infinitely better than expected. In mathematics I have found a new universe full of fantastic jewels waiting to be discovered.

Iturri zaharretik edaten dut,
ur berria edaten,
beti berri den ura,
betiko iturri zaharretik.

Joxean Artze.

I drink from the old fountain,
I drink the new water,
the water that is always new,
from the same old fountain.

Joxean Artze.

CONTENTS

1	Introduction	1
1.1	Monochromatic arithmetic progressions in automatic sequences	1
1.2	Forward limit sets of semigroups of substitutions	4
2	Background	7
2.1	Asymptotic notation	7
2.2	Spaces of words	7
2.2.1	Finite and infinite words	7
2.2.2	The word metric	8
2.2.3	Representation of integers in integer bases	9
2.2.4	Periodic and aperiodic words	10
2.2.5	Recurrent sequences	10
2.3	Arithmetic progressions and colourings	11
2.4	Substitutions	13
2.4.1	General properties	13
2.4.2	Periodic points of a primitive substitution	15
2.4.3	Forward limit set of a substitution	16
2.4.4	Substitutive sequences	17
2.4.5	Constant-length substitutions and automatic sequences	18
2.4.6	Coincidences admitted by a constant-length substitution	21
2.4.7	Column group of a bijective substitution	22
2.4.8	Height of a constant-length substitution	24
2.4.9	Hull and subshift of a substitution	25
2.4.10	Recognisability	27

2.5	Semigroups of substitutions	28
2.5.1	s-adic sequences	28
2.5.2	General properties of substitution semigroups	30
2.5.3	Presentation of a substitution semigroup	32
2.5.4	Actions of a substitution semigroup	34
2.5.5	First-letter graph of a substitution semigroup	34
2.5.6	Forward limit set of a substitution semigroup	36
2.5.7	Hull and subshift of a substitution semigroup	37
3	Monochromatic arithmetic progressions in Thue–Morse-like sequences	39
3.1	Finiteness of the length of monochromatic arithmetic progressions	40
3.2	Monochromatic arithmetic progressions in the Thue–Morse word	43
3.2.1	Properties of the Thue–Morse word and the Thue–Morse substitution	44
3.2.2	Monochromatic arithmetic progressions of difference $d = 2^n$	45
3.2.3	Monochromatic arithmetic progressions of difference $d = 2^n + 1$	46
3.2.4	Monochromatic arithmetic progressions of difference $d = 2^n - 1$	49
3.2.5	Longest monochromatic arithmetic progressions of difference $d \leq 2^n$	49
3.2.6	Plot and histogram of $A(d)$	51
3.3	Monochromatic arithmetic progressions in generalised Thue–Morse words	52
3.3.1	Properties of the generalised Thue–Morse words and Thue–Morse substitutions	52
3.3.2	Monochromatic arithmetic progressions of difference $d = Q^n$	53
3.3.3	Monochromatic arithmetic progressions of difference $d = Q^n + 1$	53
3.3.4	Monochromatic arithmetic progressions of difference $d = Q^n - 1$	57
3.3.5	Longest monochromatic arithmetic progressions of difference $d \leq Q^n + 1$	58
3.3.6	Plots of $A_{p,q}(d)$	60
3.4	Upper bounds for $A(d)$ for primitive binary bijective substitutions	60
4	Monochromatic arithmetic progressions in automatic sequences	63
4.1	Preliminaries	64
4.1.1	Column structure of constant-length substitutions	64
4.1.2	Monochromatic arithmetic progressions in substitution fixed points	66

4.1.3	Notation	67
4.2	Primitive bijective substitutions	67
4.2.1	Lower bounds and polynomial growth of $A(d)$	67
4.2.2	Lower bounds and linear growth of $A(d)$	71
4.2.3	Van der Waerden-type numbers	74
4.2.4	Upper bounds for $A(d)$ for abelian bijective substitutions	78
4.2.5	Thue–Morse sequence over L letters	83
4.3	Non-bijective substitutions with supersubstitution structure	89
4.4	Spin substitutions	92
4.4.1	The Rudin–Shapiro sequence	93
4.4.2	A different approach to the Rudin–Shapiro sequence	95
4.4.3	The Hadamard sequence	100
4.4.4	Vandermonde sequences	103
5	Forward limit sets of semigroups of semigroups of substitutions	108
5.1	Preliminaries	109
5.2	Fixed-letter-free substitution semigroups	109
5.3	Properties of forward limit sets	111
5.4	Characterisations of forward limit sets	115
5.4.1	Forward limit sets and s -adic limits	115
5.4.1.1	The Fibonacci substitution semigroup	117
5.4.2	Invariant sets	119
5.4.3	Fixed points of substitution semigroups	123
5.5	Size of forward limit sets	126
5.5.1	Cardinality of forward limit sets	126
5.5.2	Hausdorff dimension of forward limit sets	128
5.6	Hulls of substitution semigroups	133
6	Directions for further research	137
6.1	Monochromatic arithmetic progressions	137
6.1.1	Bijective constant-length substitutions	137

6.1.2	General constant-length substitutions	138
6.1.3	Higher-dimensional monochromatic arithmetic progressions	142
6.2	Forward limit sets of substitution semigroups	149
6.2.1	Forward limit sets of substitution semigroups with fixed letters	149
6.2.2	Hausdorff dimension and complexity of sets of infinite words	149
A	Computer experiments with linear recurrent sequences	152
	References	154

1. INTRODUCTION

This thesis deals with symbolic sequences generated by semigroups of substitutions acting on finite alphabets.

First, we study the underlying structure of some such sequences by considering the appearance of a fixed symbol in arithmetic progression within the sequence considered. The objective is to determine the length of these arithmetic progressions and to find sequences of such arithmetic progressions with fast growing length. The work is motivated by Ramsey theory, which is concerned with aspects of order in substructures of given structures of a known size [75], and it touches on aspects from combinatorics [111] and theoretical computer science [11].

Next, we consider semigroups generated by finite families of substitutions acting on a finite alphabet. We study sets of symbolic sequences obtained by iterating elements of an alphabet under given semigroups of substitutions. The objective is to characterise these sets and determine their size. The work is motivated by the theory of s -adic sequences, which is concerned with the dynamics of compositions of sequences of substitutions, and it is inspired by semigroup theory in other disciplines of dynamical systems, such as complex dynamics, hyperbolic dynamics, and hyperbolic geometry [12, 56, 66, 68].

In this introduction we give a selection of our most significant results and their motivation and surrounding context. Some terms will be informally defined in this chapter; formal definitions and background results from the literature will be given in Chapter 2, and the more advanced techniques will be introduced as necessary in the subsequent chapters.

1.1 Monochromatic arithmetic progressions in automatic sequences

An alphabet \mathcal{A} is a finite set of symbols, customarily chosen among the non-negative integers or the Latin alphabet, and the elements of \mathcal{A} are called letters, regardless of the set of symbols used. We denote the set of finite words over \mathcal{A} by \mathcal{A}^+ and the set of infinite words or sequences over \mathcal{A} by $\mathcal{A}^{\mathbb{N}}$. For example, 101 is a finite word over the alphabet $\{0, 1\}$ of length 3, meaning that it consists of three letters, and 101010 \dots is an infinite word over $\{0, 1\}$. We denote the n th letter of a finite or infinite word w by w_n .

A substitution of \mathcal{A} is a map $f : \mathcal{A}^+ \longrightarrow \mathcal{A}^+$ with the property $f(xy) = f(x)f(y)$, for every finite words x and y over \mathcal{A} , which is specified uniquely by the images of the letters of \mathcal{A} . A substitution f acts on an infinite word $x = x_1x_2x_3 \dots$ over \mathcal{A} as $f(x) = f(x_1)f(x_2)f(x_3) \dots$. Most of the times we use either Latin letters (f, g, h) or Greek letters (ρ, θ) to name substitutions. An example of a substitution

of the alphabet $\{0, 1\}$ is

$$\begin{aligned} 0 &\longmapsto 01, \\ 1 &\longmapsto 10. \end{aligned}$$

This substitution is called the Thue–Morse substitution [17, Section 4.6] and will play an important role in Chapter 3. It is an example of a constant-length substitution, which means that the images of all the letters have the same length. In this case, the length of the substitution is 2.

In this work, a fixed point of a substitution f is a word x (finite or infinite) with $f(x) = x$. Let f be the Thue–Morse substitution. By iterating f starting from the initial word 0 we obtain the Thue–Morse sequence [6, 8]

$$\underline{0}11\underline{0}1\underline{00}11\underline{00}1\underline{0}11\underline{0}1\underline{00}1\underline{0}11\underline{0}\dots,$$

which is a fixed point of f . For now, ignore the underlined letters. Fixed points of constant-length substitutions (and more specifically their images under a substitution of constant length one) are called automatic sequences.

We say that a sequence x over an alphabet \mathcal{A} contains a monochromatic arithmetic progression of difference d and length ℓ if there exist a starting position s and a letter $a \in \mathcal{A}$ such that

$$x_s = x_{s+d} = \dots = x_{s+(\ell-1)d} = a.$$

We refer to a as the colour of the arithmetic progression. Similarly, a sequence x contains an infinite monochromatic arithmetic progression of difference d if there exist s and a such that $x_s = x_{s+kd} = a$, for $k = 1, 2, 3, \dots$. For example, the underlined letters in the Thue–Morse sequence above show an arithmetic progression of 0s of difference 3 and length 7; notice that it cannot be extended to a monochromatic arithmetic progression of length 8 with the same starting position and difference. In Chapters 3 and 4 we study monochromatic arithmetic progressions within automatic sequences to give insight into the order underlying their structure.

Our research is inspired by van der Waerden’s theorem [109], a milestone result in Ramsey theory, which says that, for every fixed positive integers c and ℓ , one can find a positive integer n such that any colouring of the segment $\{1, 2, \dots, n\}$ with at most c colours contains a monochromatic arithmetic progression of length ℓ . For example, if $c = 2$ and $\ell = 3$, one can choose $n = 9$, since any colouring of $\{1, 2, \dots, 9\}$ with one or two colours contains a monochromatic arithmetic progression of length three (there are colourings of $\{1, 2, \dots, 8\}$ which do not contain monochromatic arithmetic progressions of length three). A consequence of this result is that every sequence over a finite alphabet contains monochromatic arithmetic progressions of every positive integer length. It is then natural to ask what happens if the difference of the arithmetic progressions is fixed.

Given a sequence x over a finite alphabet, we want to know whether, for a fixed difference d , there exist infinite monochromatic arithmetic progressions of difference d within x , and if not, whether the length of the longest monochromatic arithmetic progression of difference d is bounded above. To study these questions, we define $A_x : \mathbb{N} \longrightarrow \mathbb{N} \cup \{\infty\}$ to be the function that, for each positive integer d , assigns to $A_x(d)$ the length of the longest monochromatic arithmetic progression of difference d within

x , and if such a longest length does not exist, then we define $A_x(d) = \infty$. If the sequence x is clear from the context, we often write $A(d)$ rather than $A_x(d)$.

We show that, for a whole family of automatic sequences, $A_x(d)$ is finite, for every sequence x in the class and positive integer d ; this result extends the result in [80] for the Thue–Morse sequence to a larger class of automatic sequences. All the sequences studied in this thesis have the property $A_x(d) < \infty$ and consequently, A_x maps the set of positive integers into itself.

In Chapter 3 we deal with the Thue–Morse sequence and with other generalised Thue–Morse sequences. We give exact values of $A(d)$, for specific differences d . The case of the Thue–Morse sequence, which we denote by x in the following two theorems, has previously been studied by Parshina [90], who determined the value of $A_x(2^n - 1)$, for all positive integers n , and showed also that $A_x(d) < A_x(2^n - 1)$ for all $d < 2^n - 1$.

Theorem (Parshina [90]). *Let x be the Thue–Morse sequence. Then, for all positive integers n ,*

$$\max_{d < 2^n} A_x(d) = A_x(2^n - 1) = \begin{cases} 2^n + 4, & \text{if } n \text{ is even,} \\ 2^n, & \text{otherwise.} \end{cases}$$

Parshina’s proof relies on a case-by-case study and makes heavy use of binary arithmetic. Using different methods, which rely on the substitution structure of the Thue–Morse sequence and which have a strong visual component, we reprove Parshina’s theorem. We also identify another family of differences, specifically differences of the form $2^n + 1$, for which the monochromatic arithmetic progressions are long.

Theorem. *Let x be the Thue–Morse sequence. Then $A_x(2^n + 1) = 2^n + 2$, for all integers $n \geq 2$.*

Illustrative plots of our results can be found in Section 3.2.6. These plots show that the longest monochromatic arithmetic progressions appearing in the Thue–Morse sequence are, precisely, those of the differences we have obtained exact values for, namely, differences of the form $2^n \pm 1$.

Next, we extend the results for the Thue–Morse sequence to a class of generalised Thue–Morse sequences [14, 16, 70], which are fixed points of substitutions of the form

$$\begin{aligned} 0 &\longmapsto 0^p 1^q, \\ 1 &\longmapsto 1^p 0^q, \end{aligned}$$

for positive integers p and q . The main change compared to the Thue–Morse case is that, rather than working modulo 2, we now have to work modulo $Q = p + q$. For convenience, we write $A_{p,q}(d)$ rather than $A(d)$. In analogy with the Thue–Morse case, we give exact values of $A_{p,q}(d)$ for differences of the form $Q^n + 1$ and, when $p = q$, for $Q^n - 1$ too. The equality $p = q$ is necessary to establish $A_{p,q}(Q^n - 1)$ because only in this case are all the symmetries of the Thue–Morse case preserved. We illustrate our results with computer plots of $A(d)$, both for the $p = q$ and $p \neq q$ situations.

In Chapter 4 we consider automatic sequences arising from constant-length substitutions others than the previously considered. In particular, we work with two classes of constant-length substitutions with

an explicit group structure that provides direct access to bounding $A(d)$ for some specific values of d and allows some asymptotic estimates.

The first class of substitutions considered in Chapter 4 is the class of aperiodic, primitive, and bijective constant-length substitutions (these terms will be formally defined in Chapter 2). We prove that there exists a sequence of differences d along which $A(d)$ grows at least polynomially in d . In the following theorem, for non-zero functions $f, g, h : \mathbb{N} \rightarrow \mathbb{R}$, we write $f(n) \gtrsim g(n)$ if $f(n) \geq h(n)$ and $|h(n)/g(n)| \rightarrow 1$ as $n \rightarrow \infty$.

Theorem. *Let f be an aperiodic, primitive, bijective substitution. For any fixed point of f , there exist an increasing sequence (d_n) in \mathbb{N} and a real number α in $(0, 1]$ for which $A(d_n) \gtrsim d_n^\alpha$.*

We introduce the notion of g -palindromicity and show that, for g -palindromic substitutions, one gets $\alpha = 1$ in the previous theorem, that is, the asymptotic growth of $A(d)$ is at least linear in d .

The next substitutions we consider in Chapter 4 are spin substitutions [4, 31, 52, 96], which are a particular type of non-bijective constant-length substitutions. Given a length- L spin substitution f of the alphabet $\mathcal{A} = \{0, 1, \dots, L-1\}$ with an associated spin group G , the automatic sequence we study is obtained from a fixed point of f under a spin projection $\mathcal{A} \rightarrow G$ mapping each letter to a group element. We prove the following result.

Theorem. *Let f be a spin substitution arising from an $L \times L$ Vandermonde matrix. For the spin coding of any fixed point of f , there exist an increasing sequence (d_n) in \mathbb{N} and a real number α in $(0, 1]$ for which $A(d_n) \gtrsim d_n^\alpha / L$.*

In particular, for the Rudin–Shapiro substitution, which is the simplest of the spin substitutions with $L = 2$, we have $\alpha = 1$, that is, the asymptotic growth of $A(d)$ is at least linear in d .

The previous two theorems deal with lower bounds for $A(d)$. Under some mild assumptions on the substitutions, we also obtain upper bounds for $A(d)$. In particular, we give sufficient conditions for $A(d) < \infty$ to hold, for all d (see Propositions 4.1.4 and 4.4.23), and, for a subclass of bijective substitutions, we compute explicit upper bounds for $A(d)$ (see Corollary 4.2.31 and Proposition 4.2.34).

1.2 Forward limit sets of semigroups of substitutions

In Chapter 5 we no longer focus on individual infinite words. Instead, we study sets of infinite words that arise as forward limit sets of semigroups of substitutions. Given a family \mathcal{F} of substitutions of an alphabet \mathcal{A} , we consider the semigroup S generated by \mathcal{F} under functional composition. More precisely,

$$S = \{f_1 \circ f_2 \circ \dots \circ f_n : f_i \in \mathcal{F}, n \in \mathbb{N}\}.$$

We say that such a semigroup is a substitution semigroup.

We denote by $\tilde{\mathcal{A}}$ the set $\mathcal{A}^+ \cup \mathcal{A}^\mathbb{N}$ of all finite and infinite words over \mathcal{A} . A metric can be chosen that makes $\tilde{\mathcal{A}}$ a complete, compact metric space. We write $S(X)$ for the set $\{s(x) : s \in S, x \in X\}$ and denote the closure of a set Y in $\tilde{\mathcal{A}}$ by \overline{Y} . We can now define the central objects of interest.

Definition. The forward limit set of a subset A of \mathcal{A} for the substitution semigroup S is the set

$$\Lambda(A) = \overline{S(A)} \setminus S(A),$$

and the forward limit set of S is the set $\Lambda = \Lambda(\mathcal{A})$.

For example, consider the substitution semigroup generated by the Thue–Morse substitution f and the reversed Thue–Morse substitution g , which are given by

$$f : \begin{array}{lcl} 0 & \mapsto & 01, \\ 1 & \mapsto & 10, \end{array} \quad \text{and} \quad g : \begin{array}{lcl} 0 & \mapsto & 10, \\ 1 & \mapsto & 01. \end{array}$$

The substitution f has two fixed points, both aperiodic, namely the Thue–Morse sequence $x = 011010 \dots$ and $h(x)$, where h is the substitution given by $h(0) = 1$ and $h(1) = 0$, hence h interchanges 0 and 1 in any word. Observe that f , g and h satisfy the functional equation $g = h \circ f = f \circ h$ and consequently, $S = \{f^n : n \in \mathbb{N}\} \cup \{h \circ f^n : n \in \mathbb{N}\}$. It follows that $\Lambda = \{x, h(x)\}$.

Let us consider another example of a forward limit set, this time one associated with the substitution semigroup S generated by the three substitutions

$$f : \begin{array}{lcl} 0 & \mapsto & 01, \\ 1 & \mapsto & 0, \end{array} \quad g : \begin{array}{lcl} 0 & \mapsto & 10, \\ 1 & \mapsto & 0, \end{array} \quad h : \begin{array}{lcl} 0 & \mapsto & 1, \\ 1 & \mapsto & 0. \end{array}$$

The substitutions f and g are known as the Fibonacci substitution and the reversed Fibonacci substitution, respectively [17, Example 4.6, Remark 4.6]. It is known that S is the collection of all so-called Sturmian substitutions (others than the identity) (see [78, Chapter 2] or [57, Chapters 6 & 9]). The forward limit set of S is equal to the set of all balanced infinite words over $\{0, 1\}$; these are infinite words x over $\{0, 1\}$ with the property that the number of 0s (or 1s) in any two subwords of x of the same length differs by at most one. The proof of this result is not included in this thesis and will appear in a future preprint, as explained in (vi) in the Declaration of Authorship on page i.

We are usually concerned with fixed-letter-free substitution semigroups; a semigroup S is of this type if each substitution f in S satisfies $f(a) \neq a$, for all $a \in \mathcal{A}$. One of our main results relates forward limit sets to s -adic limits under the fixed-letter-free assumption. An infinite word x over \mathcal{A} is an s -adic limit of a family of substitutions \mathcal{F} if there exist sequences (f_n) in \mathcal{F} and (a_n) in \mathcal{A} with $f_1 \circ f_2 \circ \dots \circ f_n(a_n) \rightarrow x$ as $n \rightarrow \infty$ (see, for example, [24, Section 4.11]).

Theorem. *Let S be a fixed-letter-free substitution semigroup with finite generating set \mathcal{F} . The forward limit set of S is equal to the set of all s -adic limits of \mathcal{F} .*

The forward limit set $\Lambda(A)$ of a subset $A \subseteq \mathcal{A}$ is (by definition) the boundary of $S(A)$ in $\tilde{\mathcal{A}}$, and it lies within $\mathcal{A}^{\mathbb{N}}$ because \mathcal{A}^+ has the discrete topology and so $\overline{S(A)}$ does not accumulate in \mathcal{A}^+ . A subset X of $\mathcal{A}^{\mathbb{N}}$ is S -invariant if $S(X) \subseteq X$, and it is strongly S -invariant if $S(X) = X$. The set $\Lambda(A)$ is closed and, among other properties, it is always S -invariant. Sometimes it is also strongly S -invariant. This brings us to classifying forward limit sets by means of the action of S on $\mathcal{A}^{\mathbb{N}}$.

Theorem. *Let S be a finitely-generated fixed-letter-free substitution semigroup. A subset of $\mathcal{A}^{\mathbb{N}}$ is closed and strongly S -invariant if, and only if, it is the forward limit set of some subset of \mathcal{A} for S .*

A consequence of this theorem is another characterisation of Λ , which says that Λ is the greatest element in the poset of closed and strongly S -invariant subsets of $\mathcal{A}^{\mathbb{N}}$.

In other branches of dynamics forward limit sets and related sets can often be described in terms of fixed points. In this work we show how the forward limit set of a substitution semigroup S is characterised by the collection of all fixed points of substitutions from S , which we denote by $\text{fix}(S)$.

Theorem. *The forward limit set of a finitely-generated fixed-letter-free substitution semigroup S is equal to $\overline{S(X)}$, where $X = \text{fix}(S)$.*

The results stated so far concern characterisations of forward limit sets. Next, we move towards determining their size and prove two main theorems. The first theorem says that, under mild assumptions, the forward limit set of a substitution semigroup is uncountable (see Theorem 5.5.2 in Chapter 5). The second theorem says that forward limit sets cannot be too large. This theorem is framed using logarithmic Hausdorff dimension, which can be used to quantify the size of sets for which the usual Hausdorff dimension is zero. In this theorem the length of a finite set of substitutions \mathcal{F} is the least number of letters of $f(a)$, among all letters $a \in \mathcal{A}$ and substitutions $f \in \mathcal{F}$; the size of \mathcal{F} is the number of substitutions it consists of.

Theorem. *The forward limit set of a substitution semigroup S of \mathcal{A} generated by a finite set of substitutions \mathcal{F} of length r and size s , where $r > 1$, has logarithmic Hausdorff dimension at most $\log_r s$.*

Furthermore, given any pair of positive integers r and s with $r > 1$ and $s \leq |\mathcal{A}|^{r-1}$, there exists a substitution semigroup S with these parameters for which the bound $\log_r s$ is attained.

The assumption that $r > 1$ is not as prohibitive as it may seem, and we will see examples where it can be circumvented. The idea is to consider a different substitution semigroup S' of length $r' > 1$ the forward limit set of which is equal to the forward limit set of the original semigroup S of length $r = 1$.

The (left) shift map $\sigma : \mathcal{A}^{\mathbb{N}} \rightarrow \mathcal{A}^{\mathbb{N}}$ is defined, for any infinite word $a_1 a_2 a_3 \dots$ with $a_i \in \mathcal{A}$, as $\sigma(a_1 a_2 a_3 \dots) = a_2 a_3 \dots$. We define the hull Ω of a substitution semigroup S with forward limit set Λ as the closure of the orbit of Λ under σ . We say that S is irreducible if, for any letters $a, b \in \mathcal{A}$, there exists a substitution $f \in S$ such that the word $f(a)$ contains the letter b . We say that S is primitive if there exists a positive integer n such that, for all letters $a, b \in \mathcal{A}$, all the words $f_1 \circ f_2 \circ \dots \circ f_n(a)$ with $f_i \in \mathcal{F}$ contain the letter b , where \mathcal{F} is a generating set of S .

We finish Chapter 5 with a theorem characterising the hull of irreducible substitution semigroups, and a theorem for primitive substitution semigroups. We show that the hull of an irreducible substitution semigroup S is the least element in the poset of closed, S -invariant and shift-invariant non-empty subsets of $\mathcal{A}^{\mathbb{N}}$ (see Theorem 5.6.5). Also, we show that the hull of a primitive substitution semigroup S is equal to its subshift (which will be defined in Section 2.5.7) and it is uniquely determined by the set of fixed points of S (see Theorem 5.6.6). This result generalises a well-known similar result for single substitutions [96, Proposition 5.3] to substitution semigroups.

2. BACKGROUND

In this chapter, we introduce the mathematical background needed for the remainder of the thesis. Most of the material of this chapter can be found, for example, in [17, 24, 57, 96, 98].

The sets of integers, positive integers and non-negative integers are denoted by \mathbb{Z} , \mathbb{N} and \mathbb{N}_0 , respectively. The set of real numbers is denoted by \mathbb{R} .

2.1 Asymptotic notation

In Chapters 4 and 6 we will use standard asymptotic notation, which can be found, for example, in [63, 75].

Let $f, g : \mathbb{N} \rightarrow \mathbb{R}$ be non-zero functions. We write

$$\begin{aligned} f(n) > g(n) &\iff |f(n)/g(n)| \rightarrow \infty \text{ as } n \rightarrow \infty, \\ f(n) \sim g(n) &\iff |f(n)/g(n)| \rightarrow 1 \text{ as } n \rightarrow \infty, \\ f(n) \gtrsim g(n) &\iff \text{there exists a non-zero function } h : \mathbb{N} \rightarrow \mathbb{R} \text{ such that } f(n) \geq h(n) \text{ and } h(n) \sim g(n), \\ f(n) = O(g(n)) &\iff \text{there exists a positive real constant } C \text{ such that } |f(n)| < C|g(n)|, \\ &\text{for all but finitely many values of } n. \end{aligned}$$

2.2 Spaces of words

2.2.1 Finite and infinite words

Throughout this thesis \mathcal{A} will denote a non-empty finite set of size at least two, called an *alphabet*. The elements of \mathcal{A} are called *letters* of \mathcal{A} . The number of letters in \mathcal{A} is denoted by $|\mathcal{A}|$. Any symbols can be chosen to be letters of an alphabet, but typically we choose lower case letters or non-negative integers. Examples of alphabets that we will use are the binary alphabet $\{0, 1\}$ or the ternary alphabet $\{a, b, c\}$.

A *finite word* over \mathcal{A} is a finite sequence of letters of \mathcal{A} . We write the finite word a_1, a_2, \dots, a_n as a string $a_1 a_2 \dots a_n$. The *length* of the finite word $w = a_1 a_2 \dots a_n$, denoted $|w|$, is the length n of the sequence. We denote by \mathcal{A}^n the set of all finite words over \mathcal{A} of length n . A *subword* of the finite word $w = a_1 a_2 \dots a_n$ is any substring $a_i a_{i+1} \dots a_j$, where $1 \leq i \leq j \leq n$; when $i = 1$, the subword is said to be a *prefix* of w . The concatenation of k copies of the finite word w is written as w^k ; we consider w^0 to be the empty word. The collection of all finite words over \mathcal{A} forms a semigroup \mathcal{A}^+ with composition

given by concatenation of finite words. We exclude the empty word from \mathcal{A}^+ . We denote by \mathcal{A}^* the union of \mathcal{A}^+ and the set containing the empty word.

A *infinite word* or *infinite sequence* over \mathcal{A} is a one-sided infinite sequence of letters of \mathcal{A} . The collection of all infinite words over \mathcal{A} is denoted $\mathcal{A}^{\mathbb{N}}$. A typical element of this set is written in the form $a_1 a_2 a_3 \dots$, for letters a_i . We define subwords of infinite words similarly as for finite words. If w_1, w_2, w_3, \dots are finite words over \mathcal{A} , then $w_1 w_2 w_3 \dots$ denotes the infinite word over \mathcal{A}^+ with the obvious meaning.

We define $\tilde{\mathcal{A}} = \mathcal{A}^+ \cup \mathcal{A}^{\mathbb{N}}$, the collection of all finite and infinite words. We often refer to an element w of $\tilde{\mathcal{A}}$ simply as a *word* over \mathcal{A} , and, if needed, we specify whether w is finite or infinite.

For a non-empty set X of infinite words over \mathcal{A} and a positive integer n , we define $\mathcal{L}_n(X)$ to be the set of all subwords of elements of X of length n , and we define the *language* of X to be $\mathcal{L}(X) = \bigcup_{n=1}^{\infty} \mathcal{L}_n(X)$. The *complexity function* of X is the function $p : \mathbb{N} \rightarrow \mathbb{N}$ defined by $p(n) = |\mathcal{L}_n(X)|$. If $X = \{x\}$, for an infinite word x , we write $\mathcal{L}_n(x)$ rather than $\mathcal{L}_n(X)$, and $\mathcal{L}(x)$ rather than $\mathcal{L}(X)$.

There are occasions on which it is more appropriate to consider the first letter of a word to be indexed by 0 rather than 1 (Example 2.2.2 illustrates this idea). In these circumstances, we use \mathbb{N}_0 instead of \mathbb{N} and we write the set of infinite words as $\mathcal{A}^{\mathbb{N}_0}$. In Chapters 3 and 4 we use $\mathcal{A}^{\mathbb{N}_0}$, and in Chapter 5 we use $\mathcal{A}^{\mathbb{N}}$.

Let T be a set of functions that maps the set $\tilde{\mathcal{A}}$ into itself and let X be a subset of $\tilde{\mathcal{A}}$. We define $T(X)$ to be the set $\{t(x) : t \in T, x \in X\}$. X is *invariant under T* or *T -invariant* if $X \subseteq T(X)$, and X is *strongly invariant under T* or *strongly T -invariant* if $X = T(X)$. We will consider sets of words that are invariant under the shift map and sets of words that are invariant under substitutions and substitution semigroups, concepts that will be defined in due course.

2.2.2 The word metric

Given any word w of $\tilde{\mathcal{A}}$, we write w_k for the k th letter in the sequence w , providing that w has length at least k . If w has length less than k , then we define $w_k = \alpha$, where α is some additional letter not in \mathcal{A} (this additional letter is only needed for the definition of the metric, to follow). We write $w_{[k, \ell]}$ to denote the subword $w_k w_{k+1} \dots w_{\ell-1}$ of w , with the convention $w_{[k, k+1]} = w_k$. For the sake of readability, there are occasions on which we prefer to write the k th letter of w as $\pi_k(w)$ rather than w_k . For example, if w is the n th iterate of a word u under a map f , we write $\pi_k(f^n(u))$ rather than $(f^n(u))_k$. This notation is mainly used in Chapter 5.

We define a *metric* d on $\tilde{\mathcal{A}}$ by the formulas $d(u, u) = 0$ and

$$d(u, v) = \frac{1}{2^{n-1}}, \quad \text{where } n = \min\{k \in \mathbb{N} : \pi_k(u) \neq \pi_k(v)\},$$

for distinct elements u and v of $\tilde{\mathcal{A}}$. We call this metric the *word metric* on $\tilde{\mathcal{A}}$. The exponent $n-1$ has been chosen so that $0 \leq d(u, v) \leq 1$. With this definition $(\tilde{\mathcal{A}}, d)$ is a complete, compact metric space,

and the associated topology is the product topology of the discrete topology on \mathcal{A} . Informally speaking, two words are close to each other if they have a large common prefix.

Example 2.2.1. One of the most celebrated infinite words is the *Thue–Morse word*, also known as the *Prouhet–Thue–Morse word* after the authors who, independently, discovered it [81, 95, 106]. We refer the reader to [6, 8] for surveys of its properties. There are many ways to define the Thue–Morse word, one of which we describe in this example (alternative definitions will be given in Example 2.2.2 and Example 2.4.17).

Let w be a word over a two-letter alphabet \mathcal{A} . We write \bar{w} for the word obtained from w by exchanging the two letters of \mathcal{A} . For example, given the word $w = 0110$ over $\{0, 1\}$, we obtain $\bar{w} = 1001$. Observe that with this alphabet one has $\bar{a} = 1 - a$, for $a \in \{0, 1\}$. This ‘bar operation’ that exchanges the two letters of the alphabet is referred to as a ‘bar-swap symmetry’ in [13].

We set $w_0 = 0$ and, for each $n \geq 1$, we define $w_n = w_{n-1} \bar{w}_{n-1}$. Observe that $|w_n| = 2^n$. The first few terms of this sequence are 0, 01, 0110, 01101001, \dots . Since each term in the sequence is a prefix of the next term, the distance between them, given by

$$d(w_n, w_{n+1}) = \frac{1}{2^{|w_n|}} = \frac{1}{2^{2^n}},$$

tends to 0 as $n \rightarrow \infty$. Consequently, the sequence converges to the infinite word

$$0110100110010110100101100110\dots,$$

which is the Thue–Morse word. ❖

2.2.3 Representation of integers in integer bases

Integers (and more generally real numbers) can be represented in different number bases, in particular, in integer bases. Let us fix an integer b greater than 1 and call it the *base*. The *canonical alphabet* associated with b is $\mathcal{A}_b = \{0, 1, \dots, b-1\}$. The integer b together with \mathcal{A}_b defines the *base b numeral system*. For every non-negative integer n , there are $k+1$ digits a_0, a_1, \dots, a_k in \mathcal{A}_b , with $a_k \neq 0$, such that n can be written uniquely as

$$n = a_k \cdot b^k + a_{k-1} \cdot b^{k-1} + \dots + a_1 \cdot b + a_0.$$

We say that $[a_k, a_{k-1}, \dots, a_1, a_0]$ is the *representation of n in base b* . If $i > j$, the digit a_i is said to be more significant than the digit a_j . Thus, the *most significant digit* and the *least significant digit* of the representation are a_k and a_0 , respectively. An introduction to representations of real numbers in integer bases can be found, for example, in [24, Chapter 2].

Example 2.2.2. The Thue–Morse word introduced in Example 2.2.1 admits an alternative definition through the sum of digits in the binary representation of the integers indexing the word. More precisely, for each $n \geq 0$, the n th term of the Thue–Morse word is determined by summing all the digits in the binary representation of n and taking this sum modulo 2. In other words, the n th term is 0 if the aforementioned

sum is even, and it is 1 otherwise. Notice that, with this definition, the Thue–Morse word belongs to $\{0, 1\}^{\mathbb{N}_0}$. Let us denote the Thue–Morse word by v . We compute the value of v_{25} , the 25th term of v . The binary representation of 25 is $[1, 1, 0, 0, 1]$, with digit sum 3, an odd integer. So $v_{25} = 1$. This can be corroborated by direct inspection in Example 2.2.1, where the first few terms of the Thue–Morse word are given. ❖

2.2.4 Periodic and aperiodic words

We say that an infinite word $w = a_1 a_2 a_3 \dots$, for letters $a_i \in \mathcal{A}$, is *periodic* if there exists a positive integer p such that $a_i = a_{i+p}$, for all $i \geq 1$. The integers p satisfying this condition are the *periods* of w ; we call the smallest period of w its *minimum period*. We say that an infinite word $w = a_1 a_2 a_3 \dots$, for letters $a_i \in \mathcal{A}$, is *eventually periodic* if there exist two positive integers k and p such that $a_i = a_{i+p}$, for all $i \geq k$. For example, the word $ababab \dots$ (with obvious continuation to the right) is periodic with minimum period equal to 2, while the word $aababab \dots$ is only eventually periodic.

An infinite word that is not eventually periodic is said to be *aperiodic*. The Thue–Morse sequence introduced in Example 2.2.2 is an aperiodic word. We say that a set X of infinite words is *aperiodic* if all the words in X are not eventually periodic. Some hulls and subshifts (notions introduced in Section 2.4.9), such as the hull defined from the Thue–Morse sequence, are good examples of aperiodic sets of infinite words.

2.2.5 Recurrent sequences

An infinite word w is called *recurrent* if every one of its subwords appears in w infinitely many times. An infinite word w is called *uniformly recurrent* if every one of its subwords appears in w infinitely many times with bounded gaps. More precisely, w is uniformly recurrent if, for each subword u of w , there exists a positive integer k , depending on u , such that u appears in every subword of w of length k . Notice that periodic words are uniformly recurrent.

Example 2.2.3. Consider the infinite two-letter word

$$w = a b a^2 b^2 a b a^3 b^3 a^2 b^2 a b a^4 b^4 a^3 b^3 a^2 b^2 a b \dots$$

To construct it set $v_1 = ab$ and $v_n = a^n b^n v_{n-1}$, for every $n \geq 2$, and then $w = v_1 v_2 v_3 \dots$. The recurrent construction of w makes it clear that it is a recurrent word, which is not uniformly recurrent because the gaps between consecutive appearances of subwords get arbitrarily large. ❖

Example 2.2.4. *Chacon’s sequence* (see [29] and [57, Sections 1.2, 5.5]) is the aperiodic infinite word

$$w = 0010001010010001000101001010 \dots$$

defined as the limit of the sequence v_1, v_2, v_3, \dots of finite words given by $v_1 = 0$ and, for all $n \geq 2$, $v_n = v_{n-1} v_{n-1} 1 v_{n-1}$. From this structure, using an inductive argument, it follows that every subword of v_{n-1} appears in every subword of w of length $|v_n|$ and so Chacon’s sequence is uniformly recurrent. ❖

The Thue–Morse word introduced in Example 2.2.2 is not only uniformly recurrent, but also ‘linearly recurrent’ (see [37, 40, 42]). We say that an infinite word w is *linearly recurrent* for the constant k (or that k is a *linear recurrence constant* for w) if w is recurrent and, for any subword u of w , the greatest gap between successive occurrences of u is $k|u|$. Some literature use the term ‘repetitive’ rather than recurrent for single infinite words, and use the term ‘recurrent’ for subshifts generated by repetitive words (compare [40, 42] and [37]); here we will use the term recurrent for infinite words as well as for subshifts (see Section 2.4.9).

2.3 Arithmetic progressions and colourings

A *finite arithmetic progression of difference d and length ℓ* , where d and ℓ are positive integers, is a sequence a_1, a_2, \dots, a_ℓ , where a_1 is a fixed integer and $a_n = a_1 + (n-1)d$, for all $2 \leq n \leq \ell$. Similarly, an *infinite arithmetic progression of difference d* , where d is a positive integer, is a sequence a_1, a_2, a_3, \dots , where a_1 is a fixed integer and $a_n = a_1 + (n-1)d$, for all $n \geq 2$. For example, 1, 7, 13 is a (finite) arithmetic progression of difference 6 and length 3, and 2, 4, 6, 8, ... is an infinite arithmetic progression of difference 2.

We can interpret the letters of an alphabet \mathcal{A} to be colours and then any word over \mathcal{A} is a coloured sequence of letters. We say that a (finite) *monochromatic arithmetic progression of difference d and length ℓ* appears in a word w , where d and ℓ are positive integers, if there exists an integer n such that $w_n = w_{n+id}$, for all $0 \leq i \leq \ell - 1$. Similarly, we say that an *infinite monochromatic arithmetic progression of difference d* appears in an infinite word w , where d is a positive integer, if there exists an integer n such that $w_n = w_{n+id}$, for all $i \geq 0$.

Example 2.3.1. The *Champernowne word* [30], also known as the *Barbier word* [8], is the infinite word obtained by concatenating the decimal representation of the positive integers, that is,

$$1\,2\,3\,4\,5\,6\,7\,8\,9\,10\,11\,12\,13\,14\,15\,16\,17\,18\,19\,20\,\dots$$

Since the Champernowne word has arbitrarily long strings of the form $aa \dots a$, for every decimal digit a , it contains arbitrarily long finite arithmetic progressions of any difference and colour. ❖

Example 2.3.2. Consider the aperiodic sequence

$$0^{10} 1^{10} 0^{100} 1^{100} 0^{1000} 1^{1000} \dots$$

with obvious continuation to the right. This sequence contains finite monochromatic arithmetic progressions of any desired length, and yet contains no monochromatic arithmetic progression which is infinitely long. ❖

In Chapters 3 and 4, we consider monochromatic arithmetic progressions in certain automatic sequences (we define automatic sequences in Section 2.4.5). Our results draw inspiration from one of the best-known Ramsey-type theorems, proved in 1927 by van der Waerden in his seminal paper [109].

Theorem 2.3.3. *For every two positive integers k and ℓ , there exists a positive integer n such that any colouring of the segment $\{1, 2, \dots, n\}$ with no more than k colours contains a monochromatic arithmetic progression of length ℓ .* \square

The smallest threshold of n , for given values of k and ℓ , is the *van der Waerden number* that we denote by $W(k, \ell)$. Determining these numbers is complex. Apart from the trivial cases, namely, $W(1, \ell) = \ell$ and $W(k, 2) = k + 1$, only seven other van der Waerden numbers are known exactly [21, 22, 27, 32, 72, 73, 104]. In Chapter 4 we define van der Waerden-type numbers for automatic sequences arising from primitive bijective substitutions, and provide explicit upper bounds for them.

The following result is significantly stronger than Theorem 2.3.3. It was conjectured by Erdős and Turán [46] in 1936, and it was first proved by Szemerédi [105] in 1975.

Theorem 2.3.4. *For every $\delta > 0$ and positive integers ℓ , there exists a positive integer n such that every subset of $\{1, 2, \dots, n\}$ with at least δn elements contains an arithmetic progression of length ℓ .* \square

It is not hard to see that Szemerédi's theorem implies van der Waerden's theorem. A colouring of the set $\{1, 2, \dots, n\}$ with no more than k colours partitions this set into at most k colour classes. At least one of these classes, call it X , must contain at least n/k elements. Then, if we choose $\delta = 1/k$ in Szemerédi's theorem, the monochromatic class X contains an arithmetic progression of length ℓ and van der Waerden's theorem follows.

Example 2.3.5. The characteristic sequence of the prime numbers [85] is the infinite word w , whose n th letter is 1 if n is a prime and 0 otherwise. So it can be regarded as a 2-colouring of the positive integers. The first few terms of w are as follows.

$$w = 0\,1\,1\,0\,1\,0\,1\,0\,0\,0\,1\,0\,1\,0\,0\,0\,1\,0\,1\,0\,0\,0\,1\,\dots$$

One can easily find infinite arithmetic progressions of 0's in w . For instance, all indexes that are multiples of 4 have the colour 0 assigned. However, we cannot find infinite arithmetic progressions of 1's in w . This follows from the fact that there are arbitrarily large gaps between primes. Whether w contains arbitrarily large finite arithmetic progressions of 1's is a significantly harder question. It is not implied by Szemerédi's theorem because there are too few primes in the set $\{1, 2, \dots, n\}$, for any n . The answer turns out to be that w does contain arbitrarily long arithmetic progressions of 1's. This result was proved in 2008 by Green and Tao [62] who showed that the prime numbers contain an arithmetic progression of any positive integer length. \blacklozenge

2.4 Substitutions

2.4.1 General properties

One way of generating new words out of other existing words is by means of substitutions. A *substitution* of an alphabet \mathcal{A} is a function f from \mathcal{A}^+ to \mathcal{A}^+ with the property

$$f(uv) = f(u)f(v),$$

for any two finite words u and v . These functions are called *non-erasing morphisms* in some literature. A substitution is specified uniquely by the images of the letters of the alphabet. We often display a substitution f of an alphabet $\{a_1, a_2, \dots, a_k\}$, where $k = |\mathcal{A}|$ is the cardinality of the alphabet, as

$$\begin{array}{rcl} & a_1 & \mapsto f(a_1), \\ f : & a_2 & \mapsto f(a_2), \\ & \vdots & \\ & a_k & \mapsto f(a_k). \end{array}$$

A substitution f can be extended to a function from $\mathcal{A}^{\mathbb{N}}$ to $\mathcal{A}^{\mathbb{N}}$ by

$$f(w) = f(w_1)f(w_2)f(w_3)\dots,$$

for any infinite word $w = w_1w_2w_3\dots$, where $w_i \in \mathcal{A}$ for all $i \in \mathbb{N}$.

Sometimes it is convenient to work with injective substitutions. The following result, which can be found in [78, Proposition 6.1.3], characterises injective substitutions.

Lemma 2.4.1. *A substitution f of \mathcal{A} is injective on finite words if, and only if, the letters of \mathcal{A} are mapped to distinct words and, for all words $u_1, u_2, \dots, u_n, v_1, v_2, \dots, v_m$ in $f(\mathcal{A})$, the equality $u_1u_2\dots u_n = v_1v_2\dots v_m$ implies $n = m$ and $u_i = v_i$, for $i = 1, 2, \dots, n$. \square*

Given two substitutions f and g of the alphabet \mathcal{A} , we denote by $f \circ g$ the functional composition of first g and then f , and we denote by $f^n = f \circ f \circ \dots \circ f$ the n -fold composition of f with itself.

We say that a substitution f of \mathcal{A} is *irreducible* if, for any letters a and b in \mathcal{A} , there exists a positive integer n such that the word $f^n(a)$ contains the letter b . If n does not depend on the letters considered, we say that f is *primitive*. In other words, f is primitive if there is a positive integer n such that, for every letter a , all the letters in \mathcal{A} appear in the word $f^n(a)$.

Testing a substitution for primitivity can always be done in a finite number of steps. The following theorem gives an upper bound for the substitution power to be inspected (see, for example, [100] or [94, Theorem 37.4.2]). This bound is known as *Wielandt's bound* [110].

Theorem 2.4.2. *Let f be a primitive substitution of the alphabet \mathcal{A} . For every letter $a \in \mathcal{A}$, all the letters in \mathcal{A} are subwords of the word $f^{k^2-2k+2}(a)$, where $k = |\mathcal{A}|$. \square*

Let f be a substitution of an alphabet $\{a_1, a_2, \dots, a_k\}$ containing k letters. The *incidence matrix* of f is the $k \times k$ matrix whose (i, j) th entry is equal to the number of times the letter a_i appears in the word $f(a_j)$. If we want to determine whether a substitution f is irreducible or primitive, we can use its incidence matrix. Let us denote the incidence matrix of f by M . The substitution f is irreducible if, and only if, for each pair i and j there exists a positive integer n such that $(M^n)_{i,j} > 0$. The substitution f is primitive if, and only if, there exists a positive integer n such that every entry of M^n is positive.

Example 2.4.3. Consider the substitution f of the alphabet $\{a, b\}$ given by

$$f : \begin{array}{lcl} a & \mapsto & bb, \\ b & \mapsto & aa. \end{array}$$

It is easy to see that, for any positive integer n , the n th power of the incidence matrix of f is

$$\begin{pmatrix} 0 & 2^n \\ 2^n & 0 \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} 2^n & 0 \\ 0 & 2^n \end{pmatrix},$$

depending on whether n is odd or even, respectively. It follows that f is irreducible but not primitive. ❖

Example 2.4.4. The *Fibonacci substitution* f of the alphabet $\{a, b\}$, which is given by

$$f : \begin{array}{lcl} a & \mapsto & ab, \\ b & \mapsto & a, \end{array}$$

is a primitive substitution. Indeed, both letters a and b appear in each of the words $f^2(a)$ and $f^2(b)$. The primitivity of f also follows from the square of the incidence matrix M of f , which is given by

$$M^2 = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}.$$

The substitution f has a unique fixed point w , which means that $f(w) = w$. The fixed point w of the Fibonacci substitution is known as the *Fibonacci word* and can be obtained under the iteration of f as

$$w = \lim_{n \rightarrow \infty} f^n(a) = abaaababaaabababababab \dots$$

❖

An infinite word $w = w_1 w_2 w_3 \dots$ which is a fixed point of a substitution f can be written, for each non-negative integer n , as $w = f^n(w_1) f^n(w_2) f^n(w_3) \dots$. We suppose that f^0 is the identity substitution. Each of the words $f^n(w_k)$ in the sequence, for $k = 1, 2, 3, \dots$, is called a *level- n superword* of w .

The *language of a substitution* f , denoted \mathcal{L}_f , is the set of all subwords of the words of the form $f^n(a)$, where n is a positive integer and a is a letter from \mathcal{A} . A word that belongs to \mathcal{L}_f is said to be *legal* for f . The following well-known lemma can be found, for example, in [96, Section 5.2].

Lemma 2.4.5. *For every primitive substitution f and every positive integer n , the languages of f and f^n are equal.* □

2.4.2 Periodic points of a primitive substitution

In Example 2.4.4, we introduced the fixed point of the Fibonacci substitution. More generally, given a substitution f , we consider fixed points of f^n , for positive integers n , that is, words w (finite or infinite) such that $f^n(w) = w$. We say that these words are *periodic points* of f or, if $n = 1$, *fixed points* of f . Periodic points of a substitution must not be confused with periodic sequences over an alphabet. In this section we present some well-known results concerning periodic points of primitive substitutions.

It is straightforward to see that any periodic point of a primitive substitution must be an infinite word. The following two lemmas, the proof of which we omit, are well-known facts that can be found, for example, in [96, Section 5.1].

Lemma 2.4.6. *Let f be a substitution of \mathcal{A} . Assume that, for some letter $a \in \mathcal{A}$, the first letter of the word $f(a)$ is a and its length is greater than 1. Then, the sequence of finite words $f(a), f^2(a), f^3(a), \dots$ converges to an infinite word over \mathcal{A} , which is the unique fixed point of f with first letter equal to a . \square*

Lemma 2.4.7. *Every primitive substitution has a non-zero finite number of periodic points. \square*

It is not difficult to show that any periodic point w of a primitive substitution f is a uniformly recurrent sequence. It can also be shown that w is linearly recurrent [40].

Theorem 2.4.8. *If f is a primitive substitution, then any periodic point of f is linearly recurrent. \square*

Therefore the Fibonacci word (see Example 2.4.4) is uniformly recurrent. However, a substitution f can have uniformly recurrent periodic points and not be a primitive substitution. For example, the infinite fixed point of the non-primitive substitution

$$\begin{aligned} 0 &\mapsto 0010, \\ 1 &\mapsto 1, \end{aligned}$$

is Chacon's sequence which, as we saw in Example 2.2.4, is uniformly recurrent.

The Perron–Frobenius' theorem (see, for example, [17, Section 2.4] or [96, Section 5.3.1]) implies that the incidence matrix M of a primitive substitution f has a simple positive (real-valued) eigenvalue that is larger in modulus than any other eigenvalue of M . This eigenvalue is called the *Perron–Frobenius eigenvalue* of M or f . The following theorem (which can be found, for example, in [17, Section 4.4]) provides a criterion for the aperiodicity of a fixed point of a primitive substitution.

Theorem 2.4.9. *Let f be a primitive substitution and w a periodic point of f . If the Perron–Frobenius eigenvalue of f is irrational, then w is an aperiodic infinite word. \square*

Note that it is the Perron–Frobenius eigenvalue of f that matters, not that of f^n , which can be rational. For example, the Perron–Frobenius eigenvalue of the Fibonacci substitution of Example 2.4.4 is the *golden ratio* $\frac{1}{2}(1 + \sqrt{5})$ which is an irrational number. So the Fibonacci word is an aperiodic infinite word.

There exist other aperiodicity tests that can be used when the Perron–Frobenius eigenvalue is rational (see, for example, Theorem 2.4.28 in Section 2.4.7).

2.4.3 Forward limit set of a substitution

In this section we define the forward limit set of a substitution f and show that, when there is not any letter that is fixed by any power of f , the forward limit set of f coincides with the set of periodic points of f . In Section 2.5.6 we will generalise the notion of forward limit set of a substitution to the forward limit set of a semigroup of substitutions.

Definition 2.4.10. The *forward limit set* of a subset A of \mathcal{A} for a substitution f is the set

$$\Lambda_f(A) = \{u \in \mathcal{A}^{\mathbb{N}} : f^{n_k}(a) \rightarrow u \text{ for some letter } a \text{ in } A \text{ and strictly increasing sequence } (n_k) \text{ in } \mathbb{N}\}.$$

The forward limit set of f is the set $\Lambda_f(\mathcal{A})$. We denote this set by Λ_f .

Observe that the forward limit set of a substitution f is, by definition, a closed subset of $\mathcal{A}^{\mathbb{N}}$ which is invariant under f .

We say that a substitution f of \mathcal{A} is *periodic-letter-free* if $f^n(a) \neq a$, for all letters $a \in \mathcal{A}$ and positive integers n .

Lemma 2.4.11. A substitution f of a finite alphabet \mathcal{A} has the periodic-letter-free property if, and only if, $|f^n(a)| \rightarrow \infty$ as $n \rightarrow \infty$, for each letter $a \in \mathcal{A}$.

Proof. If f is not periodic-letter-free, then there exist a positive integer k and a letter $a \in \mathcal{A}$ such that $f^k(a) = a$, so $|f^{kn}(a)| = 1$, for all positive integers n . Hence $|f^n(a)| \not\rightarrow \infty$ as $n \rightarrow \infty$. Conversely, suppose that $|f^n(a)| \rightarrow \infty$ as $n \rightarrow \infty$, for some letter $a \in \mathcal{A}$. The sequence $(|f^n(a)|)$ cannot be decreasing with n , so it must be eventually constant. Since \mathcal{A} is finite, we can find positive integers r and s (with $r > s$) for which $|f^r(a)| = |f^s(a)|$ and $\pi_1(f^r(a)) = \pi_1(f^s(a))$. Let $u = f^s(a)$, $v = f^r(a)$, $\ell = |u| = |v|$, $b = \pi_1(u) = \pi_1(v)$, and $g = f^{r-s}$. The fact that $v = g(u)$ and $|v| = |u|$ implies that $\pi_i(v) = g(\pi_i(u))$, for $i = 1, 2, \dots, \ell$. In particular, $g(\pi_1(u)) = \pi_1(v)$, so $g(b) = b$. Hence b is a periodic letter of f . \square

It can easily be shown that any periodic point of a periodic-letter-free substitution is an infinite word. The following lemma characterises the forward limit set of a periodic-letter-free substitution in terms of its periodic points.

Lemma 2.4.12. The forward limit set of a periodic-letter-free substitution f is equal to the set of all periodic points of f .

Proof. Since f is periodic-letter-free, any periodic point of f is an infinite word. Let $u \in \mathcal{A}^{\mathbb{N}}$ be a periodic point of f . Then there exists a positive integer m such that $f^m(u) = u$. Since f is periodic-letter-free, $|f^{mn}(\pi_1(u))| \rightarrow \infty$ as $n \rightarrow \infty$, so the sequence of words $f^m(\pi_1(u))$, $f^{2m}(\pi_1(u))$, $f^{3m}(\pi_1(u))$, \dots is a sequence of prefixes of u of increasing length. Therefore $f^{mn}(\pi_1(u)) \rightarrow u$ as $n \rightarrow \infty$, hence $u \in \Lambda_f$.

Conversely, let u be a point in Λ_f and let $b = \pi_1(u)$. Then there exist a letter $a \in \mathcal{A}$ and a sequence (n_k) of increasing positive integers such that $f^{n_k}(a) \rightarrow u$ as $k \rightarrow \infty$. Since \mathcal{A} is finite, by restricting to a

subsequence of (n_k) , we can assume that $\pi_1(f^{n_k}(a)) = b$, for all positive integers k . Then, for all positive integers i and j with $i < j$,

$$\pi_1(f^{n_j-n_i}(b)) = \pi_1(f^{n_j-n_i}(\pi_1(f^{n_i}(a)))) = \pi_1(f^{n_j-n_i} \circ f^{n_i}(a)) = \pi_1(f^{n_j}(a)) = b,$$

so $\pi_1(f^m(b)) = b$, where $m = n_j - n_i$. Since f is periodic-letter-free, $|f^m(b)| \rightarrow \infty$ as $m \rightarrow \infty$. Consequently there exists a non-empty finite word x over \mathcal{A} such that $f^m(b) = bx$. Then, by Lemma 2.4.6, $f^m(b) \rightarrow u$ and u is the unique fixed point of f^m with $\pi_1(u) = b$. \square

Example 2.4.13. Consider the three-letter substitution

$$\begin{aligned} a &\mapsto ab, \\ f: b &\mapsto ca, \\ c &\mapsto ba. \end{aligned}$$

Since f is periodic-letter-free, Λ_f is equal to the set of periodic points of f . The substitution f has only one fixed point $x = ab \dots$. But the substitution f^2 , given by

$$\begin{aligned} a &\mapsto abca, \\ f^2: b &\mapsto baab, \\ c &\mapsto caab, \end{aligned}$$

has three fixed points, x , $y = baab \dots$ and $z = caab \dots$. It then follows that $\Lambda_f = \{x, y, z\}$. \blacklozenge

The following example shows that we cannot relax the periodic-letter-free property in Lemma 2.4.12.

Example 2.4.14. Consider the two-letter substitution

$$\begin{aligned} f: a &\mapsto ab, \\ b &\mapsto b. \end{aligned}$$

For every increasing sequence (n_k) of positive integers, $f^{n_k}(b) \rightarrow b$ and $f^{n_k}(a) \rightarrow u$, where $u = abbb \dots$. So the forward limit set of f contains only the point u . The set of infinite words that are periodic (in fact fixed) points of f is $\{b^n abbb \dots : n \in \mathbb{N}_0\}$. \blacklozenge

2.4.4 Substitutive sequences

Lemma 2.4.6 says that, given a substitution f , if there is a letter a for which the word $f(a)$ starts with a and the sequence of lengths $|a|, |f(a)|, |f^2(a)|, \dots$ is unbounded as $n \rightarrow \infty$, then the sequence of words $a, f(a), f^2(a), \dots$ converges to an infinite word that is the unique fixed point of f starting with the letter a . Such an infinite word is called *purely substitutive*. The image of a purely substitutive infinite word under a *letter-to-letter substitution*, namely, a substitution that maps each letter to a letter, is called *substitutive*. (These notions are also called *purely morphic* and *morphic* in some of the literature.) Clearly, if an infinite word w is purely substitutive then it is substitutive, since w is mapped to itself under the identity

substitution. The following example illustrates that there are substitutive infinite words that are not purely substitutive.

Example 2.4.15. Consider the infinite word

$$w = a b a^2 b a^3 b a^4 b a^5 b \dots$$

whose reading presents, separated by the letter b , the increasing powers of the letter a . This sequence is substitutive. To see this, consider the substitution of the alphabet $\{a, b, c, d\}$ given by

$$g : \begin{aligned} a &\mapsto a, \\ b &\mapsto ba, \\ c &\mapsto cd, \\ d &\mapsto aaba. \end{aligned}$$

It is straightforward to show that $g^n(d) = a^2 b a^n$, for all positive integers n . It follows from the proof of Lemma 2.4.6 that the fixed point of g starting with the letter c is

$$v = \lim_{n \rightarrow \infty} g^n(c) = c d g(d) g^2(d) \dots = c d a^2 b a^3 b a^4 b a^5 b \dots,$$

which coincides with w from the third letter on. Now, let h be the letter-to-letter substitution given by

$$h : a \mapsto a, \quad b \mapsto b, \quad c \mapsto a, \quad d \mapsto b.$$

Then $w = h(v)$ and so w is substitutive. If w is also purely substitutive, then it must be the fixed point of some substitution f satisfying $f(a) = ax$, for some word $x \in \mathcal{A}^+$. Observe that w contains subwords $aa \dots a$ of arbitrary length, which are not preserved under f because $\pi_1(x) = b$. Then, w is not fixed by f , which is a contradiction. So w is not purely substitutive. \diamond

2.4.5 Constant-length substitutions and automatic sequences

Among the substitutive words, the class of automatic sequences has been widely studied. In 1972, Cobham introduced and studied automatic sequences as sequences generated by ‘uniform tag systems’ [34], also known as ‘finite automata with output function’ (background on automata theory can be found, for example, in [7, 93, 98]). Cobham showed that automatic sequences can also be defined using constant-length substitutions. This is the approach we take in this section.

We say that a substitution f of \mathcal{A} has *constant length* ℓ if, for every letter a , $f(a)$ is a word of length ℓ . In such a case, we can describe the substitution with ℓ functions $[f]_0, [f]_1, \dots, [f]_{\ell-1}$ from \mathcal{A} to \mathcal{A} such that

$$f(a) = [f]_0(a) [f]_1(a) \dots [f]_{\ell-1}(a),$$

for all $a \in \mathcal{A}$. We say that the functions $[f]_i$ are the *columns* of f .

Remark 2.4.16. Columns of constant-length substitutions will always be written with square brackets.

For a constant-length substitution f , $[f]_k$ denotes the k th column of f , $[f]_k^n$ or $([f]_k)^n$ denote the n -fold composition of $[f]_k$ with itself, and $[f^n]_k$ denotes the k th column of the substitution f^n . On the other hand, f_k^n or $(f_k)^n$ denote the n -fold composition of a substitution called f_k with itself. Expressions of the form $[f]^n$ and $[f_k]^n$ will not be used. ❖

The columns of a constant length substitution are examples of substitutions of constant length 1 or letter-to-letter substitutions, which are also known as *codings*. An *automatic sequence* is an infinite word that is the image, under a coding, of a fixed point of a constant-length substitution. If this last substitution has constant length ℓ , for some integer ℓ greater than 1, we say that the infinite word is ℓ -*automatic*.

Example 2.4.17. In Examples 2.2.1 and 2.2.2 we defined the Thue–Morse word v , first by using the bar operation that replaces 0s with 1s and 1s with 0s and second by taking the sum of the binary digits of the non-negative integers (modulo 2). The infinite word v also admits a definition as a 2-automatic sequence, since it can be obtained as one of the two fixed points of the *Thue–Morse substitution* θ , given by

$$\theta: \begin{array}{lcl} 0 & \mapsto & 01, \\ 1 & \mapsto & 10. \end{array}$$

The Thue–Morse word is the fixed point of θ starting with the letter 0. The other fixed point of θ is \bar{u} . ❖

Example 2.4.18. Consider folding a piece of paper onto itself n times and unfolding it afterwards, and code the “up” folds and “down” folds in a binary word w_n over two symbols, say 0 and 1. The sequence of finite words obtained for $n = 1, 2, 3, \dots$, namely,

$$w_1 = 0, \quad w_2 = 001, \quad w_3 = 0010011, \quad w_4 = 001001100011011, \quad \dots,$$

converges to the infinite word

$$00100110001101100010011100110110\dots,$$

known as the *paper-folding sequence*. This sequence is a 2-automatic sequence, which can be obtained by considering the fixed point of the substitution

$$\begin{array}{lcl} a & \mapsto & ab, \\ b & \mapsto & cb, \\ c & \mapsto & ad, \\ d & \mapsto & cd, \end{array}$$

known as the *paper-folding substitution*, and computing the image of that fixed point under the coding

$$a \mapsto 0, \quad b \mapsto 0, \quad c \mapsto 1, \quad d \mapsto 1,$$

(see, for example, [5, Part I, Seccion 3] and [17, Section 4.5.2]). ❖

A sequence can be ℓ -automatic and k -automatic for two different integers ℓ and k . For instance, Eilenberg showed that a sequence is ℓ -automatic if, and only if, it is ℓ^n -automatic for every positive

integer n [45]. Thus the Thue–Morse word is 2^n -automatic for all $n \in \mathbb{N}$. Another important result is due to Cobham. We say that two real numbers k and ℓ greater than one are *multiplicatively independent* if the only integers n and m such that $k^n = \ell^m$ are $n = m = 0$, otherwise k and ℓ are *multiplicatively dependent*. Equivalently, k and ℓ are multiplicatively independent if $\log k / \log \ell$ is irrational and multiplicatively dependent otherwise. Cobham showed that if an infinite word is both k -automatic and ℓ -automatic, for multiplicatively independent positive integers k and ℓ , then it is eventually periodic [33].

Example 2.4.19. The periodic infinite word $w = ababa \dots$ is ℓ -automatic, for every integer ℓ greater than one. Indeed, for all positive integers n , w is a fixed point of each of the binary substitutions

$$\begin{array}{ll} a \mapsto (ab)^n, & \text{and} \quad a \mapsto (ab)^n a, \\ b \mapsto (ab)^n, & b \mapsto (ba)^n b. \end{array}$$

❖

The following example is interesting because it shows the non-trivial fact that the fixed point of a non-constant-length substitution can be automatic.

Example 2.4.20. For every positive integer n , let u_n be the number of 1s between the n th and $(n + 1)$ st occurrence of 0 in the Thue–Morse word. Then, the infinite word u defined as

$$u = u_1 u_2 u_3 \dots = 210201210120210201 \dots$$

is the unique fixed point of the substitution

$$\begin{array}{ll} 0 \mapsto 1, \\ 1 \mapsto 20, \\ 2 \mapsto 210, \end{array}$$

as shown by Brestel in [26]. He also showed that u is 2-automatic. Indeed, it can be obtained as the image of the fixed point beginning with 0 of the substitution

$$\begin{array}{ll} 0 \mapsto 01, \\ 1 \mapsto 20, \\ 2 \mapsto 23, \\ 3 \mapsto 02, \end{array}$$

under the coding

$$0 \mapsto 2, \quad 1 \mapsto 1, \quad 2 \mapsto 0, \quad 3 \mapsto 1.$$

❖

There are also fixed points of non-constant-length substitutions which are not automatic, such as the Fibonacci word of Example 2.4.4 or the following example.

Example 2.4.21. The substitution

$$\begin{aligned} a &\mapsto cac, \\ b &\mapsto accac, \\ c &\mapsto abcac, \end{aligned}$$

has no fixed point, but its square has two fixed points, neither of which are ℓ -automatic for any value of $\ell \geq 2$ (see [5, Part I, Section 4]). \diamond

In a recent paper by Allouche and Shallit [9] we find an interesting counterpoint to the previous examples. Their result shows that any ℓ -automatic sequence, with $\ell \geq 2$, can be obtained as the fixed point, under a coding, of a non-constant-length substitution. In the paper, no explicit example is given. Following the steps in their proof, we have constructed the following example to illustrate this result.

Example 2.4.22. The Thue–Morse word (Example 2.2.2) can be obtained as the image of the fixed point beginning with 0 of the non-constant-length substitution

$$\begin{aligned} 0 &\mapsto 01123001, \\ 1 &\mapsto 10010110, \\ 2 &\mapsto 0, \\ 3 &\mapsto 110100110010110, \end{aligned}$$

under the coding

$$0 \mapsto 0, \quad 1 \mapsto 1, \quad 2 \mapsto 0, \quad 3 \mapsto 1.$$

\diamond

2.4.6 Coincidences admitted by a constant-length substitution

We say that a substitution f of constant length ℓ admits a *coincidence* at order n , for some positive integer n , if the substitution f^n has a column all of whose entries are equal. In other words, f admits a coincidence at order n if there exists an integer $0 \leq k \leq \ell^n - 1$ such that $[f^n]_k(a) = [f^n]_k(b)$, for all letters a and b in \mathcal{A} (see, for example, [38] and [96, Section 6.3.1]). If $[f^n]_k(a) = [f^n]_k(b)$, for all letters a and b in a subset $A \subseteq \mathcal{A}$ with $1 < |A| < |\mathcal{A}|$, then we say that f admits a *partial coincidence* at order n .

Example 2.4.23. One of the simplest substitutions admitting coincidences is the two-letter substitution f given by

$$f: \begin{aligned} 0 &\mapsto 01, \\ 1 &\mapsto 00, \end{aligned}$$

which is known as the *period-doubling substitution* (see, for example, [17, Section 4.5.1]). This substitution is also known as *Feigenbaum's substitution*, as it is related to the itinerary of the critical value of Feigenbaum's interval map (see, for example, [74]). The unique fixed point of f ,

$$0100010101000100010001010100\dots,$$

is known as the *period-doubling word*. Let us call it w and index its first entry with 1, that is, $w = w_1 w_2 w_3 \dots$. Then, for each $n \geq 1$, we can determine w_n by taking, modulo 2, the exponent of the largest power 2^k dividing n . In other words,

$$w_n \equiv \max\{k \geq 0 : 2^k \mid n\} \pmod{2}.$$

For example, $w_{96} = 1$ because $96 = 2^5 \cdot 3$ and $5 \equiv 1 \pmod{2}$. The period-doubling word is an example of a *Toeplitz sequence*, namely, an infinite word every one of whose letters is part of an infinite monochromatic arithmetic progression. More precisely, for each position $n \geq 1$, there exists a difference $d \geq 1$ such that $w_n = w_{n+dk}$ holds for all $k \geq 0$ (see [55, 67]). ♦

Example 2.4.24. Consider the paper-folding substitution introduced in Example 2.4.18, which we recall is given by

$$f : \begin{array}{lcl} a & \mapsto & a b, \\ b & \mapsto & c b, \\ c & \mapsto & a d, \\ d & \mapsto & c d. \end{array}$$

Observe that there are two partial coincidences in each of the leftmost and rightmost columns of f . Consequently, f admit (total) coincidences at order 2, explicitly displayed here

$$f^2 : \begin{array}{lcl} a & \mapsto & a b c b, \\ b & \mapsto & a d c b, \\ c & \mapsto & a b c d, \\ d & \mapsto & a d c d. \end{array}$$

♦

2.4.7 Column group of a bijective substitution

We say that a substitution f of constant length ℓ is *bijective* if each of the functions $[f]_i$ defining a column is a bijection, that is, if $[f]_i(a) \neq [f]_i(b)$ whenever a and b are different letters of \mathcal{A} . Therefore, each of the columns of a bijective substitution can be interpreted as a permutation of \mathcal{A} . Consequently, a bijective substitution admits no coincidences at any order. We refer to the group generated by the columns of a bijective substitution f as the *column group* of f , referred to as the ‘group automaton’ in [96] (other uses of the column group include [19, 28], where generalised symmetries of shift spaces are studied, and [71], where the column group of f is related to the Ellis semigroup of the subshift generated by f).

Example 2.4.25. The Thue–Morse substitution defined in Example 2.4.17 is a bijective substitution. Its columns correspond to the two permutations of the binary alphabet $\{0, 1\}$, so the column group of the Thue–Morse substitution is isomorphic to S_2 , the symmetric group of order 2. ♦

Example 2.4.26. Consider the substitution f of the alphabet $\{a, b, c\}$ given by

$$\begin{aligned} a &\mapsto abb, \\ f : b &\mapsto bac, \\ c &\mapsto cca. \end{aligned}$$

The columns of f are the permutations $[f]_0 = \text{id}$, $[f]_1 = (ab)$ and $[f]_2 = (abc)$, which we write using disjoint cycle notation. The group generated by these columns is the symmetric group S_3 . ❖

Example 2.4.27. Let f be the substitution of the alphabet $\{a, b, c, d\}$ given by

$$\begin{aligned} a &\mapsto abb, \\ f : b &\mapsto bca, \\ c &\mapsto cad, \\ d &\mapsto ddc, \end{aligned}$$

whose columns are $[f]_0 = \text{id}$, $[f]_1 = (abc)$ and $[f]_2 = (ab)(cd)$. It is straightforward to show that the group generated by the columns of f is the alternating group A_4 . ❖

In Chapter 4, we will use the column group of bijective substitutions to obtain results about monochromatic arithmetic progressions in the fixed points of these substitutions. We will need that the fixed points considered are aperiodic infinite words. Theorem 2.4.9 introduced in Section 2.4.2 says that a fixed point of a primitive substitution is aperiodic, if the Perron–Frobenius eigenvalue of the substitution is irrational. However, we cannot determine whether the fixed point is aperiodic, if the Perron–Frobenius eigenvalue is rational. If the infinite words considered are fixed points (or, in general, substitution periodic points) of bijective substitutions, there exist sufficient and necessary conditions for aperiodicity, as the following theorem states (see [71, Proposition 4.1]).

Theorem 2.4.28. *Let f be a primitive, bijective substitution of a finite alphabet \mathcal{A} . Then a fixed point of f is aperiodic if, and only if, there exist distinct legal words of length 2 which either share the same starting or ending letter.* □

Example 2.4.29. Consider the Thue–Morse substitution θ introduced in Example 2.4.17. The incidence matrix of θ is

$$\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix},$$

and one can easily check that its Perron–Frobenius eigenvalue is rational. So the Perron–Frobenius criterion cannot be used to check whether the Thue–Morse sequence w , the fixed point of θ starting with 0, is aperiodic. Nonetheless, since 00 and 01 are both subwords of w , the Thue–Morse sequence is aperiodic, by Theorem 2.4.28. ❖

2.4.8 Height of a constant-length substitution

Consider a substitution f of \mathcal{A} of constant length ℓ , which has an infinite fixed point $w \in \mathcal{A}^{\mathbb{N}_0}$. Observe that the first letter of w is assumed to be at position 0. The *height* of f is the greatest integer that is coprime with ℓ and divides every position i with $w_i = w_0$. We denote it by $h(f)$. In other words, the height of f is

$$h(f) = \max \{n \geq 1 : \gcd(n, \ell) = 1, n \mid \gcd\{i : w_i = w_0\}\}.$$

It can be shown that $1 \leq h(f) \leq k$, where k is the cardinality of \mathcal{A} , and if $h(f) = k$, then w is periodic. Moreover, for a given substitution f , $h(f)$ can be algorithmically computed. Details can be found, for instance, in [38] and [96, Section 6.1]. It can also be shown that the height of a primitive constant-length substitution f is independent of the fixed point chosen for its definition. In other words, if f is primitive, $h(f)$ is uniquely defined. This may not be the case if f is not primitive, as Example 2.4.30 shows. Consequently, we shall only be concerned about the height of primitive substitutions of constant length.

Example 2.4.30. Consider the two-letter substitution f of constant length $\ell = 3$ given by

$$f : \begin{array}{lcl} a & \mapsto & a b a, \\ b & \mapsto & b b b. \end{array}$$

Let $w \in \mathcal{A}^{\mathbb{N}_0}$ be the fixed point of f that starts with the letter a , which is given by

$$w = a b a b^3 a b a b^9 a b a b^3 a b a b \dots.$$

It is not difficult to see that the a letters come precisely at even positions and so

$$\gcd\{i \geq 1 : w_i = w_0\} = 2,$$

which, together with the fact that $\gcd\{2, \ell\} = 1$, gives a height of 2. On the other hand, the fixed point of f starting with the letter b is the infinite word $bbb \dots$, which leads to a height of 1. \diamond

Let f be a primitive substitution of a finite alphabet \mathcal{A} that has constant length ℓ and height $h = h(f)$, and let $w \in \mathcal{A}^{\mathbb{N}_0}$ be a fixed point of f . We can split w into words over \mathcal{A} of length h and use these words as the symbols to define an alphabet \mathcal{B} . More precisely,

$$\mathcal{B} = \{w_{[nh, (n+1)h)} : n \geq 0\}.$$

Notice that \mathcal{B} is finite because the number of words over \mathcal{A} of length h is always finite. Since a ‘letter’ in \mathcal{B} is a word of the form $x \in \mathcal{A}^h$, the word $f(x)$ has length $h\ell$ over \mathcal{A} and it has length ℓ over \mathcal{B} . We can then define a substitution g over \mathcal{B} of constant length ℓ by setting $g(x)$ equal to the splitting of $f(x)$ into words of length h , for each $x \in \mathcal{B}$. The new substitution g is called the *pure base* of f . It can be shown that the height of g is always 1. Moreover, $g = f$ if $h(f) = 1$, because in this case $\mathcal{B} = \mathcal{A}$.

We do not give more details, which can be found, for instance, in [38] and [96, Section 6.3.1]. Instead, let us consider an example.

Example 2.4.31. Consider the substitution f of the alphabet $\mathcal{A} = \{a, b, c\}$ given by

$$\begin{aligned} a &\longmapsto aba, \\ f: b &\longmapsto bac, \\ c &\longmapsto cab, \end{aligned}$$

which has length $\ell = 3$. Since, as one can easily check, f is a primitive substitution, $h(f)$ does not depend on the fixed point employed in its definition. So, among the fixed points of f , we can choose $u \in \mathcal{A}^{\mathbb{N}_0}$ that starts with a , which looks like

$$u = ababacababacababacabababacac \dots$$

It is not difficult to see, from the substitution itself, that the only words of length 2 occurring in the language of f , hence in u , are ab , ba , ac and ca . It then follows that $u_n = a$ if, and only if, n is even. Therefore,

$$\gcd\{i \geq 1 : u_i = u_0\} = \gcd\{i \geq 1 : i \in 2\mathbb{N}\} = 2$$

and since 2 and ℓ are relatively prime integers, then $h(f) = 2$.

Let us now obtain the pure base g of f . The words of length $h(f) = 2$ that appear in the positions where the a letters occur in u are ab and ac . Thus, we can split u as follows

$$u = ab \ ab \ ac \ ab \ ab \ ac \ ab \ ac \ ab \ ab \ ab \ ac \dots$$

Since

$$f(ab) = ab \ ab \ ac \quad \text{and} \quad f(ac) = ab \ ac \ ab,$$

we can identify ab and ac with two new symbols x and y , respectively, and write the pure base of f as

$$g: \begin{aligned} x &\longmapsto xxy, \\ y &\longmapsto xyx. \end{aligned}$$

This new substitution is obviously primitive and it has height 1. Indeed, let $v \in \{x, y\}^{\mathbb{N}_0}$ be the fixed point of g starting with the letter x . The beginning of v , which look like $v = xxyxxyxyx \dots$, shows that $v_3 = v_4 = v_0$ and since 3 and 4 are coprime, the result follows. \blacklozenge

2.4.9 Hull and subshift of a substitution

Consider the *shift map* $\sigma: \tilde{\mathcal{A}} \rightarrow \tilde{\mathcal{A}}$ given by $\sigma(a_1 a_2 \dots) = a_2 a_3 \dots$ with $a_i \in \mathcal{A}$. More precisely, σ is the self-map of $\tilde{\mathcal{A}}$ that, for any $w \in \tilde{\mathcal{A}}$, satisfies

$$\pi_k(\sigma(w)) = \pi_{k+1}(w),$$

for all $k \in \mathbb{N}$ (with $k < |w|$ if w is finite). This map is continuous.

We now define the hull and the subshift of a substitution f . The closure of a subset $Y \subseteq \tilde{\mathcal{A}}$ in $\tilde{\mathcal{A}}$ is denoted by \overline{Y} . We write $\Lambda_f(a)$ for $\Lambda_f(\{a\})$, where a is a letter of \mathcal{A} . Recall that, moreover, $\sigma(Y)$ denotes the set $\{\sigma(y) : y \in Y\}$.

Definition 2.4.32. The *hull* of the letter a of \mathcal{A} for the substitution f is the set

$$\Omega_f(a) = \overline{\bigcup_{n=0}^{\infty} \sigma^n(\Lambda_f(a))}.$$

The *hull* of f is the set $\bigcup_{a \in \mathcal{A}} \Omega_f(a)$. We denote this set by Ω_f .

For a set X of infinite words, the set $\bigcup_{n=0}^{\infty} \sigma^n(X)$ is called the *shift-orbit* of X . So the hull of a letter a of \mathcal{A} for the substitution f is the closure of the shift-orbit of $\Lambda_f(a)$ and, since \mathcal{A} is a finite set, the hull of f is the closure of the shift-orbit of its forward limit set, that is, $\Omega_f = \overline{\bigcup_n \sigma^n(\Lambda_f)}$.

From Section 2.2.1, we recall that the language $\mathcal{L}(w)$ of an infinite word w over \mathcal{A} is the set of all subwords of w . From Section 2.4.1, we recall also that the language \mathcal{L}_f of a substitution f is the set of all subwords of the words of the form $f^n(a)$, where n is a positive integer and a is a letter from \mathcal{A} .

Definition 2.4.33. The *subshift* of a substitution f of \mathcal{A} is the set

$$\mathbb{X}_f = \{w \in \mathcal{A}^{\mathbb{N}} : \mathcal{L}(w) \subseteq \mathcal{L}_f\}.$$

Example 2.4.34. Consider the substitution

$$f : \begin{array}{ll} a & \mapsto b a b, \\ b & \mapsto b. \end{array}$$

It is straightforward to see that $f^n(a) = b^n a b^n$, for all positive integers n . So $f^{n_k}(a) \rightarrow u$ where $u = bbb \dots$, for all increasing sequences (n_k) in \mathbb{N} . Then, $\Lambda_f = \{u\}$ and therefore, the hull of f is $\Omega_f = \{u\}$. On the other hand, the subshift of f is $\mathbb{X}_f = \{bbb \dots\} \cup \{b^n abbb \dots : n \in \mathbb{N}_0\}$. \diamond

The hull of a substitution is necessarily included in its subshift, that is, $\Omega_f \subseteq \mathbb{X}_f$, and in general equality does not hold (consider the previous example). Nevertheless, Ω_f and \mathbb{X}_f are equal when f is a primitive substitution (see, for example, [96, Proposition 5.3]).

Theorem 2.4.35. *The hull and the subshift of a primitive substitution f are equal to each other, and they are uniquely given by the closure of the shift-orbit of any periodic point of f .* \square

A *shift dynamical system* (Y, σ) consists of a closed subset Y of $\tilde{\mathcal{A}}$ that is invariant under σ . It is easy to verify that both Ω_f and \mathbb{X}_f are closed and shift-invariant subsets of $\mathcal{A}^{\mathbb{N}}$, hence (Ω_f, σ) and (\mathbb{X}_f, σ) are shift dynamical systems. We say that a shift dynamical system (Y, σ) is *aperiodic* if each $y \in Y$ is an aperiodic infinite word, and we say that a substitution f is *aperiodic* if (\mathbb{X}_f, σ) is aperiodic. For example, the Fibonacci and the Thue–Morse substitutions are aperiodic.

A shift dynamical system (Y, σ) is *linearly recurrent* if each $y \in Y$ is a linearly recurrent infinite word. Durand proved the following result in [40] (see also [42]).

Theorem 2.4.36. *If a substitution f is primitive, then (\mathbb{X}_f, σ) is linearly recurrent.* \square

Furthermore, there are non-primitive substitutions f for which (\mathbb{X}_f, σ) is linearly recurrent.

A shift dynamical system (Y, σ) is *minimal* if, for all $y \in Y$, the shift-orbit of y is dense in Y . This implies that the only closed subsets of Y that are invariant under σ are the empty set and Y itself. In 2006, Damanik and Lenz proved the following result [37].

Theorem 2.4.37. *(\mathbb{X}_f, σ) is linearly recurrent if, and only if, it is minimal.* \square

For example, the dynamical systems associated with the Fibonacci substitution and with the Thue–Morse substitution are aperiodic, minimal and linearly recurrent. Background in subshifts and hulls can be found, for example, in [17, Chapter 4] and [96, Chapter 5].

2.4.10 Recognisability

For a substitution f and a long enough word w in the language of f , recognisability is a form of injectivity of f that allows one to uniquely desubstitute the word w to another word v in the language of f , that is, to express w as a concatenation of substitution words dictated by the letters of v . The precise definition is the following.

Definition 2.4.38. A substitution f of \mathcal{A} is *recognisable* if there is a positive integer n such that every word in the language of f of length at least n can be uniquely written as $xf^k(u)y$, where k is a positive integer, x is a suffix of $f^k(a)$ with $a \in \mathcal{A}$ or the empty word, y is a prefix of $f^k(b)$ with $b \in \mathcal{A}$ or the empty word, and u is a word over \mathcal{A} such that aub belongs to the language of f .

Background material in recognisability can be found, for example, in [96, Section 5.5.2] and [74, Section 4.3], and references therein. For the latest advances regarding recognisability we refer the reader to [20,25]. In Chapter 3 we will use the fact that the Thue–Morse substitution, as well as some generalised Thue–Morse substitutions, are recognisable.

Example 2.4.39. Let θ be the Thue–Morse substitution of Example 2.4.17, which we recall is given by

$$\begin{aligned} \theta : \quad 0 &\longmapsto 01, \\ 1 &\longmapsto 10. \end{aligned}$$

Consider, for example, the word $w = 0010$, which belongs to the language of θ . This word can be written as $x\theta^k(u)y$ with $k = 1$ and $u = x = y = 0$, where x is the rightmost letter of $\theta^k(a)$ with $a = 1$ and y is the leftmost letter of $\theta^k(b)$ with $b = 0$. Also, note that the word aub belongs to the language of θ . Furthermore, there is no other way to write w as in Definition 2.4.38; otherwise we could write w as a concatenations of two substitution words from $\{\theta(0), \theta(1)\}$, which is not possible since 00 is not

a substitution word. Similarly, it can be shown that every word of length at least 4 in the language of θ can be written as in Definition 2.4.38 in a unique way. So the Thue–Morse substitution is recognisable (see [96, Section 5.5.2, Example 1] for further details). ❖

Example 2.4.40. The Fibonacci substitution of Example 2.4.4, which we recall is given by

$$f : \begin{array}{lcl} a & \mapsto & ab, \\ b & \mapsto & a, \end{array}$$

can easily be seen to be recognisable, since each letter a in a word that belongs to the language of f is the beginning of some substitution word $f(0)$ or $f(1)$ [96, Section 5.5.2, Example 2]. ❖

2.5 Semigroups of substitutions

In the previous sections we introduced the notions of forward limit set, hull and subshift of a substitution. Now, we consider the semigroup generated by a given family of substitutions and define its forward limit set (Section 2.5.6) and its hull and subshift (Section 2.5.7). Throughout this thesis \mathcal{F} will denote a non-empty collection of substitutions defined over the same alphabet, which will typically be finite. We can form words over \mathcal{F} , just as we formed words over \mathcal{A} (see Section 2.2.1), giving rise to a semigroup \mathcal{F}^+ with composition given by concatenation of words. This is not the semigroup of primary interest though; our main focus is the semigroup obtained from \mathcal{F} through composition of functions, which we will call the substitution semigroup generated by \mathcal{F} .

The dynamics of compositions of sequences of substitutions is studied by the theory of s-adic sequences, so we first introduce the notion of s-adic sequence (Section 2.5.1). In Chapter 5 we will see that the forward limit set of a substitution semigroup generated by a finite set of substitutions \mathcal{F} typically coincides with the set of all possible s-adic limits of \mathcal{F} , and thus gives a global view of s-adic systems.

2.5.1 s-adic sequences

We recall from Section 2.4.4 that a purely substitutive sequence x over an alphabet \mathcal{A} is the limit of $f^n(a)$ as n goes to infinity, for some substitution f of \mathcal{A} and letter a in \mathcal{A} . In other words,

$$x = \lim_{n \rightarrow \infty} f^n(a).$$

The limit exists because $f(a)$ is a word of length at least 2, which has a as its first letter. A purely substitutive sequence is an example of an s-adic sequence. More precisely, we say that x is an s-adic limit of f . The ‘s’ in s-adic stands for ‘substitutive’ and the term ‘adic’ refers to an inverse limit for a product of substitutions. Background theory of s-adic sequences can be found, for example, in [24, Section 4.11], [108, Chapter 3], and [23].

Definition 2.5.1. An infinite word x over \mathcal{A} is an *s-adic limit* of a family of substitutions \mathcal{F} if there exist

sequences (f_n) in \mathcal{F} and (a_n) in \mathcal{A} with $f_1 \circ f_2 \circ \cdots \circ f_n(a_n) \rightarrow x$ as $n \rightarrow \infty$. In other words,

$$x = \lim_{n \rightarrow \infty} f_1 \circ f_2 \circ \cdots \circ f_n(a_n).$$

The sequence f_1, f_2, f_3, \dots is called the *directive sequence* for x .

There is a more general definition of s-adic limit where the substitutions in the directive sequence are defined on possibly different alphabets. A usual requirement is that either the sizes of those alphabets are bounded or, as in our case, that all the substitutions are defined on the same alphabet (see, for instance, [23]). Typically one considers a finite family of substitutions, and sometimes further requirements may be necessary in order for the limit to make sense.

Example 2.5.2. Consider the Fibonacci substitution and the Thue–Morse substitution introduced in Examples 2.4.4 and 2.4.17, respectively, which using the alphabet $\mathcal{A} = \{a, b\}$ are given by

$$f : \begin{array}{lcl} a & \mapsto & ab, \\ b & \mapsto & a, \end{array} \quad \text{and} \quad g : \begin{array}{lcl} a & \mapsto & ab, \\ b & \mapsto & ba. \end{array}$$

The unique fixed point of the substitution $f \circ g$ is the s-adic limit of $\{f, g\}$ given by

$$\lim_{n \rightarrow \infty} (f \circ g)^n(a) = abaaababababababab \dots$$

Observe that the directive sequence for this infinite word is periodic, namely, f, g, f, g, f, g, \dots .

We can also consider a directive sequence (f_n) that is not periodic, such as, $f_n = g$ if n is prime and $f_n = f$ otherwise. This is the directive sequence for the infinite word obtained as the limit of the sequence $(F_n(a))$, where $F_n = f_1 \circ f_2 \circ \cdots \circ f_n$,

$$\begin{aligned} F_1(a) &= f(a) = ab, \\ F_2(a) &= f \circ g(a) = abab, \\ F_3(a) &= f \circ g \circ g(a) = abaaab, \\ F_4(a) &= f \circ g \circ g \circ f(a) = abaaabababab, \\ F_5(a) &= f \circ g \circ g \circ f \circ g(a) = abaaababababababab, \\ &\dots \end{aligned}$$

Since $f(a) = g(a) = ab$, we see that

$$F_{n+1}(a) = F_n \circ f_{n+1}(a) = F_n(ab) = F_n(a) F_n(b),$$

for every positive integer n . Since $|F_n(a)| \rightarrow \infty$ as $n \rightarrow \infty$, we see that

$$d(F_n(a), F_{n+1}(a)) = \frac{1}{2^{|F_n(a)|}} \rightarrow 0,$$

so the sequence $(F_n(a))$ converges to a word $x \in \tilde{\mathcal{A}}$, by completeness of the metric space $(\tilde{\mathcal{A}}, d)$. In fact,

$x \in \mathcal{A}^{\mathbb{N}}$ because $|F_n(a)| \rightarrow \infty$, so x is an s-adic limit of $\{f, g\}$.

If instead we choose the sequence of letters (a_n) with $a_n = b$ if n is prime and $a_n = a$ otherwise, and we consider the same sequence of substitutions (f_n) , then

$$\begin{aligned} F_1(a_1) &= f(a) = a b, \\ F_2(a_2) &= f \circ g(b) = a a b, \\ F_3(a_3) &= f \circ g \circ g(b) = a a b a b a, \\ F_4(a_4) &= f \circ g \circ g \circ f(a) = a b a a a b a b a b a, \\ F_5(a_5) &= f \circ g \circ g \circ f \circ g(b) = a b a a a b a b a a a b a b a b a, \\ &\dots \end{aligned}$$

Next, we show that this sequence does not converge. Assume, to the contrary, that $(F_n(a_n))$ is a convergent sequence. Then, for all large enough n , $F_n(a_n)$ is a prefix of $F_{n+1}(a_{n+1})$. For every prime $n \geq 3$,

$$F_n(a_n) = F_n(b) \quad \text{and} \quad F_{n+1}(a_{n+1}) = F_n \circ f(a) = F_n(a) F_n(b).$$

Observe that both $f_n(a) = g(a)$ and $f_n(b) = g(b)$ consists of one a letter and one b letter. This implies that $|F_n(a)| = |F_n(b)|$. Furthermore, the last letter of $f(a)$ and the last letter of $f(b)$ are different, and similarly, the last letter of $g(a)$ and the last letter of $g(b)$ are different. This implies that the last letter of $F_n(a)$ and the last letter of $F_n(b)$ are different. So $F_n(b)$ is not a prefix of $F_n(a)$. Consequently, $F_n(a_n)$ is not a prefix of $F_{n+1}(a_{n+1})$, which contradicts the assumption we made. Hence $(F_n(a_n))$ does not converge, as required. \diamond

2.5.2 General properties of substitution semigroups

Definition 2.5.3. The *substitution semigroup* generated by a set of substitutions \mathcal{F} is the set of all finite compositions of functions from \mathcal{F} . We denote it by S . In other words,

$$S = \{f_1 \circ f_2 \circ \dots \circ f_n : f_i \in \mathcal{F}, n \in \mathbb{N}\}.$$

We say that S is *finitely-generated* if it has a finite generating set.

The *language of a substitution semigroup* S , denoted \mathcal{L} , is the set of all words appearing as subwords of $f(a)$, for some letter $a \in \mathcal{A}$ and substitution $f \in S$. Any of these words is said to be *legal* for S . If S is generated by a single substitution, this definition coincides with the definition of the language of a substitution given in Section 2.4.

We say that a substitution semigroup S is *irreducible* if, for any two letters $a, b \in \mathcal{A}$, there exists a substitution $f \in S$ such that the word $f(a)$ contains the letter b . If S is generated by a single substitution, this definition coincides with the definition of an irreducible substitution given in Section 2.4.

The definition of a primitive substitution, however, cannot so easily be extended to multiple substitutions. Observe that the functional composition of non-primitive substitutions may result in a primitive

substitution. For example, neither

$$f: \begin{array}{l} a \mapsto ab, \\ b \mapsto b, \end{array} \quad \text{nor} \quad g: \begin{array}{l} a \mapsto a, \\ b \mapsto ba, \end{array}$$

is primitive, but

$$f \circ g: \begin{array}{l} a \mapsto ab, \\ b \mapsto bab, \end{array}$$

is primitive. The opposite is also true; the composition of primitive substitutions may result in a non-primitive substitution. Consider, for example,

$$f: \begin{array}{l} a \mapsto ab, \\ b \mapsto a, \end{array} \quad \text{and} \quad g: \begin{array}{l} a \mapsto b, \\ b \mapsto ba, \end{array}$$

both of which are primitive substitutions, whereas

$$f \circ g: \begin{array}{l} a \mapsto a, \\ b \mapsto aab, \end{array}$$

is not primitive.

We will define primitive substitution semigroups as an extension of primitive directive sequences in the theory of s-adic sequences [23]. We say that a substitution semigroup S with generating set \mathcal{F} is *primitive* if there exists a positive integer n such that, for all letters $a, b \in \mathcal{A}$, all the words of the form $f_1 \circ f_2 \circ \cdots \circ f_n(a)$, where $f_i \in \mathcal{F}$, contain the letter b . If S is generated by a single substitution, this definition coincides with the definition of a primitive substitution given in Section 2.4. Note that S being primitive implies that every $f \in S$ is a primitive substitution (in particular, every generator from \mathcal{F} is primitive) and that S is irreducible.

Example 2.5.4. The substitution semigroup S generated by the Fibonacci substitution f and the Thue–Morse substitution g , which are given by

$$f: \begin{array}{l} a \mapsto ab, \\ b \mapsto a, \end{array} \quad \text{and} \quad g: \begin{array}{l} a \mapsto ab, \\ b \mapsto ba, \end{array}$$

is primitive (hence it is also irreducible). ❖

Example 2.5.5. Consider the substitution semigroup S generated by

$$f: \begin{array}{l} a \mapsto ab, \\ b \mapsto a, \end{array} \quad \text{and} \quad g: \begin{array}{l} a \mapsto b, \\ b \mapsto ba, \end{array}$$

both of which are primitive substitutions. The semigroup S is irreducible. However, it is not primitive. For example, the substitution

$$f \circ g: \begin{array}{l} a \mapsto a, \\ b \mapsto aab, \end{array}$$

is not primitive. ❖

2.5.3 Presentation of a substitution semigroup

Let S be a substitution semigroup generated by \mathcal{F} . As we mentioned earlier, we must distinguish a word over \mathcal{F} from the element of S it represents.

Definition 2.5.6. Let F be the map from \mathcal{F}^+ onto S that sends the n -letter word $f_1 f_2 \cdots f_n$ over the alphabet \mathcal{F} to the substitution $f_1 \circ f_2 \circ \cdots \circ f_n$ in S . In other words,

$$F(f_1 f_2 \cdots f_n) = f_1 \circ f_2 \circ \cdots \circ f_n.$$

We say that the word $f_1 f_2 \cdots f_n$ *represents* the substitution $f_1 \circ f_2 \circ \cdots \circ f_n$.

Let \mathcal{R} be a subset of $\mathcal{F}^+ \times \mathcal{F}^+$ and let f and g be two words over \mathcal{F} . We say that g is *obtained from f by one application of one pair from \mathcal{R}* if there exist $u, v \in \mathcal{F}^*$ and $(s, t) \in \mathcal{R}$ such that $f = usv$ and $g = utv$. We say that g is *obtained from f by applications of pairs from \mathcal{R}* if there exists a finite sequence h_1, h_2, \dots, h_n in \mathcal{F}^+ such that $h_1 = f$, $h_n = g$ and h_i is obtained from h_{i-1} by one application of one pair from \mathcal{R} , for all $i = 2, 3, \dots, n$.

We say that $\langle \mathcal{F} \mid \mathcal{R} \rangle$ is a *presentation* of a substitution semigroup S if \mathcal{F} is a generating set of S and \mathcal{R} is a set of pairs $(u, v) \in \mathcal{F}^+ \times \mathcal{F}^+$ such that, for any pair $(f, g) \in \mathcal{F}^+ \times \mathcal{F}^+$ for which $F(f) = F(g)$, f is obtained from g by applications of pairs from \mathcal{R} . The set \mathcal{R} is called a *set of defining relations* for S . If \mathcal{R} is empty, which means that the semigroup S is free, we write the presentation $\langle \mathcal{F} \mid \rangle$ as $\langle \mathcal{F} \rangle$. We say that S is *finitely presented* if \mathcal{F} and \mathcal{R} are finite sets. In other words, S is finitely presented if $\mathcal{F} = \{f_1, f_2, \dots, f_n\}$ and $\mathcal{R} = \{(g_1, h_1), (g_2, h_2), \dots, (g_m, h_m)\}$, for some positive integers n and m . In that case, we write the presentation of S as

$$\langle f_1, f_2, \dots, f_n \mid g_1 = h_1, g_2 = h_2, \dots, g_m = h_m \rangle.$$

Example 2.5.7. Consider the substitution semigroup S generated by the pair of substitutions

$$f: \begin{array}{lcl} a & \mapsto & ab, \\ b & \mapsto & ba, \end{array} \quad \text{and} \quad g: \begin{array}{lcl} a & \mapsto & ba, \\ b & \mapsto & ab. \end{array}$$

The substitution f is the Thue–Morse substitution of Example 2.4.17 (using different symbols) and the substitution g is called the *reversed Thue–Morse substitution*. It can be shown that a presentation for S is given by

$$\langle f, g \mid fg = gf, f^2 = g^2 \rangle.$$

❖

Example 2.5.8. Consider the semigroup S generated by the pair of substitutions

$$f: \begin{array}{lcl} a & \mapsto & ab, \\ b & \mapsto & a, \end{array} \quad \text{and} \quad g: \begin{array}{lcl} a & \mapsto & ba, \\ b & \mapsto & a. \end{array}$$

The substitution f is the Fibonacci substitution introduced in Example 2.4.4 and the substitution g is called the *reversed Fibonacci substitution*. A presentation for S is

$$\langle f, g \mid f^2 g = g^2 f \rangle.$$

A sketch of the proof is as follows. Since both f and g are injective on finite words, S is a left and right cancellative semigroup, meaning that, if $\alpha, \beta, \delta \in S$, then each of $\alpha \circ \delta = \beta \circ \delta$ and $\delta \circ \alpha = \delta \circ \beta$ imply that $\alpha = \beta$. It then follows that any two finite words over \mathcal{F} representing the same substitution in S must have the same length, say $n \in \mathbb{N}$. We check directly that, if $n \leq 3$, the only existing relation is $f^2 \circ g = g^2 \circ f$. Finally, the proof can be completed by induction on the length n . \diamond

The previous example and the next example are related to Sturmian words. A *Sturmian sequence* or *Sturmian infinite word* is an infinite word that has precisely $n + 1$ different subwords of length n , for each positive integer n . A *Sturmian finite word* is a finite subword of a Sturmian sequence. Observe that every Sturmian word is a binary sequence because it has exactly two subwords of length one (or letters). Let the alphabet be $\{a, b\}$. A *Sturmian substitution* is a substitution f of $\{a, b\}$ that preserves Sturmian words, both finite and infinite. Survey chapters on Sturmian words and substitutions can be found, for instance, in [78, Chapter 2] and [57, Chapter 6].

Example 2.5.9. Sturmian substitutions are closed under functional composition and the semigroup of all Sturmian substitutions, which we denote by S in this example, is called the *Sturmian semigroup*. There are different sets of substitutions one can use to generate S , one example being the trio of substitutions f, g and h , where f and g are the substitutions of Example 2.5.8 and h is the substitution that exchanges the letters a and b . Séébold showed in [101] that S has the presentation

$$\langle f, g, h \mid h^2 = \text{id}, \quad g(gh)^n hf = f(fh)^n hg \text{ for all } n \in \mathbb{N}_0 \rangle.$$

Restricting ourselves to the subsemigroup of S generated by $\{f, g\}$ we recover the presentation of Example 2.5.8. \diamond

One of the properties of Sturmian words is balanceness. A (finite or infinite) word w over $\{a, b\}$ is *balanced* if for every letter $c \in \{a, b\}$, the number of c 's in any two subwords of w of equal length differ by at most one. A word $w \in \{a, b\}^+$ is a Sturmian finite word if, and only if, it is balanced [41]. A word $w \in \mathcal{A}^{\mathbb{N}}$ is a Sturmian infinite word if, and only if, it is balanced and not eventually periodic [78, Theorem 2.1.5]. The set of all Sturmian infinite words is not closed in $\{a, b\}^{\mathbb{N}}$, and its closure is equal to the set of all balanced infinite words [57, Theorem 6.1.8].

On the other hand, one of the properties of Sturmian substitutions is that they are precisely the invertible automorphisms of the free semigroup of words generated by $\{a, b, a^{-1}, b^{-1}\}$ under concatenation. More precisely, an automorphism of $\{a, b, a^{-1}, b^{-1}\}^+$ is a function f satisfying $f(uv) = f(u)f(v)$, for all words over $\{a, b, a^{-1}, b^{-1}\}$. We say that an automorphism f of $\{a, b, a^{-1}, b^{-1}\}^+$ is *invertible* if both $f(a)$ and $f(b)$ are words over $\{a, b\}$.

2.5.4 Actions of a substitution semigroup

The elements of a substitution semigroup S are substitutions of \mathcal{A} , which are functions from \mathcal{A}^+ to itself. Consequently, S has been defined by its action on \mathcal{A}^+ . There are, however, two other actions of S of interest to us. The first is on the collection of infinite words $\mathcal{A}^\mathbb{N}$. Given a substitution f in S and an infinite word $a_1 a_2 a_3 \dots$, where $a_i \in \mathcal{A}$, we define

$$f(a_1 a_2 \dots) = f(a_1) f(a_2) \dots$$

As promised, this defines an action of the semigroup S on $\mathcal{A}^\mathbb{N}$. Notice that if $f \in S$, and if $u, v \in \tilde{\mathcal{A}}$ share the same first letter (that is, $\pi_1(u) = \pi_1(v)$), then

$$d(f(u), f(v)) \leq d(u, v).$$

Hence the semigroup action is continuous.

The second action of S that we consider is an action on the alphabet \mathcal{A} itself. For $f \in \mathcal{F}$ and $a \in \mathcal{A}$, we define

$$f[a] = \pi_1(f(a)).$$

Thus $f[a]$ is the first letter of $f(a)$. The square brackets in $f[a]$ distinguish this single letter $f[a]$ from the word $f(a)$.

2.5.5 First-letter graph of a substitution semigroup

The second of these two actions can be visualised using the finite directed graph $G_{\mathcal{F}}$ with vertex set \mathcal{A} and, for each $f \in \mathcal{F}$ and $a \in \mathcal{A}$, a directed edge from a to $f[a]$. Note that $G_{\mathcal{F}}$ may include multiple edges between any pair of vertices and edges from any vertex to itself (loops). We call $G_{\mathcal{F}}$ the *first-letter graph* for \mathcal{F} . This graph is used to frame some of our later results in Chapter 5.

Example 2.5.10. Consider the semigroup S generated by the three substitutions

$$\begin{array}{lll} a \mapsto ea, & a \mapsto bc, & a \mapsto ca, \\ b \mapsto de, & b \mapsto bd, & b \mapsto cb, \\ f: c \mapsto ce, & g: c \mapsto ce, & h: c \mapsto cc, \\ d \mapsto da, & d \mapsto db, & d \mapsto ed, \\ e \mapsto eb, & e \mapsto ec, & e \mapsto dc. \end{array}$$

The first-letter graph for $\{f, g, h\}$ is shown in Figure 2.5.1, with labels for loops omitted.

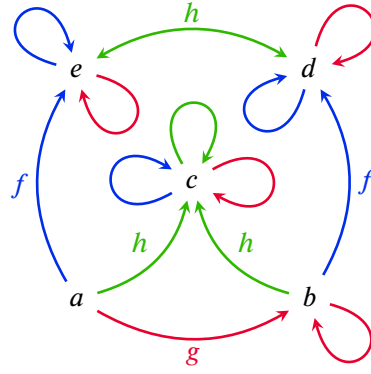


Figure 2.5.1: First-letter graph for $\{f, g, h\}$. Blue for f -edges, red for g -edges, and green for h -edges.

❖

Example 2.5.11. The first-letter graph for the Thue–Morse substitutions $\{f, g\}$ of Example 2.5.7 is displayed in Figure 2.5.2.



Figure 2.5.2: First-letter graph for $\{f, g\}$, where f is the Thue–Morse substitution and g is the reversed Thue–Morse substitution.

❖

Example 2.5.12. The first-letter graph for the Fibonacci substitutions $\{f, g\}$ of Example 2.5.8 is displayed in Figure 2.5.3.

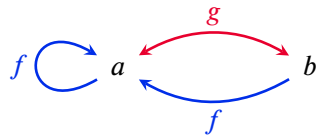


Figure 2.5.3: First-letter graph for $\{f, g\}$, where f is the Fibonacci substitution and g is the reversed Fibonacci substitution.

❖

Two vertices a and b of a first-letter graph $G_{\mathcal{F}}$ (for some finite set of substitutions \mathcal{F}) are said to be *strongly connected* if there is a directed walk from a to b and another directed walk from b to a . In other words, a and b are strongly connected if there exists $f, g \in \mathcal{F}$ with $f[a] = b$ and $g[b] = a$. Let \mathcal{A}_0 denote the subset of \mathcal{A} comprising those vertices of $G_{\mathcal{F}}$ that are strongly connected to themselves. The property

of being strongly connected is an equivalence relation on \mathcal{A}_0 ; the equivalence classes are called *strongly connected components* of $G_{\mathcal{F}}$.

A *terminal component* of $G_{\mathcal{F}}$ is a strongly connected component A for which every walk with initial vertex in A also has final vertex in A . In other words, a terminal component is a strongly connected component A with the property that if $a \in A$ and $g \in S$, then the vertex $g[a]$ also belongs to A .

Example 2.5.13. For example, in Figure 2.5.1 we have $\mathcal{A}_0 = \{b, c, d, e\}$ and the strongly connected components of $G_{\mathcal{F}}$ are $\{b\}$, $\{c\}$ and $\{d, e\}$. The terminal components are $\{c\}$ and $\{d, e\}$. \blacklozenge

2.5.6 Forward limit set of a substitution semigroup

In this section we introduce the forward limit set of a substitution semigroup S . From the last paragraph in Section 2.2.1, we recall that, if Y is a subset of $\tilde{\mathcal{A}}$, the set $\{s(y) : s \in S, y \in Y\}$ is denoted by $S(Y)$.

Definition 2.5.14. The *forward limit set* of the subset A of \mathcal{A} for the substitution semigroup S is the set

$$\Lambda(A) = \overline{S(A)} \setminus S(A).$$

The *forward limit set* of S is the set $\Lambda(\mathcal{A})$. We denote this set by Λ .

If the semigroup S is generated by a single substitution f , this definition coincides with the definition of the forward limit set of f given in Section 2.4.3. Recall in particular that, if f is periodic-letter-free, the forward limit set of f is equal to the set of all periodic points of f (Lemma 2.4.12).

Example 2.5.15. Consider the substitution semigroup S generated by the pair of substitutions

$$f : \begin{array}{l} a \mapsto a, \\ b \mapsto ab, \end{array} \quad \text{and} \quad g : \begin{array}{l} a \mapsto a, \\ b \mapsto ba. \end{array}$$

It is straightforward to check that f and g commute ($f \circ g = g \circ f$), so every element of S can be written as $f^n \circ g^m$, where n and m are non-negative integers that are not simultaneously equal to 0. Noticing that

$$f^n : \begin{array}{l} a \mapsto a, \\ b \mapsto a^n b, \end{array} \quad g^n : \begin{array}{l} a \mapsto a, \\ b \mapsto b a^n, \end{array} \quad \text{and} \quad f^n \circ g^m : \begin{array}{l} a \mapsto a, \\ b \mapsto a^n b a^m, \end{array}$$

it is also easy to see that a presentation for S is

$$\langle f, g \mid fg = gf \rangle.$$

Indeed, suppose that there are $u, v \in \mathcal{F}^+$ such that $F(u) = F(v)$. Then, $F(u) = f^m \circ g^n$ and $F(v) = f^p \circ g^q$, where m and n are the number of f and g letters in u , respectively, and p and q are the number of f and g letters in v , respectively. Since the equality $f^m \circ g^n = f^p \circ g^q$ holds only when $m = p$ and $n = q$, we get no new relations. It follows from the previous expressions that the forward limit set of S is

$$\Lambda = \{aaaa \cdots, a^n baaa \cdots : n \in \mathbb{N}_0\},$$

that is, Λ consists of the infinite words over $\{a, b\}$ containing a single b or no b at all. It is easy to see that the set of all periodic points of elements of S is $\{a^n : n \in \mathbb{N}\} \cup \Lambda$. \diamond

Example 2.5.16. Consider the substitution semigroup of Example 2.5.7, namely, the semigroup S generated by the Thue–Morse substitution f and the reversed Thue–Morse substitution g . The substitution f has two fixed points, both aperiodic, namely

$$x = abbabaa \dots \quad \text{and} \quad h(x),$$

where h is the substitution given by $h(a) = b$ and $h(b) = a$. We notice that $g = h \circ f = f \circ h$. Consequently every element of S can be written either as f^n or as $h \circ f^n$, for some positive integer n . This implies that the forward limit set of S is $\Lambda = \{x, h(x)\}$. \diamond

Example 2.5.17. Consider the Sturmian semigroup S which, as we saw in Example 2.5.9, can be generated by the Fibonacci substitution f , the reversed Fibonacci substitution g and the letter-exchange substitution h . Since Sturmian substitutions, elements of S , preserve Sturmian words, one may expect that the set of all s-adic sequences of $\{f, g, h\}$ is the set of all Sturmian infinite words. However, this is not true, as we can easily see by an example. Consider the substitution $s = h \circ g$, which is given by

$$s : \begin{array}{lcl} a & \mapsto & ab, \\ b & \mapsto & b. \end{array}$$

Then $s^n(a) \longrightarrow aaa \dots$ as $n \rightarrow \infty$, which is not an Sturmian infinite word, since it is not aperiodic; recall from the paragraph following Example 2.5.9 that Sturmian sequences are aperiodic and balanced. Hence the set of all s-adic sequences of $\{f, g, h\}$ contains and is larger than the set of all Sturmian infinite words. \diamond

2.5.7 Hull and subshift of a substitution semigroup

In this section, we introduce the hull and the subshift of a substitution semigroup S . Here and henceforth we write $\Lambda(a)$ for $\Lambda(\{a\})$, where a is a letter of \mathcal{A} .

Definition 2.5.18. The *hull* of the letter a of \mathcal{A} for the substitution semigroup S is the set

$$\Omega(a) = \overline{\bigcup_{n=0}^{\infty} \sigma^n(\Lambda(a))}.$$

The *hull* of S is the set $\bigcup_{a \in \mathcal{A}} \Omega(a)$. We denote this set by Ω .

The hull of a substitution semigroup S can be written as the closure of the shift-orbit of the forward limit set of S . In other words, $\Omega = \overline{\bigcup_n \sigma^n(\Lambda)}$.

The hull Ω of a substitution semigroup S is closed and invariant under the shift map σ , as can easily be verified. In Chapter 5, we will see that Ω is also invariant under the semigroup S . When S is

generated by a single substitution, Definition 2.5.18 coincides with its single-substitution counterpart, Definition 2.4.32.

Definition 2.5.19. The *subshift* of a substitution semigroup S with language \mathcal{L} is the set

$$\mathbb{X} = \{w \in \mathcal{A}^{\mathbb{N}} : \mathcal{L}(w) \subseteq \mathcal{L}\}.$$

It is not difficult to verify that the subshift \mathbb{X} of a substitution semigroup S is closed, invariant under σ and invariant under S . When S is generated by a single substitution, Definition 2.5.19 coincides with its single-substitution counterpart, Definition 2.4.33.

Example 2.5.20. Consider the substitution semigroup S of Example 2.5.15. We saw that the forward limit set Λ of S consists of the infinite words over $\{a, b\}$ containing a single b or no b at all. In other words, $\Lambda = \{aaaa \dots, a^n baaa \dots : n \in \mathbb{N}_0\}$. Then it is easy to see that the hull Ω of S is equal to Λ . We also saw that every element of S is a substitution of the form

$$f^n \circ g^m : \begin{array}{lcl} a & \mapsto & a, \\ b & \mapsto & a^n b a^m, \end{array}$$

where n and m are non-negative integers that are not simultaneously equal to 0. Therefore, the language of S is the set of all finite words over $\{a, b\}$ containing a single b or no b at all. This implies that the subshift \mathbb{X} of S is contained in Ω , hence they are equal. In summary, $\Lambda = \Omega = \mathbb{X}$. \diamond

Example 2.5.21. Consider the substitution semigroup S generated by the Thue–Morse substitution f and the reversed Thue–Morse substitution g , as in Examples 2.5.7 and 2.5.16. The forward limit set of S has two points, the Thue–Morse sequence u and $h(u)$, where h is the substitution that exchanges the two letters of the alphabet. Both points are periodic points of f and also of g . This implies that the hull of f and the hull of g are equal. Moreover, since f is a primitive substitution, by Theorem 2.4.35, its hull and subshift are equal, and they are uniquely determined by any periodic point of f . Obviously, the same is true for g . These results imply that the hull Ω and the subshift \mathbb{X} of S are equal, and they are given by the closure of the shift-orbit of u . Since the dynamical system (\mathbb{X}, σ) is equal to the dynamical system (\mathbb{X}_f, σ) , where \mathbb{X}_f is the subshift of f , it is a linearly recurrent and minimal system, by Theorems 2.4.36 and 2.4.37. \diamond

Example 2.5.22. Consider the substitution semigroup S generated by the Fibonacci substitution f and the reversed Fibonacci substitution g , as in Example 2.5.8. In Section 5.4.1.1 we will prove that the forward limit set Λ , the hull Ω and the subshift \mathbb{X} of S are all equal, and that they are given by the closure of the shift-orbit of the Fibonacci word, the fixed point of f . This is again a linearly recurrent and minimal dynamical system. \diamond

Observe that in the previous examples the hull and the subshift of each substitution semigroup considered are equal. In Chapter 5 we will see that this is a general result for primitive substitution semigroups (see Theorem 5.6.6).

3. MONOCHROMATIC ARITHMETIC PROGRESSIONS IN THUE–MORSE-LIKE SEQUENCES

This chapter and Chapter 4 are devoted to the study of monochromatic arithmetic progressions that we can find in infinite words. In this chapter, we explore the Thue–Morse word and a class of generalised Thue–Morse words over a two-letter alphabet. In Chapter 4, we will consider automatic sequences over larger alphabets.

First, we recall from Section 2.3 the notion of a ‘monochromatic arithmetic progression’. Identifying each letter from an alphabet \mathcal{A} with a colour, we interpret an infinite word $w \in \mathcal{A}^{\mathbb{N}_0}$ as a coloured sequence of letters from \mathcal{A} . We say that a monochromatic arithmetic progression of difference $d \in \mathbb{N}$ and length $M \in \mathbb{N}$ appears in w , if there exists a starting position $n \in \mathbb{N}_0$ such that $w_n = w_{n+kd}$, for $k = 0, 1, \dots, M-1$. The arithmetic progression has colour $a \in \mathcal{A}$, if $w_n = a$. The monochromatic arithmetic progression is infinite if $w_n = w_{n+kd}$, for $k = 0, 1, \dots$.

The study of the monochromatic arithmetic progressions appearing in an infinite word w gives information about the order or global structure of w . Periodic sequences always contain infinitely long monochromatic arithmetic progressions. Instead, we consider w to be aperiodic and ask how long monochromatic arithmetic progressions occurring in w can be. We have adapted the following definition from [90, 91].

Definition 3.0.1. For an infinite word w , we define a function $A_w : \mathbb{N} \longrightarrow \mathbb{N} \cup \{\infty\}$ as follows. For each positive integer d , $A_w(d)$ is the length of the longest monochromatic arithmetic progression of difference d within w , or if there exists an infinite monochromatic arithmetic progression of difference d within w , then $A_w(d) = \infty$.

If the sequence w is clear from the context, we often write $A(d)$ rather than $A_w(d)$. We will see that all the sequences studied in this thesis have the property that $A_w(d) < \infty$ and consequently, A_w is a well-defined function with values in \mathbb{N} .

As mentioned in Section 2.3, our research is inspired by van der Waerden’s theorem. For any finite colouring of \mathbb{N} , van der Waerden’s theorem says that, for any given positive integer M , there always exists a long enough initial segment of \mathbb{N} which contains a monochromatic arithmetic progression of length M (see Theorem 2.3.3, or van der Waerden’s original paper [109]). This implies that, given an infinite word w over a finite alphabet, w contains monochromatic arithmetic progressions of every positive integer length M . Van der Waerden’s theorem says nothing, however, about the difference d of the arithmetic progressions. In our research, we fix d and consider whether there are monochromatic

arithmetic progressions in w of difference d . In the affirmative case, we are interested in determining the maximum length of these progressions, namely, the magnitude $A_w(d)$ introduced in the previous paragraph.

It is known that for some infinite words, for a fixed difference d , the lengths of the monochromatic arithmetic progressions of difference d cannot be as large as desired. Morgenbesser et al. [80] showed this in the case of the Thue–Morse sequence, and Parshina [90, 92] studied the longest monochromatic arithmetic progressions that it contains for some fixed differences. In this chapter, we reprove some of these results using a completely different approach, and we extend them for other differences. We also prove similar results for some generalisations of the Thue–Morse word, which are fixed points of binary bijective substitutions.

This chapter is structured as follows. In Section 3.1, we prove, for a family of infinite words which includes the Thue–Morse word, that the maximum length $A(d)$ of a monochromatic arithmetic progression of difference d is finite, for any positive integer d (see Proposition 3.1.4 and Corollary 3.1.6). This generalises the result in [80]. In Section 3.2, we set out our main technique and we use it to study monochromatic arithmetic progressions in the Thue–Morse word. Our main results determine the exact values of $A(d)$ for differences of the form $2^n \pm 1$, thus reproving the results in [90] (see Theorem 3.2.12, Proposition 3.2.13, and Corollary 3.2.16). In Section 3.3, we apply our techniques to generalise some of the previous results to other binary sequences with a similar substitution structure (see Theorems 3.3.8 and 3.3.9). Appropriate plots illustrate the results both for the Thue–Morse sequence and for the generalised Thue–Morse sequences (see Sections 3.2.6 and 3.3.6, respectively). In Section 3.4, we consider fixed points of any primitive, bijective, binary substitution and establish upper bounds for $A(d)$, for certain differences d (see Propositions 3.4.1 and 3.4.2).

3.1 Finiteness of the length of monochromatic arithmetic progressions

The goal of this section is to show that the infinite words that we will study in the rest of the thesis do not contain arbitrarily long monochromatic arithmetic progressions of any fixed difference. To be more precise, consider a fixed point $w \in \mathcal{A}^{\mathbb{N}_0}$ of a primitive constant-length substitution ρ . We want to know whether every monochromatic arithmetic progression that appears in w is finite, and, if this is true, we want to determine, for each positive integer d , whether the length of the monochromatic arithmetic progressions of difference d can be arbitrarily large. To answer these questions, we will use results from the spectral theory of substitution dynamical systems; the following paragraphs give the minimum background to state these results.

A *bi-infinite word* over \mathcal{A} is a two-sided infinite sequence of letters of \mathcal{A} ; the collection of all bi-infinite words over \mathcal{A} is denoted $\mathcal{A}^{\mathbb{Z}}$. Let ρ a primitive substitution of \mathcal{A} and let $w \in \mathcal{A}^{\mathbb{N}_0}$ and $x \in \mathcal{A}^{\mathbb{Z}}$ be an infinite and a bi-infinite fixed point of ρ , respectively. Since ρ is primitive, both w and x have the same language (see, for example, [17, Remark 4.1]), so every monochromatic arithmetic progression that appears in w appears in x , and the other way round. Therefore, rather than considering one-sided infinite fixed points of ρ , we can consider bi-infinite fixed points of ρ , and study the monochromatic arithmetic progressions that appear in the latter.

All definitions introduced for infinite words in Chapter 2 apply to bi-infinite words directly or with obvious minor modifications. In particular, the two-sided subshift \mathbb{X} of a substitution ρ is the set of all bi-infinite words x such that every subword of x is an element of the language of ρ . The subshift \mathbb{X} is a closed subset of $\mathcal{A}^{\mathbb{Z}}$ that is invariant under the shift map σ (with \mathbb{Z} -action), so the pair (\mathbb{X}, σ) is a shift dynamical system.

For a primitive substitution ρ with two-sided subshift \mathbb{X} , the system (\mathbb{X}, σ) is *uniquely ergodic*, which means that there is a unique σ -invariant Borel probability measure μ on \mathbb{X} (this was proved in [79]; see also [96, Theorem 5.6]). The measure μ measures the frequency of words; unique ergodicity implies that every word in the language of ρ occurs with a well-defined positive frequency in every element of \mathbb{X} . The shift map σ induces a unitary operator U on $L^2(\mathbb{X}, \mu)$, the Hilbert space of complex-valued square integrable functions on \mathbb{X} , which is given by $f(x) \mapsto f(\sigma(x))$, for all $x \in \mathbb{X}$ and $f \in L^2(\mathbb{X}, \mu)$. The *dynamical spectrum* of the measure-theoretic dynamical system $(\mathbb{X}, \sigma, \mu)$ is defined to be the spectrum of the operator U . This spectrum is also referred to as the dynamical spectrum of the substitution ρ . The dynamical spectrum has, in general, a discrete component and a continuous component, the latter separated into a singular component and an absolutely continuous component. If the dynamical spectrum of ρ is purely discrete (the continuous components are null), then we say that ρ has *pure point dynamical spectrum*. For general background material on the spectral theory of dynamical systems, see, for example, [96]; a brief summary can be found in [17, Appendix B].

A bi-infinite word has a corresponding geometric counterpart which is a tiling of the real line. In this setting, the alphabet \mathcal{A} is no longer a finite set of letters, but a finite set of intervals of \mathbb{R} called *prototiles*. A substitution can be interpreted as an *inflation rule* for these prototiles. Similarly to the symbolic case, we can define the two-sided subshift \mathbb{X} of an inflation rule as the set of all tilings of the real line by prototiles from \mathcal{A} , the language of which is contained in the language of the inflation rule. This is a closed subset of $\mathcal{A}^{\mathbb{R}}$ that is invariant under \mathbb{R} -translations. Then (\mathbb{X}, σ) is a shift dynamical system, where the shift map σ is now defined by \mathbb{R} -translations. For an extensive development of the theory of tilings (in particular, substitution-tilings) we refer the reader to [17].

It is known that the subshift (with \mathbb{Z} -shift action) of a constant-length substitution has pure point discrete spectrum if, and only if, the corresponding tiling dynamical system (with \mathbb{R} -translation action) has pure point dynamical spectrum [44, 76]. Using this fact, Theorem 5.1 in [84] by Nagai, Akiyama, and Lee can be reformulated in the following form.

Theorem 3.1.1. *A bi-infinite fixed point of a primitive constant-length substitution ρ contains infinitely long monochromatic arithmetic progressions if, and only if, ρ has pure point dynamical spectrum. \square*

We recall from Section 2.4.6 that a constant-length substitution admits a coincidence, if there is a power of the substitution that has a column with all entries given by the same letter. In Section 2.4.8, we introduced the height of a primitive constant-length substitution. In the case of a primitive constant-length substitutions ρ of height 1, having pure point dynamical spectrum is equivalent to admitting a coincidence, as the following theorem states, which was proved by Dekking (we refer the interested reader to Dekking's original paper [38] and, for an exposition closer to our approach, to [96, Section 6.3.1, Theorem 6.6]).

Theorem 3.1.2. *A primitive constant-length substitution of height 1 has pure point dynamical spectrum if, and only if, it admits a coincidence.* \square

Dekking used this theorem to design an algorithm to check if ρ has pure point dynamical spectrum [38]. Dekking's paper also relates ρ with its pure base. We introduced the pure base ρ' of a primitive constant-length substitution ρ in Section 2.4.8 (in Example 2.4.31 we showed how ρ' can be directly derived from ρ). Dekking proved that ρ' is primitive, that its height is 1, and that it has pure point dynamical spectrum if, and only if, ρ has pure point dynamical spectrum [38]. We can use these facts together with Theorems 3.1.1 and 3.1.2 to prove the following result.

Proposition 3.1.3. *Every monochromatic arithmetic progression in a fixed point of a primitive constant-length substitution ρ has finite length if, and only if, the pure base of ρ does not admit any coincidence.*

Proof. Let ρ' be the pure base of ρ . Since ρ' is a primitive constant-length substitution of height 1, by Theorem 3.1.2, it does not admit any coincidence if, and only if, its dynamical spectrum is not pure point. Since the dynamical spectrum of ρ' is not pure point if, and only if, the dynamical spectrum of ρ is not pure point, we see that ρ' does not admit any coincidence if, and only if, the dynamical spectrum of ρ is not pure point. Then, by Theorem 3.1.1, every monochromatic arithmetic progression in a bi-infinite fixed point of ρ has finite length if, and only if, ρ' does not admit any coincidence, as required. \square

We observe that the previous proposition holds for all elements that belong to the (one-sided or two-sided) hull of ρ because, as we said earlier, since ρ is primitive, all the elements in its hull have the same language and consequently, they all contain the same monochromatic arithmetic progressions.

Let ρ be a primitive constant-length substitution whose pure base does not admit any coincidence, let w be a fixed point of ρ , and let d be a positive integer. By the previous proposition, every monochromatic arithmetic progression of difference d within w has finite length. In the next proposition we show that the lengths of the monochromatic arithmetic progressions of difference d that appear in w are bounded above. In other words, it is impossible to find ever longer monochromatic arithmetic progressions of difference d within w .

Proposition 3.1.4. *Let ρ be a primitive constant-length substitution whose pure base admits no coincidences. For each positive integer d , there exists a positive integer N_d such that every monochromatic arithmetic progression of difference d within a fixed point of ρ has length less than or equal to N_d .*

Proof. Let $w \in \mathcal{A}^{\mathbb{N}_0}$ be a fixed point of ρ and let P_d be the set of monochromatic arithmetic progressions of difference d within w . We will first prove that, for each sequence $s := (p_n)$ in P_d , there exists a positive integer M_s such that $|p_n| \rightarrow M_s$ as $n \rightarrow \infty$, where $|p_n|$ denotes the length of the arithmetic progression p_n . Notice that, for each n , $|p_n| < \infty$, by Proposition 3.1.3.

To the contrary, assume that there exists a sequence $s = (p_n)$ in P_d such that $|p_n| \rightarrow \infty$ as $n \rightarrow \infty$. For each arithmetic progression p_n , there exists a non-negative integer k_n such that p_n occurs in $\sigma^{k_n}(w)$ starting from the origin, where σ is the shift map. Notice that $(\sigma^{k_n}(w))$ is a sequence in the hull Ω_ρ of ρ . Since

Ω_ϱ is a compact space, there exist a sequence (ℓ_n) of non-negative integers and an infinite word $v \in \Omega_\varrho$ such that $(\sigma^{k_{\ell_n}}(w)) \rightarrow v$ as $n \rightarrow \infty$. Since $|p_{\ell_n}| \rightarrow \infty$, we see that v contains a monochromatic arithmetic progression of difference d which is infinitely long. But this is not possible, by Proposition 3.1.3. Therefore, $|p_n| \nrightarrow \infty$, so there must exist $M_s \in \mathbb{N}$ such that $|p_n| \rightarrow M_s$ as $n \rightarrow \infty$.

Now, let X be the set $\{M_s : s \text{ is a sequence in } P_d\}$. Notice that for every sequence (M_{s_n}) in X , $M_{s_n} \nrightarrow \infty$ as $n \rightarrow \infty$. Otherwise there exists a sequence (p_n) in P_d , where p_n is an element of s_n with $|p_n| = M_{s_n}$, such that $|p_n| \rightarrow \infty$, which is not possible. Therefore, there must exist $N_d \in \mathbb{N}$ such that $M_{s_n} \rightarrow N_d$ as $n \rightarrow \infty$, as required. \square

Corollary 3.1.5. *Let ϱ be a primitive constant-length substitution whose pure base does not admit any coincidence and let w be a fixed point of ϱ . Then $A_w(d) = N_d < \infty$.*

Proof. The claim is an immediate consequence of Proposition 3.1.4. \square

With the previous proposition, we directly recover the following fact regarding the Thue–Morse sequence, which was initially proved in [80] (which is based on [58]). Notice that the Thue–Morse substitution is its own pure base and it does not admit any coincidence.

Corollary 3.1.6. *The Thue–Morse word does not contain arbitrarily long monochromatic arithmetic progressions of any fixed difference d .* \square

Observe that Proposition 3.1.4 allows one to do the same analysis on larger classes of automatic sequences not covered by [80], for example, those which are codings of fixed points of constant-length substitutions which are a priori known to have mixed spectrum. This will be addressed in Chapter 4.

For the remainder of this chapter, we will always consider infinite words generated by substitutions which satisfy the conditions of Proposition 3.1.4.

3.2 Monochromatic arithmetic progressions in the Thue–Morse word

The study of monochromatic arithmetic progressions appearing in the Thue–Morse word has been previously address by Parshina, who proved the following result [90], as well as a generalisation to similar sequences over larger alphabets [91,92]. Her proofs for the Thue–Morse case [90] are based on a detailed analysis of binary arithmetic.

Theorem 3.2.1 (Parshina [90]). *Consider the Thue–Morse word. Then, for all positive integers n ,*

$$\max_{d < 2^n} A(d) = A(2^n - 1) = \begin{cases} 2^n + 4, & \text{if } n \text{ is even,} \\ 2^n, & \text{otherwise.} \end{cases}$$

In this section, we obtain exact expressions for $A(d)$, for the Thue–Morse word, for certain values of d . In Section 3.3, we obtain similar results for generalised Thue–Morse words, which are different generalisations from those considered in [90–92]. In particular, all our sequences are over a two-letter

alphabet. Our results include a simple proof of the value of $A(2^n - 1)$ stated in Theorem 3.2.1, but also identify a second series of long monochromatic arithmetic progressions in the Thue–Morse word, which becomes the ‘longest’ in some cases, provided one considers the maximum over a different range for d .

3.2.1 Properties of the Thue–Morse word and the Thue–Morse substitution

Let v be the Thue–Morse word over the alphabet $\{0, 1\}$. We have previously considered the Thue–Morse word in Chapter 2 (see Examples 2.2.2, 2.2.1 and 2.4.17). Recall that v arises from the substitution

$$\theta: \begin{array}{ll} 0 & \mapsto 01 \\ 1 & \mapsto 10, \end{array} \quad (3.2.1)$$

as the fixed point $v = \lim_{n \rightarrow \infty} \theta^n(0)$. Throughout the whole Section 3.2, θ and v will always be given as here.

Notice that θ is a bijective substitution and symmetric under the ‘bar’ operation that exchanges the two letters, namely, $\bar{a} = 1 - a$ for $a \in \{0, 1\}$ (we used this notation in Example 2.2.1). This also implies that $\bar{v} = \lim_{n \rightarrow \infty} \theta^n(1)$ is another fixed-point word.

We say that a word w over $\{0, 1\}$ is *symmetric* under reflection if it is read exactly equally from left to right and the other way round; in other words, it is a palindrome. We say that w is *antisymmetric* under reflection if the right-to-left reading gives the word \bar{w} .

Lemma 3.2.2. *For all $a \in \{0, 1\}$, the word $\theta^n(a)$ is symmetric if n is even, and antisymmetric if n is odd.*

Proof. Notice that $\theta(a) = a\bar{a}$, for $a = 0, 1$. So, $\theta(0)$ and $\theta(1)$ are antisymmetric words. It suffices to prove that θ maps symmetric words to antisymmetric words, and the other way round. For every symmetric word w , there are letters a_1, \dots, a_k and a possibly empty letter b in $\{0, 1\}$ such that $w = a_1 \dots a_k b a_k \dots a_1$. Then $\theta(w) = a_1 \bar{a}_1 \dots a_k \bar{a}_k \bar{b} a_k \bar{a}_k \dots a_1 \bar{a}_1$, which is an antisymmetric word. Similarly, for every antisymmetric word w , there are letters a_1, \dots, a_k in $\{0, 1\}$ such that $w = a_1 \dots a_k \bar{a}_k \dots \bar{a}_1$. Then $\theta(w) = a_1 \bar{a}_1 \dots a_k \bar{a}_k \bar{a}_k a_k \dots \bar{a}_1 a_1$, which is a symmetric word. \square

We recall from Example 2.2.2 that, for each non-negative integer n , v_n is 0 if the binary representation of n contains an even number of 1s, and 1 otherwise. Since multiplying by 2 does not change the number of 1s in the binary representation of an integer, then

$$v_{2n} = v_n \quad \text{and} \quad v_{2n+1} = \bar{v}_n, \quad (3.2.2)$$

for all non-negative integers n .

We should also mention that v is *overlap-free*, which means that, for any non-empty finite word w , v does not contain www_0 as a subword, where w_0 denotes the first letter of w (this result is due to Thue [106, 107]; see also [8, Theorem 1.6.1]). In particular, v is cube-free, that is, it does not have any subword of the form www .

For all non-negative integers n and $a \in \{0, 1\}$, we have the well-known recursions

$$\theta^{n+1}(a) = \theta^n(a) \theta^n(\bar{a}) = \theta^n(a) \overline{\theta^n(a)}, \quad (3.2.3)$$

where the first equality is due to $\theta^{n+1}(a) = \theta^n(\theta(a)) = \theta^n(a\bar{a})$ and the second equality holds because θ is a binary bijective substitution. This implies the following property.

Lemma 3.2.3. *For all $n, m \in \mathbb{N}_0$ with $n < m$ and all $a \in \{0, 1\}$, the word $\theta^m(a)$ consists of a sequence of the two words $\theta^n(a)$ and $\theta^n(\bar{a})$, arranged according to the sequence that corresponds to $\theta^{m-n}(b)$ with the letters b and \bar{b} replaced by the words $\theta^n(a)$ and $\theta^n(\bar{a})$, respectively.*

Proof. Clearly, $\theta(a) = \theta^0(a) \theta^0(\bar{a}) = a\bar{a}$. Now, let $w = \theta^n(a)$ and $\bar{w} = \theta^n(\bar{a})$. Then, $\theta(w) = w\bar{w}$ by the recursion (3.2.3), which is the same form as the Thue–Morse substitution, now on the alphabet $\{w, \bar{w}\}$. Hence $\theta^m(a) = \theta^{m-n}(\theta^n(a)) = \theta^{m-n}(w)$ is the sequence $\theta^{m-n}(b)$ with b and \bar{b} replaced by w and \bar{w} , respectively. \square

3.2.2 Monochromatic arithmetic progressions of difference $d = 2^n$

Lemma 3.2.4. *For the Thue–Morse word v , $A(2^n d) = A(d)$, for all positive integers d and n .*

Proof. The claim will follow from $A(2^n d) = A(2^{n-1} d)$, which we prove next.

Let $v_{m+k2^{n-1}d} = a$ be a monochromatic arithmetic progression of difference $2^{n-1}d$ and length $A(2^{n-1}d)$ appearing in v , for $k = 0, 1, \dots, A(2^{n-1}d) - 1$, a non-negative integer m and $a \in \{0, 1\}$. By Equation (3.2.2), $v_{m+k2^{n-1}d} = v_{2m+k2^nd}$, which implies that $A(2^nd) \geq A(2^{n-1}d)$.

Conversely, let $v_{m+k2^nd} = a$ be a monochromatic arithmetic progression of difference 2^nd and length $A(2^nd)$ appearing in v , for $k = 0, 1, \dots, A(2^nd) - 1$, a non-negative integer m , and $a \in \{0, 1\}$. There exist a unique non-negative integer i and $j \in \{0, 1\}$ for which $m = 2i + j$, so $v_{m+k2^nd} = v_{2(i+k2^{n-1}d)+j}$. By Equation (3.2.2), we see that either $v_{m+k2^nd} = v_{i+k2^{n-1}d}$ or $v_{m+k2^nd} = \overline{v_{i+k2^{n-1}d}}$. Hence, there exists a fixed element $b \in \{0, 1\}$ such that $v_{i+k2^{n-1}d} = b$, for $k = 0, 1, \dots, A(2^{n-1}d) - 1$. This implies that $A(2^{n-1}d) \geq A(2^nd)$. Therefore $A(2^nd) = A(2^{n-1}d)$, as required. \square

Lemma 3.2.4 is a consequence of $\theta^n(v) = v$ and the fact that the length of a word is doubled under the action of θ . In particular, since v is cube-free, it follows that $A(1) = 2$, so Lemma 3.2.4 implies that $A(2^n) = 2$, for all non-negative integers n . The following results show that $A(d) = 2$ holds only for differences d that are powers of 2.

Lemma 3.2.5. *For the Thue–Morse word v , $A(d) \geq 3$, for every odd integer $d > 1$.*

Proof. Assume first that the binary representation of d contains an even number of 1s. Since multiplication by 2 preserves the number of 1s, we have $v_0 = v_d = v_{2d} = 0$ and so $A(d) \geq 3$.

Now consider the case that the binary representation of d contains an odd number of 1s, and hence contains at least three 1s. Write $d = 2^m + 2^n + k$, with $m > n$ and $k < 2^n$, so k again contains an odd number

of 1s in its binary representation. Let $i = 2^{m+1} + 2^n$, with $v_i = 0$. Then $i + d = 2^{m+1} + 2^m + 2^{n+1} + k$. If $m > n + 1$, the number of 1s in the binary representation of $i + d$ is even. If $m = n + 1$, then $i + d = 2^{n+3} + k$ and so the number of 1s in its binary representation is even too. Hence $v_{i+d} = 0$. Furthermore, $i + 2d = 2^{m+2} + 2^{n+1} + 2^n + 2k$. If $2k < 2^n$, the number of 1s in the binary representation of $i + 2d$ is even. If $2^n \leq 2k < 2^{n+1}$, we write $2k = 2^n + t$, where the number of 1s in the binary representation of t is even, so $i + 2d = 2^{m+2} + 2^{n+2} + t$ and its binary representation has an even number of 1s. Hence $v_{i+2d} = 0$. Consequently, $v_i = v_{i+d} = v_{i+2d} = 0$, so $A(d) \geq 3$. \square

Corollary 3.2.6. *Consider the Thue–Morse word. Then $A(d) = 2$ if, and only if, $d = 2^n$, for some $n \in \mathbb{N}_0$.*

Proof. By Lemma 3.2.4, $A(2^n) = A(1) = 2$, for all $n \in \mathbb{N}_0$. Conversely, if $A(d) = 2$, then d does not have any odd prime factor, by Lemma 3.2.5, so $d = 2^n$, for some $n \in \mathbb{N}_0$. \square

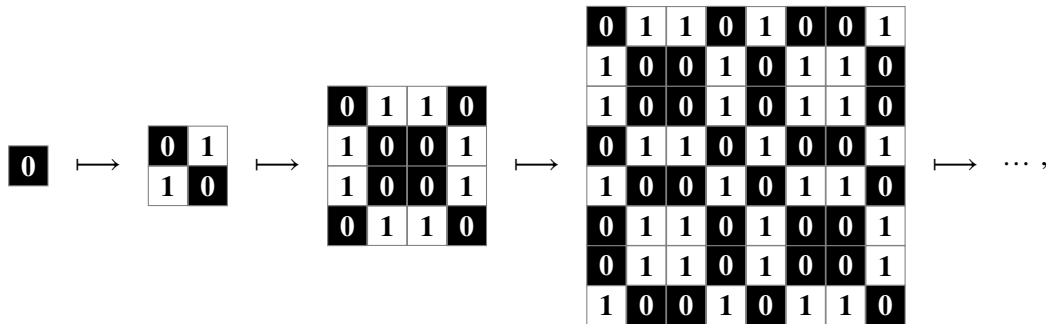
3.2.3 Monochromatic arithmetic progressions of difference $d = 2^n + 1$

To prove our main results, we will use a two-dimensional block substitution of the alphabet $\{0, 1\}$ (for an introduction to block substitutions we refer the reader to [17, Section 4.9] and references therein). In our case, a two-dimensional block substitution of the alphabet \mathcal{A} is a map $\mathcal{A} \rightarrow \mathcal{A}^{(0,1,\dots,n) \times (0,1,\dots,m)}$, for some non-negative integers n and m , not both equal to 0.

Definition 3.2.7. Let Θ be the block substitution of the alphabet $\{0, 1\}$ defined by

$$\Theta: \quad 0 \mapsto \begin{array}{cc} 0 & 1 \\ 1 & 0 \end{array}, \quad 1 \mapsto \begin{array}{cc} 1 & 0 \\ 0 & 1 \end{array}.$$

Iterating Θ on a single letter produces square blocks of size $2^n \times 2^n$. For instance,



where we used black (for 0) and white (for 1) squares to emphasise the block structure. Notice that the blocks along both diagonals are always of the same colour.

Lemma 3.2.8. *The block $\Theta^n(a)$, read row-wise from left to right, from top to bottom, is the word $\theta^{2^n}(a)$, for every $a \in \{0, 1\}$ and non-negative integer n .*

Proof. This follows by induction from noticing that

$$\Theta: \quad 0 \mapsto \begin{matrix} \theta(0) \\ \theta(1) \end{matrix}, \quad 1 \mapsto \begin{matrix} \theta(1) \\ \theta(0) \end{matrix},$$

so that, read row-wise from the top, the image of a under Θ is $\theta(a) \theta(\bar{a}) = \theta^2(a)$. \square

The images of letters under Θ^n have the following properties.

Lemma 3.2.9. *Let n be a non-negative integer and let $a \in \{0, 1\}$. The block $\Theta^n(a)$ consists of only two types of row and column words, and it is symmetric under reflection in either diagonals. Furthermore, all entries of the main diagonal are a , while entries of the second diagonal are a if n is even and \bar{a} otherwise.*

Proof. As shown in Lemma 3.2.8, $\Theta^n(a)$ when read row-wise from the top is the word $\theta^{2n}(a) = \theta^n(\theta^n(a))$. By Lemma 3.2.3, this consists of 2^n words from $\{\theta^n(0), \theta^n(1)\}$. So each row is one of these two words.

The symmetry in the diagonals follows from the symmetry of the block substitution Θ , which also implies that all columns are either $\theta^n(0)$ or $\theta^n(1)$.

It is obvious from the block substitution that the elements of $\Theta^n(a)$ on the main diagonal are always a . Notice that, on the second diagonal, $\Theta(a)$ has \bar{a} while $\Theta^2(a)$ has a , which implies the claim. \square

Lemma 3.2.10. *Consider the Thue–Morse word. Then $A(2^n \pm 1) \geq 2^n$, for all positive integers n . Furthermore, $A(2^n - 1) \geq 2^n + 2$, for all even positive integers n .*

Proof. Consider the block $\Theta^n(a)$, which, when read row-wise from the top, is the word $\theta^{2n}(a)$. As shown in Lemma 3.2.9, all elements on the main diagonal are a , so we find that $A(2^n + 1) \geq 2^n$. Similarly, the elements on the second diagonal are either all a or \bar{a} , so we also have $A(2^n - 1) \geq 2^n$. For even n , both diagonals have a entries, so the first and last letter of $\theta^{2n}(a)$ are also part of the arithmetic progression of a letters of difference $2^n - 1$, which implies the claim. \square

Before we establish the values for $A(2^n \pm 1)$, we prove a useful result, which exploits the recognisability of the substitution (see [17] and references therein for general background).

Lemma 3.2.11. *Let n be a non-negative integer and let $a \in \{0, 1\}$. The word $w = \theta^n(a)$ occurs in the Thue–Morse word either as the level- n superword itself, or in the centre of the two level- n superwords $\theta^n(\bar{a}) \theta^n(\bar{a})$. Furthermore, w is the level- n superword, if it is followed by the letter \bar{a} , or if it is preceded by the letter a for n odd, or \bar{a} for n even.*

Proof. Clearly w can occur as the level- n superword. The second possibility arises from

$$\begin{aligned} \theta^n(\bar{a}\bar{a}) &= \theta^n(\bar{a}) \theta^n(\bar{a}) \\ &= \theta^{n-1}(\bar{a}a) \theta^{n-1}(\bar{a}a) \\ &= \theta^{n-1}(\bar{a}) \theta^{n-1}(a) \theta^{n-1}(\bar{a}) \theta^{n-1}(a) \\ &= \theta^{n-1}(\bar{a}) w \theta^{n-1}(a). \end{aligned}$$

To show that these are the only two possibilities, we use that

$$\theta^n(a) = \theta^{n-2}(a\bar{a}\bar{a}a) = \theta^{n-2}(a)\theta^{n-2}(\bar{a})\theta^{n-2}(\bar{a})\theta^{n-2}(a),$$

which holds for all $n \geq 2$. By recognisability, the two adjacent level- $(n-2)$ superwords $\theta^{n-2}(\bar{a})$ cannot belong to the same level- $(n-1)$ superword, so we know that $\theta^n(a)$ has to consist of two level- $(n-1)$ superwords, which only leaves the two possibilities, since the boundaries of all level- $(n-1)$ superwords are determined.

If $w = \theta^{n-1}(a)\theta^{n-1}(\bar{a})$ is followed by a letter \bar{a} , the next level- $(n-1)$ superword is determined to be $\theta^{n-1}(\bar{a})$, and the level- n superword boundary has to fall between w and the subsequent letter a , which shows that w is the level- n superword. The same happens when w is preceded by the final letter of the superword $\theta^{n-1}(a)$, which is a for odd n and \bar{a} for even n . \square

Theorem 3.2.12. *Consider the Thue–Morse word. Then $A(2^n+1) = 2^n + 2$, for all integers $n \geq 2$.*

Proof. We first show that there exist monochromatic arithmetic progressions of length $2^n + 2$. From the proof of Lemma 3.2.10, we already have a monochromatic arithmetic progression of length 2^n in the word $w = \theta^{2n}(a)$, with the first and final letter being part of the progression.

Now, consider how many letters can be added at either end of the progression of length 2^n in the superword $w = \theta^{2n}(a)$. From Lemma 3.2.11, we know that $w = \theta^{2n-1}(a)\theta^{2n-1}(\bar{a})$ and that these are the actual level- $(2n-1)$ superwords. There are four possibilities how this superword can be bordered by level- $(2n-1)$ superwords: we can have $\theta^{2n-1}(b)w\theta^{2n-1}(c)$ with $b, c \in \{a, \bar{a}\}$.

Since $d = 2^n + 1$, no element of the progression is in the level- n superwords adjacent at either end. Since all superwords start or end with a level-2 superword $b\bar{b}\bar{b}b$, the next two members on either side would have to be the first and the second letter of the same superword $\theta^n(\bar{b})$, which however are different letters (where we use that $n > 1$). This shows that the progression can at most be extended by one in either direction. Since all combinations of superwords on either side can appear, there are instances where the progression can be extended by exactly one step in both directions, showing that $A(2^n+1) \geq 2^n + 2$.

It remains to be shown that this is the maximum length of a progression. Assume that we have a progression of length $M > 2^n$. The elements in this progression hit each position in the superwords of level- n at least once. Now, once we hit the first position of such a superword, the following members of the progression determine the sequence of level- n superwords uniquely, which is the same sequence as that of the superword w . If there are at least 2^n terms in the progression following this position, they determine the level- (2^n-1) superword by the second part of Lemma 3.2.11, and hence we are back considering the word w from above. If there are fewer terms left, we can use the previous member of the progression which hits in the last position of a level- n superword, and determine the sequence of level- n superwords preceding it in the progression. Again, this determines the level- (2^n-1) superword by the second part of Lemma 3.2.11, and we are back in the case considered above, showing that $M \leq 2^n + 2$. \square

Observe that Theorem 3.2.12 does not hold for $d = 1$. This case is covered by Proposition 3.2.13 (to follow); notice that $2^1 + 1 = 2^2 - 1$.

3.2.4 Monochromatic arithmetic progressions of difference $d = 2^n - 1$

Similarly, as mentioned above, we can rederive the value of $A(2^n - 1)$ stated in Theorem 3.2.1.

Proposition 3.2.13. *Consider the Thue–Morse word. Then, for all positive integers n ,*

$$A(2^n - 1) = \begin{cases} 2^n + 4, & \text{if } n \text{ is even,} \\ 2^n, & \text{otherwise.} \end{cases}$$

Proof. From Lemma 3.2.10, we already know that $A(2^n - 1) \geq 2^n$ for n odd and $A(2^n - 1) \geq 2^n + 2$ for n even.

Let us first consider the case that n is odd. Since the superwords $\theta^n(a)$ are antisymmetric under reflection, their first and last letters differ. This means that once our progression hits the first letter of a superword, it stops. Since addition by $2^n - 1$ means that the elements in the progression cycle through all positions in the superword, we obtain the upper limit $A(2^n - 1) \leq 2^n$, implying that $A(2^n - 1) = 2^n$.

Now consider the case of n even. Here, the superwords are symmetric under reflection, so we can have two elements of the progression within one superword. Assume that this occurs for a superword $\theta^n(a)$ which has first and last letter a . If the progression continued to the left and to the right, the neighbouring superwords are determined by having the letter a at the next two positions, which force both of them to be \bar{a} , and by symmetry this applies to either side of the superword, hence we obtain $\theta^n(\bar{a})\theta^n(\bar{a})\theta^n(a)\theta^n(\bar{a})\theta^n(\bar{a})$. Clearly, the word $\bar{a}\bar{a}a\bar{a}\bar{a}$ does not belong to the Thue–Morse language. This means that once the progression hits the first and last letter, it can only be extended by at most one in either direction, so we obtain $A(2^n - 1) \leq 2^n + 4$. That this bound is attained can be seen by looking at $\theta^{2^n}(a)$, which by Lemma 3.2.10 contains a progression of length $2^n + 2$ starting and ending with a superword $\theta^n(a)$ that contain two elements of the progression. The superwords either side of $\theta^{2^n}(a)$ can both be $\theta^{2^n}(\bar{a})$, since $\bar{a}a\bar{a}$ is in the Thue–Morse language. Hence the progression can be continued by one additional step to either direction, and the bound is attained. \square

3.2.5 Longest monochromatic arithmetic progressions of difference $d \leq 2^n$

The following two lemmas prove that there are no longer monochromatic arithmetic progressions for differences up to powers of 2.

Lemma 3.2.14. *Consider the Thue–Morse word. Then $A(2^n - k) \leq 2^n$, for all odd positive integers n and k with $0 < k < 2^{n-1}$.*

Proof. Let us assume that there are odd positive integers n and $0 < k < 2^{n-1}$ for which the Thue–Morse word v contains a monochromatic arithmetic progression of difference $d = 2^n - k$ and length $2^n + 1$. Such a progression lies within a subword of v of length $2^nd + 1$, so it lies within $d + 1$ consecutive superwords of length 2^n . Since d is odd and hence coprime with 2^n , for each $0 \leq j \leq 2^n - 1$, the monochromatic arithmetic progression visits one of the superwords at position j . In other words, for each $0 \leq j \leq 2^n - 1$, there exists a letter $a \in \{0, 1\}$ such that $\pi_j(\theta^n(a))$ is an element of the monochromatic

arithmetic progression. In particular, for $j = \frac{k-1}{2}$, we have $j + d = 2^n - \frac{k+1}{2}$, so there exists a unique superword $\theta^n(a)$, where $a \in \{0, 1\}$, whose j th and $(j + d)$ th letters are elements of the monochromatic arithmetic progression, that is,

$$\theta^n(a)_j = \theta^n(a)_{j+d}.$$

However, this is not possible because, for odd n , the superwords of length 2^n are antisymmetric under reflection, by Lemma 3.2.2. Therefore, our initial assumption is false, so $A(2^n - k) \leq 2^n$, as required. \square

Lemma 3.2.15. *Consider the Thue–Morse word. Then $A(2^n - k) \leq 2^n$, for all integers $n > 1$ and odd integers $2 < k < 2^{n-1}$.*

Proof. Let us assume that there are a positive integer n and an odd integer $2 < k < 2^{n-1}$ for which the Thue–Morse word v contains a monochromatic arithmetic progression of difference $d = 2^n - k$ and length $2^n + 1$. Such a progression lies within a subword of v of length $2^n d + 1$, so it lies within $d + 1$ consecutive superwords of length 2^n . Since

$$\frac{2^n + 1}{d + 1} = 1 + \frac{k}{d + 1},$$

there are precisely k instances where two elements of the progression appear within the same superword of length 2^n , and hence the corresponding letters within the superword have to agree. Since $\theta^n(\bar{a}) = \overline{\theta^n(a)}$, both superwords have to agree on all these positions. As a consequence, for $a \in \{0, 1\}$ and the superword $\theta^n(a)$, the word w consisting of its first k letters, namely,

$$w = \theta^n(a)_{[0,k)},$$

also has to appear at the end of the superword, so $w = \theta^n(a)_{[2^n-k, 2^n)}$. Since $k \geq 3$ and $\theta^n(a)$ starts with $a\bar{a}\bar{a}$, the word w always contains a repeated letter and hence the level-1 superwords of length 2 are uniquely determined. This results in a contradiction because the length of w is odd, and the superword $\theta^n(a)$ thus cannot end in w , since the level-1 superword boundaries do not match. Hence $A(d) \leq 2^n$, as required. \square

Notice that, in contrast to Lemma 3.2.14, the result of Lemma 3.2.15 does not extend to the case $k = 1$, since in this case there is only one instance of a word containing two elements of the arithmetic progression and, for even n , the superwords $\theta^n(a)$ start and end on a , so this can (and does) appear in a long monochromatic arithmetic progression.

Corollary 3.2.16. *In the Thue–Morse word, for all $n \in \mathbb{N}$, we have that*

$$\max_{d \leq 2^n + 1} A(d) = \begin{cases} A(2^n - 1) = 2^n + 4, & \text{if } n \text{ is even,} \\ A(2^n + 1) = 2^n + 2, & \text{otherwise.} \end{cases}$$

Proof. The result follows from Corollary 3.2.6, Lemma 3.2.14 and Lemma 3.2.15. \square

3.2.6 Plot and histogram of $A(d)$

In Chapter 2, we mentioned that the Thue–Morse sequence v is linearly recurrent. We can take advantage of this fact to obtain, experimentally, further values of $A(d)$. The key idea is that, by linear recurrence, we can compute $A(d)$ using a sufficiently long prefix of v . An algorithm can be defined to choose the length of this prefix in a finite number of steps. For a rigorous explanation the reader is referred to Appendix A.

The data obtained with this method confirm our results, including Theorems 3.2.1 and 3.2.12. These data are presented in Figure 3.2.1, which exhibits $A(d)$ for $d = 1, 2, \dots, 1100$. A list of values of $A(d)$ can be found in the data underlying this thesis and also in [87].

The histogram in Figure 3.2.2 counts, for each value y taken by $A(d)$, how many d 's satisfy $A(d) = y$. We observe that short monochromatic arithmetic progressions are more frequent than long ones. If the range of differences d was larger, the peak of the histogram would be taller but roughly, situated in the same place, due to linear recurrence of the Thue–Morse word. It seems that $A(d)$ never takes certain values, the smallest value among them being 3.

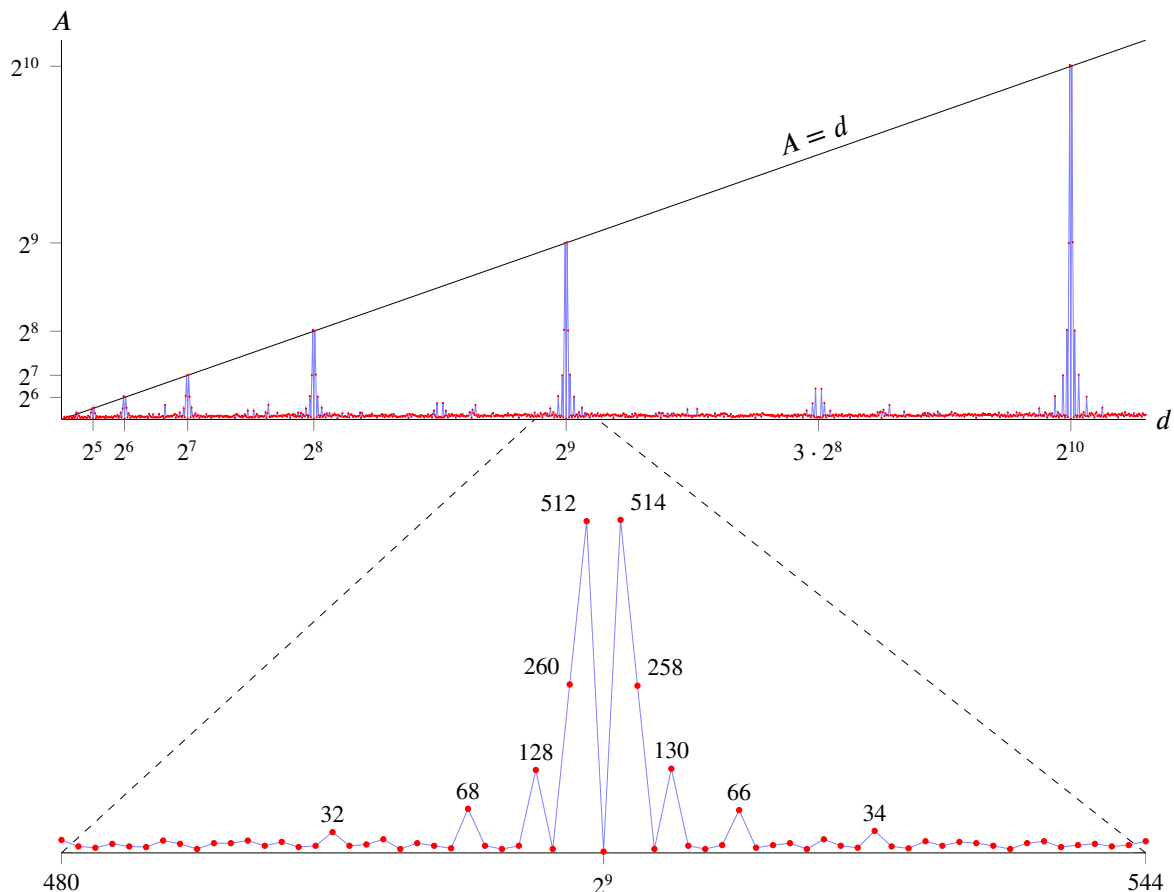


Figure 3.2.1: $A(d)$, for $d = 1, 2, \dots, 1100$, for the Thue–Morse word.

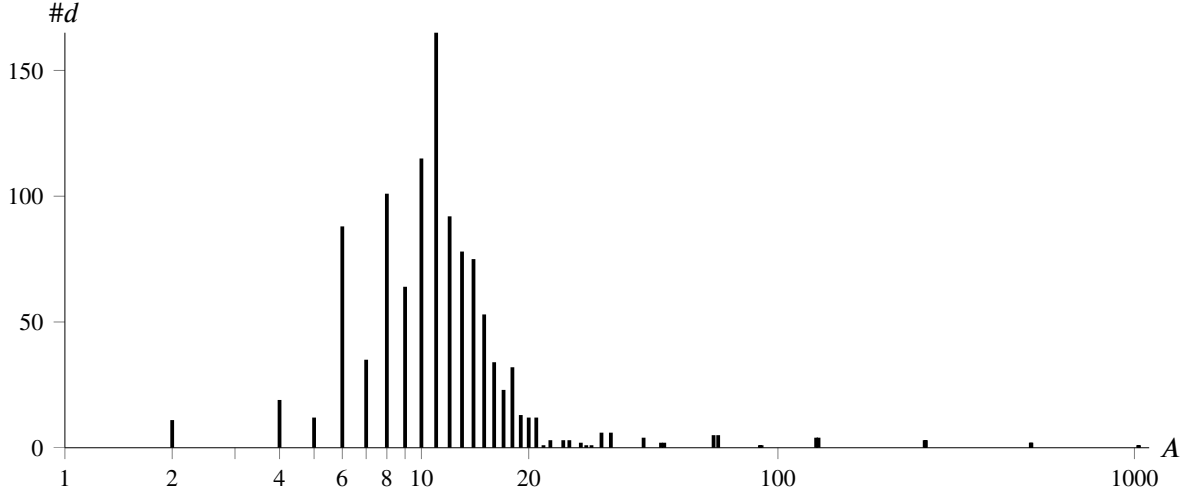


Figure 3.2.2: Histogram corresponding to the values of Figure 3.2.1.

3.3 Monochromatic arithmetic progressions in generalised Thue–Morse words

In this section, we extend the study on the Thue–Morse word to a class of generalised Thue–Morse words. We note that Parshina also considered generalised Thue–Morse words [91], but in her work the generalisation is to larger alphabets, whereas here, we consider a generalisation of the Thue–Morse sequence along the lines of [14, 16, 70], restricting ourselves to the binary case. More precisely, we consider the fixed points of the generalised Thue–Morse substitution rules $\theta_{p,q}$ defined, for positive integers p and q , by

$$\theta_{p,q} : \begin{array}{ll} 0 & \mapsto 0^p 1^q, \\ 1 & \mapsto 1^p 0^q. \end{array} \quad (3.3.1)$$

The original Thue–Morse substitution corresponds to $p = q = 1$.

3.3.1 Properties of the generalised Thue–Morse words and Thue–Morse substitutions

The binary bijective substitutions given by rule (3.3.1) share many properties with the Thue–Morse substitution, given by rule (3.2.1). In particular, we still have the ‘bar-swap’ symmetry $\theta^n(\bar{a}) = \overline{\theta^n(a)}$. This implies that, once again, superwords are uniquely determined as soon as we know a single letter at any position. Notice that, however, the symmetry of superwords is only preserved when $p = q$, with superwords for even n being symmetric while those for odd n being antisymmetric under reflection. The other main difference is that, rather than working modulo 2, we now have to work modulo

$$Q := p + q.$$

Also, it is clear from the substitution rule (3.3.1) that the language of $\theta_{p,q}$ is $(Q+1)$ -powerfree (in fact, $(Q + \epsilon)$ -powerfree for any integer $\epsilon > 0$), generalising the cube-freeness of the Thue–Morse case.

Since the rule $\theta_{p,p}^2$ is symmetric under reflection, the corresponding language is reflection symmetric too. However, if $p \neq q$, reflection swaps the languages defined by $\theta_{p,q}$ and $\theta_{q,p}$. As we shall now show, both of these languages are not reflection symmetric.

Lemma 3.3.1. *For $p \neq q$, the languages $\mathcal{L}_{p,q}$ and $\mathcal{L}_{q,p}$ defined, respectively, by the substitutions $\theta_{p,q}$ and $\theta_{q,p}$ are different. In particular, for $a \in \{0, 1\}$, the words $\bar{a}^{q+1} a^p \bar{a}$ belong to $\mathcal{L}_{q,p}$ but not to $\mathcal{L}_{p,q}$.*

Proof. It is easy to verify that $a\bar{a}\bar{a} \in \mathcal{L}_{q,p}$, for any $p, q \in \mathbb{N}$. Now,

$$\theta_{p,q}(a\bar{a}\bar{a}) = a^q \bar{a}^p \bar{a}^q a^p \bar{a}^q a^p = a^q \bar{a}^{p-1} (\bar{a}^{q+1} a^p \bar{a}) \bar{a}^{q-1} a^p,$$

so $\bar{a}^{q+1} a^p \bar{a} \in \mathcal{L}_{q,p}$, for all $p \neq q$. However, $\bar{a}^{q+1} a^p \bar{a} \notin \mathcal{L}_{p,q}$, which we are going to show now.

Noting that $p \neq q$ and that $\mathcal{L}_{p,q}$ can only contain strings of the type $\bar{a} a^m \bar{a}$ for $m \in \{p, q, p+q\}$, it follows by recognisability that $a^p \bar{a}$ in $\bar{a}^{q+1} a^p \bar{a}$ has to be the beginning of the level-1 superword $\theta_{p,q}(a)$. However, it then has to be preceded by the level-1 superword that ends in \bar{a} , which is again $\theta_{p,q}(a) = a^p \bar{a}^q$. This is clearly impossible, establishing the claim. \square

Remark 3.3.2. Similarly, considering the word $aa\bar{a} \in \mathcal{L}_{q,p}$, with

$$\theta_{q,p}(aa\bar{a}) = a^q \bar{a}^p a^q \bar{a}^p \bar{a}^q a^p = a^q \bar{a}^{p-1} (\bar{a} a^q \bar{a}^{p+1}) \bar{a}^{q-1} a^p,$$

we can show that $\bar{a} a^q \bar{a}^{p+1}$ belongs to $\mathcal{L}_{q,p}$, but it does not belong to $\mathcal{L}_{p,q}$, for $p \neq q$. \diamond

It is not difficult to show that, for positive integers p and q , the height of $\theta_{p,q}$ is 1, so $\theta_{p,q}$ is its own pure base, by [38]. Furthermore, $\theta_{p,q}$ is bijective, so it does not admit any coincidence. Therefore, by Proposition 3.1.4, the maximum length that a monochromatic arithmetic progression within a fixed points $w_{p,q}$ of $\theta_{p,q}$ can have is finite, that is, $A_{w_{p,q}}(d) < \infty$. From now on, $A_{w_{p,q}}(d)$ will be written as $A_{p,q}(d)$.

3.3.2 Monochromatic arithmetic progressions of difference $d = Q^n$

As a consequence of the structure of the substitutions $\theta_{p,q}$ and recognisability, the following result can be proved.

Lemma 3.3.3. *Consider the generalised Thue–Morse word, which is a fixed point of the substitution $\theta_{p,q}$. Then $A_{p,q}(Q^n d) = A_{p,q}(d)$, for all positive integers d and n . In particular, $A_{p,q}(Q^n) = A_{p,q}(1) = Q$.*

3.3.3 Monochromatic arithmetic progressions of difference $d = Q^n + 1$

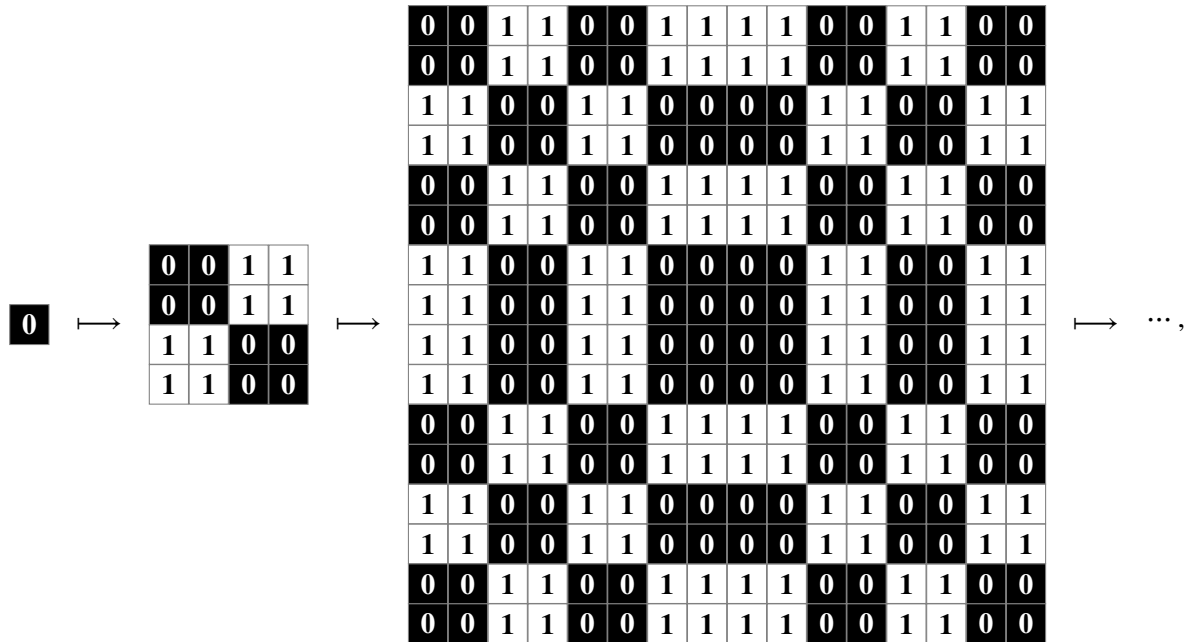
We can again find long monochromatic arithmetic progressions by considering a block substitution.

Definition 3.3.4. Let $\Theta_{p,q}$ be the block substitution of the alphabet $\{0, 1\}$ defined by

$$\Theta_{p,q} : \quad 0 \mapsto \begin{array}{c} 0^p 1^q \\ 0^p 1^q \\ \vdots \\ 0^p 1^q \\ 1^p 0^q \\ 1^p 0^q \\ \vdots \\ 1^p 0^q \end{array} \left. \vphantom{\begin{array}{c} 0^p 1^q \\ 0^p 1^q \\ \vdots \\ 0^p 1^q \\ 1^p 0^q \\ 1^p 0^q \\ \vdots \\ 1^p 0^q \end{array}} \right\} \begin{array}{l} p \\ q \end{array}, \quad 1 \mapsto \begin{array}{c} 1^p 0^q \\ 1^p 0^q \\ \vdots \\ 1^p 0^q \\ 0^p 1^q \\ 0^p 1^q \\ \vdots \\ 0^p 1^q \end{array} \left. \vphantom{\begin{array}{c} 1^p 0^q \\ 1^p 0^q \\ \vdots \\ 1^p 0^q \\ 0^p 1^q \\ 0^p 1^q \\ \vdots \\ 0^p 1^q \end{array}} \right\} \begin{array}{l} p \\ q \end{array}.$$

The block substitution $\Theta_{p,q}$ maps a single letter a to a $Q \times Q$ block of letters, which, when read line by line, coincides with the word $\theta_{p,q}^2(a)$. To illustrate the properties of $\Theta_{p,q}$, let us consider a couple of examples.

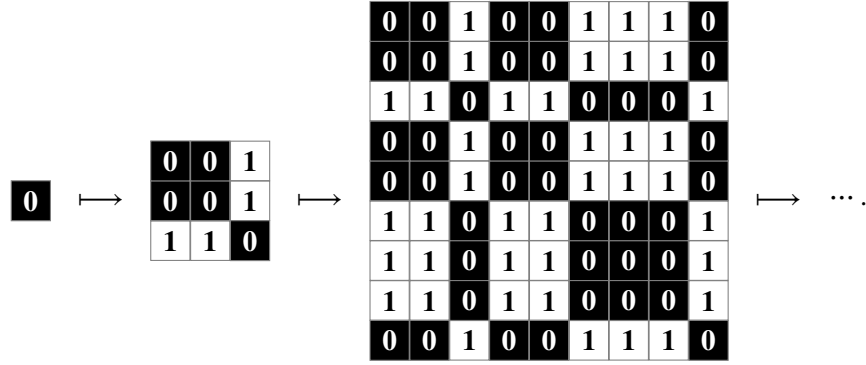
Example 3.3.5. We first consider an example where $p = q$, namely $\Theta_{2,2}$. The first two substitution steps of the letter 0 are as follows,



which has a similar structure to the Thue–Morse case arising from the block substitution of Definition 3.2.7. In particular, all squares along the diagonals are of the same colour.

The situation is different for $p \neq q$. Here we consider the block substitution $\Theta_{2,1}$ as an example,

which acts on the letter 0 as



Notice that, while we retain the same letter along the main diagonal, this is no longer the case along the diagonal from the lower left to the top right. Considering the second iteration (third block) shown above, it appears that there is a long monochromatic progression of difference $3^2 - 1 = 8$, starting from the central black square on the top row and moving down diagonally, and then continuing on from the final black square on the middle row. By a computer experiment, which applies the algorithm developed in Appendix A, we find that for $d = 8$ the longest monochromatic arithmetic progressions have length 12, and the first time one such progression occurs in the generalised Thue–Morse sequence starts at position 239. However, this pattern does not persist for further iterations. ❖

As in the Thue–Morse case, the image of a letter a has all entries a along the main diagonal of this block. However, as illustrated in Example 3.3.5, in general this is no longer the case for the other diagonal, except when $p = q$, in which case the entries of this diagonal are all \bar{a} . This means that we obtain the existence of long monochromatic arithmetic progressions, as in the Thue–Morse case, for $d = Q^n + 1$ for all values of p and q , while long monochromatic arithmetic progressions for $d = Q^n - 1$ may only exist if $p = q$.

Noting that Lemma 3.2.8 and Lemma 3.2.9 generalise in a straightforward manner, we obtain the following existence result for long monochromatic arithmetic progressions in generalised Thue–Morse words, generalising the result of Lemma 3.2.10.

Lemma 3.3.6. *Consider the generalised Thue–Morse word, which is a fixed point of the substitution $\theta_{p,q}$. Then $A_{p,q}(Q^n+1) \geq Q^n$ and $A_{p,p}(Q^n-1) \geq Q^n$, for all positive integers n , where $Q = p+q$. Furthermore, $A_{p,p}(Q^n-1) \geq Q^n + 2$, if n is even.*

Proof. This follows by the same line of argument as for the Thue–Morse case in the proof of Lemma 3.2.10. □

The following results implicitly use the fact that, as in the Thue–Morse case, a level- n superword of $\theta_{p,q}$ within any word in $\mathcal{L}_{p,q}$ only occurs in certain ways. We obtain the following generalisation of Lemma 3.2.11.

Lemma 3.3.7. *Let be an integer $n > 1$ and a letter $a \in \{0, 1\}$. The word $w = \theta_{p,q}^n(a)$ occurs inside sufficiently long words in $\mathcal{L}_{p,q}$ either as the level- n superword itself, or, for $p = q$, in the centre of two level- n superwords $\theta_{p,p}^n(\bar{a})\theta_{p,p}^n(a)$. Furthermore, for $p = q$, w is the level- n superword, if it is followed by the letter \bar{a} , or if it is preceded by the letter a for n odd, or \bar{a} for n even.*

Proof. The proof is a straightforward generalisation from that of Lemma 3.2.11. The only difference is that, for $p \neq q$, the word w can only occur as the level- n superword, because the level- $(n-1)$ superwords are determined and with $p \neq q$ they can only be combined to the level- n superword in one way. \square

Theorem 3.3.8. *Consider the generalised Thue–Morse word, which is a fixed point of $\theta_{p,q}$. Then*

$$A_{p,q}(Q^n+1) = \begin{cases} Q^n + Q - 2, & \text{if } p > 1 \text{ and } q > 1, \\ Q^n + Q - 1, & \text{if } q > p = 1 \text{ or } p > q = 1, \\ Q^n + Q, & \text{if } p = q = 1, \end{cases}$$

for all positive integers n, p and q , with $n > 1$, where $Q = p + q$.

Proof. From the proof of Lemma 3.3.6, we have an arithmetic progression of length Q^n of the letter a in the word

$$w = \theta_{p,q}^{2n}(a) = (\theta_{p,q}^n(a))^p (\theta_{p,q}^n(\bar{a}))^q \dots (\theta_{p,q}^n(\bar{a}))^p (\theta_{p,q}^n(a))^q,$$

with the first and final letter being part of the progression (as before, because we are looking at an even number of substitutions, the word w starts and ends with the same letter). Notice that, since the elements in the progression of difference $Q^n + 1$ visit successive positions in superwords $\theta_{p,q}^n(a)$ in order, we know that, irrespective of where we start, once we hit the first letter of a superword $\theta_{p,q}^n(a)$ (which has to happen for any progression of length Q^n) the progression follows this same sequence, and the same backwards from when we hit the final position in a level- n superword. Using the same argument as in the proof of Theorem 3.2.12, we conclude that any progression of length larger than Q^n has to include this superword.

Now consider how many letters can be added at either end of the progression of length Q^n in the superword w . For $Q > 2$, all four possibilities for this superword being bordered by level- n superwords $u = \theta_{p,q}^n(a)$ or $\bar{u} = \theta_{p,q}^n(\bar{a})$ can occur, so we need to consider w followed or preceded by either u or \bar{u} .

If w is followed by u , it is followed by u^p and we can extend the arithmetic progression by exactly $p - 1$ to the right. If it is followed by \bar{u} , we cannot extend at all unless $p = 1$. For $p = 1$, we can extend by exactly one step.

If w is preceded by u (for n odd) or \bar{u} (for n even), we cannot extend at all unless $q = 1$, in which case we can extend by precisely one step. If it is preceded by \bar{u} (for n odd) or u (for n even), we can extend by exactly $q - 1$ steps to the left.

Choosing the combination with the longest available progression yields the result. \square

Notice that for $p = q = 1$ we recover the result of Theorem 3.2.12.

3.3.4 Monochromatic arithmetic progressions of difference $d = Q^n - 1$

Theorem 3.3.9. *Consider the generalised Thue–Morse word, which is a fixed point of $\theta_{p,p}$. Then*

$$A_{p,p}(Q^n - 1) = \begin{cases} Q^n, & \text{if } n \text{ is odd,} \\ Q^n + Q, & \text{if } n \text{ is even and } p > 1, \\ Q^n + Q + 2, & \text{if } n \text{ is even and } p = 1, \end{cases}$$

for all positive integers n and p , with $n > 1$, where $Q = 2p$.

Proof. From Lemma 3.3.6, we already know that long monochromatic arithmetic progressions of difference $d = Q^n - 1$ exist, with $A_{p,p}(d) \geq Q^n$, within the superword

$$w = \theta_{p,p}^{2n}(a) = (\theta_{p,p}^n(a))^p (\theta_{p,p}^n(\bar{a}))^p \dots (\theta_{p,p}^n(\bar{a}))^p (\theta_{p,p}^n(a))^p.$$

Accordingly, such a long progression visits every position in level- n superwords (again because d and Q^n are coprime).

For odd values of n , the superwords $\theta_{p,p}^n(b)$ start with b and end on \bar{b} , so it is not possible to have the first and last letter in the same monochromatic arithmetic progression. This implies that $A_{p,p}(d) \leq Q^n$, and hence $A_{p,p}(d) = Q^n$ in this case.

For even values of n , all superwords $\theta_{p,p}^n(b)$ start and end in the same letter, so $A_{p,p}(d) \geq Q^n + 2$, as shown in Lemma 3.3.6, with the first and last letter in the superword w belonging to the arithmetic progression. What is left to consider is how far this can be extended on either side. The word w can be preceded and succeeded by level- n superwords $u = \theta_{p,p}^n(a)$ or $\bar{u} = \theta_{p,p}^n(\bar{a})$; for $p = 1$ one has to ensure cube-freeness.

If w is succeeded by u and hence by u^p , it can be extended by exactly $p - 1$ steps. If it is succeeded by \bar{u} , no extension is possible, unless $p = 1$ in which case we can extend by exactly one step. Due to symmetry of all these words for even n , the same argument applies at the other end, which completes the proof. \square

Proposition 3.3.10. *Consider the generalised Thue–Morse word, which is a fixed point of the substitution $\theta_{p,q}$ with $p \neq q$. Then $A_{p,q}(Q^n - 1) \leq Q^n$, for all positive integers $n > 2$, where $Q = p + q$.*

Proof. Assume to the contrary that a long monochromatic arithmetic progression of difference $Q^n - 1$ and length larger than Q^n exists. Then this progression contains a level- n superword $w = \theta_{p,q}^n(a)$ with two instances of this progression, implying that the first and last letter of w agree. If n is odd, this is not possible, since w starts with a and ends on \bar{a} .

If $n > 2$ is even, w starts and ends with

$$\theta_{p,q}^2(a) = \theta_{p,q}(a^p) \theta_{p,q}(\bar{a}^q) = (a^p \bar{a}^q)^p (\bar{a}^p a^q)^q.$$

Since by bijectivity a single letter determines the superwords, we can read off the sequence of words to the left and to the right of the word w with two instances of the progression, provided the progression extends.

Consider first the case $p > 1$. Assume that the progression continues to the right of w . As we are considering the difference $d = Q^n - 1$, we are effectively reading the word w “backwards” to determine the sequence of superwords that is required. As mentioned above, w ends on $\theta_{p,q}^2(a)$, which, read backwards, is of the form

$$x(\bar{a}^{q+1}a^p\bar{a})y,$$

with $x, y \in \{0, 1\}^+$ and $|x| = qQ - 1$. According to Lemma 3.3.1, the word $\bar{a}^{q+1}a^p\bar{a}$ does not occur in $\mathcal{L}_{p,q}$, since we are considering the case that $p \neq q$. This implies that the sequence of superwords required to continue the progression to the right contains a subsequence that corresponds to the images of a word under $\theta_{p,q}$ that is not in the language $\mathcal{L}_{p,q}$, which is a contradiction. From here it follows that the progression cannot continue to the right for more than $qQ - 1$ steps at most.

An analogous argument holds if we assume that the progression extends to the left, showing that it can at most continue for $pQ - 1$ steps to the left. So the total length of the progression is at most $(pQ - 1) + 2 + (qQ - 1) = Q^2$, which is less than Q^n , for $n > 2$.

If $p = 1$ and hence $q > 1$, we can use the same arguments as above, based on the word $\bar{a}a^q\bar{a}^{p+1}$ from Remark 3.3.2, which occurs within the backwards reading of $\theta_{p,q}^2(a)$ in this case. \square

3.3.5 Longest monochromatic arithmetic progressions of difference $d \leq Q^n + 1$

We have established the existence of long monochromatic arithmetic progressions for all generalised Thue–Morse sequences for differences $d = Q^n + 1$, as well as for differences $d = Q^n - 1$ in the case that $p = q$. The obvious conjecture is that these are again the longest monochromatic arithmetic progressions that one can find, up to the given difference, in these systems, which we state as a conjecture.

Conjecture 3.3.11. *Consider the generalised Thue–Morse word. For all positive integers $n > 1$ and p ,*

$$\max_{d \leq Q^n + 1} A_{p,p}(d) = \begin{cases} A_{p,p}(Q^n - 1) = Q^n + Q, & \text{if } p > 1 \text{ and } n \text{ even,} \\ A_{p,p}(Q^n + 1) = Q^n + Q - 2, & \text{if } p > 1 \text{ and } n \text{ odd,} \end{cases}$$

where $Q = 2p$. Furthermore, for all positive integers $n > 2$, p and q ,

$$\max_{d \leq Q^n + 1} A_{p,q}(d) = \begin{cases} A_{p,q}(Q^n + 1) = Q^n + Q - 1, & \text{if } p > q = 1 \text{ or } q > p = 1, \\ A_{p,q}(Q^n + 1) = Q^n + Q - 2, & \text{if } p > q > 1 \text{ or } q > p > 1, \end{cases}$$

where $Q = p + q$.

To establish this conjecture, we would need to generalise the results of Lemmas 3.2.14 and 3.2.15. This is not straightforward, though, because we now have to consider differences $d = Q^n - k$, where

we may have that k is a non-trivial divisor of Q , in which case the argument that in a long arithmetic progression all congruence classes modulo Q^n appear is no longer applicable.

The following lemma details the relations within superwords arising from an assumed existence of long monochromatic arithmetic progressions.

Lemma 3.3.12. *Consider a fixed point of $\theta_{p,q}$ and let $Q = p + q$. For all positive integers n and k with $n > 1$ and $1 < k < Q^{n-1}$, let $s = \gcd(k, Q)$ and assume that $s \neq Q$. If there exists a monochromatic arithmetic progression of difference $d = Q^n - k$ and length larger than $\frac{Q^n}{s}$, the level- n superwords $w = \theta_{p,q}^n(a)$ have to satisfy $w_{r+\ell s} = w_{r+\ell s+d}$, for some $0 \leq r < s$ and for all $0 \leq \ell < \frac{k}{s}$.*

Proof. We have $\gcd(d, Q) = \gcd(k, Q) = s$ and $r \equiv d \pmod{Q}$, so any such arithmetic progression of length larger than $\frac{Q^n}{s}$ visits all positions

$$\{r' : 0 \leq r' < Q^n, r' \equiv r \pmod{Q^n}\} = \{r + \ell s : 0 \leq \ell < \frac{Q^n}{s}\}$$

in a superword $w = \theta_{p,q}^n(a)$, for some letter $a \in \{0, 1\}$ and for some $0 \leq r < s$. Whenever there are two instances within a superword, the corresponding letters have to agree for either superword, since $\theta_{p,q}^n(\bar{a}) = \overline{\theta_{p,q}^n(a)}$. The condition for having two instances within a superword is $r' + d < Q^n$, which implies $r' < k$. With $r' = r + \ell s$, this results in $\ell < \frac{k-r}{s}$ and, since $r < s$, this is equivalent to $\ell < \frac{k}{s}$, establishing the claim. \square

Proposition 3.3.13. *Consider a fixed point of $\theta_{p,q}$, for $Q = p + q$ prime. Then, for all positive integers n (with $n > 1$) and $Q < k < Q^{n-1}$, the length of every monochromatic arithmetic progression of difference $d = Q^n - k$ is less than or equal to Q^n .*

Proof. Since Q is prime, $\gcd(k, Q) = 1$. By Lemma 3.3.12, if there exists a monochromatic arithmetic progression of length larger than Q^n , the superwords $w = \theta_{p,q}^n(a)$ have to satisfy

$$w_0 \cdots w_{k-1} = w_{Q^n-k} \cdots w_{Q^n-1}.$$

If $k > Q$, this produces a contradiction, since the final Q letters of $w_0 \cdots w_{k-1}$ cannot be a valid level-1 superword, but w has to end on a level-1 superword. \square

Notice that this lemma does not cover the differences $d = Q^n - k$, where $1 < k < Q$, which we would need to establish the conjecture for prime values of Q (except for $Q = 2$, which brings us back to the Thue–Morse case). A partial result for $\min(p, q) = 1$ is next, establishing Conjecture 3.3.11 for this class.

Proposition 3.3.14. *Consider a fixed point of $\theta_{p,q}$, for $Q = p + q$ prime and $\min(p, q) = 1$. Then, for all positive integers n and any $1 < k < Q^{n-1}$, the length of every monochromatic arithmetic progression of difference $d = Q^n - k$ is less than or equal to Q^n .*

Proof. From Proposition 3.3.13, we know that the claim holds for $k > Q$.

If $p = 1$, the level-1 superwords are of the form $a\bar{a}^q$ with $a \in \{0, 1\}$. This implies that, for $1 < k < Q$, the superwords $w = \theta_{1,q}^n(a)$ start with $w_0 \cdots w_{k-1} = a\bar{a}^{k-1}$. Since $1 \leq k-1 < q$, this string of letters cannot occur at the end of the superword w .

Similarly, if $q = 1$, the superwords $w = \theta_{p,1}^n(a)$ start with $w_0 \cdots w_{k-1} = a^k$. Since $k > q = 1$, this string of letters cannot occur at the end of the superword w . \square

3.3.6 Plots of $A_{p,q}(d)$

We finish this section with plots of $A_{p,q}(d)$. To depict the difference between the $p = q$ case and the $p \neq q$ case, we present Figures 3.3.1 and 3.3.2, the former for $p = q = 2$ and the latter for $p = 3$ and $q = 1$, so $Q = 4$ in both cases. Experimental data, which can be found in the data underlying this thesis, agree with our results, including Theorems 3.3.8 and 3.3.9, and also give credibility to Conjecture 3.3.11.

In Figure 3.3.1, the equality of p and q preserves the symmetry of superwords of the Thue–Morse substitution and consequently, it is qualitatively similar to Figure 3.2.1. In particular, we observe the large monochromatic arithmetic progressions at differences $d = Q^n \pm 1 = 4^n \pm 1$. It is interesting to notice that there is another series of large peaks around differences d of the form 2^n for odd n , similarly to Figure 3.2.1 for the Thue–Morse case; however, the largest values are not at $d = 2^n \pm 1$, but at $d = 2^n - 2$. On the other hand, when $p \neq q$, the output differs qualitatively from the Thue–Morse case, as can be seen in Figure 3.3.2.

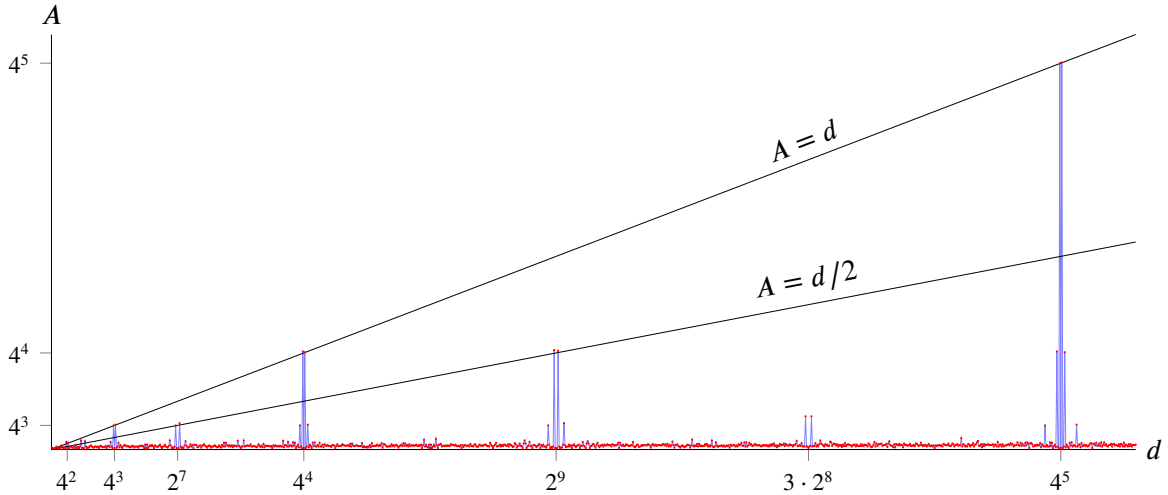


Figure 3.3.1: $A_{2,2}(d)$, for $d = 1, 2, \dots, 1100$.

3.4 Upper bounds for $A(d)$ for primitive binary bijective substitutions

In this section, we state a partial result for general primitive bijective (hence constant-length) substitutions of the binary alphabet $\{0, 1\}$, which include those treated in Section 3.3.

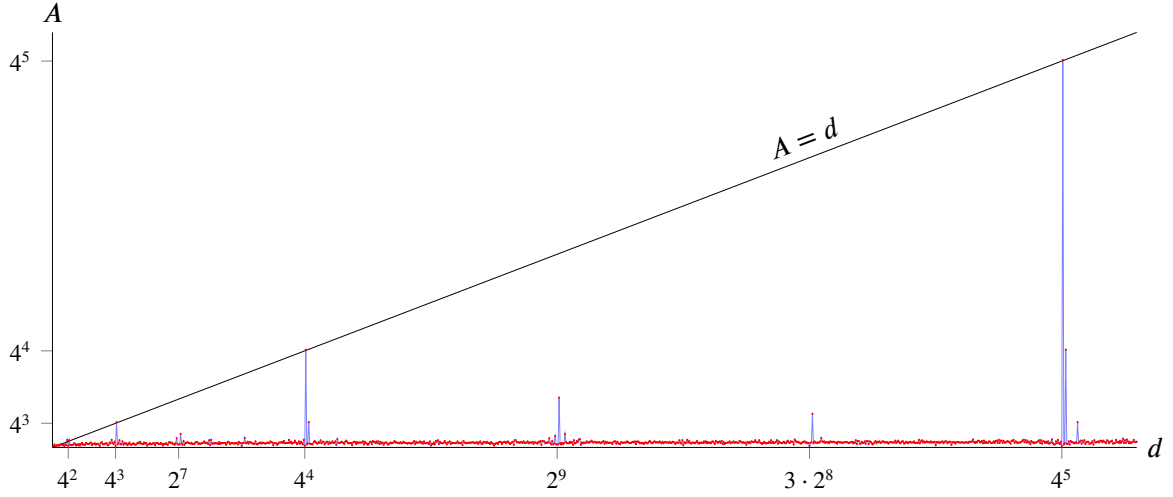


Figure 3.3.2: $A_{3,1}(d)$, for $d = 1, 2, \dots, 1100$.

Let k be a positive integer and, for a non-negative integer n , let $w = w_0 w_1 \dots w_n$ be a word over $\{0, 1\}$ of length $n + 1$. We say that a pattern $P(w, k)$ is allowed within a long enough word v over $\{0, 1\}$, if there exists a non-negative integer s such that

$$v_s = w_0, \quad v_{s+k} = w_1, \quad v_{s+2k} = w_2, \quad \dots, \quad v_{s+nk} = w_n.$$

That is, $P(w, k)$ is an arithmetic subword (not necessarily monochromatic) of difference k and length $n + 1$ within v . A monochromatic progression corresponds to either case $w = 0^{n+1}$ or 1^{n+1} .

Proposition 3.4.1. *Let φ be a primitive bijective substitution of $\{0, 1\}$ of length Q and let $v \in \{0, 1\}^{\mathbb{N}_0}$ be a fixed point of φ . Let k, d and m be positive integers and, for a non-negative integer n , let w be a word over $\{0, 1\}$ of length $n + 1$. Suppose that*

- (i) Q and d are coprime,
- (ii) $P(w, k)$ is not allowed within v , and
- (iii) $P(w, d)$ is allowed within $\varphi^m(0)$.

Then the pattern $P(0^{n'}, d')$ is not allowed within v , where $n' = Q^m + n$ and $d' = Q^m k + d$. So v does not contain any monochromatic arithmetic progressions of difference d' and length n' . In other words, $A_v(Q^m k + d) < Q^m + n$.

Proof. The proof is by contradiction. Assume that $P(0^{n'}, d')$ is allowed within v . Then there exists a non-negative integer t such that $v_{t+sd'} = 0$, for $s = 0, 1, \dots, n' - 1$. By condition (iii) upright, there exists a non-negative integer l_0 such that the $(l_0 + jd)$ th letter of $\varphi^m(0)$ is w_j , for $j = 0, 1, \dots, n$, which implies that $0 \leq l_0 + jd \leq Q^m - 1$. By condition (i) upright, there must exist an integer $0 \leq s \leq Q^m - 1$ such that $l_0 \equiv t + sd' \pmod{Q^m}$, so $t + sd' = l_0 + iQ^m$, for some non-negative integer i . Then

$$t + (s + j)d' = l_0 + jd + (i + jk)Q^m,$$

for $j = 0, 1, \dots, n$. Since $0 \leq l_0 + jd \leq Q^m - 1$, this implies that $v_{l_0 + jd}$ is the $(l_0 + jd)$ th letter in a superword, which we denote by $\varphi^m(a_j)$, where $a_j \in \{0, 1\}$.

If $w_j = 0$, then the $(l_0 + jd)$ th letter of $\varphi^m(0)$ is 0, so the $(l_0 + jd)$ th letter of $\varphi^m(0)$ and $\varphi^m(a_j)$ coincide, which implies that $a_j = 0$. If $w_j = 1$, then the $(l_0 + jd)$ th letter of $\varphi^m(0)$ is 1, so the $(l_0 + jd)$ th letter of $\varphi^m(0)$ and $\varphi^m(a_j)$ differ, which implies that $a_j = 1$. In both cases $w_j = a_j$. Then $v_{i+jk} = w_j$, for $j = 0, 1, \dots, n$, and the pattern $P(w, k)$ occurs within v . However, this contradicts condition (ii) upright and therefore, the assumption initially made is false. \square

Proposition 3.4.2. *Let φ be a primitive bijective substitution of $\{0, 1\}$ of length Q and let $v \in \{0, 1\}^{\mathbb{N}_0}$ be a fixed point of φ . Let k, d and m be positive integers and, for a non-negative integer n , let $w = w_0 w_1 \dots w_n$ be a word over $\{0, 1\}$ of length $n + 1$. Suppose that*

- (i) Q and d are coprime,
- (ii) $P(w, k)$ is not allowed within v , and
- (iii) $P(w_n \dots w_1 w_0, d)$ is allowed within $\varphi^m(0)$.

Then the pattern $P(0^{n'}, d')$ is not allowed within v , where $n' = Q^m + n$ and $d' = Q^m k - d$. So v does not contain any monochromatic arithmetic progressions of difference d' and length n' . In other words, $A_v(Q^m k - d) < Q^m + n$.

Proof. A proof of this proposition can be obtained from the proof of Proposition 3.4.1 by judicious replacement of j with $n - j$ where necessary. \square

Example 3.4.3. Let φ be the substitution

$$\varphi: \begin{array}{lcl} 0 & \mapsto & 0101, \\ 1 & \mapsto & 1010, \end{array}$$

and let v be a fixed point of φ , and set $w = 101$. The pattern $P(w, 2)$ is not allowed within v . Moreover, for each positive integer m , w occurs in $\varphi^m(0)$, so the pattern $P(w, 1)$ is allowed within $\varphi^m(0)$. Therefore, by Propositions 3.4.1 and 3.4.2 with $Q = 4$, $d = 1$ and $k = n = 2$, v does not contain monochromatic arithmetic progressions of difference $d' = 2 \cdot 4^m \pm 1$ and length $n' = 4^m + 2$. This can also be written as $A_v(2^\ell \pm 1) < 2^{\ell-1} + 2$, for all odd integers $\ell > 1$. \diamond

4. MONOCHROMATIC ARITHMETIC PROGRESSIONS IN AUTOMATIC SEQUENCES

In the previous chapter, we focused on long monochromatic arithmetic progressions appearing in Thue–Morse-like infinite words. For some differences d , we determined $A(d)$, namely, the maximum length that a monochromatic arithmetic progression of difference d occurring in the considered infinite word can have. Since these infinite words are automatic sequences arising from binary bijective substitutions, it is natural to consider automatic sequences arising from other substitutions too.

In this chapter, we focus on fixed points of constant-length substitutions of alphabets of any finite size, and their images under codings. We mainly consider two classes of substitutions with an explicit group structure, which provides direct access to bounding $A(d)$ for some specific values of d and allows some asymptotic estimates. The first class is the class of bijective substitutions, which are generalisations of the Thue–Morse substitution. To a bijective substitution, one can associate a finite group, namely, the column group described in Section 2.4.7. The second class is the class of spin substitutions, which are a particular type of non-bijective substitutions. To a spin substitution, one can associate a finite group each of whose elements represents a different spin state that a letter of the associated alphabet can be on (see Section 4.4). Apart from these two families, we also deal with non-bijective substitutions with a ‘supersubstitution’ structure; these are substitutions that are non-bijective but for which we can define a bijective substitution of a different alphabet to obtain results about the original non-bijective substitution (see Section 4.3).

In the case of fixed points of bijective substitutions, we prove the following result in Section 4.2.1.

Theorem 4.0.1. *Let ϱ be an aperiodic, primitive, bijective substitution. For any fixed point of ϱ , there exist an increasing sequence (d_n) in \mathbb{N} and a real number α in $(0, 1]$ for which $A(d_n) \gtrsim d_n^\alpha$.*

In Section 4.2.2, we introduce the notion of g -palindromicity and show that, for g -palindromic substitutions, one gets $\alpha = 1$ in Theorem 4.0.1, that is, the asymptotic growth of $A(d)$ is at least linear in d .

In the case of fixed points of spin substitutions we prove the following result in Section 4.4.4.

Theorem 4.0.2. *Let θ be a spin substitution arising from an $L \times L$ Vandermonde matrix. For the spin coding of any fixed point of θ , there exist an increasing sequence (d_n) in \mathbb{N} and a real number α in $(0, 1]$ for which $A(d_n) \gtrsim d_n^\alpha / L$.*

In particular, for the Rudin–Shapiro substitution, which is the simplest of the Vandermonde substitutions with $L = 2$, we have $\alpha = 1$, that is, the asymptotic growth of $A(d)$ is at least linear in d .

Notice that Theorems 4.0.1 and 4.0.2 deal with lower bounds for $A(d)$. Under some mild assumptions on the substitution, one can also obtain upper bounds for $A(d)$. In particular, sufficient conditions for $A(d) < \infty$ to hold, for all d , are given in Propositions 4.1.4 and 4.4.23. For a subclass of bijective substitutions and for certain differences, explicit and computable upper bounds are given in Corollary 4.2.31 and Proposition 4.2.34.

The lower bounds we obtain depend only on the size c of the alphabet and the length L of the substitution. This allows one to associate a *van der Waerden-type number* $W(\mathcal{B}(c, L), M)$ to a family of bijective substitutions sharing these same attributes (this is done in Section 4.2.3).

This chapter is organised as follows. In Section 4.1 we introduce some preliminaries. In Section 4.2 we focus on bijective substitutions, extending the results on lower bounds in [2, 90, 91] and Theorems 3.3.8 and 3.3.9 in Chapter 3 to this family. This includes the class of symmetric morphisms in [54] and group substitutions in [60]. In Section 4.2.3 we develop the notion of van der Waerden-type numbers for bijective substitutions and provide explicit upper bounds. We use recurrence properties for substitutive words and the results obtained in Section 4.2.1 to compute these bounds. Section 4.2.4 deals with upper bounds for $A(d)$ for bijective substitutions with additional properties. Each result is illustrated with examples, and Section 4.2.5 is completely devoted to the family of cyclic Thue–Morse substitutions. In Section 4.3 we introduce non-bijective substitutions with supersubstitution structure. In Section 4.4, we deal with spin substitutions. We begin with the case of the Rudin–Shapiro substitution in Sections 4.4.1 and 4.4.2, where we derive lower bounds using two combinatorial approaches, namely, the spin matrix approach and the staggered substitution approach. The former extends to other automatic sequences derived from other spin matrices. We carry this out in Section 4.4.3 in the case of a Hadamard matrix, and in Section 4.4.4 in the case of a Vandermonde matrix.

4.1 Preliminaries

4.1.1 Column structure of constant-length substitutions

In this section we prove Proposition 4.1.1, which says how to determine the columns of a composition of constant-length substitutions. In particular, for a composition of powers of a single substitution, we obtain Proposition 4.1.2. These results are known (see [96, Section 5.1] and [77, Section 2]), but their proof merits inclusion here because we will use them repeatedly.

Proposition 4.1.1. *For a positive integer n , let $\varrho_1, \varrho_2, \dots, \varrho_n$ be constant-length substitutions of lengths L_1, L_2, \dots, L_n , respectively. Let $\ell_0 = 1$ and, for $i = 1, 2, \dots, n$, let $\ell_i = L_1 \cdot L_2 \cdot \dots \cdot L_i$. Then, for $k = 0, 1, \dots, \ell_n - 1$, the k th column of the substitution $\varrho_1 \circ \varrho_2 \circ \dots \circ \varrho_n$ is given by the functional composition*

$$[\varrho_1 \circ \varrho_2 \circ \dots \circ \varrho_n]_k = [\varrho_1]_{k_0} \circ [\varrho_2]_{k_1} \circ \dots \circ [\varrho_n]_{k_{n-1}},$$

where the indices k_0, k_1, \dots, k_{n-1} , which satisfy $0 \leq k_i \leq L_{i+1} - 1$, are the unique integers for which $k = \sum_{i=0}^{n-1} k_i \cdot \ell_i$.

Proof. For $n = 1$ there is nothing to prove. We first prove the statement for $n = 2$. Observe that, for any letter $a \in \mathcal{A}$,

$$\varphi_1(\varphi_2(a)) = \varphi_1([\varphi_2]_0(a)) \cdots \varphi_1([\varphi_2]_{L_2-1}(a))$$

and, for $i = 0, 1, \dots, L_2 - 1$,

$$\varphi_1([\varphi_2]_i(a)) = [\varphi_1]_0 \circ [\varphi_2]_i(a) \cdots [\varphi_1]_{L_1-1} \circ [\varphi_2]_i(a).$$

This implies that the k th column of $\varphi_1 \circ \varphi_2$ is given by

$$[\varphi_1 \circ \varphi_2]_k = [\varphi_1]_{k_0} \circ [\varphi_2]_{k_1},$$

where $0 \leq k_0 \leq L_1 - 1$ and $0 \leq k_1 \leq L_2 - 1$ are such that $k = k_1 \cdot L_1 + k_0$, with a unique choice for k_0 and k_1 . For $n > 2$, we define the substitution $\rho_{n-1} = \varphi_1 \circ \varphi_2 \circ \cdots \circ \varphi_{n-1}$, which has constant length ℓ_{n-1} , and we write $\varphi_1 \circ \varphi_2 \circ \cdots \circ \varphi_n$ as $\rho_{n-1} \circ \varphi_n$. Then, using the result for $n = 2$, we see that the k th column of $\rho_{n-1} \circ \varphi_n$ is given by

$$[\rho_{n-1} \circ \varphi_n]_k = [\rho_{n-1}]_{k_0} \circ [\varphi_n]_{k_1},$$

where $0 \leq k_0 \leq \ell_{n-1} - 1$ and $0 \leq k_1 \leq L_n - 1$ are such that $k = k_1 \cdot \ell_{n-1} + k_0$, with a unique choice for k_0 and k_1 . An iterative application of the result for $n = 2$ completes the proof. \square

Proposition 4.1.2. *Let φ be a substitution of constant length L , and let n be a positive integer. For $k = 0, 1, \dots, L^n - 1$, the k th column of the substitution φ^n is given by*

$$[\varphi^n]_k = [\varphi]_{k_0} \circ [\varphi]_{k_1} \circ \cdots \circ [\varphi]_{k_{n-1}},$$

where $[k_{n-1}, \dots, k_1, k_0]$ is the base- L representation of k (perhaps extended by non-significant 0's).

Proof. The result follows directly from Proposition 4.1.1. \square

Example 4.1.3. Let φ_1 and φ_2 be the binary substitutions

$$\varphi_1 : \begin{array}{lcl} a & \mapsto & ab, \\ b & \mapsto & aa, \end{array} \quad \text{and} \quad \varphi_2 : \begin{array}{lcl} a & \mapsto & baa, \\ b & \mapsto & aba, \end{array}$$

of constant length $L_1 = 2$ and $L_2 = 3$, respectively.

First, consider the substitution φ_1^4 , which is a substitution of constant-length 16. Given that the binary representation of 13 is $[1, 1, 0, 1]$, the 13th column of φ_1^4 is given by

$$[\varphi_1^4]_{13} = [\varphi_1]_1 \circ [\varphi_1]_0 \circ [\varphi_1]_1 \circ [\varphi_1]_1,$$

by Proposition 4.1.2. This turns out to be

$$[\varrho_1^4]_{13} : \begin{array}{lcl} a & \mapsto & b, \\ b & \mapsto & b. \end{array}$$

Now, consider the substitution ϱ_2^3 , which is a substitution of constant length 27. Given that the ternary representation of 7 is $[0, 2, 1]$ (observe the non-significant 0), the 7th column of ϱ_2^3 is given by

$$[\varrho_2^3]_7 = [\varrho_2]_1 \circ [\varrho_2]_2 \circ [\varrho_2]_0,$$

by Proposition 4.1.2. This turns out to be

$$[\varrho_2^3]_7 : \begin{array}{lcl} a & \mapsto & a, \\ b & \mapsto & a. \end{array}$$

Finally, consider the substitution $\varrho_1 \circ \varrho_2$, which is a substitution of constant length 6. We can apply Proposition 4.1.2 with $\ell_1 = L_1 = 2$ and $\ell_2 = L_1 L_2 = 6$. We obtain the unique representation of 5 in the form $k_1 \ell_1 + k_0 \ell_0$, where $0 \leq k_1 \leq 2$ and $0 \leq k_0 \leq 1$, by choosing $k_1 = 2$ and $k_0 = 1$. Then, the 5th column of the substitution $\varrho_1 \circ \varrho_2$ is given by

$$[\varrho_1 \circ \varrho_2]_5 = [\varrho_1]_1 \circ [\varrho_2]_2,$$

by Proposition 4.1.1. This turns out to be

$$[\varrho_1 \circ \varrho_2]_5 : \begin{array}{lcl} a & \mapsto & b, \\ b & \mapsto & b. \end{array}$$

❖

4.1.2 Monochromatic arithmetic progressions in substitution fixed points

We recall from Section 2.3 that an infinite word $w \in \mathcal{A}^{\mathbb{N}_0}$ contains a monochromatic arithmetic progression of difference d and length M , if there exists a starting position n such that $w_n = w_{n+kd}$, for $k = 0, 1, \dots, M-1$. The monochromatic arithmetic progression is infinite if $w_n = w_{n+kd}$, for $k = 0, 1, \dots$. The maximum length that a monochromatic arithmetic progression of difference d which appears in w can have is denoted by $A_w(d)$, or by $A(d)$ if the infinite word is clear from the context.

We find convenient to adapt Corollary 3.1.5 from Section 3.1.4 for the purposes of this chapter. This result gives sufficient condition for the finiteness of $A(d)$, for all positive integers d , for a fixed point w in terms of the columns of ϱ .

Proposition 4.1.4. *Let ϱ be an aperiodic, primitive, constant-length substitution of height 1, and let w be a fixed point of any power of ϱ . Then, $A(d) < \infty$ for all positive integers d if, and only if, ϱ does not admit a coincidence.*

This finiteness result carries over to codings of certain substitution fixed points; see Section 4.4 for the treatment of the Rudin–Shapiro substitution and its generalisations.

4.1.3 Notation

We recall from Section 2.1 the following notation concerning asymptotics of non-negative functions. Let $f, g : \mathbb{N} \rightarrow \mathbb{R}$ be non-zero functions. We write $f(n) \sim g(n)$, if $\lim_{n \rightarrow \infty} |f(n)/g(n)| = 1$. We write $f(n) \gtrsim g(n)$, if $f(n)$ grows asymptotically at least as $g(n)$ grows, or in other words, if there exists a non-zero function $h : \mathbb{N} \rightarrow \mathbb{R}$ with $f(n) \geq h(n)$ and $h(n) \sim g(n)$.

4.2 Primitive bijective substitutions

Throughout this section, we will consider constant-length substitutions which are aperiodic, primitive and bijective. We will also require that the leftmost column of the considered substitutions is equal to the identity. This is a natural constraint for a bijective substitution ϱ and can be achieved by taking a suitable power of ϱ (compare Examples 4.2.4 and 4.2.8). The primitivity condition implies that all the points in the subshift of ϱ have the same language, which in turns implies that our results apply to every point in the subshift. The aperiodicity condition is natural for a primitive substitution ϱ , otherwise every point in the subshift of ϱ contains infinitely long monochromatic arithmetic progressions, for certain differences.

The following is a version of Proposition 4.1.4 for bijective substitutions which does not need the height-1 condition. The proof is based on results from [76, 84]. Recall from Section 3.1 that, for a primitive substitution ϱ , we can equivalently consider monochromatic arithmetic progressions in one-sided or in two-sided fixed points of ϱ , and that for any such fixed point there is a corresponding tiling of the real line.

Proposition 4.2.1. *Let ϱ be an aperiodic, primitive and bijective substitution. Every monochromatic arithmetic progression in a fixed point of a power of ϱ has finite length.*

Proof. Let w be a fixed point of a power of ϱ . Since w is not periodic, the corresponding tiling of the real line is neither periodic and, by Lee–Moody–Solomyak’s overlap algorithm [76, Theorem 4.7, Lemma A.9], ϱ has not pure point dynamical spectrum. Then, by Theorem 3.1.1, w does not contain infinitely long monochromatic arithmetic progressions. \square

4.2.1 Lower bounds and polynomial growth of $A(d)$

In this section, we provide lower bounds for $A(d)$ for specific values of d . The main result is Proposition 4.2.2, which shows that, for fixed points of an aperiodic, primitive, bijective substitution, there exists a sequence of differences d for which $A(d)$ grows at least polynomially in d .

Proposition 4.2.2. *Let ϱ be an aperiodic, primitive, bijective substitution of length L with $[\varrho]_0 = \text{id}$ and column group G . Then, for any fixed point of ϱ and for every positive integer n ,*

$$L^n \leq A \left(\frac{L^{|G|} - 1}{L^n - 1} \right) < \infty.$$

Proof. To prove the lower bound for $n = 1$, we consider the substitution $\varrho^{|G|}$, which has length $L^{|G|}$. Let i_0, i_1, \dots, i_{L-1} be an arithmetic progression of difference

$$d = \frac{L^{|G|} - 1}{L - 1} = \sum_{j=0}^{|G|-1} L^j,$$

where $i_k = kd$, for $k = 0, 1, \dots, L - 1$. Then the base- L representation of i_k is $[k, k, \dots, k]$, which implies that the i_k th column of $\varrho^{|G|}$ is equal to the identity. Indeed,

$$[\varrho^{|G|}]_{i_k} = [\varrho]_k \circ \dots \circ [\varrho]_k = [\varrho]_k^{|G|} = \text{id},$$

where the first equality holds by Proposition 4.1.2, and the last equality holds because $g^{|G|} = \text{id}$, for every group element $g \in G$. Since $\varrho^{|G|}$ has L columns equal to the identity substitution distributed in arithmetic progression of difference d , any fixed point of ϱ contains a monochromatic arithmetic progression of difference d and length at least L . This completes the proof for the lower bound for $n = 1$.

The previous argument extends to every positive integer n because, since ϱ has a column which is equal to the identity substitution (the leftmost column), the column group of ϱ is equal to the column group of ϱ^n (see [28]). This implies that, for a fixed positive integer n , we can consider the substitution $\varrho^{n|G|}$ and the arithmetic progression $i_k = kd$, for $k = 0, 1, \dots, L^n - 1$, where the difference is now given by

$$d = \frac{L^{n|G|} - 1}{L^n - 1} = \sum_{j=0}^{n|G|-1} L^{nj}.$$

Finally, the finiteness of $A(d)$ follows by Proposition 4.1.4, for every positive integer n . □

The following is an immediate consequence of Proposition 4.2.2.

Corollary 4.2.3. *Let ϱ be an aperiodic, primitive, bijective substitution of length L with $[\varrho]_0 = \text{id}$ and column group G . Then, for every fixed point of ϱ , $A(d_n) \gtrsim d_n^\alpha$, where*

$$\alpha = \frac{1}{|G| - 1} \quad \text{and} \quad d_n = \frac{L^{n|G|} - 1}{L^n - 1},$$

for all positive integers n .

Theorem 4.0.1 follows directly from Corollary 4.2.3. In Section 6.1.3, we will prove a generalisation of Proposition 4.2.2 and Corollary 4.2.3 in the context of higher-dimensional words, which will be defined in that section (see Proposition 6.1.16 and Corollary 6.1.17).

Example 4.2.4. Let ρ be the three-letter substitution of length $L = 3$ given by

$$\begin{aligned} a &\mapsto a b b, \\ \rho: b &\mapsto b a c, \\ c &\mapsto c c a. \end{aligned}$$

The columns of ρ are the permutations $[\rho]_0 = \text{id}$, $[\rho]_1 = (ab)$ and $[\rho]_2 = (abc)$, written using disjoint cycle notation. The group G generated by these columns is the symmetric group S_3 , so $|G| = 6$. Since ρ satisfies the conditions in Proposition 4.2.2, we see that $A(d_n) \geq 3^n$, for all positive integers n , where

$$d_n = \frac{3^{6n} - 1}{3^n - 1} = 1 + 3^n + 3^{2n} + 3^{3n} + 3^{4n} + 3^{5n}.$$

Hence, along this sequence of differences, $A(d_n)$ grows at least like $d_n^{1/5}$. For instance, for $n = 1$ and $n = 2$, Proposition 4.2.2 says that $A(d_1) \geq 3$ and $A(d_2) \geq 9$, respectively. A computer-assisted search provided us with the exact values $A(d_1) = 8$ and $A(d_2) = 12$. Details on how to compute exact values can be found in Appendix A. \diamond

In the proof of Proposition 4.2.2, we used the fact that $g^{|G|}$ is equal to the identity, for every permutation $g \in G$. We note that replacing the group order $|G|$ with the least common multiple of the elements of the set $\{\text{ord}(g) : g \in G\}$, where $\text{ord}(g)$ is the order of g as a group element, we get the same lower bound. Thus, we have another immediate corollary of Proposition 4.2.2.

Corollary 4.2.5. *Let ρ be an aperiodic, primitive, bijective substitution of length L with $[\rho]_0 = \text{id}$. Then, for any fixed point of ρ and for every positive integer n ,*

$$L^n \leq A\left(\frac{L^{n\lambda} - 1}{L^n - 1}\right) < \infty,$$

where $\lambda = \text{lcm}\{\text{ord}(g) : g \in G\}$ with G the column group of ρ .

Example 4.2.6. Consider the four-letter substitution of length $L = 3$

$$\begin{aligned} a &\mapsto a b b, \\ \rho: b &\mapsto b c a, \\ c &\mapsto c a d, \\ d &\mapsto d d c, \end{aligned}$$

with columns given by the permutations $[\rho]_0 = \text{id}$, $[\rho]_1 = (abc)$ and $[\rho]_2 = (ab)(cd)$. The group G generated by these columns is the alternating group A_4 , which consists of $|G| = 12$ elements. Since ρ satisfies the conditions in Proposition 4.2.2, we see that $A(d_n) \geq 3^n$, for all positive integers n , where

$$d_n = \frac{3^{12n} - 1}{3^n - 1} = 1 + 3^n + 3^{2n} + \dots + 3^{11n}.$$

Hence $A(d_n) \gtrsim d_n^{1/11}$. However, by Corollary 4.2.5, instead of the group order $|G|$, we can use the least common multiple of the elements of A_4 , which is 6. Then we see that $A(d_n) \geq 3^n$, for all positive integers

n , where

$$d_n = \frac{3^{6n} - 1}{3^n - 1} = 1 + 3^n + 3^{2n} + 3^{3n} + 3^{4n} + 3^{5n}.$$

Consequently $A(d_n) \gtrsim d_n^{1/5}$. Observe that this asymptotic estimate is better, since $d_n^{1/5} > d_n^{1/11}$. \blacklozenge

Proposition 4.2.2 applies to aperiodic, primitive, bijective substitutions with the leftmost column equal to the identity. As we mentioned earlier, the later condition is not restrictive for a bijective substitution ϱ because there always exist a positive integer n for which the leftmost column of ϱ^n is equal to the identity. Consequently, Proposition 4.2.2 can be re-stated as follows.

Proposition 4.2.7. *Let ϱ be an aperiodic, primitive, bijective substitution of length L . Then, for any fixed point of ϱ and for every positive integer n ,*

$$L^n \leq A \left(\frac{L^{n|G|} - 1}{L^n - 1} \right) < \infty,$$

where G is the column group of the least power of ϱ with leftmost column equal to the identity.

Notice that Corollary 4.2.3 and Corollary 4.2.5, which follow from Proposition 4.2.2, can be converted to corollaries of Proposition 4.2.7 considering that G is the group generated by the columns of the least power of ϱ with leftmost column equal to the identity.

To illustrate Proposition 4.2.7 we consider a substitution that we found in [15, Example 3.8].

Example 4.2.8. Consider the four-letter substitution

$$\begin{aligned} \varrho: \quad a &\mapsto ad, \\ b &\mapsto bc, \\ c &\mapsto da, \\ d &\mapsto cb, \end{aligned}$$

which is aperiodic, primitive and bijective. Since $[\varrho]_0$ is not equal to the identity, we cannot apply Proposition 4.2.2. Notice that the group generated by the columns of ϱ , given by $[\varrho]_0 = (cd)$ and $[\varrho]_1 = (adbc)$, is isomorphic to the dihedral group D_4 , which has order 8 and it is not Abelian.

The first power of ϱ with leftmost column equal to the identity is ϱ^2 ,

$$\begin{aligned} \varrho^2: \quad a &\mapsto adcb, \\ b &\mapsto bcda, \\ c &\mapsto cbad, \\ d &\mapsto dab c. \end{aligned}$$

The column group G of ϱ^2 , generated by $[\varrho^2]_1 = (ad)(bc)$, $[\varrho^2]_2 = (ac)(bd)$ and $[\varrho^2]_3 = (ab)(cd)$, is isomorphic to Klein's four-group of order 4 (hence it is Abelian). Then, by Proposition 4.2.7, we see that $A(d_n) \geq 2^n$, for all positive integers n and differences of the form

$$d_n = \frac{2^{4n} - 1}{2^n - 1} = 1 + 2^n + 2^{2n} + 2^{3n}.$$

So $A(d_n) \gtrsim d_n^{1/3}$. A better asymptotic behavior can be obtained by the obvious corollary of Proposition 4.2.7 which is analogous to Corollary 4.2.5. Since all the non-identity elements of G have order 2, we have that $A(d_n) \geq 2^n$, for all positive integers n and differences

$$d_n = \frac{2^{2n} - 1}{2^n - 1} = 1 + 2^n.$$

So $A(d_n) \gtrsim d_n$, and observe that $d_n > d_n^{1/3}$. ❖

4.2.2 Lower bounds and linear growth of $A(d)$

By Proposition 4.2.2 (and directly by Corollary 4.2.3), we notice that, for $|G| = 2$, there exists a sequence of differences, namely, $(L^n + 1)$, for which $A(d)$ grows linearly in d . This is exactly the subfamily treated in Chapter 3 for Thue–Morse-like substitutions. In Proposition 4.2.11, we provide another sufficient condition for a bijective substitution (now of a possibly larger alphabet) to admit an infinite sequence of differences along which $A(d)$ grows linearly in d . We begin with the following definition.

Definition 4.2.9. Let ρ be a bijective substitution of length L with Abelian column group G . If there exists $g \in G$ such that $[\rho]_i \circ [\rho]_{L-1-i} = g$, for all $0 \leq i \leq L-1$, we say that ρ is *g-palindromic*. If $g = \text{id}$, we say that ρ is *inverse palindromic*.

Example 4.2.10. Consider the Thue–Morse substitution $\rho : 0 \mapsto 01, 1 \mapsto 10$. For $a \in \{0, 1\}$, the word $\rho^n(a)$ is symmetric or antisymmetric under reflection if n is even or odd, respectively (see Lemma 3.2.2). This implies that, for every positive integer n , ρ^n is inverse palindromic if n is even, and *g-palindromic* otherwise, where $g = (0, 1)$ is the non-identity element of C_2 , the column group of ρ .

More generally, as we will see in Section 4.2.5, one can define an L -letter Thue–Morse substitution ρ , for an integer $L > 1$ (for $L = 2$, we have the classical Thue–Morse substitution). We will see that, for every positive integer n , ρ^n is $g^{n(L-1)}$ -palindromic, or equivalently, g^{-n} -palindromic, where g is the generator of C_L that corresponds to adding 1 (mod L). In particular, ρ^L is inverse palindromic. ❖

Proposition 4.2.11. Let ρ be an aperiodic, primitive, bijective substitution of length L . Suppose that the column group G of ρ is Abelian and that ρ is *g-palindromic*, for $g \in G$. Then, for any fixed point of ρ ,

$$L^n \leq A\left(\frac{L^{n\ell} - 1}{L^n + 1}\right) < \infty,$$

for every positive integer n and even positive integer ℓ .

Proof. To prove the lower bound for $n = 1$ and ℓ an even positive integer, we consider the substitution ρ^ℓ , which has length L^ℓ . Let i_1, i_2, \dots, i_L be an arithmetic progression of difference

$$d = \frac{L^\ell - 1}{L + 1} = \sum_{j=0}^{\ell-1} (-1)^{j+1} L^j,$$

where $i_k = kd$, for $k = 1, 2, \dots, L$. Using the identity

$$k \sum_{j=0}^{\ell-1} (-1)^{j+1} L^j = (k-1) \sum_{j=0}^{\frac{\ell-2}{2}} L^{2j+1} + (L-k) \sum_{j=0}^{\frac{\ell-2}{2}} L^{2j},$$

we see that the base- L representation of i_k is $[k-1, L-k, k-1, L-k, \dots, k-1, L-k]$, with all the even digits equal to $L-k$, and all the odd digits equal to $k-1$. Then, the i_k th column of φ^ℓ is given by

$$\begin{aligned} [\varphi^\ell]_{i_k} &= [\varphi]_{L-k} \circ [\varphi]_{k-1} \circ \dots \circ [\varphi]_{L-k} \circ [\varphi]_{k-1} = \\ &= \underbrace{[\varphi]_{L-k} \circ [\varphi]_{L-1-(L-k)}}_{=g} \circ \dots \circ \underbrace{[\varphi]_{L-k} \circ [\varphi]_{L-1-(L-k)}}_{=g} = g^{\frac{\ell}{2}}, \end{aligned}$$

where the first equality holds by Proposition 4.1.2, and the last equality holds because φ is g -palindromic. So φ^ℓ has L equal columns distributed in arithmetic progression of difference d , which implies that any fixed point of φ contains a monochromatic arithmetic progression of difference d and length at least L . Hence, for $n = 1$, $A(d) \geq L$, as required.

To prove the claim for an integer $n \geq 2$, it suffices to show that φ^n is g^n -palindromic when φ is g -palindromic. Notice that φ^n has length L^n . Let $[i_{n-1}, \dots, i_1, i_0]$ be the base- L representation of an integer $i \in \{0, 1, \dots, L^n - 1\}$. It is easy to check that the base- L representation of $L^n - 1 - i$ is $[L-1-i_{n-1}, \dots, L-1-i_1, L-1-i_0]$. Then

$$\begin{aligned} [\varphi^n]_i \circ [\varphi^n]_{L^n-1-i} &= ([\varphi]_{i_0} \circ \dots \circ [\varphi]_{i_{n-1}}) \circ ([\varphi]_{L-1-i_0} \circ \dots \circ [\varphi]_{L-1-i_{n-1}}) = \\ &= \underbrace{[\varphi]_{i_0} \circ [\varphi]_{L-1-i_0}}_{=g} \circ \dots \circ \underbrace{[\varphi]_{i_{n-1}} \circ [\varphi]_{L-1-i_{n-1}}}_{=g} = g^n, \end{aligned}$$

where the first equality holds by Proposition 4.1.2, the second equality holds because G is Abelian, and the last equality holds because φ is g -palindromic. So φ^n is g^n -palindromic. Then, following the same steps as for $n = 1$, we see that, for $k = 1, 2, \dots, L^n$ and

$$d = \frac{L^{n\ell} - 1}{L^n + 1},$$

the base- L^n representation of $i_k = kd$ is $[k-1, L^n-k, \dots, k-1, L^n-k]$, which implies that $[\varphi^{n\ell}]_{i_k} = g^{\frac{n\ell}{2}}$. This implies that any fixed point of φ^n contains a monochromatic arithmetic progression of difference d and length at least L^n . Hence, for all integers $n \geq 2$, $A(d) \geq L^n$, as required.

Finally, the finiteness of $A(d)$ follows by Proposition 4.1.4, for every positive integer n . \square

Notice that if we pick $\ell = 2|G|$ in Proposition 4.2.11, we get an analogue of Proposition 4.2.2 for another family of differences.

Remark 4.2.12. We observe that there are substitutions for which the monochromatic arithmetic progression found in Proposition 4.2.11 can be extended by one or by two. From the base- L representations of $0d$ and $(L+1)d$, which are $[0, \dots, 0]$ and $[L-1, \dots, L-1]$, respectively, it is easy to see that $[\varphi^\ell]_{0d} = [\varphi]_0^\ell$

and $[\varrho^\ell]_{(L+1)d} = [\varrho]_{L-1}^\ell$. This implies that, if either $[\varrho]_0^2$ or $[\varrho]_{L-1}^2$ is equal to g , then $A(d) \geq L^n + 1$, and if furthermore $[\varrho]_0 = [\varrho]_{L-1}$, then $A(d) \geq L^n + 2$, for every positive integer n . \diamond

The following is an immediate consequence of Proposition 4.2.11.

Corollary 4.2.13. *Let ϱ be an aperiodic, primitive, bijective substitution of length L . Suppose that the column group G of ϱ is Abelian and that ϱ is g -palindromic, for $g \in G$. Then, for every fixed point of ϱ , $A(d_n) \gtrsim d_n^\alpha$, where*

$$\alpha = \frac{1}{\ell - 1} \quad \text{and} \quad d_n = \frac{L^{n\ell} - 1}{L^n + 1},$$

for all positive integers n and even positive integers ℓ . In particular, if $\ell = 2$, then $A(d_n) \gtrsim d_n$ for differences of the form $d_n = L^n - 1$.

Example 4.2.14. Consider the following aperiodic, primitive and bijective substitution,

$$\begin{aligned} \varrho: \quad a &\mapsto a c a b a, \\ b &\mapsto b a b c b, \\ c &\mapsto c b c a c. \end{aligned}$$

Observe that the columns of ϱ satisfy $[\varrho]_0 = [\varrho]_2 = [\varrho]_4 = \text{id}$ and $[\varrho]_1 = [\varrho]_3^{-1} = (acb)$. Hence, ϱ is inverse palindromic. The column group of ϱ , which is generated by $[\varrho]_1$ and $[\varrho]_1^{-1}$, is isomorphic to C_3 , which is Abelian. Then, by Proposition 4.2.11 and Remark 4.2.12 with $L = 5$, we see that $A(d_n) \geq 5^n + 2$, where

$$d_n = \frac{5^{n\ell} - 1}{5^n + 1} = 5^{(\ell-1)n} - 5^{(\ell-2)n} + \dots + 5^n - 1,$$

for every positive integer n and even positive integer ℓ . In particular, $A(d_n) \gtrsim d$ for $d_n = 5^n - 1$, by Corollary 4.2.13. \diamond

We finish this section with an example that illustrates why the Abelian assumption is necessary in Proposition 4.2.11.

Example 4.2.15. Consider the length-5 substitution ϱ given by

$$\begin{aligned} \varrho: \quad a &\mapsto a b b c a, \\ b &\mapsto b c a a b, \\ c &\mapsto c a c b c. \end{aligned}$$

Since the columns of ϱ are given by $[\varrho]_0 = [\varrho]_4 = \text{id}$, $[\varrho]_1 = [\varrho]_3^{-1} = (abc)$ and $[\varrho]_2 = (ab)$, we see that ϱ is inverse palindromic. Moreover, it can be easily verified that its column group is isomorphic to the symmetric group S_3 , which is not Abelian. Observe that the second part of the proof of Proposition 4.2.11 requires ϱ^n to be inverse palindromic, for every positive integer n . However, ϱ^2 is not inverse palindromic, as can be verified by direct inspection. In fact, ϱ^2 is not g -palindromic for any $g \in G$, where G is the column group of ϱ^2 , which is equal to the column group of ϱ . More precisely, one can check that

$[\varrho^2]_i \circ [\varrho^2]_{24-i} = \text{id}$, for all $i \in \{0, 1, \dots, 24\} \setminus \{7, 11, 13, 17\}$, whereas

$$\begin{aligned} [\varrho^2]_7 \circ [\varrho^2]_{17} &= ([\varrho^2]_{17} \circ [\varrho^2]_7)^{-1} = (abc) \quad , \\ [\varrho^2]_{11} \circ [\varrho^2]_{13} &= ([\varrho^2]_{13} \circ [\varrho^2]_{11})^{-1} = (abc)^{-1} . \end{aligned}$$

❖

4.2.3 Van der Waerden-type numbers

In Section 2.3 we stated Van der Waerden's theorem (Theorem 2.3.3), which says that, for every positive integers c and M , there exists a positive integer n such that any colouring of $\{1, 2, \dots, n\}$ with c many colours contains a monochromatic arithmetic progression of length M . The smallest threshold of n , for given values of c and M , is the van der Waerden number $W(c, M)$. In this section, we define van der Waerden-type numbers for automatic sequences arising from aperiodic primitive bijective substitutions, and provide explicit upper bounds.

We recall from Section 2.2.5 that an infinite word x is linearly recurrent if all finite subword u of x appears in x infinitely often, bounded by gaps that are linear in $|u|$, that is, there exists a positive constant R_x such that the distance between any two occurrences of u is at most $R_x|u|$. We say that R_x is a linear recurrence constant for x . Since the fixed points of a primitive substitution ϱ are linearly recurrent (Theorem 2.4.36), and moreover, one can find an R_x that is independent of x and depends only on ϱ [40, Theorem 18], we can associate a *linear recurrence constant* to ϱ , and denote it by $R = R_\varrho$, which is a linear recurrence constant for any fixed point x of ϱ . In that case, we say that ϱ is linearly recurrent for the constant R .

Let x be an infinite word and u a subword of x . We say that a word v is a *return word* to u if vu is a subword of x which has u as a prefix and contains exactly two occurrences of u . The following is a well known result on the linear recurrence constant for primitive substitutions (see [40, 42]).

Theorem 4.2.16. *An aperiodic, primitive substitution ϱ of constant length L is linearly recurrent for the constant $R = LK$, where K is the maximum length of a return word to a two-letter legal word for ϱ . Furthermore, every legal word of length n occurs in every legal word of length $(R + 1)n$. \square*

Example 4.2.17. Consider the Thue–Morse substitution $\varrho : 0 \mapsto 01, 1 \mapsto 10$. The words of length 2 in its language are 00, 01, 10 and 11. It can be checked that the longest return words to these four words have length 8. So, by Theorem 4.2.16 with $L = 2$ and $K = 8$, ϱ is linearly recurrent for the constant $R = 16$. Using Walnut software [82] it is possible to show that the optimal constant is $R = 9$ (see [43, Example 3.13]). Therefore, every word in the language of ϱ appears in every word that is 10 times longer, by Theorem 4.2.16. \diamond

Definition 4.2.18. Consider the class of aperiodic, primitive, bijective substitutions of an alphabet of size c which have length L and leftmost column equal to the identity, and denote the set of all fixed points of substitutions from this class by $\mathcal{B}(c, L)$.

Remark 4.2.19. Observe that Definition 4.2.18 implicitly assumes that $c, L \geq 2$, otherwise $\mathcal{B}(c, L)$ is not a well-defined class. Therefore, we will assume this condition whenever we refer to $\mathcal{B}(c, L)$, even if we do not state it explicitly. \blacklozenge

One can compute R in Theorem 4.2.16, which works for all infinite words in $\mathcal{B}(c, L)$, by computing an upper bound for the constant K that depends only on c and L . For this we introduce the notion of an ‘induced substitution’.

Let ϱ be an aperiodic, primitive, bijective substitution of constant length L of an alphabet \mathcal{A} , and let \mathcal{L} be the language of ϱ . For the remainder of this section (Section 4.2.3), we denote by \mathcal{A}_2 the set of *right-collared words* given by

$$\{a_b : a, b \in \mathcal{A} \text{ and } ab \in \mathcal{L}\},$$

and we denote by ϱ_2 the *level-2 induced substitution* of constant length L of the alphabet \mathcal{A}_2 that arises from ϱ and respects the collaring. For an introduction to induced substitutions we refer the reader to [17, Section 4.8.3]. We illustrate the idea with the following example.

Example 4.2.20. Consider the Thue–Morse substitution $\varrho : 0 \mapsto 01, 1 \mapsto 10$. The level-2 induced substitution arising from ϱ is the substitution ϱ_2 of the alphabet $\mathcal{A}_2 = \{0_0, 0_1, 1_0, 1_1\}$ given by

$$\varrho_2 : \begin{array}{ll} 0_0 & \mapsto 0_1 1_0, \\ 0_1 & \mapsto 0_1 1_1, \\ 1_0 & \mapsto 1_0 0_0, \\ 1_1 & \mapsto 1_0 0_1. \end{array}$$

Since ϱ is primitive, ϱ_2 is also primitive (see [17, Proposition 4.14]). The fixed points of ϱ_2 are

$$0_1 1_1 1_0 0_1 1_0 0_0 0_1 1_1 \cdots \quad \text{and} \quad 1_0 0_0 0_1 1_0 0_1 1_1 1_0 0_0 \cdots,$$

which can be obtained from the fixed points of ϱ by considering consecutive (overlapping) two-letter subwords. \blacklozenge

Now, we recall Wielandt’s theorem on the upper bound for the index of primitivity of a primitive substitution (Theorem 2.4.2). Let ϱ be a primitive substitution of an alphabet \mathcal{A} of size c . Wielandt’s theorem implies that, for every letter $a \in \mathcal{A}$, all the letters in \mathcal{A} are subwords of the word $\varrho^n(a)$, where $n = c^2 - 2c + 2$.

Combining Theorem 4.2.16 with Theorem 2.4.2, we obtain a linear recurrence constant for the infinite words in the class $\mathcal{B}(c, L)$.

Proposition 4.2.21. *Let c and L be two integers with $c, L \geq 2$. A linear recurrence constant for every word in $\mathcal{B}(c, L)$ is*

$$R = 2L^n - L,$$

where $n = c^4 - 2c^2 + 3$.

Proof. Let $x \in \mathcal{B}(c, L)$ and let ρ be the corresponding substitution of which x is a fixed point. So ρ is aperiodic, primitive and bijective with $[\rho]_0 = \text{id}$, it has length L , and it is defined on an alphabet \mathcal{A} of size c . Let ρ_2 be the level-2 induced substitution arising from ρ . Notice that \mathcal{A}_2 , the alphabet on which ρ_2 is defined, has size at most c^2 . So, by Wielandt's bound, for every $a_b \in \mathcal{A}_2$, the word $\rho_2^m(a_b)$ contains all the collared words in \mathcal{A}_2 , where $m = c^4 - 2c^2 + 2$. Then any two consecutive level- m superwords of ρ_2 contain two occurrences of each $a_b \in \mathcal{A}_2$ (possibly at the borders), so the longest return word to a_b has length at most $2L^m - 1$. Consequently, all level- m superwords of ρ admit at least one occurrence of each two-letter word ab that is legal for ρ , and the longest return word to ab has length at most $2L^m - 1$. Notice that we can write x as a concatenation of level- m superwords of ρ . The claim then follows by applying the formula in Theorem 4.2.16 with $k = 2L^m - 1$. \square

Remark 4.2.22. We comment on the generality of the proof of Proposition 4.2.21. First, notice that it only depends on the size c of the alphabet and the length L of the substitution, and hence it gives a linear recurrence constant for all substitutions in the class considered in this section, parametrised by c and L . Second, since bijectivity is invoked nowhere in the proof, the bound found can be used for more general classes of substitutions. \blacklozenge

Notice that, for any c and L (both ≥ 2), the set $\mathcal{B}(c, L)$ is a non-empty proper subset of $\mathcal{A}^{\mathbb{N}_0}$. The following result follows from van der Waerden's theorem.

Proposition 4.2.23. *For every positive integers c, L and M , where $c, L \geq 2$, there exists a positive integer n such that every length- n subword of every element of $\mathcal{B}(c, L)$ contains a length- M monochromatic arithmetic progression.*

Proof. For every infinite word $w_0w_1w_2 \dots$ in $\mathcal{B}(c, L)$ and every non-negative integer k , the infinite word $w_kw_{k+1}w_{k+2} \dots$ has a prefix of length $W(c, M)$ containing a monochromatic arithmetic progression of length M , where $W(c, M)$ is the classical van der Waerden number. Hence, choosing $n = W(c, M)$ we fulfil the requirements of the proposition. \square

Definition 4.2.24. Let c, L and M be positive integers with $c, L \geq 2$. We call the smallest threshold for the number n predicted by Proposition 4.2.23 a *van der Waerden-type number* for $\mathcal{B}(c, L)$. We denote it by $W(\mathcal{B}(c, L), M)$.

It is clear that an upper bound for $W(\mathcal{B}(c, L), M)$ is the classical van der Waerden number $W(c, M)$. As mentioned in Section 2.3, very few van der Waerden numbers are known, and furthermore, the best known upper bound for $W(c, M)$, which is due to Gowers, is superexponential [61]. Here we find better upper bounds for $W(\mathcal{B}(c, L), M)$, which depend on c, L and M .

Proposition 4.2.25. *Let c, L and M be positive integers with $c, L \geq 2$. Then*

$$W(\mathcal{B}(c, L), M) \leq (R + 1)L^{kc!},$$

where $k = \lceil \log_L M \rceil$ and $R = 2L^n - L$ with $n = c^4 - 2c^2 + 3$.

Proof. By Proposition 4.2.2, any $x \in \mathcal{B}(c, L)$ satisfies, for every positive integer n , $A(d_n) \geq L^n$, where

$$d_n = \frac{L^{n|G|} - 1}{L^n - 1},$$

with G the column group of the corresponding substitution of which x is a fixed point. Let k be the least non-negative integer n such that $L^n \geq M$; observe that we can write k as $\lceil \log_L M \rceil$. Then

$$A(d_k) \geq L^k \geq M.$$

Since the monochromatic arithmetic progression from the proof of Proposition 4.2.2 starts at position 0, the infinite word x has a prefix of length $1 + (L^k - 1) \cdot d_k = L^{k|G|}$ containing a monochromatic arithmetic progression of difference d_k and length M .

From the discussion above, we know that x is linearly recurrent for some positive constant R_x . By Theorem 4.2.16, all subwords of x of length $L^{k|G|}$ (in particular the aforementioned prefix containing the monochromatic arithmetic progression) appear in every subword of length $(R_x + 1)L^{k|G|}$. So every subword of x of length $(R_x + 1)L^{k|G|}$ contains a monochromatic arithmetic progression of difference d_k and length M . By Proposition 4.2.21, one can choose R_x to be $2L^n - L$, where $n = c^4 - 2c^2 + 3$; notice that this linear recurrence constant is valid for all elements of $\mathcal{B}(c, L)$. Finally, since G is a subgroup of the symmetric group S_c and $|S_c| = c!$, we have that $L^{k|G|} \leq L^{kc!}$. Therefore $W(\mathcal{B}(c, L), M) \leq (R + 1)L^{kc!}$, as required. \square

Proposition 4.2.25 can be reformulated as follows: if ρ is an aperiodic, primitive, bijective substitution of an alphabet of size c which has length L and $[\rho]_0 = \text{id}$, and M is a positive integer, then every legal word for ρ of length at least $(R + 1)L^{kc!}$ contains a monochromatic arithmetic progression of length M .

Example 4.2.26. Consider the case $c = L = 2$, generated by the Thue–Morse substitution, which has two fixed points. In Example 4.2.17 we saw that 16 is a linear recurrence constant for this substitution, and that the optimal linear recurrence constant is $R = 9$. Combining this result with Proposition 4.2.25 we obtain $W(\mathcal{B}(2, 2), M) \leq 10 \cdot 4^k$, where $k = \lceil \log_2 M \rceil$. Thus, the upper bounds for the first few van der Waerden-type numbers are

$$\begin{array}{ll} W(\mathcal{B}(2, 2), M) \leq 640, & \text{for } M = 6, 7, 8, \\ W(\mathcal{B}(2, 2), M) \leq 2560, & \text{for } 8 < M \leq 16, \\ W(\mathcal{B}(2, 2), M) \leq 10240, & \text{for } 16 < M \leq 32, \\ W(\mathcal{B}(2, 2), M) \leq 40960, & \text{for } 32 < M \leq 64, \\ W(\mathcal{B}(2, 2), M) \leq 163840, & \text{for } 64 < M \leq 128, \end{array}$$

which are significantly lower than the respective known upper bounds for the general van der Waerden numbers $W(2, M)$. \blacklozenge

The bound for R established in Proposition 4.2.21 is far from optimal and hence, so is the bound for $\mathcal{B}(2, 2)$ given in Proposition 4.2.25. For example, for the family $\mathcal{B}(2, 2)$ studied in Example 4.2.26, we

obtain $R \leq 2^{12} - 2 = 4094$ and consequently,

$$W(\mathcal{B}(2, 2), M) \leq 4095 \cdot 4^k, \quad \text{where} \quad k = \lceil \log_2 M \rceil,$$

which is a weaker bound than the bound obtained in Example 4.2.26 using the optimal value of the linear recurrence constant ($R = 9$). It would be interesting to obtain a better method to compute the constant R in Proposition 4.2.25 and hence, the upper bound for $W(\mathcal{B}(c, L), M)$.

4.2.4 Upper bounds for $A(d)$ for abelian bijective substitutions

The main result of this section is Proposition 4.2.30, where we establish an upper bound for $A(d)$, for aperiodic, primitive and bijective substitutions ρ with $[\rho]_0 = \text{id}$. This upper bound holds for all substitution lengths L and for all differences d not larger than some value that depends on ρ . We overcome the restriction on d by restricting L to a subclass for which we provide an upper bound for $A(d)$, for all d (Proposition 4.2.34). We use this result to give lower bounds for van der Waerden-type numbers $W(\mathcal{B}(c, L), M)$, for certain values of L and M .

We start with the following lemma on transitive Abelian groups. The result follows easily from well-known results on permutation groups, but we include a proof of the lemma as we did not find a reference with the statement in the form given here. A group G of permutations of an alphabet \mathcal{A} is *transitive* on \mathcal{A} if, for each $a, b \in \mathcal{A}$, there exists $g \in G$ such that $g(a) = b$.

Lemma 4.2.27. *Let G be a group of permutations of \mathcal{A} that is transitive and Abelian, and let $g_1, g_2 \in G$. If $g_1(a) = g_2(a)$ for some $a \in \mathcal{A}$, then $g_1 = g_2$.*

Proof. We first show that the stabiliser in G of each letter $a \in \mathcal{A}$, which is the subset of G given by $\{f \in G : f(a) = a\}$, is trivial. On the contrary, assume that, for each $a \in \mathcal{A}$, there exists a permutation $f \in G$ different to the identity for which $f(a) = a$. By transitivity, for each $b \in \mathcal{A}$, there is an element $h \in G$ such that $h(a) = b$ and then, since G is Abelian,

$$f(b) = f(h(a)) = h(f(a)) = h(a) = b.$$

This implies that f fixes every letter of \mathcal{A} , which contradicts the fact f is not the identity.

Suppose now that, for some $a \in \mathcal{A}$, there are $g_1, g_2 \in G$ such that $g_1(a) = g_2(a)$. Then $g_2^{-1}g_1(a) = a$, where g_2^{-1} is the inverse of g_2 , so $g_2^{-1}g_1$ is an element of the stabiliser of a . Since the stabiliser contains only the identity, we see that $g_1 = g_2$. \square

Next, we prove results regarding certain columns of a power of ρ under the existence of a monochromatic arithmetic progression of certain length in a fixed point of ρ .

Lemma 4.2.28. *Let ρ be a primitive, bijective substitution of length L with $[\rho]_0 = \text{id}$ and Abelian column group. Let d and k be positive integers with $d \leq L^k - 1$ and let $\ell = \gcd(d, L^k)$. Suppose that a fixed point of ρ contains a monochromatic arithmetic progression of difference d and length $\frac{L^k}{\ell} + 1$ starting at position n . Then $[\rho^k]_{n+m\ell} = [\rho^k]_{n+m\ell+d}$, for all integers m for which $0 \leq n+m\ell < n+m\ell+d \leq L^k - 1$.*

Proof. Let w be a fixed point of φ that contains a monochromatic arithmetic progression of difference d and length $\frac{L^k}{\ell} + 1$ starting at position n . In other words, $w_n = w_{n+jd}$, for $j = 0, 1, \dots, \frac{L^k}{\ell}$. Let S_1 be the set of equivalence classes mod L^k of integers that are congruent to $n \bmod \ell$. In other words,

$$S_1 = \{\langle m \rangle_{L^k} : m \in \mathbb{Z}, m \equiv n \bmod \ell\},$$

where $\langle \rangle_{L^k}$ denotes an equivalence class mod L^k . The fact that L^k is a positive multiple of ℓ implies that $|S_1| = \frac{L^k}{\ell}$. Consider also the set S_2 of equivalence classes mod L^k of integers of the form $n + jd$, for all integers $j \in X$, where $X = \{0, 1, \dots, \frac{L^k}{\ell} - 1\}$. In other words,

$$S_2 = \{\langle n + jd \rangle_{L^k} : j \in X\}.$$

Since d is a multiple of ℓ , $S_2 \subseteq S_1$. In fact, $S_2 = S_1$. To prove this it suffices to show that $|S_2| = \frac{L^k}{\ell}$, or equivalently, that $n + id \not\equiv n + jd \bmod L^k$, for all distinct $i, j \in X$. On the contrary, assume that there exists an integer t such that $(j - i)d = tL^k$, or equivalently, $(j - i)\frac{d}{\ell} = t\frac{L^k}{\ell}$. Since $\ell = \gcd(d, L^k)$, this implies that $j - i$ is a multiple of $\frac{L^k}{\ell}$, which is not possible because $|j - i| \in X$. Therefore, $S_2 = S_1$.

Now, consider the set S_3 of equivalence classes mod L^k of integers of the form $n + m\ell$, where m is an integer. In other words,

$$S_3 = \{\langle n + m\ell \rangle_{L^k} : m \in \mathbb{Z}\}.$$

Since $S_3 \subseteq S_1$ and $S_1 = S_2$, we see that for each integer m , there exists an integer $j \in X$ such that

$$n + m\ell \equiv n + jd \bmod L^k.$$

Let m be any integer for which $0 \leq n + m\ell < n + m\ell + d \leq L^k - 1$. Then, there exist a non-negative integer s and an integer $j \in X$ such that

$$sL^k + n + m\ell = n + jd \quad \text{and} \quad sL^k + n + m\ell + d = n + (j + 1)d.$$

Observe that $\varphi^k(w_s)$ is the subword of w starting at position sL^k and ending at position $sL^k + L^k - 1$. So the $(n + m\ell)$ th and $(n + m\ell + d)$ th letters of $\varphi^k(w_s)$ are w_{n+jd} and $w_{n+(j+1)d}$, respectively. By assumption, $w_{n+jd} = w_{n+(j+1)d}$ because $j \in X$, so $w_{sL^k+n+m\ell} = w_{sL^k+n+m\ell+d}$. In other words,

$$[\varphi^k]_{n+m\ell}(w_s) = [\varphi^k]_{n+m\ell+d}(w_s).$$

It is known that a bijective substitution φ is primitive if, and only if, the column group of the least power of φ with a column equal to the identity is transitive [28, 96]. So the column group of φ is transitive on \mathcal{A} . Since it is also Abelian, using Lemma 4.2.27, we see that the columns $[\varphi^k]_{n+m\ell}$ and $[\varphi^k]_{n+m\ell+d}$ (seen as permutations of \mathcal{A}) must coincide, as required. \square

We can relate the column equality result in the previous lemma with the existence of infinitely long monochromatic arithmetic progressions in w .

Lemma 4.2.29. *Let ϱ be a constant-length substitution of length L and let N be the least positive integer such that, for every letter a , all the two-letter legal words for ϱ occur in $\varrho^N(a)$. Let d , M and ℓ be positive integers such that $d \leq L^M$ and ℓ divides L^M . Suppose that there exists a non-negative integer n such that $[\varrho^{N+M}]_{n+m\ell} = [\varrho^{N+M}]_{n+m\ell+d}$, for all integers m for which $0 \leq n+m\ell < n+m\ell+d \leq L^{N+M}-1$. Then every fixed point of ϱ is periodic.*

Proof. Let s and j be non-negative integers, let w be a fixed point of ϱ , and let x be the subword of w starting at position $s+jd$ and ending at position $s+(j+1)d$, that is, $x = w_{s+jd}w_{s+jd+1} \cdots w_{s+(j+1)d}$. Since $|x| = d+1 \leq L^M+1$, there are two consecutive superwords of length L^M containing w . In other words, there exist letters $a_1, a_2 \in \mathcal{A}$ and words $y, z \in \mathcal{A}^*$ such that $\varrho^M(a_1a_2) = yxz$.

On the other hand, for every letter $b \in \mathcal{A}$, the word $\varrho^N(b)$ has all the two-letter legal words as subwords. In particular, a_1a_2 is a subword of $\varrho^N(b)$. So there exist words $u, v \in \mathcal{A}^*$ such that $\varrho^N(b) = ua_1a_2v$. Then, x is a subword of $\varrho^{N+M}(b)$. More precisely,

$$\varrho^{N+M}(b) = \varrho^M(\varrho^N(b)) = \varrho^M(ua_1a_2v) = \varrho^M(u)yx_0x_1 \cdots x_dz\varrho^M(v),$$

where we have written x as $x_0x_1 \cdots x_d$ with $x_i = w_{i+s+jd}$, for $i = 0, 1, \dots, d$.

Let r be the position of x_0 as a subword of $\varrho^{N+M}(b)$. Then $r = |\varrho^M(u)| + |y| = |u|L^M + |y|$. Since $|y| \leq 2L^M - d - 1$ and $|u| \leq L^N - 2$, we have that $r \leq L^{N+M} - 1 - d$. Furthermore, since L^M is a multiple of ℓ , there exists a non-negative integer m such that $r = n + m\ell$, where $n = |y|$. This implies that

$$0 \leq n + m\ell < n + m\ell + d \leq L^{N+M} - 1.$$

Since n and m satisfy the condition in the statement, we have that $[\varrho^{N+M}]_{n+m\ell} = [\varrho^{N+M}]_{n+m\ell+d}$, so $x_0 = x_d$, or in other words, $w_{s+jd} = w_{s+(j+1)d}$. Since this is true for all non-negative integers s and j , we see that w can be written as $w = ppp \cdots$, where $p = w_0w_1 \cdots w_{d-1}$. Therefore, w is a periodic infinite word, as required. \square

Using the previous two lemmas we establish an upper bound for $A(d)$, for differences d satisfying $d \leq L^M$ and $\gcd(d, L^M) = \gcd(d, L^{N+M})$, where N and M are defined as in Lemma 4.2.29.

Proposition 4.2.30. *Let ϱ be an aperiodic, primitive, bijective substitution of length L with $[\varrho]_0 = \text{id}$ and Abelian column group. Let N be the least positive integer such that, for every letter a , all the two-letter legal words for ϱ occur in $\varrho^N(a)$. Let d , M and ℓ be positive integers such that $d \leq L^M$ and $\ell = \gcd(d, L^M) = \gcd(d, L^{N+M})$. Then $A(d) \leq \frac{L^{N+M}}{\ell}$, for every fixed point of ϱ .*

Proof. Let w be any fixed point of ϱ . Assume that there exists a non-negative integer n such that $w_n = w_{n+jd}$, for $j = 0, 1, \dots, \frac{L^{N+M}}{\ell}$. It follows from Lemmas 4.2.28 and 4.2.29 that w must be periodic, which is impossible because ϱ is an aperiodic substitution. So our initial assumption is false, which implies the claim on $A(d)$. \square

Corollary 4.2.31. *Let ϱ be an aperiodic, primitive, bijective substitution of length L with $[\varrho]_0 = \text{id}$ and Abelian column group. Then, for every fixed point of ϱ and for all positive integers n ,*

$$L^n \leq A \left(\frac{L^{n|G|} - 1}{L^n - 1} \right) \leq L^{n|G|+N},$$

where N is the least positive integer such that, for every letter a , all the two-letter legal words for ϱ occur in $\varrho^N(a)$.

Proof. We proved the lower bound in Proposition 4.2.2. To prove the upper bound it suffices to apply Proposition 4.2.30 with $M = n|G|$ and

$$d = \frac{L^{n|G|} - 1}{L^n - 1} = 1 + L^n + \dots + L^{n(|G|-1)},$$

since this implies that $d < L^M$ and $\gcd(d, L^M) = \gcd(d, L^{M+N}) = 1$. □

Remark 4.2.32. Observe that, from Lemma 4.2.21, N is bounded above by $c^4 - 2c^2 + 3$, where c is the size of the alphabet (this is one more than Wielandt's bound for the level-2 induced substitution, to include the case when a collared word a_b appears at the boundary).

Also, it is easy to see that $|G| = c$. Since ϱ is primitive, there exists a power ϱ^m of ϱ such that, for any letter $a \in \mathcal{A}$, the word $\varrho^m(a)$ contains all the letters from \mathcal{A} . Consequently, G has at least c different elements g_1, g_2, \dots, g_c . Since \mathcal{A} has size c , for any $g \in G$ and $a \in \mathcal{A}$, there exists $1 \leq i \leq c$ such that $g(a) = g_i(a)$ and, since G is Abelian, $g = g_i$, by Lemma 4.2.27. Therefore, $|G| = c$, as required. ❖

Example 4.2.33. Consider the aperiodic, primitive, bijective substitution ϱ of Example 4.2.14, whose column group G is isomorphic to the cyclic group C_3 , which is Abelian. The set of two-letter legal words is $\{ab, ac, ba, bc, ca, cb\}$ and by direct inspection, we see that all of them appear in $\varrho^2(x)$, for $x = a, b, c$,

$$\begin{aligned} a &\mapsto acabacbcacacabababcbacaba, \\ \varrho^2: b &\mapsto babcbacabababcbcbcbcbabcb, \\ c &\mapsto cbcacbabcbcbcbcbcbcbcbcbcb. \end{aligned}$$

By Corollary 4.2.31 with $L = 5$, $|G| = 3$ and $N = 2$, we have

$$5^n \leq A(25^n + 5^n + 1) \leq 25 \cdot 5^{3n},$$

for every positive integer n . ❖

The result given in Proposition 4.2.30 holds, for an arbitrary substitution length L , only for certain differences d . Next, we give a subclass of lengths for which it is possible to establish an upper bound for $A(d)$, for all d .

Proposition 4.2.34. *Let ϱ be an aperiodic, primitive, bijective substitution with $[\varrho]_0 = \text{id}$ and Abelian column group, and let N be the least positive integer such that, for every letter a , all the two-letter legal*

words for ϱ occur in $\varrho^N(a)$. Suppose that the length L of ϱ can be factorised as $p_1^{n_1} p_2^{n_2} \cdots p_t^{n_t}$ with primes $p_1 < p_2 < \cdots < p_t$ and positive integers $n_1 \leq n_2 \leq \cdots \leq n_t$.

Then, for each positive integer d , there exists a positive integer M such that $d \leq L^M$ and $\gcd(d, L^M) = \gcd(d, L^{N+M})$. Furthermore, for every fixed point of ϱ , $A(d) \leq L^{N+1} d^B$, where $B = \frac{\log L}{n_1 \log p_1}$.

Proof. We can choose M such that $p_1^{n_1(M-1)} \leq d < p_1^{n_1 M}$. Then $d < p_1^{n_1 M} < p_2^{n_2 M} < \cdots < p_t^{n_t M} < L^M$, so $d \leq L^M$ holds. Since $p_i^{n_i M}$ does not divide d , for $i = 1, 2, \dots, t$, we see that

$$\gcd(d, p_i^{n_i M}) = \gcd(d, p_i^{n_i(N+M)}),$$

which implies that $\gcd(d, L^M) = \gcd(d, L^{N+M})$. Furthermore, $A(d) \leq L^{N+M} = L^{N+1} L^{M-1}$, by Proposition 4.2.30. Since $L = (p_1^{n_1})^B$, where

$$B = \frac{\log L}{n_1 \log p_1},$$

then $L^{M-1} = (p_1^{n_1})^{(M-1)B} \leq d^B$, and so $A(d) \leq L^{N+1} d^B$, as required. \square

In particular, if L is a power of a prime, then $t = 1$, so $B = 1$ and $A(d) \leq L^{N+1} d$. We can leverage the previous proposition to obtain lower bounds for van der Waerden-type numbers $W(\mathcal{B}(c, L), M)$, for certain values of L and M .

Corollary 4.2.35. *Let c and k be positive integers and let $L = p_1^{n_1} p_2^{n_2} \cdots p_t^{n_t}$, for primes $p_1 < p_2 < \cdots < p_t$ and positive integers $n_1 \leq n_2 \leq \cdots \leq n_t$. Then*

$$W(\mathcal{B}(c, L), M) > (M - 1)k + 1,$$

where $M = L^{N_0+1} k^{\lceil B \rceil} + 1$ with $N_0 = c^4 - 2c^2 + 3$ and $B = \frac{\log L}{n_1 \log p_1}$.

Proof. We will prove the stronger statement that there exists an $x \in \mathcal{B}(c, L)$ such that none of the subwords of x of length $(M - 1)k + 1$ contains a monochromatic arithmetic progression of length M .

Consider a substitution ϱ , which is aperiodic, primitive and bijective of length L with $[\varrho]_0 = \text{id}$ and Abelian column group G . First, we prove that such a substitution always exists. Without loss of generality, we can force G to be the cyclic group C_c of order c , which is Abelian and transitive on $\mathcal{A} = \{0, 1, \dots, c - 1\}$. Transitivity is already sufficient to ensure primitivity [28, Proposition 2.3].

It remains to construct an aperiodic bijective substitution with that group profile, for any given length. By Theorem 2.4.28, a sufficient condition for the aperiodicity of a primitive and bijective substitution is the existence of two length-two legal words which share the same starting letter or the same ending letter.

If $L = 2$, we choose $[\varrho]_0 = \text{id}$ and $[\varrho]_1 = (1, 2, \dots, 0)$, which generates G . This implies that $\varrho^2(c - 1) = (c - 1)001$, so 00 and 01 are both legal words for ϱ , hence ϱ is aperiodic. If $L \geq 3$, we choose $[\varrho]_0 = [\varrho]_1 = \text{id}$ and $[\varrho]_2 = (1, 2, \dots, 0)$, and we fill the other columns with any permutations from C_c . By construction, we immediately see that 00 and 01 are both legal words for ϱ , hence ϱ is aperiodic.

Let x be a fixed point of ρ and let N be the least positive integer such that, for every $a \in \mathcal{A}$, all the two-letter legal words for ρ occur in $\rho^N(a)$. By the argument of Proposition 4.2.21, we see that $N \leq N_0$. By Proposition 4.2.34, $A_x(d) \leq L^{N_0+1}d^{\lceil B \rceil}$, for every positive integer d , so $A_x(d) \leq L^{N_0+1}d^{\lceil B \rceil}$.

If $d \leq k$, we have that $A_x(d) \leq L^{N_0+1}k^{\lceil B \rceil}$ and consequently, x does not contain monochromatic arithmetic progressions of difference d and length $L^{N_0+1}k^{\lceil B \rceil} + 1 = M$. If $d > k$, the monochromatic arithmetic progressions of difference d and length M span as long as $L^{N_0+1}d^{\lceil B \rceil}d + 1$ and cannot be contained in a subword of length $L^{N_0+1}k^{\lceil B \rceil+1} + 1 = (M-1)k + 1$. In either case, the subwords of x of length $(M-1)k + 1$ do not contain monochromatic arithmetic progressions of length M , which implies the claim on the van der Waerden-type numbers. \square

4.2.5 Thue–Morse sequence over L letters

The *Thue–Morse sequence* over the alphabet $\mathcal{A}_L = \{0, 1, \dots, L-1\}$ is the infinite word $w = w_0w_1w_2 \dots$ with w_i given by the sum (mod L) of the digits in the base- L representation of i (see [35]). This sequence can also be defined as the fixed point, with first letter 0, of the so-called *L -letter Thue–Morse substitution* [19]. This is the substitution φ defined, for each letter a of \mathcal{A}_L , as

$$\varphi(a) = [\varphi]_0(a) [\varphi]_1(a) \dots [\varphi]_{L-1}(a), \quad \text{where} \quad [\varphi]_i(a) \equiv a + i \pmod{L}.$$

The exact values of $A(L^n - 1)$ for $L = 2$ and $L = 3$ were obtained in [89] and [90], respectively, and it was shown that the same arguments can be used for any prime number L (see [91]). In Chapter 3 we have reestablished the result for $L = 2$ using a different approach (see also [2]). The key argument of our approach can be easily generalised for all L , giving Proposition 4.2.38 below as a result.

The group G generated by the columns of φ is the cyclic group C_L of order L , which is Abelian. We write $C_L = \langle g \rangle$ multiplicatively, where $g = [\varphi]_1$ corresponds to adding 1 (mod L). It is easy to see that $[\varphi]_\ell$, the ℓ -th column of φ , is given by g^ℓ . Indeed, for $0 \leq a, \ell \leq L-1$,

$$[\varphi]_\ell(a) = \overbrace{1 + \dots + 1}^\ell + a = \overbrace{1 + \dots + 1}^{\ell-1} + [\varphi]_1(a) = \overbrace{1 + \dots + 1}^{\ell-2} + [\varphi]_1^2(a) = \dots = [\varphi]_1^\ell(a) = g^\ell(a).$$

Using this fact, we next show that φ^n is actually $g^{n(L-1)}$ -palindromic, for every positive integer n , or equivalently, g^{-n} -palindromic. In particular, φ^L is inverse palindromic.

Lemma 4.2.36. *Let φ be the L -letter Thue–Morse substitution. The substitution φ^n is $g^{n(L-1)}$ -palindromic, for every positive integer n .*

Proof. Applying Proposition 4.1.2 we see that, for each $0 \leq i, j \leq L^n - 1$ with $j = (L-1) - i$,

$$[\varphi^n]_i \circ [\varphi^n]_j = [\varphi]_{i_0} \circ \dots \circ [\varphi]_{i_{n-1}} \circ [\varphi]_{j_0} \circ \dots \circ [\varphi]_{j_{n-1}},$$

where $[i_{n-1}, \dots, i_1, i_0]$ and $[j_{n-1}, \dots, j_1, j_0]$ are the base- L representations of i and j , respectively. Then,

since the column group is Abelian,

$$[\varphi^n]_i \circ [\varphi^n]_j = g^{i_0+j_0} \circ \dots \circ g^{i_{n-1}+j_{n-1}}.$$

But $i_\ell + j_\ell = L - 1$, for every $0 \leq \ell \leq L - 1$, so $[\varphi^n]_i \circ [\varphi^n]_j = g^{n(L-1)}$, as required. \square

Proposition 4.2.37. *Let φ be the L -letter Thue–Morse substitution. For every fixed point of φ and for all positive integers n ,*

$$A(L^n - 1) \geq L^n.$$

Proof. Since φ is g^{L-1} -palindromic, where $g = [\varphi]_1$, we can apply Proposition 4.2.11. Choosing $\ell = 2$ in that proposition we get the desired result. \square

We can improve the lower bounds given in Proposition 4.2.37 when $n \equiv 0 \pmod L$ by looking at the concatenation of three level- n superwords, which we carry out below. This result extends the result in Proposition 3.2.13 in Chapter 3 for $L = 2$ to any arbitrary L .

Proposition 4.2.38. *Let φ be the L -letter Thue–Morse substitution. For every fixed point of φ and for all positive integers n ,*

$$A(L^n - 1) \geq \begin{cases} L^n + 2L, & \text{if } n \equiv 0 \pmod L, \\ L^n, & \text{otherwise.} \end{cases}$$

Proof. The case when $n \not\equiv 0 \pmod L$ is already covered by Proposition 4.2.37, so we assume from hereon that $n \equiv 0 \pmod L$. Notice that the substitution φ^n , which by Lemma 4.2.36 is $g^{n(L-1)}$ -palindromic, is inverse palindromic for $n \equiv 0 \pmod L$, since $g^{n(L-1)} = \text{id}$. This implies, in particular, that $[\varphi]_0 = [\varphi]_{L^n-1} = \text{id}$.

We start by looking at the superword $\varphi^{2n}(a)$ and prove that, starting from its first letter, it contains a monochromatic arithmetic progression of letter a of difference $L^n - 1$ and length $L^n + 2$. We first show that $[\varphi^{2n}]_{i_k} = \text{id}$, for $1 \leq k \leq L^n$, where $i_k = k(L^n - 1)$. Indeed, for $1 \leq k \leq L^n$, the base- L^n representation of i_k is $[k - 1, L^n - k]$, so, using Proposition 4.1.2,

$$[\varphi^{2n}]_{i_k} = [\varphi^n]_{L^n-k} \circ [\varphi^n]_{k-1} = [\varphi^n]_{L^n-1-(k-1)} \circ [\varphi^n]_{k-1} = \text{id},$$

where the latter equality holds because φ^n is inverse palindromic. We also notice that

$$\begin{aligned} [\varphi^{2n}]_0 &= [\varphi^n]_0^2 = \text{id}, \\ [\varphi^{2n}]_{(L^n+1)(L^n-1)} &= [\varphi^{2n}]_{L^{2n}-1} = [\varphi^n]_{L^n-1}^2 = \text{id}. \end{aligned}$$

where the latter equalities hold because $[\varphi]_0 = [\varphi]_{L^n-1} = \text{id}$. Altogether, this yields a monochromatic arithmetic progression of letter a letters of length $L^n + 2$ within the superword $\varphi^{2n}(a)$.

The goal is now to look at progressions of letter a in $\varphi^{2n}(a-1)$ and $\varphi^{2n}(a+1)$ of the same difference. We then extend the progression from $\varphi^{2n}(a)$ to a longer progression in $\varphi^{2n}(w)$, where w is the three-letter word $(a-1)a(a+1)$, which is legal for every $a \in \mathcal{A}_L$.

First, we look at the superword $\varphi^{2n}(a-1)$. We show that, for $0 \leq k \leq L-2$, one has $[\varphi^{2n}]_{i_k} = \text{id}$ at positions $i_k = L^{2n} - (k+1)(L^n - 1)$. These are the positions which correspond to the continuation of the progression from $\varphi^{2n}(a)$ with difference $d = L^n - 1$ (see Figure 4.2.1). Indeed, since the base- L^n representation of i_k is $[L^n - (k+1), k+1]$ and since φ^n is inverse palindromic,

$$[\varphi^{2n}]_{i_k} = [\varphi^n]_{k+1} \circ [\varphi^n]_{L^n - (k+1)} = \text{id}.$$

We also check that this is not true for $k = L-1$. In that case, the base- L^n representation of i_k is $[L^n - L, L]$, so $[\varphi^{2n}]_{i_k} = [\varphi^n]_L \circ [\varphi^n]_{L^n - L}$. Since the base- L representations of L and $L^n - L$ are $[0, \dots, 0, 1, 0]$ and $[L-1, \dots, L-1, 0]$, respectively,

$$[\varphi^n]_L = [\varphi]_0 \circ [\varphi]_1 \circ [\varphi]_0^{n-2} = [\varphi]_1 = g,$$

$$[\varphi^n]_{L^n - L} = [\varphi]_0 \circ [\varphi]_{L-1}^{n-1} = [\varphi]_{L-1}^{n-1} = g^{(n-1)(L-1)} = g,$$

where we noted that $[\varphi]_\ell = g^\ell$, for each $\ell \in \mathcal{A}_L$, and also that $g^{-(L-1)} = g$, since g corresponds to adding 1 (mod L). Consequently, $[\varphi^{2n}]_{i_k} = g^2$, so $[\varphi^{2n}]_{i_k}(a-1) \equiv (a-1) + 2 = a+1 \pmod{L}$. Since a and $a+1$ are coprime, for every $0 \leq a \leq L-1$, we see that the extension of the arithmetic progression of a letters in $\varphi^{2n}(a-1)$ has length at most $L-1$.

One can do an analogous analysis for the superword on the right, which is $\varphi^{2n}(a+1)$. Here the relevant positions are of the form $j_k = L^n - 2 + k(L^n - 1)$, for $0 \leq k \leq L-2$, and one needs to show that $[\varphi^{2n}]_{j_k} = g^{L-1} = g^{-1}$. Since the proof uses the same arguments above, we omit the details. In this case, one can also show that, for $k = L-1$, $[\varphi^{2n}]_{j_k}(a+1)$ is not equivalent to $a \pmod{L}$, which implies that the extension to the right also has length at most $L-1$. Considering the progression of letter a which straddles these three superwords verifies the claim.

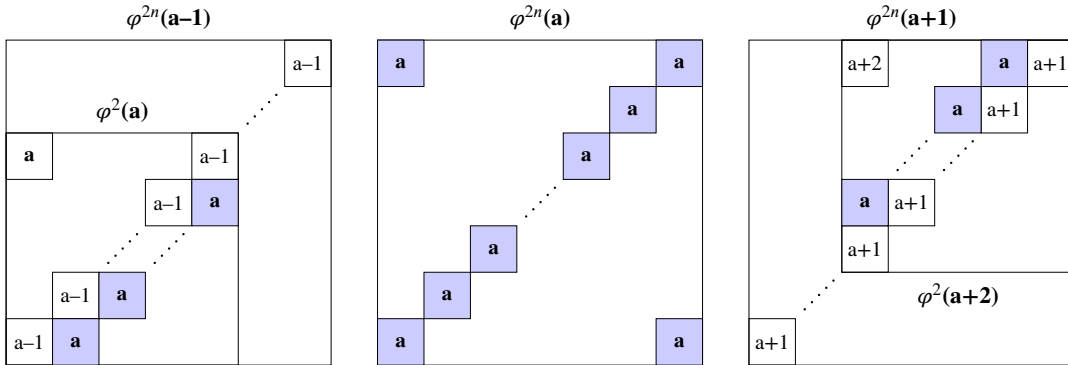


Figure 4.2.1: A monochromatic arithmetic progression of a s of length $L^n + 2L$ accommodated within the superwords $\varphi^{2n}(a-1)$, $\varphi^{2n}(a)$ and $\varphi^{2n}(a+1)$. Here level- $2n$ superwords are written as $L^n \times L^n$ blocks, which are read from left to right, and then top to bottom. The bottom-most shaded square in $\varphi^{2n}(a-1)$ is its $(L^{2n} - L^n + 1)$ th letter while the top-most shaded square in $\varphi^{2n}(a+1)$ is its $(L^n - 2)$ th letter.

□

We conjecture that the lower bounds given in the previous are actually exact values. This has been

settled when L is a prime number in [91], where it is also proved that the largest value of $A(d)$ for all d up to L^n is $A(L^n - 1)$.

Now, we look at other differences d . From Proposition 4.2.2, we directly obtain the lower bound

$$A\left(\frac{L^{L^n} - 1}{L^n - 1}\right) \geq L^n,$$

for every positive integer n . This result can be geometrically visualised as in the previous proposition. We illustrate this with the following example.

Example 4.2.39. We fix $L = 3$ and consider the 3-letter Thue–Morse sequence, also known as the *ternary Thue–Morse sequence*. This is the fixed point $012 \dots$ of the substitution

$$\begin{aligned} 0 &\mapsto 012, \\ \varphi: 1 &\mapsto 120, \\ 2 &\mapsto 201. \end{aligned}$$

For differences of the form $d = 3^n - 1$, Proposition 4.2.38 implies that $A(3^n - 1) \geq 3^n$, for all positive integers n , and furthermore, $A(3^n - 1) \geq 3^n + 6$, if n is a multiple of 3. For differences of the form $d = 3^{2n} + 3^n + 1$, Corollary 4.2.31 (with $|G| = 3$ and $N = 4$) implies that

$$3^n \leq A(3^{2n} + 3^n + 1) \leq 81 \cdot 3^n,$$

for all positive integers n . See Figure 4.2.2 for a plot of $A(d)$, for differences up to 2200 (the list of values can be found in the data underlying this thesis).

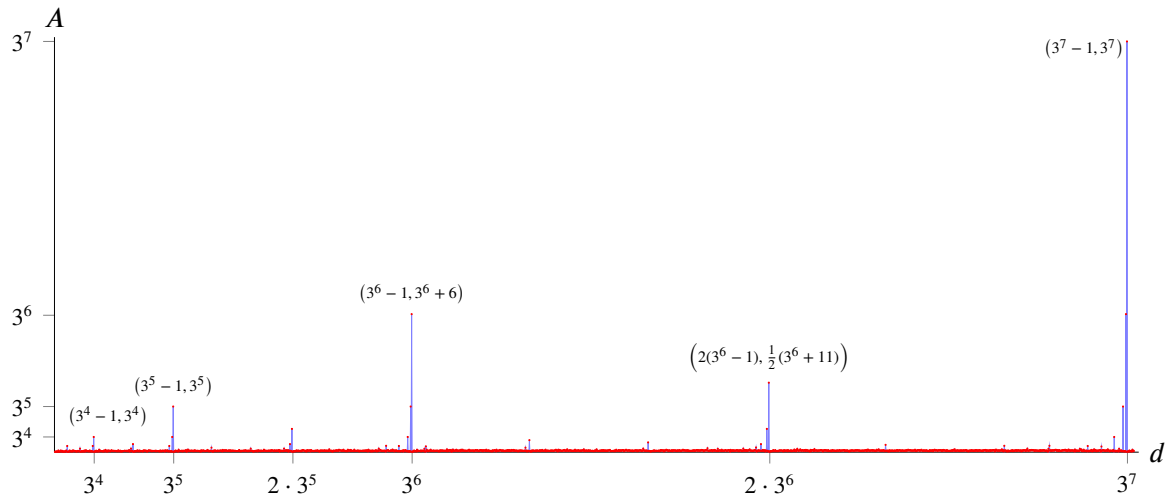


Figure 4.2.2: $A(d)$ for $d = 1, 2, \dots, 2200$, for the ternary Thue–Morse sequence.

We can give an alternative visual approach by identifying a long monochromatic arithmetic progression across a diagonal of a block substitution, as in the proof of Proposition 4.2.38, but now in three dimensions. As in Figure 4.2.1, we can consider the word $\varphi^{3^n}(0)$ and arrange it inside a block. The dif-

ference is that now, we arrange it in a three-dimensional cube of side-length 3^n . There is no fixed choice of fitting the word inside a cube, and one must only be consistent when going up and through a layer.

In our choice depicted in Figure 4.2.3, we start from the lower left corner of the cube, traverse along the x -direction, then go up the next row. Once all rows in the bottom-most layer are filled, one moves one layer up and starts directly above the point where the origin is. The red shaded squares precisely correspond to the monochromatic arithmetic progression of difference $d = 3^{2n} + 3^n + 1$ and length 3^n that starts at the origin.

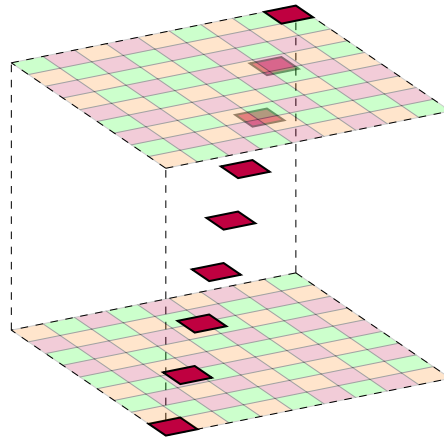


Figure 4.2.3: A monochromatic arithmetic progression of difference $d = 3^{2n} + 3^n + 1$ and length 3^n in the word $\varphi^{3^n}(0)$, with $n = 2$.



Another look at Proposition 4.2.38

To finish this section, we remark that the approach used in the proof of Proposition 4.2.38 is similar to the approach we used in Chapter 3, where we considered a block substitution (Definition 3.2.7), rather than working with the columns of the substitution directly. Here the same thing can be done. In this case,

we need to define a block substitution ϕ that is given, for each $a \in \mathcal{A}_L$, by

$$\phi(a) = \begin{array}{cccccccc} a & a+1 & \cdots & L-1 & 0 & \cdots & a-2 & a-1 \\ a+1 & a+2 & \cdots & 0 & 1 & \cdots & a-1 & a \\ \vdots & \vdots & & & & \ddots & \vdots & \vdots \\ L-1 & 0 & & & \ddots & & L-3 & L-2 \\ 0 & 1 & & \ddots & & & L-2 & L-1 \\ \vdots & \vdots & \ddots & & & & \vdots & \vdots \\ a-2 & a-1 & \cdots & L-3 & L-2 & \cdots & a-4 & a-3 \\ a-1 & a & \cdots & L-2 & L-1 & \cdots & a-3 & a-2 \end{array}$$

Lemma 4.2.40. *For each $a \in \mathcal{A}_L$ and every positive integer n , the block $\phi^n(a)$ read row-wise from left to right and from top to bottom is the word $\varphi^{2^n}(a)$, where φ is the L -letter Thue–Morse substitution.*

Proof. The rows of $\phi(a)$, read from top to bottom, are $\varphi(a), \varphi(a+1), \dots, \varphi(L-1), \varphi(0), \dots, \varphi(a-1)$. So, read row-wise from top to bottom, $\phi(a)$ becomes $\varphi(\phi(a)) = \varphi^2(a)$. The result then follows by induction. \square

Therefore, we can equivalently look for arithmetic progressions in words obtained under the iteration of φ or in blocks obtained under the iteration of ϕ .

Another proof of Proposition 4.2.38. Observe that, for each $a \in \mathcal{A}_L$, all the elements of the second diagonal of the block $\phi(a)$ are equal. It can be easily shown that this property remains true for $\phi^n(a)$, for all n . Since, when read row-wise from top to bottom, the block $\phi^n(a)$ is the word $\varphi^{2^n}(a)$, we obtain an arithmetic progression across the second diagonal, which implies that $A(L^n - 1) \geq L^n$, for all n .

Since the first row of $\phi^n(a)$ is $\varphi^n(a)$, the colour of the arithmetic progression located on the second diagonal is determined by the last letter of $\varphi^n(a)$, which cycles through every symbol of \mathcal{A}_L with the property of being a if $n \equiv 0 \pmod L$. This arithmetic progression of a 's can be followed once to the left and once to the right, reaching the upper left corner and the lower right corner of the block $\phi^n(a)$, which are, respectively, the first letter of $\varphi^{2^n}(a)$ (hence equal to a) and the last letter of $\varphi^{2^n}(a)$ (hence equal to a , since $n \equiv 0 \pmod L$). Consequently, $A(L^n - 1) \geq L^n + 2$, for all $n \equiv 0 \pmod L$. To complete the proof, we need to show that this a -coloured arithmetic progression of length $L^n + 2$ obtained across the block $\phi^n(a)$ can be followed $L - 1$ times each side when $n \equiv 0 \pmod L$.

Let $n \equiv 0 \pmod L$. Since $(a-1)(a)(a+1)$ is a legal word, the block $\phi^n(a-1)$ followed by $\phi^n(a)$ followed by $\phi^n(a+1)$, each of them read row-wise from top to bottom, must occur as a subword of the

Thue–Morse sequence over L letters. Consider the a -coloured arithmetic progression of length $L^n + 2$ accommodated in the middle block $\phi^n(a)$. Following this arithmetic progression to the left, we reach the entry located to the right of the lower left most entry of $\phi^n(a - 1)$. But observe that the $L \times L$ block accommodated in the lower left corner of $\phi^n(a - 1)$ must be $\phi(a)$, which has a diagonal of $L - 1$ a 's adjacent to the second diagonal of $a - 1$'s, and therefore, our arithmetic progression can be followed $L - 1$ times to the left. Similarly, our arithmetic progression can be followed $L - 1$ times to the right because the $L \times L$ block accommodated in upper right corner of $\phi^n(a + 1)$ must be $\phi(a + 2)$, which has a diagonal of $L - 1$ a 's adjacent to the second diagonal of $a + 1$'s. This provides us with an arithmetic progression of a 's of length $L^n + 2L$, as required. \square

4.3 Non-bijective substitutions with supersubstitution structure

In this section, we consider non-bijective substitutions ρ of \mathcal{A} that admit partial coincidences and for which we can define a new substitution ξ on a partition of \mathcal{A} . If the new substitution ξ is a bijective substitution, we can apply the lower bounds obtained in Section 4.2.1. Under mild assumptions, these lower bounds give lower bounds for ρ too.

Definition 4.3.1. Let ρ be a substitution of a finite alphabet \mathcal{A} of constant length L . Suppose that there exists a partition $\mathcal{A}_1 \cup \mathcal{A}_2 \cup \dots \cup \mathcal{A}_p$ of \mathcal{A} , for a positive integer p , such that, for every $1 \leq i \leq p$ and for each $0 \leq \ell \leq L - 1$, there exists $1 \leq j \leq p$ for which $[\rho]_\ell(a) \in \mathcal{A}_j$, for all $a \in \mathcal{A}_i$. Then we define a constant-length substitution ξ of the alphabet $\{1, 2, \dots, p\}$ by setting, for every $1 \leq i \leq p$ and for each $0 \leq \ell \leq L - 1$, $[\xi]_\ell(i) = j$, where j is such that $[\rho]_\ell(a) \in \mathcal{A}_j$, for any $a \in \mathcal{A}_i$. We say that ξ is a *supersubstitution* for ρ induced by the partition of \mathcal{A} considered.

Definition 4.3.2. For a partition $\mathcal{A}_1 \cup \mathcal{A}_2 \cup \dots \cup \mathcal{A}_p$ of a finite alphabet \mathcal{A} , let θ be the map defined, for each $a \in \mathcal{A}$, as $\theta(a) = i$, where $1 \leq i \leq p$ is such that $a \in \mathcal{A}_i$. We say that θ is the *projection map* for the partition of \mathcal{A} considered.

The following lemma relates the substitution ρ with the supersubstitution ξ via the projection map θ .

Lemma 4.3.3. Let ρ be a constant-length substitution of \mathcal{A} for which there exists a supersubstitution ξ induced by some partition of \mathcal{A} , and let θ be the projection map for that partition. Then $\theta \circ \rho = \xi \circ \theta$.

Proof. Let L be the length of ρ and let p be the number of subsets into which \mathcal{A} has been partitioned. To establish the claim, we must show that $\theta \circ [\rho]_\ell = [\xi]_\ell \circ \theta$, for each $0 \leq \ell \leq L - 1$. For each $a \in \mathcal{A}$, let $1 \leq i_a \leq p$ be such that $a \in \mathcal{A}_{i_a}$ and let $x^a \in \mathcal{A}^L$ be such that $\rho(a) = x^a$. This implies that $\theta(a) = i_a$ and $\rho(a) = x_0^a x_1^a \dots x_{L-1}^a$. Then

$$\theta \circ [\rho]_\ell(a) = \theta(x_\ell^a) = i_{x_\ell^a} = [\xi]_\ell(i_a) = [\xi]_\ell \circ \theta(a),$$

for every $a \in \mathcal{A}$, as required. \square

Remark 4.3.4. Let ρ be a constant-length substitution of \mathcal{A} for which there exists a supersubstitution ξ induced by a partition of \mathcal{A} , and let θ be the projection map for that partition. Notice that, if ρ has a fixed point v and the first letter of v belongs to the element \mathcal{A}_i of the partition of \mathcal{A} , then ξ has a fixed point w with first letter i . Moreover, $w = \theta(v)$ because, since $\theta(v) = \theta(\rho(v)) = \xi(\theta(v))$, $\theta(v)$ is a fixed point of ξ and, since $\theta(v_0) = i$, where v_0 is the first letter of v , $\theta(v)$ is precisely w . By a relabeling of the partition of the alphabet, without loss of generality, we can assume that $i = 1$. \diamond

The following result gives a lower bound for $A_v(d)$ when ξ satisfies the conditions of Proposition 4.2.2, under the additional assumption that the element of the partition of \mathcal{A} to which v_0 belongs is a singleton.

Proposition 4.3.5. *Let ρ be a substitution of \mathcal{A} of constant length L and let ξ be a supersubstitution for ρ induced by a partition of \mathcal{A} . Let v be a fixed point of ρ whose starting letter is in the element \mathcal{A}_1 of the partition. Suppose that $|\mathcal{A}_1| = 1$ and that ξ is aperiodic, primitive and bijective with $[\xi]_0 = \text{id}$. Then*

$$A_v\left(\frac{L^{n|G|} - 1}{L^n - 1}\right) \geq L^n,$$

for every positive integer n , where G is the column group of ξ .

Proof. Let w be the fixed point of ξ starting with the letter 1. Then $w = \theta(v)$, where θ is the projection map for the partition of the alphabet (see Remark 4.3.4). From the proof of Proposition 4.2.2, we see that $[\xi^{n|G|}]_{kd} = \text{id}$, for $k = 0, 1, \dots, L^n - 1$, where $d = \frac{L^{n|G|} - 1}{L^n - 1}$. Since w is a fixed point of $\xi^{n|G|}$ and starts with the letter 1, we see that $w_{kd} = 1$, for $k = 0, 1, \dots, L^n - 1$. Let $a \in \mathcal{A}_1$ be the starting letter of v . Since $|\mathcal{A}_1| = 1$, the map θ^{-1} is uniquely defined for 1 as $\theta^{-1}(1) = v_0$. Consequently, $v_{kd} = a$, for $k = 0, 1, \dots, L^n - 1$. In other words, v contains a monochromatic arithmetic progression of difference d and length L^n that starts at position 0, which implies the claim. \square

Example 4.3.6. Let ρ be the non-bijective substitution of $\mathcal{A} = \{a, b, c, d, e\}$ given by

$$\begin{aligned} a &\mapsto a c d a e c, \\ b &\mapsto b a b e a d, \\ \rho: c &\mapsto b a c e a d, \\ d &\mapsto d d a b c a, \\ e &\mapsto e d a b c a. \end{aligned}$$

The partition $\mathcal{A} = \mathcal{A}_1 \cup \mathcal{A}_2 \cup \mathcal{A}_3$, where $\mathcal{A}_1 = \{a\}$, $\mathcal{A}_2 = \{b, c\}$ and $\mathcal{A}_3 = \{d, e\}$, induces the supersubstitution ξ given by

$$\begin{aligned} 1 &\mapsto 1 2 3 1 3 2, \\ \xi: 2 &\mapsto 2 1 2 3 1 3, \\ 3 &\mapsto 3 3 1 2 2 1. \end{aligned}$$

This substitution is aperiodic, primitive and bijective. Its leftmost column is equal to the identity and its column group G is the symmetric group S_3 , as can be easily verified. Then, by Proposition 4.3.5, for the

fixed point v of ϱ starting with a ,

$$A_v\left(\frac{L^{6n} - 1}{L^n - 1}\right) \geq L^n,$$

for every positive integer n . ❖

The singleton condition in Proposition 4.3.5 can be replaced by some restrictions on the columns of ϱ . The following lemma considers these restrictions.

Lemma 4.3.7. *Let ϱ be a substitution of \mathcal{A} of constant length L and let ξ be a supersubstitution for ϱ induced by a partition of \mathcal{A} . Let v be a fixed point of ϱ starting with a letter a which belongs to the element \mathcal{A}_1 of the partition, and let w be the fixed point of ξ starting with the letter 1.*

- (i) *Suppose that there exists a subset C of $\{0, 1, \dots, L-1\}$ such that $[\varrho]_c(b) = a$, for all $c \in C$ and $b \in \mathcal{A}_1$. If $w_r = 1$, for a non-negative integer r , then $v_s = a$, where $s = Lr + c$ with $c \in C$.*
- (ii) *Suppose further that $0 \in C$. If $w_r = 1$, for a non-negative integer r , then $v_s = a$, where $s = L^m r + c$ with $c \in C$ and m a positive integer.*

Proof of (i). Writing the base- L representation of r as $[r_{k-1}, \dots, r_1, r_0]$, where $k \in \mathbb{N}$, the base- L representation of s is $[r_{k-1}, \dots, r_1, r_0, c]$. Then, using Proposition 4.1.2, we see that

$$v_s = [\varrho^{k+1}]_s(a) = [\varrho]_c \circ [\varrho^k]_r(a) = [\varrho]_c(v_r).$$

Since $w = \theta(v)$, $w_r = 1$ implies that $\theta(v_r) = 1$, so $v_r \in \mathcal{A}_1$. This implies that $v_s = a$, as required. □

Proof of (ii). Writing the base- L representation of r as $[r_{k-1}, \dots, r_1, r_0]$, where $k \in \mathbb{N}$, the base- L representation of s is $[r_{k-1}, \dots, r_1, r_0, 0, \dots, 0, c]$, where the sequence of 0s has length $m-1$. Then,

$$v_s = [\varrho^{k+m}]_s(a) = [\varrho]_c \circ [\varrho]_0^{m-1} \circ [\varrho^k]_r(a) = [\varrho]_c \circ [\varrho]_0^{m-1}(v_r).$$

Since $w = \theta(v)$, $w_r = 1$ implies that $\theta(v_r) = 1$, so $v_r \in \mathcal{A}_1$. Furthermore $0, c \in C$, which implies that $v_s = a$, as required. □

Proposition 4.3.8. *Let ϱ be a substitution of \mathcal{A} of constant length L and let ξ be a supersubstitution for ϱ induced by a partition of \mathcal{A} . Let v be a fixed point of ϱ starting with a letter a which belongs to the element \mathcal{A}_1 of the partition, and let w be the fixed point of ξ starting with the letter 1. Suppose that ξ is aperiodic, primitive and bijective with $[\xi]_0 = \text{id}$ and column group G . Let n be a positive integer and let*

$$d = \frac{L^{n|G|} - 1}{L^n - 1}.$$

- (1) *If there is $C \subseteq \{0, 1, \dots, L-1\}$ such that $[\varrho]_c(b) = a$, for all $c \in C$ and $b \in \mathcal{A}_1$, then $A_v(Ld) \geq L^n$.*
- (2) *If furthermore $0 \in C$, then $A_v(L^m d) \geq L^n$, for every positive integer m .*

Proof. From the proof of Proposition 4.3.5 we have that $w_{kd} = 1$, for $k = 0, 1, \dots, L^n - 1$. If the condition in (1) is satisfied, by (i) in Lemma 4.3.7, we see that $v_{kLd+c} = a$, for $k = 0, 1, \dots, L^n - 1$ and any $c \in C$. This proves the claim in (1). Similarly, if the condition in (2) is satisfied, by (ii) in Lemma 4.3.7, we see that $v_{kL^m d+c} = a$, for $k = 0, 1, \dots, L^n - 1$, any $c \in C$ and any $m \in \mathbb{N}$. This proves the claim in (2). \square

Example 4.3.9. Let ϱ be the non-bijective substitution of $\mathcal{A} = \{a, b, c, d, e, f\}$ of length $L = 6$ given by

$$\varrho: \begin{array}{lll} a \mapsto abbabd, & c \mapsto cddcce, & e \mapsto effeea, \\ b \mapsto aabaac, & d \mapsto dccddf, & f \mapsto fefefb. \end{array}$$

The partition $\mathcal{A} = \mathcal{A}_1 \cup \mathcal{A}_2 \cup \mathcal{A}_3$, where $\mathcal{A}_1 = \{a, b\}$, $\mathcal{A}_2 = \{c, d\}$ and $\mathcal{A}_3 = \{e, f\}$, induces the supersubstitution ξ given by

$$\begin{array}{ll} 1 \mapsto 111112, \\ \xi: 2 \mapsto 222223, \\ 3 \mapsto 333331. \end{array}$$

This substitution is aperiodic, primitive and bijective, its leftmost column is equal to the identity and its column group G is the cyclic group C_3 , so $|G| = 3$. Observe that $[\varrho]_0(a) = [\varrho]_3(a) = [\varrho]_0(b) = [\varrho]_3(b) = a$, so the condition in (2) in Proposition 4.3.8 is satisfied. Therefore $A_v(6^m d) \geq 6^n$, where

$$d = \frac{6^{3n} - 1}{6^n - 1} = 6^{2n} + 6^n + 1,$$

for every positive integers n and m .

Now, we consider the details of this result. Notice that, for $k = 0, 1, \dots, L^n - 1$, the base-6ⁿ representation of kd is $[k, k, k]$ and consequently, $[\xi^{n3}]_{kd} = [\xi^n]_k \circ [\xi^n]_k \circ [\xi^n]_k = [\xi^n]_k^3 = [\xi^n]_k^{|G|} = \text{id}$, where the last equality holds because $g^{|G|} = \text{id}$, for every $g \in G$. Then $w_{kd} = [\xi^{n3}]_{kd}(1) = 1$, and so, by Lemma 4.3.7, $v_{kL^m d} = a$, for $k = 0, 1, \dots, L^n - 1$. Therefore, v has monochromatic arithmetic progression of a s of difference $L^m d$ and length L^n . \diamond

4.4 Spin substitutions

We consider monochromatic arithmetic progressions in infinite words arising from so called ‘spin substitutions’. A *spin substitution* θ is a special type of constant-length substitution. A finite set \mathcal{D} of digits is considered, each of which, carrying a spin, can be in a finite number of distinct states. The spin states are represented using a finite Abelian group G , called the *spin group*. This results in the alphabet $\mathcal{A} = \mathcal{D} \times G$. The substitution θ is then completely determined using a $|\mathcal{D}| \times |\mathcal{D}|$ matrix V with entries in G , which is called the *spin matrix*. The matrix V encodes, for each digit $d \in \mathcal{D}$, the spin state of the letters of the image of d under the substitution. For background on spin substitutions and generalisations, we refer the reader to [4, 31, 52, 96].

In Sections 4.4.1 and 4.4.2 we study $A(d)$ for the Rudin–Shapiro sequence. We give lower bounds for $A(d)$ for two sequences of differences along which $A(d)$ grows at least linearly in d , in analogy to

the classical Thue–Morse case studied in Chapter 3. We extend the previous results to the Hadamard sequence (Section 4.4.3) and also to Vandermonde sequences (Section 4.4.4).

4.4.1 The Rudin–Shapiro sequence

Consider the spin substitution θ with digit set $\mathcal{D} = \{0, 1\}$, spin group $G = C_2 = \{+1, -1\}$ and spin matrix

$$V = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \quad (4.4.1)$$

The resulting alphabet is

$$\mathcal{A} = \mathcal{D} \times G = \{0, 1, \tilde{0}, \tilde{1}\},$$

where ‘tilded’ letters have non-trivial spin. The spin matrix determines the positions of the tildes in $\theta(0)$ and $\theta(1)$; the positions of the tildes in $\theta(\tilde{0})$ and $\theta(\tilde{1})$ are determined via the invariance relation $\theta(\tilde{a}) = \widetilde{\theta(a)}$ with number of tildes modulo 2, for $a \in \mathcal{D}$. The resulting substitution is

$$\theta: \begin{array}{ll} 0 \mapsto 01, & \tilde{0} \mapsto \tilde{0}\tilde{1}, \\ 1 \mapsto 0\tilde{1}, & \tilde{1} \mapsto \tilde{0}1. \end{array}$$

The *Rudin–Shapiro sequence* u over the alphabet $\{1, -1\}$ is obtained from the fixed point of θ starting with 0 under the projection

$$\pi_G: 0, 1 \mapsto 1, \quad \tilde{0}, \tilde{1} \mapsto -1.$$

(see [17, Section 7.7.1]). The first few terms of u (with commas inserted for the sake of clarity) are

$$u = 1, 1, 1, -1, 1, 1, -1, 1, 1, 1, 1, -1, -1, -1, 1, -1, \dots$$

(see [86]). The n th element of u can be derived from V as

$$u_n = \prod_{i=0}^{k-1} V(n_{i+1}, n_i) = V(n_k, n_{k-1}) \cdots V(n_2, n_1) V(n_1, n_0), \quad (4.4.2)$$

where $[n_k, \dots, n_1, n_0]$ is the binary representation of n with n_0 the least significant digit and n_k the most significant digit, and $V(i, j)$ is the (i, j) th entry of V [4, 52]. Alternatively, u_n can be defined as $(-1)^{t(n)}$, where $t(n)$ counts the number of (possibly overlapping) occurrences of the word 11 in the binary representation of the integer n [8].

Lemma 4.4.1. *The entries of the Rudin–Shapiro sequence u satisfy, for all non-negative integers n , the recurrence relations*

$$u_{2n} = u_n, \quad u_{2n+1} = (-1)^n u_n. \quad (4.4.3)$$

Proof. Let $[n_k, \dots, n_1, n_0]$ be the binary representation of n . On the one hand, the binary representation of $2n$ is $[n_k, \dots, n_1, n_0, 0]$, so $u_{2n} = u_n V(n_0, 0) = u_n$. On the other hand, the binary representation of $2n + 1$ is $[n_k, \dots, n_1, n_0, 1]$, so $u_{2n+1} = u_n V(n_0, 1)$. Since n is even if, and only if, $n_0 = 0$ (equivalently, n

is odd if, and only if, $n_0 = 1$), we see that $u_{2n+1} = u_n$ if n is even, and $u_{2n+1} = -u_n$ otherwise, which can be written as in the Equation (4.4.3). \square

A simple argument will show that, for the sequence u , $A(d) < \infty$, for all positive integers d .

Proposition 4.4.2. *Every monochromatic arithmetic progression in the Rudin–Shapiro sequence u has finite length.*

Proof. Let v be the fixed point of θ starting with 0. It follows from the definition of θ that $v_{2n+a} \in \{a, \tilde{a}\}$, for all $a \in \mathcal{D}$ and $n \in \mathbb{N}_0$. Then, since $u = \pi_G(v)$, we know that $u_{2n+a} = 1$ (resp. -1) implies $v_{2n+a} = a$ (resp. \tilde{a}), for all $a \in \mathcal{D}$ and $n \in \mathbb{N}_0$. The proof is by contradiction. Assume there exist $s \in \mathbb{N}_0$ and $d \in \mathbb{N}$ such that $u_{s+nd} = 1$ (resp. -1), for all $n \in \mathbb{N}_0$. This implies that $v_{s+nd} = a$ (resp. \tilde{a}) for all $n \in 2\mathbb{N}_0$, where $a \equiv s \pmod{2}$. But this is a contradiction because θ is an aperiodic, primitive, constant-length substitution of height 1, and so, by Proposition 4.1.4, every monochromatic arithmetic progression in v has finite length. \square

It is not difficult to show that $A(2^n d) = A(d)$, for all positive integers d and n . We omit the proof, which is similar to Lemma 3.2.4 for the Thue–Morse case. From here it is easy to see that $A(2^n) = 4$, for all non-negative integers n . The next two propositions, where we find sequences of long monochromatic arithmetic progressions for differences of the form $2^n \pm 1$, are analogues of Proposition 4.2.2 for spin substitutions.

Proposition 4.4.3. *For the Rudin–Shapiro sequence u , for all positive integers n , $A(2^n + 1) \geq 2^{n-1} + 2$.*

Proof. It is easy to see, by direct inspection of u , that the result holds for $n = 1$. For $n > 1$, we will show that $u_k = 1$, where $k = 2^{2n+1} + m(2^n + 1)$, for all integers $-1 \leq m \leq 2^{n-1}$. This will then imply the claim. Let us fix n .

For $m = -1$, $k = 2^{2n+1} - 2^n - 1$. One can check that the binary representation of k is of the form $[1, \dots, 1, 0, 1, \dots, 1]$, consisting of two sequences of n consecutive 1's separated by a single 0. Then, by Equation (4.4.2), we see that $u_k = 1$.

For $0 \leq m \leq 2^{n-1}$, let the binary representation of m be $[m_r, \dots, m_1, m_0]$, where $0 \leq r \leq n-1$. Then one can check that the binary representation of $k = 2^{2n+1} + m(2^n + 1)$ is

$$[1, \overbrace{0, \dots, 0}^{n-r}, m_r, \dots, m_1, m_0, \overbrace{0, \dots, 0}^{n-r-1}, m_r, \dots, m_1, m_0].$$

For $0 \leq r < n-1$, we have $n-r \geq 1$ and $n-r-1 \geq 1$. Then, by Equation (4.4.2), we see that $u_k = 1$. For $r = n-1$, we have $n-r-1 = 0$ and then, by Equation (4.4.2), $u_k = V(m_0, m_r)$. But, for $r = n-1$, we also have $m = 2^{n-1} = [1, 0, 0, \dots, 0]$, so $u_k = V(m_0, m_r) = V(0, 1) = 1$. \square

Proposition 4.4.4. *For the Rudin–Shapiro sequence u , for all positive integers n ,*

$$A(2^n - 1) \geq \begin{cases} 2^{n-1} + 1, & \text{if } n \text{ is even,} \\ 2^{n-1} + 3, & \text{otherwise.} \end{cases}$$

Proof. For $n = 1$ the result holds because, as mentioned earlier, $A(1) = 4$. So, we assume that $n \geq 2$. We will first show that, for every integer $n \geq 2$ and all integers $0 \leq m \leq 2^{n-1}$, there exists $a \in \{1, -1\}$ such that $u_k = a$, where $k = 2^{2n} + (m+1)(2^n - 1)$. Fix n and write the binary representation of m as $[m_{n-1}, \dots, m_1, m_0]$, where $m_i \in \{0, 1\}$ for all $0 \leq i \leq n-1$. Then, one can check that the binary representation of k takes the form $[1, m_{n-1}, \dots, m_1, m_0, \overline{m_{n-1}}, \dots, \overline{m_1}, \overline{m_0}]$, where $\overline{m_i} = 1 - m_i$. By Equation (4.4.2) and given that, for each $0 \leq i \leq n-2$, $V(m_{i+1}, m_i)V(\overline{m_{i+1}}, \overline{m_i})$ is equal to -1 if $m_{i+1} = m_i$, and to 1 otherwise, we see that

$$u_k = V(1, m_{n-1}) V(m_0, \overline{m_{n-1}}) (-1)^{n-1+m_{n-1}-m_0}$$

If $m_{n-1} \neq m_0$, then $u_k = (-1)^{n-1}$. If $m_{n-1} = m_0$, then $m_{n-1} = m_0 = 0$ because $m \leq 2^{n-1}$, and again $u_k = (-1)^{n-1}$. If n is even, this implies that $u_k = -1$, which completes the proof for the even cases. If n is odd, it implies that $u_k = 1$. In this case, it can also be easily verified that $u_k = 1$ for $m = -1$ and $m = -2$, which completes the proof for the odd cases. Indeed, for $m = -1$, $k = 2^{2n}$ with binary representation $[1, 0, \dots, 0]$. So, by Equation (4.4.2), $u_k = 1$. Similarly, for $m = -2$, $k = 2^{2n} - 2^n + 1$ with binary representation $[1, \dots, 1, 0, \dots, 0, 1]$ comprising a sequence of n consecutive 1's followed by a sequence of $n-1$ consecutive 0's followed by a single 1. So, by Equation (4.4.2), $u_k = (-1)^{n-1} = 1$, as n is odd. \square

Corollary 4.4.5. *For the Rudin–Shapiro sequence, for all $d_n = 2^n \pm 1$ with $n \geq 1$, $A(d_n) \gtrsim \frac{d_n}{2}$.*

Proof. The claim follows directly from Propositions 4.4.3 and 4.4.4. \square

By computer experiments we have verified the preceding results for $1 \leq d \leq 4200$. In fact, we have seen that the inequalities in Propositions 4.4.3 and 4.4.4 are equalities, if $n \geq 4$ and if $n \geq 5$, respectively. Moreover, the differences of the form $2^n \pm 1$ are those for which the Rudin–Shapiro sequence has the longest monochromatic arithmetic progressions, in the sense that $A(d)$ has local maximums at these differences. The plot of $A(d)$ in Figure 4.4.1 is analogous to the similar plot in Figure 3.2.1 (Section 3.2.6) for the Thue–Morse sequence. A list of values of $A(d)$ can be found in the data underlying this thesis.

Remark 4.4.6. A recent paper by Sobolewski [102] concerns the computation of upper bounds for $A_w(d)$, for sequences $w \in \mathcal{A}^{\mathbb{N}_0}$ defined using a block-counting function. More precisely, given a binary block $v \in \mathcal{A}^+$, the digit w_n is given by the sum mod 2 of (possibly overlapping) occurrences of v in the binary representation of n , for all $n \in \mathbb{N}_0$. The author focuses most of his attention on the $v = 11$ case, for which w is the Rudin–Shapiro sequence. In this case, an upper bound for the maximum length of monochromatic arithmetic progressions starting at position 0 is given, and exact values of $A(d)$ are determined for differences of the form $2^n \pm 1$. \diamond

4.4.2 A different approach to the Rudin–Shapiro sequence

The Rudin–Shapiro sequence can alternatively be obtained by a staggered substitution or by a substitution acting on an alphabet consisting of pairs of letters in $\{1, -1\}$, say $\{v, \tilde{v}, w, \tilde{w}\}$ with $v = 11$, $w = 1-1$

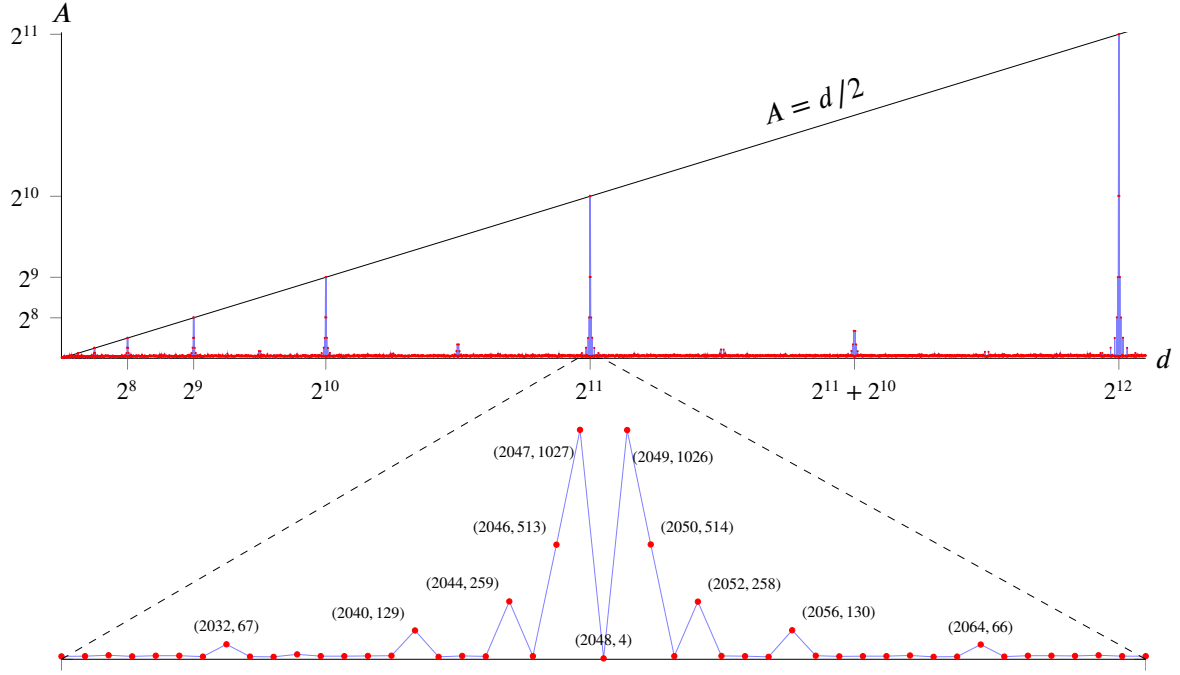


Figure 4.4.1: $A(d)$ for $1 \leq d \leq 4200$, for the Rudin–Shapiro word.

and $\tilde{x} = \tilde{x}_0 \tilde{x}_1$, for $x \in \{v, w\}$, where $\tilde{1} = -1$ and $\widetilde{-1} = 1$. The substitution reads

$$\varphi: \begin{array}{ll} v \mapsto vw, & \tilde{v} \mapsto \tilde{v}\tilde{w}, \\ w \mapsto v\tilde{w}, & \tilde{w} \mapsto \tilde{v}w. \end{array}$$

Note that this substitution is exactly the same as the original four-letter substitution, except that we now interpret v and w as two-letter words in $\{1, -1\}$. Note that the substitution is invariant under the letter exchange in the sense that $\varphi(\tilde{a}) = \widetilde{\varphi(a)}$ for all $a \in \{v, w, \tilde{w}, \tilde{v}\}$. Moreover, the first part of $\varphi(a)$ for any $a \in \{v, w, \tilde{w}, \tilde{v}\}$ is either v or \tilde{v} , and the last is either w or \tilde{w} . By induction, this structure is preserved for larger superwords as follows.

Lemma 4.4.7. *Let $v^{(0)} = v$, $w^{(0)} = w$ and, for all positive integers n , $v^{(n)} = \varphi^n(v)$ and $w^{(n)} = \varphi^n(w)$. Then, $v^{(n)} = v^{(n-1)}w^{(n-1)}$ and $w^{(n)} = v^{(n-1)}\tilde{w}^{(n-1)}$.*

Proof. Clearly, this is true for $n = 1$. Assuming the structure holds for n , we find that

$$v^{(n+1)} = \varphi(v^{(n)}) = \varphi(v^{(n-1)}w^{(n-1)}) = \varphi(v^{(n-1)})\varphi(w^{(n-1)}) = v^{(n)}w^{(n)}$$

and

$$w^{(n+1)} = \varphi(w^{(n)}) = \varphi(v^{(n-1)}\tilde{w}^{(n-1)}) = \varphi(v^{(n-1)})\varphi(\tilde{w}^{(n-1)}) = v^{(n)}\tilde{w}^{(n)},$$

which completes the proof. \square

For the rest of the section, we consider the superword $v^{(2n-1)} = \varphi^{2n-1}(v)$ for $n \geq 2$, and write the resulting word in the alphabet $\{1, -1\}$, which has 2^{2n} letters, as a square array of letters with 2^n rows of

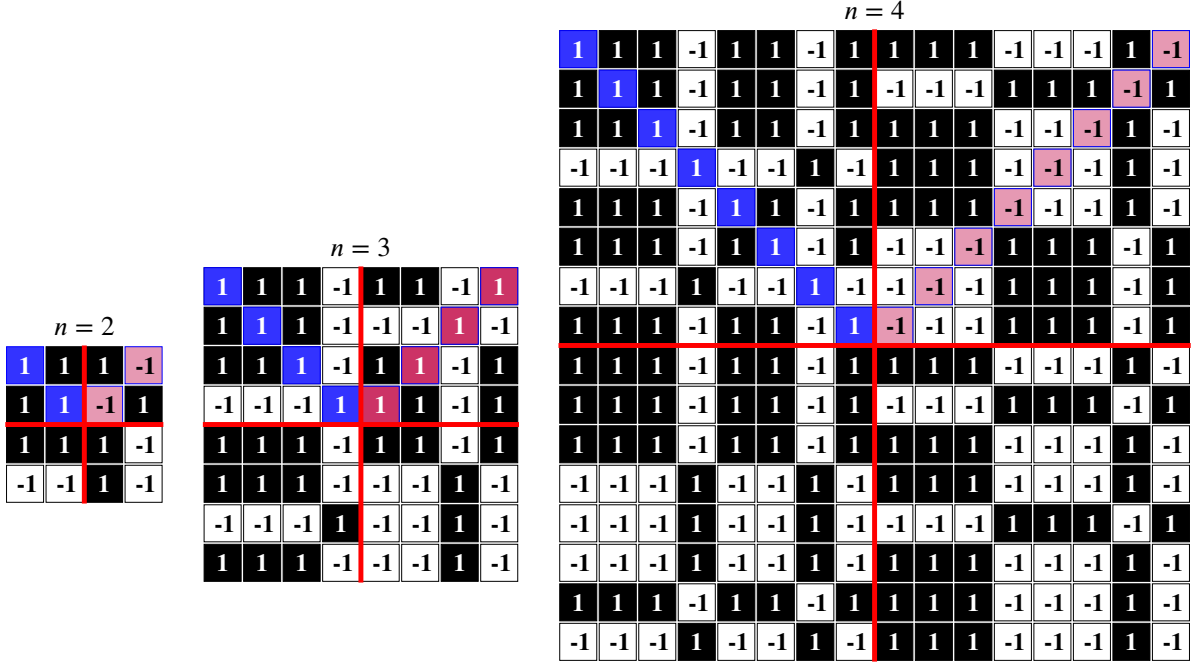


Figure 4.4.2: The square array of letters in $v^{(2n-1)}$, for $n \in \{2, 3, 4\}$. The highlighted letters on the diagonals form monochromatic arithmetic progressions of length 2^{n-1} for differences $d = 2^n + 1$ (upper left quadrant) or $d = 2^n - 1$ (upper right quadrant).

length 2^n . For $n \in \{2, 3, 4\}$, they are shown in Figure 4.4.2. Let us denote the (i, j) th entry of this matrix by $a_{i-1, j-1}$. With this notation, one has $v^{(2n-1)} = a_{0,0} a_{0,1} \cdots a_{2^n-1, 2^n-1}$. In particular, the sequence $a_{0,0} a_{0,1} \cdots a_{0,2^n-1}$ corresponds to the topmost row of the block (or the first row of the matrix). In what follows, $v_j^{(n)}$ (resp. $w_j^{(n)}$) denotes the j th letter of $v^{(n)}$ (resp. $w^{(n)}$) seen as a word over $\{1, -1\}$.

Lemma 4.4.8. *Let $v^{(n)}$ and $w^{(n)}$ be as in Lemma 4.4.7. Then*

- (i) $v_0^{(n)} = v_{2^n}^{(n)} = 1$, $v_{2^n-1}^{(n)} = \begin{cases} -1, & n \in 2\mathbb{N}_0, \\ 1, & n \in 2\mathbb{N}_0 + 1, \end{cases}$ $v_{2^{n+1}-1}^{(n)} = \begin{cases} 1, & n \in 2\mathbb{N}_0, \\ -1, & n \in 2\mathbb{N}_0 + 1. \end{cases}$
- (ii) $w_0^{(n)} = 1$, $w_{2^n}^{(n)} = -1$, $w_{2^n-1}^{(n)} = \begin{cases} -1, & n \in 2\mathbb{N}_0, \\ 1, & n \in 2\mathbb{N}_0 + 1, \end{cases}$ $w_{2^{n+1}-1}^{(n)} = \begin{cases} -1, & n \in 2\mathbb{N}_0, \\ 1, & n \in 2\mathbb{N}_0 + 1. \end{cases}$

Proof. Note that the word $v^{(n)}$ always starts with 1, and ends with 1 if n is even or -1 if n is odd. Similarly, the word $w^{(n)}$, starts with 1 and ends with -1 if n is even or 1 if n is odd. The properties above then follow from Lemma 4.4.7 by induction. \square

Notice that from the substitution structure, one has

$$\phi^n(a_{0,2i} a_{0,2i+1}) = a_{2i,0} a_{2i,1} \cdots a_{2i,2^n-1} a_{2i+1,0} a_{2i+1,1} \cdots a_{2i+1,2^n-1}.$$

Using this together with Lemma 4.4.8 we get the following.

Lemma 4.4.9. *Let $v^{(2n-1)} = a_{0,0} a_{0,1} \cdots a_{2^n-1, 2^n-1}$ as above. Then*

(i) (From top to left)

If $a_{0,2i} a_{0,2i+1} = v$, then $a_{2i,0} a_{2i+1,0} = v$. If $a_{0,2i} a_{0,2i+1} = w$, then $a_{2i,0} a_{2i+1,0} = w$.

(ii) (From top to right)

If $a_{0,2i} a_{0,2i+1} = v$, then $a_{2i,2^n-1} a_{2i+1,2^n-1}$ is w if n is odd and \tilde{w} if n is even.

If $a_{0,2i} a_{0,2i+1} = w$, then $a_{2i,2^n-1} a_{2i+1,2^n-1}$ is v if n is odd and \tilde{v} if n is even.

There are obvious extensions to the cases when $a_{0,2i} a_{0,2i+1}$ is \tilde{v} or \tilde{w} .

The previous lemma relates words in the topmost row of the matrix to words found along the leftmost and the rightmost columns. We can define the following maps which convert words in the topmost row in the matrix to the words along the rightmost column. Note that v read backwards is still v and that w read backwards is \tilde{w} .

Definition 4.4.10. We define two maps I_{odd} and I_{even} by their action on letters of the alphabet $\{v, w, \tilde{v}, \tilde{w}\}$ and their action on words over the alphabet $\{v, w, \tilde{v}, \tilde{w}\}$, which are given, respectively, by

$$I_{\text{odd}} : \begin{array}{ll} v \mapsto \tilde{w}, & \tilde{v} \mapsto w, \\ w \mapsto v, & \tilde{w} \mapsto \tilde{v}, \end{array} \quad I_{\text{even}} : \begin{array}{ll} v \mapsto w, & \tilde{v} \mapsto \tilde{w}, \\ w \mapsto \tilde{v}, & \tilde{w} \mapsto v, \end{array}$$

and

$$I_*(b_1 b_2 \cdots b_n) = I_*(b_n) I_*(b_{n-1}) \cdots I_*(b_1),$$

where $*$ \in {even, odd} and $b_i \in \{v, w, \tilde{v}, \tilde{w}\}$.

From (ii) in Lemma 4.4.9, the rightmost column, read from bottom to top, is $I_{\text{even}}(v^{(n-1)})$ if n is even and $I_{\text{odd}}(v^{(n-1)})$ if n is odd. Now, we express $I_*(v^{(n-1)})$ as a level- n superword.

Lemma 4.4.11. For $*$ \in {even, odd},

$$I_*(v^{(n-1)}) = \varphi^{n-1}(\tilde{w}) \quad \text{and} \quad I_*(w^{(n-1)}) = \varphi^{n-1}(v).$$

Proof. We present only the proof for the even case and omit the proof for the odd case, which is similar. We proceed by induction. The statement is clear for $n = 2$. If the statement holds for some even n , then for $n + 2$ we have

$$\begin{aligned} I_{\text{even}}(\varphi^{n+1}(v)) &= I_{\text{even}}(\varphi^{n-1} \varphi^2(v)) \\ &= I_{\text{even}}(\varphi^{n-1}(v w v \tilde{w})) \\ &= I_{\text{even}}(\varphi^{n-1}(\tilde{w})) I_{\text{even}}(\varphi^{n-1}(v)) I_{\text{even}}(\varphi^{n-1}(w)) I_{\text{even}}(\varphi^{n-1}(v)) \\ &= \varphi^{n-1}(\tilde{v}) \varphi^{n-1}(\tilde{w}) \varphi^{n-1}(v) \varphi^{n-1}(\tilde{w}) \\ &= \varphi^{n-1}(\tilde{v} \tilde{w} v \tilde{w}) \\ &= \varphi^{n+1}(\tilde{w}). \end{aligned}$$

By a similar computation, we also have $I_{\text{even}}(\varphi^{n-1}(w)) = \varphi^{n-1}(v)$. □

To prove the existence of monochromatic arithmetic progressions, we first need the following result.

Lemma 4.4.12. *The word which appears on the leftmost column of the top left quadrant is $v^{(n-2)}$. The word which appears on the rightmost column of the top-right quadrant, read from bottom to top, is $w^{(n-2)}$.*

Proof. The first claim follows immediately from (i) in Lemma 4.4.9. The second claim follows from (ii) in Lemma 4.4.9, Lemma 4.4.11 and the fact that the word on the upper half of the rightmost quadrant (read from bottom to top) is the second half of $\varphi^{n-1}(\tilde{w}) = \varphi^{n-2}(\tilde{v}w) = \varphi^{n-2}(\tilde{v})\varphi^{n-2}(w)$, which is $w^{(n-2)}$. This is illustrated in Figure 4.4.3. \square

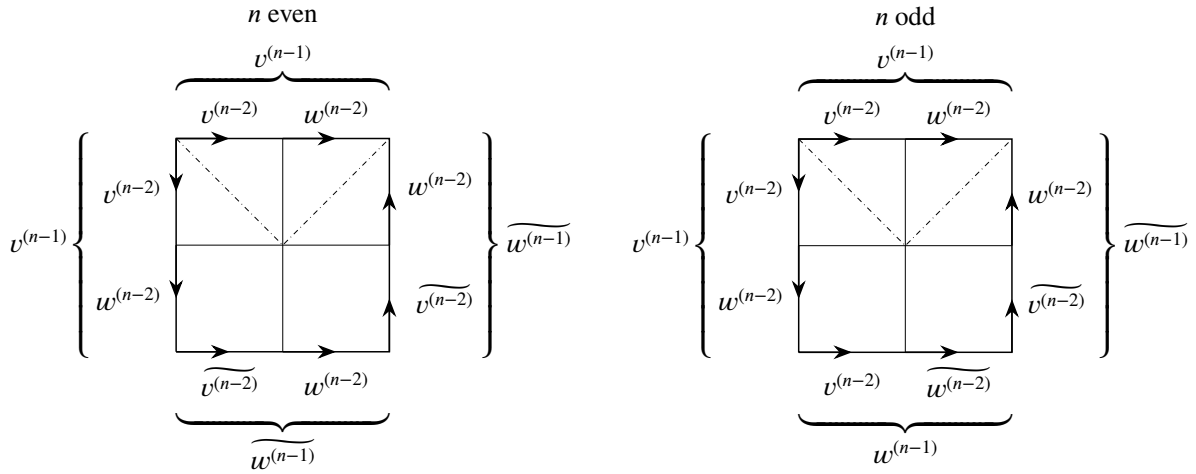


Figure 4.4.3: Schematic representation of block arrangement of the superword $v^{(2n-1)}$; the dashed lines indicate the reflection symmetries of the upper left and upper right quadrants.

Now we can prove the existence of monochromatic diagonals and anti-diagonals.

Proposition 4.4.13. *For all $0 \leq j \leq 2^{n-1} - 1$, one has $a_{j,j} = 1$ (these correspond to the blue diagonals in Figure 4.4.2).*

Proof. Each left half-row $a_{i,0} a_{i,1} \cdots a_{i,2^{n-1}-1}$ is either $v^{(n-2)}$ or $\widetilde{v^{(n-2)}}$ and the topmost half-row (with $i = 0$) is always $v^{(n-2)}$. If $a_{0,j} = 1$, then $a_{j,0} = 1$, by Lemma 4.4.12. This implies that the j th row is $v^{(n-2)}$, which in turn implies that $a_{j,j} = a_{0,j} = 1$. If $a_{0,j} = -1$, then $a_{j,0} = -1$, by Lemma 4.4.12. This implies that the j th row is $\widetilde{v^{(n-2)}}$, and then $a_{j,j} = \widetilde{a_{0,j}} = 1$. \square

Proposition 4.4.14. *If n is odd, then $a_{j,2^n-j-1} = 1$, for all $0 \leq j \leq 2^{n-1} - 1$ (this corresponds to the dark pink diagonal in Figure 4.4.2). If n is even, then $a_{j,2^n-j-1} = -1$, for all $0 \leq j \leq 2^{n-1} - 1$ (these correspond to the light pink diagonals in Figure 4.4.2).*

Proof. The i th right half-row $a_{i,2^{n-1}} a_{i,2^{n-1}+1} \cdots a_{i,2^n-1}$ is either $w^{(n-2)}$ or $\widetilde{w^{(n-2)}}$, and the topmost right half-row is always $w^{(n-2)}$. Assume that n is odd. Then $a_{0,2^n-1} = 1$. If $a_{0,2^n-j-1} = 1$, then $a_{j,2^n-1} = 1$, by Lemma 4.4.12. This implies that the j th right half-row is $w^{(n-2)}$ and it is the same as the topmost right half-row. It follows that $a_{j,2^n-j-1} = a_{0,2^n-j-1} = 1$. If $a_{0,2^n-j-1} = -1$, then $a_{j,2^n-1} = -1$, by

Lemma 4.4.12. This implies that the j th right half-row is $\widetilde{w^{(n-2)}}$. Then $a_{j,2^n-j-1} = \widetilde{a_{0,2^n-j-1}} = 1$. We omit the proof for the case when n is even, which is analogous to the proof presented here. \square

Notice that Proposition 4.4.13 proves the existence of a monochromatic arithmetic progression of difference $d = 2^n + 1$ and length 2^{n-1} , while Proposition 4.4.14 proves the existence of a monochromatic arithmetic progression of difference $d = 2^n - 1$ and length 2^{n-1} . Consequently, we obtain the following corollary, comparable version of Propositions 4.4.3 and 4.4.4 in Section 4.4.1.

Corollary 4.4.15. *For the Rudin–Shapiro sequence, for all positive integers n , $A(2^n \pm 1) \geq 2^{n-1}$.*

4.4.3 The Hadamard sequence

The arguments for the Rudin–Shapiro sequence we used in Section 4.4.1 can be extended to the case when the spin matrix is the Hadamard matrix [54]

$$V = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \quad (4.4.4)$$

and hence, θ is a substitution of the eight-letter alphabet $\mathcal{A} = \mathcal{D} \times C_2 = \{+1, -1\}$, where $\mathcal{D} = \{0, 1, 2, 3\}$. More precisely,

$$\begin{aligned} \theta: \quad 0 &\mapsto 0123, \\ 1 &\mapsto 0\tilde{1}2\tilde{3}, \\ 2 &\mapsto 01\tilde{2}\tilde{3}, \\ 3 &\mapsto 0\tilde{1}\tilde{2}3. \end{aligned}$$

The images of the tilded letters are again determined via the invariance relation $\theta(\tilde{a}) = \widetilde{\theta(a)}$ with number of tildes modulo 2, for $a \in \mathcal{D}$. Similar to what we did in Section 4.4.1, we consider the infinite word u over the alphabet $\{1, -1\}$ obtained from the fixed point of θ starting with 0 under the projection

$$\pi_G: \quad 0, 1, 2, 3 \mapsto 1, \quad \tilde{0}, \tilde{1}, \tilde{2}, \tilde{3} \mapsto -1.$$

We call u a *Hadamard sequence*. Again, the elements of u satisfy Equation (4.4.2), namely, $u_n = \prod_{i=0}^{k-1} V(n_{i+1}, n_i)$, where $[n_k, \dots, n_1, n_0]$ is now the base-4 representation of n . We can easily obtain analogous recurrence relations to those in Equation (4.4.3).

Lemma 4.4.16. *The entries in the Hadamard sequence u satisfy, for all non-negative integers n , the*

following recurrence relations,

$$\begin{aligned}
u_{4n} &= u_n, \\
u_{4n+1} &= \begin{cases} u_n, & \text{if } n \equiv 0 \text{ or } 2 \pmod{4}, \\ -u_n, & \text{otherwise,} \end{cases} \\
u_{4n+2} &= \begin{cases} u_n, & \text{if } n \equiv 0 \text{ or } 1 \pmod{4}, \\ -u_n, & \text{otherwise,} \end{cases} \\
u_{4n+3} &= \begin{cases} u_n, & \text{if } n \equiv 0 \text{ or } 3 \pmod{4}, \\ -u_n, & \text{otherwise.} \end{cases}
\end{aligned}$$

Proof. Let $[n_k, \dots, n_1, n_0]$ be the base-4 representation of n . The base-4 representation of $4n + a$ is $[n_k, \dots, n_1, n_0, a]$, where $a \in \{0, 1, 2, 3\}$, so $u_{4n+a} = u_n \cdot V(n_0, a)$. It is then straightforward to complete the proof by the spin matrix of Equation (4.4.4); we omit the details. \square

The same as in Section 4.4.1 for the Rudin–Shapiro section, in this case $A(d) < \infty$, for all positive integers d . We omit the proof of this fact, which is similar to the proof of Proposition 4.4.2. We can also derive results analogous to Propositions 4.4.3 and 4.4.4. First, we prove the following result.

Lemma 4.4.17. *Consider the Hadamard sequence u . For all positive integers d and n , $A(4^n d) = A(d)$.*

Proof. The claim will follow from $A(4^n d) = A(4^{n-1} d)$, for all positive integers d and n . Next, we prove this.

Let $u_{m+k4^{n-1}d} = a$ be a monochromatic arithmetic progression of difference $4^{n-1}d$ and length $A(4^{n-1}d)$ appearing in u , for $k = 0, 1, \dots, A(4^{n-1}d) - 1$, a non-negative integer m , and $a \in \{1, -1\}$. We know that $u_{m+k4^{n-1}d} = u_{4m+k4^nd}$, by Lemma 4.4.16, which implies that $A(4^n d) \geq A(4^{n-1} d)$.

Conversely, let $u_{m+k4^nd} = a$ be a monochromatic arithmetic progression of difference 4^nd and length $A(4^n d)$ appearing in u , for $k = 0, 1, \dots, A(4^n d) - 1$, a non-negative integer m , and $a \in \{1, -1\}$. There exist non-negative integers i and $j \in \{0, 1, 2, 3\}$ for which $m = 4i + j$, so $u_{m+k4^nd} = u_{4(i+k4^{n-1}d)+j}$. Then, by Lemma 4.4.16,

$$u_{m+k4^nd} = \begin{cases} u_{i+k4^{n+1}d}, & \text{if } j = 0, \\ & \text{or } j = 1 \text{ and } i \equiv 0 \text{ or } 2 \pmod{4}, \\ & \text{or } j = 2 \text{ and } i \equiv 0 \text{ or } 1 \pmod{4}, \\ & \text{or } j = 3 \text{ and } i \equiv 0 \text{ or } 3 \pmod{4}, \\ -u_{i+k4^{n+1}d}, & \text{otherwise.} \end{cases}$$

So, there is a fixed element $b \in \{1, -1\}$ for which $u_{i+k4^{n+1}d} = b$, for $k = 0, 1, \dots, A(4^n d) - 1$. This implies that $A(4^{n+1}d) \geq A(4^n d)$. Therefore $A(4^n d) = A(4^{n-1}d)$, as required. \square

Corollary 4.4.18. *For the Hadamard sequence u , for all non-negative integers n , $A(4^n) = 6$.*

Proof. Let $v \in \mathcal{A}^{\mathbb{N}_0}$ be the fixed point of θ starting with 0; so $u = \pi_G(v)$. It is easy to see, by structure of θ , that we can find six but no more consecutive letters in v with the same spin, hence six but no more consecutive equal letters in u . So $A(1) = 6$. The result then follows by Proposition 4.4.17. \square

The next two propositions, where we find sequences of long monochromatic arithmetic progressions for differences of the form $4^n \pm 1$, are analogous to Propositions 4.4.3 and 4.4.4.

Proposition 4.4.19. *For the Hadamard sequence u , for all positive integers n , $A(4^n + 1) \geq 4^{n-1} + 2$.*

Proof. It is easy to see, by direct inspection of u , that the result holds for $n = 1$. For $n > 1$, we will show that $u_k = 1$, where $k = 4^{2n+1} + m(4^n + 1)$, for all integers $-1 \leq m \leq 4^{n-1}$. Fix n . For $m = -1$, $k = 4^{2n+1} - 4^n - 1$ with base-4 representation given by $[3, \dots, 3, 2, 3, \dots, 3]$, consisting on two sequences of n consecutive 3's separated by a single 2. Then, by Equation (4.4.2), $u_k = 1$. For $0 \leq m \leq 4^{n-1}$, let the base-4 representation of m be $[m_r, \dots, m_1, m_0]$, where $0 \leq r \leq n-1$. Then the base-4 representation of $k = 4^{2n+1} + m(4^n + 1)$ is

$$[1, \overbrace{0, \dots, 0}^{n-r}, m_r, \dots, m_1, m_0, \overbrace{0, \dots, 0}^{n-r-1}, m_r, \dots, m_1, m_0].$$

For $0 \leq r < n-1$, we have $n-r \geq 1$ and $n-r-1 \geq 1$. Then, using Equation (4.4.2), we see that $u_k = 1$. For $r = n-1$, we have $n-r-1 = 0$ and then, by Equation (4.4.2), $u_k = V(m_0, m_r)$. But for $r = n-1$, we also have $m = 4^{n-1} = [1, 0, 0, \dots, 0]$, so $u_k = V(m_0, m_r) = V(0, 1) = 1$. \square

Proposition 4.4.20. *For the Hadamard sequence u , for all positive integers n , $A(4^n - 1) \geq 4^{n-1} + 3$.*

Proof. Let n be a positive integer. To prove the claim we will show that, for all integers $-2 \leq m \leq 4^{n-1}$, $u_k = 1$ with $k = 3 \cdot 4^{2n+2} + 4^n - 1 + m(4^{n+1} - 1)$.

If $m = -2$, $k = 3 \cdot 4^{2n+2} + 4^n - 1 - 2(4^{n+1} - 1)$. One can check that the base-4 representation of k is

$$[2, \overbrace{3, \dots, 3}^n, 2, 1, \overbrace{0, \dots, 0}^{n-1}, 1].$$

Then, by Equation (4.4.2), we see that $u_k = 1$.

If $m = -1$, $k = 3 \cdot 4^{2n+2} + 4^n - 1 - (4^{n+1} - 1)$. One can check that the base-4 representation of k is

$$[2, \overbrace{3, \dots, 3}^{n+1}, 1, \overbrace{0, \dots, 0}^n].$$

Then, by Equation (4.4.2), we see that $u_k = 1$.

If $0 \leq m \leq 4^{n-1}$, write m as $[m_{n-1}, \dots, m_1, m_0]$, where $m_i \in \{0, 1, 2, 3\}$ for all $0 \leq i \leq n-1$. Then one can check that the base-4 representation of k is given by

$$[3, 0, m_{n-1}, \dots, m_1, m_0, 0, \overline{m_{n-1}}, \dots, \overline{m_1}, \overline{m_0}],$$

where $\overline{m_i} = 3 - m_i$. Observe that, for each $0 \leq i \leq n-2$, $V(m_{i+1}, m_i) \cdot V(\overline{m_{i+1}}, \overline{m_i})$ is equal to 1 if $m_{i+1} \in \{m_i, \overline{m_i}\}$, and to -1 otherwise. In other words, $V(m_{i+1}, m_i) \cdot V(\overline{m_{i+1}}, \overline{m_i})$ is given by

$$(-1)^{(m_{i+1}-m_i)(m_{i+1}-\overline{m_i})},$$

which can also be written as

$$(-1)^{m_{i+1}(m_{i+1}-1)} \cdot (-1)^{m_i(m_i-1)}.$$

Since, for any integer x , the product $x(x-1)$ is even, $V(m_{i+1}, m_i) \cdot V(\overline{m_{i+1}}, \overline{m_i}) = 1$. Then, by Equation (4.4.2), $u_k = 1$. This completes the proof. \square

Corollary 4.4.21. *For the Hadamard sequence, for all $d_n = 4^n \pm 1$ with $n \geq 1$, $A(d_n) \gtrsim \frac{d_n}{4}$.*

Proof. The claim follows directly from Propositions 4.4.19 and 4.4.20. \square

Computer experiments suggest that, for the Hadamard sequence,

$$A(2^m) = 6, \quad A(2^n + 1) \geq 2^{n-2} + 2, \quad A(2^n - 1) \geq \begin{cases} 2^{n-2} + 3, & \text{if } n \text{ is even,} \\ 2^{n-2} + 1, & \text{otherwise,} \end{cases}$$

for all integers $m \geq 0$ and $n \geq 2$ considered (see the data underlying this thesis for a list of values of $A(d)$). This may be explored noticing that the Hadamard matrix of Equation 4.4.4 can be written as

$$V = \begin{pmatrix} V' & V' \\ V' & -V' \end{pmatrix} = V' \otimes V',$$

where V' is the Rudin–Shapiro matrix of Equation 4.4.1. We explore this observation no further here.

4.4.4 Vandermonde sequences

In this section we consider general Vandermonde substitutions, the simplest of which is the Rudin–Shapiro substitution. Let be a spin substitution with digit set $\mathcal{D} = \{0, 1, \dots, L-1\} \subseteq \mathbb{N}_0$ and spin group $G = \{1, \omega, \omega^2, \dots, \omega^{L-1}\} \subseteq \mathbb{S}^1$, where \mathbb{S}^1 is the unit circle and $\omega = e^{-2\pi i/L}$. These generate the alphabet $\mathcal{A} = \mathcal{D} \times G$. We will consider the *digit projection* $\pi_{\mathcal{D}} : \mathcal{A} \rightarrow \mathcal{D}$, defined by $\pi_{\mathcal{D}}(a)$ to be the digit of a , and the *spin projection* $\pi_G : \mathcal{A} \rightarrow G$, defined by $\pi_G(a)$ to be spin of a . For each letter $a \in \mathcal{A}$, let $s_a \in \{0, 1, \dots, L-1\} \subseteq \mathbb{N}_0$ be the *spin number* of a , given by the exponent of ω in $\pi_G(a)$. Let the spin matrix V of the spin substitution be a *Vandermonde matrix*, given by $V(k, \ell) = \omega^{k\ell \bmod L}$, for all $k, \ell \in \mathcal{D}$. In matrix form

$$V = \begin{pmatrix} 1 & 1 & 1 & \dots & 1 & 1 \\ 1 & \omega & \omega^2 & \dots & \omega^{L-2} & \omega^{L-1} \\ 1 & \omega^2 & \omega^4 & \dots & \omega^{2(L-2)} & \omega^{2(L-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & \omega^{L-1} & \omega^{(L-1)2} & \dots & \omega^{(L-1)(L-2)} & \omega^{(L-1)(L-1)} \end{pmatrix}.$$

Now, let the spin substitution $\theta : \mathcal{A} \longrightarrow \mathcal{A}^L$ be defined, for each $a \in \mathcal{A}$, by $\theta(a) = a_0 a_1 \cdots a_{L-1}$, where, for each $0 \leq k \leq L-1$, $a_k \in \mathcal{A}$ is such that $\pi_{\mathcal{D}}(a_k) = k$ and

$$\pi_G(a_k) = V(k, \pi_{\mathcal{D}}(a)) \pi_G(a) = \omega^{k \cdot \pi_{\mathcal{D}}(a) + s_a \bmod L}.$$

We call θ a *Vandermonde substitution*.

We call the infinite word u obtained from the fixed point of θ starting with 0 under the projection π_G a *Vandermonde sequence*. The first few terms of u (with commas inserted for the sake of clarity) are

$$u = \overbrace{1, 1, \dots, 1}^L, 1, \omega, \omega^2, \dots, \omega^{L-2}, \omega^{L-1}, 1, \omega^2, \omega^3, \dots, \omega^{L-1}, \omega, 1, \omega^3, \omega^4, \dots.$$

The n th element of u can be obtained from V using again Equation (4.4.2), namely, $u_n = \prod_{i=0}^{k-1} V(n_{i+1}, n_i)$, where $[n_k, \dots, n_1, n_0]$ is now the base- L representation of n . Using this we can prove the following lemma, which gives analogous recurrence relations to those in Equation (4.4.3) for the Rudin–Shapiro sequence.

Lemma 4.4.22. *The entries of the Vandermonde sequence u satisfy, for all $n \in \mathbb{N}_0$ and each $a \in \mathcal{D}$, the recurrence relation $u_{Ln+a} = V(a, b) u_n$, where $b \in \mathcal{D}$ is such that $n \equiv b \bmod L$.*

Proof. Let $[n_k, \dots, n_1, n_0]$ be the base- L representation of $n \in \mathbb{N}_0$. For each $0 \leq a \leq L-1$, the base- L representation of $Ln+a$ is $[n_k, \dots, n_1, n_0, a]$ and so $u_{Ln+a} = V(a, n_0) u_n$, where we noted that, since V is symmetric under the main diagonal, $V(n_0, a) = V(a, n_0)$. Defining $b = n_0$, we see that $u_{Ln+a} = V(a, b) u_n$ and, since $n = L \cdot [n_k, \dots, n_1] + b$, we also see that $n \equiv b \bmod L$, as required. \square

A simple argument, similar to that used in Proposition 4.4.2, can be used to show that, for the Vandermonde sequence, $A(d) < \infty$, for all positive integers d .

Proposition 4.4.23. *Every monochromatic arithmetic progression appearing in the Vandermonde sequence u has finite length.*

Proof. We start by assuming the existence of an infinitely long monochromatic arithmetic progression in u and prove that it leads to a contradiction. Assume there exist $s \in \mathbb{N}_0$ and $d \in \mathbb{N}$ such that $u_{s+nd} = g$, for some $g \in G$ and all $n \in \mathbb{N}_0$. Then $u_{s+nLd} = g$, for all $n \in \mathbb{N}_0$. Let $v \in \mathcal{A}^{\mathbb{N}_0}$ be the fixed point of θ starting with 0, hence $u = \pi_G(v)$. Then $\pi_G(v_{s+nLd}) = g$, for all $n \in \mathbb{N}_0$. Furthermore, from how θ is defined, we see that there must exist some $k \in \mathcal{D}$ such that $\pi_{\mathcal{D}}(v_{s+nLd}) = k$, for all $n \in \mathbb{N}_0$. Therefore, v contains an infinitely long monochromatic arithmetic progression. But, since θ is an aperiodic, primitive, constant-length substitution of height 1, this is a contradiction, by Proposition 4.1.4. \square

The following lemma determines $A(d)$ for differences d which are multiples of powers of L .

Proposition 4.4.24. *For the Vandermonde sequence u , for all positive integers d and n , $A(L^n d) = A(d)$.*

Proof. The claim will follow from $A(L^n d) = A(L^{n-1} d)$, for all positive integers d and n . Next, we prove this.

Let $u_{m+kL^{n-1}d} = g$ be a monochromatic arithmetic progression of difference $L^{n-1}d$ and length $A(L^{n-1}d)$ appearing in u , for $k = 0, 1, \dots, A(L^{n-1}d) - 1$, a non-negative integer m , and $g \in G$. By Lemma 4.4.22, $u_{m+kL^{n-1}d} = u_{Lm+kL^n d}$, which implies that $A(L^n d) \geq A(L^{n-1} d)$.

Conversely, let $u_{m+kL^n d} = g$ be a monochromatic arithmetic progression of difference $L^n d$ and length $A(L^n d)$ appearing in u , for $k = 0, 1, \dots, A(L^n d) - 1$, a non-negative integer m , and $g \in G$. There exist a non-negative integer i and $a \in \mathcal{D}$ for which $m = iL + a$, so $u_{m+kL^n d} = u_{L(i+kL^{n-1}d)+a}$. Then, by Lemma 4.4.22, $u_{m+kL^n d} = V(a, b)u_{i+kL^{n-1}d}$, where $b \in \mathcal{D}$ is such that $b \equiv i \pmod{L}$. Defining $h = V(a, b)$, which is a fixed element of G , we see that $u_{i+kL^{n-1}d} = h^{-1}g$, for $k = 0, 1, \dots, A(L^{n-1}d) - 1$. This implies that $A(L^{n-1}d) \geq A(L^n d)$. Therefore $A(L^n d) = A(L^{n-1}d)$, as required. \square

Corollary 4.4.25. *For the Vandermonde sequence u , for all non-negative integers n , $A(L^n) = L + 2$.*

Proof. For the sake of readability, in this proof, a letter in the alphabet $\mathcal{A} = \mathcal{D} \times G$ with digit $x \in \mathcal{D}$ and spin $g \in G$ will be denoted by x_g . Let $v \in \mathcal{A}^{\mathbb{N}_0}$ be the fixed point of θ starting with 0_1 . Since the word $\theta(0_1)$ contains the subword $0_1 1_1$, the word $\theta^2(0_1)$ contains the subword $(L-1)_1 0_1$, which implies that $\theta^3(0_1)$ contains the subword $(L-1)_\omega 0_1 1_1$, where ω is the L th root of unity $e^{-2\pi i/L}$. Notice that, for any positive integer k , the last letter of $\theta^k((L-1)_\omega)$ is $(L-1)_{\omega^{k+1}}$ and the first $L+1$ letters of $\theta^k(0_1 1_1)$ are $0_1 1_1 \dots (L-1)_1 0_1$. Since the powers of ω have to be taken modulo L (hence $\omega^{kL} = 1$), we see that, for $L = 2, 3, \dots$, the word $\theta^{L+2}(0_1)$ contains the subword $(L-1)_1 0_1 1_1 \dots (L-1)_1 0_1$ comprising $L+2$ letters with spin 1. Furthermore, v cannot contain a subword of more than $L+2$ consecutive letters with spin 1, otherwise it necessarily occurs in the image under θ of a word containing the subword $0_1 0_1$, which is not in the language of θ . Observe that the same argument is true if the spin 1 is replaced by any $g \in G$. Therefore, the maximum length of a subword of v consisting of letters all of which have the same spin is $L+2$ and, since $u = \pi_G(v)$, we have, for the sequence u , that $A(1) = L+2$. The result then follows by Proposition 4.4.24. \square

As an analogy with the Rudin–Shapiro sequence, in the following proposition we look at the differences of the form

$$L^{(L-1)n} + L^{(L-2)n} + \dots + L^n + 1 = \frac{L^{nL} - 1}{L^n - 1}.$$

Proposition 4.4.26. *Consider the Vandermonde sequence u . For all positive integers n ,*

$$A\left(\frac{L^{nL} - 1}{L^n - 1}\right) \geq L^{n-1} + 1.$$

Proof. Let us first consider the case $n = 1$. Note that $u_1 = 1$. Next, we will show that $u_{d+1} = 1$, where $d = \frac{L^L - 1}{L - 1}$, which will imply that $A(d) \geq 2$, as required. For $L = 2$, the binary representation of $d+1 = 4$ is $[1, 0, 0]$, so $u_4 = V(1, 0) \cdot V(0, 0) = 1$, by Equation (4.4.2). For $L > 2$, since the base- L representation of d consists of L digits equal to 1, the base- L representation of $d+1$ consist of $L-1$ digits equal to 1

and the least significant digit equal to 2, that is, $[1, \dots, 1, 1, 2]$. So

$$u_{d+1} = (V(1, 1))^{L-2} \cdot V(1, 2) = \omega^{L-2} \cdot \omega^2 = \omega^{L \bmod L} = 1.$$

Let us now consider the case $n > 1$. To prove the claim, we will show that $u_k = 1$, where $k = L^{Ln+1} + m(L^{(L-1)n} + \dots + L^n + 1)$, for all integers $0 \leq m \leq L^{n-1}$. Let the base- L representation of m be $[m_r, \dots, m_1, m_0]$, where $0 \leq r \leq n-1$. Then the base- L representation of k is given by

$$\overbrace{[1, 0, \overbrace{0, \dots, 0}^{n-r-1}, m_r, \dots, m_1, m_0, \dots, \dots, \overbrace{0, \dots, 0}^{n-r-1}, m_r, \dots, m_1, m_0]}^L].$$

For $0 \leq m \leq L^{n-1} - 1$, we have $n - r - 1 \geq 1$ and, by Equation (4.4.2), $u_k = \prod_{i=0}^{r-1} (V(m_{i+1}, m_i))^L = 1$. For $m = L^{n-1}$, we have $n - r - 1 = 0$, but also $m_i = 0$, for all $0 \leq i \leq r - 1$. Consequently, the base- L representation of k consists of $L + 1$ isolated digits equal to 1 separated by sequences of digits equal to 0, which, by Equation (4.4.2), implies that $u_k = 1$. \square

We notice that the arithmetic progression of 1's found in the proof of Proposition 4.4.26 cannot be extended to the right. Indeed, since the base- L representation of $m = L^{n-1} + 1$ is of the form $[1, 0, \dots, 0, 1]$, with two digits equal to 1 separated by $n - 2$ digits equal to 0, the base- L representation of $k = L^{Ln+1} + m(L^{(L-1)n} + \dots + L^n + 1)$ is

$$\overbrace{[1, 0, 1, \overbrace{0, \dots, 0}^{n-2}, 1, 1, \overbrace{0, \dots, 0}^{n-2}, 1, \dots, \dots, 1, \overbrace{0, \dots, 0}^{n-2}, 1, 1, \overbrace{0, \dots, 0}^{n-2}, 1]}^L].$$

This implies that $u_k = (V(1, 1))^{L-1} = \omega^{L-1} \neq 1$.

We also notice that the arithmetic progression of 1's can neither be extended to the left, except if $L = 2$. Indeed, the base- L representation of $k = L^{Ln+1} - (L^{(L-1)n} + \dots + L^n + 1)$ can be checked to be

$$\overbrace{[\overbrace{L-1, \dots, L-1}^n, L-2, \overbrace{L-1, \dots, L-1}^{n-1}, \dots, L-2, \overbrace{L-1, \dots, L-1}^{n-1}, L-2, \overbrace{L-1, \dots, L-1}^n]}^{L-2}],$$

and so, by Equation (4.4.2),

$$u_k = (V(L-1, L-1))^{L(n-2)+2} (V(L-1, L-2))^{L-1} (V(L-2, L-1))^{L-1}.$$

Since $V(L-1, L-1) = \omega$ and $V(L-1, L-2) = V(L-2, L-1) = \omega^2$, we see that $u_k = \omega^{L-2}$, which is equal to 1 only if $L = 2$. This yields Proposition 4.4.3 for the Rudin-Shapiro sequence as a corollary.

Corollary 4.4.27. *For the Vandermonde sequence, $A(d_n) \gtrsim \frac{d_n^\alpha}{L}$, where*

$$\alpha = \frac{1}{L-1} \quad \text{and} \quad d_n = \frac{L^{nL} - 1}{L^n - 1},$$

for all positive integers n . In particular, for the Rudin–Shapiro sequence, $A(d_n) \gtrsim \frac{d_n}{2}$.

Proof. The claim follows directly from Propositions 4.4.26. □

Theorem 4.0.2 follows directly from Corollary 4.4.27.

Example 4.4.28. To look upon a particular Vandermonde sequence other than the Rudin–Shapiro sequence, consider $L = 3$ (see, for example, [31, Example 4.1]). In this case, the digit set is $\mathcal{D} = \{0, 1, 2\}$, the spin group is $G = C_3$ and the spin matrix is

$$V = \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix},$$

where $\omega = e^{-2\pi i/3}$. We write the alphabet $\mathcal{A} = G \times \mathcal{D}$ as $\{0, \tilde{0}, \tilde{\tilde{0}}, 1, \tilde{1}, \tilde{\tilde{1}}, 2, \tilde{2}, \tilde{\tilde{2}}\}$, where ‘tilded’ and ‘double-tilded’ letters have different non-trivial spins. The Vandermonde substitution is

$$\begin{aligned} 0 &\mapsto 0\,1\,2, \\ \theta: 1 &\mapsto 0\,\tilde{1}\,\tilde{\tilde{2}}, \\ 2 &\mapsto 0\,\tilde{\tilde{1}}\,\tilde{2}, \end{aligned}$$

where we have omitted the images of the tilded and double-tilded letters. The Vandermonde sequence u is obtained from the fixed point of θ starting with 0 under the projection

$$\pi_G: \quad 0, 1, 2 \mapsto 1, \quad \tilde{0}, \tilde{1}, \tilde{2} \mapsto \omega, \quad \tilde{\tilde{0}}, \tilde{\tilde{1}}, \tilde{\tilde{2}} \mapsto \omega^2.$$

The n th element of u is given by $u_n = \prod_{i=0}^{k-1} V(n_{i+1}, n_i)$, where $[n_k, \dots, n_1, n_0]$ is the ternary representation of n . The recurrence relations arising from Lemma 4.4.22 are

$$u_{3n} = u_n, \quad u_{3n+1} = \begin{cases} u_n, & \text{if } n \equiv 0 \pmod{3}, \\ \omega u_n, & \text{if } n \equiv 1 \pmod{3}, \\ \omega^2 u_n, & \text{if } n \equiv 2 \pmod{3}, \end{cases} \quad u_{3n+2} = \begin{cases} u_n, & \text{if } n \equiv 0 \pmod{3}, \\ \omega^2 u_n, & \text{if } n \equiv 1 \pmod{3}, \\ \omega u_n, & \text{if } n \equiv 2 \pmod{3}, \end{cases}$$

Every monochromatic arithmetic progression occurring in the sequence u is finite and, by Proposition 4.4.26, $A(3^{2n} + 3^n + 1) \geq 3^{n-1} + 1$, for all positive integers n . A list of $A(d)$ can be found in the data underlying this thesis. ❖

5. FORWARD LIMIT SETS OF SEMIGROUPS OF SUBSTITUTIONS

In the preceding two chapters, the objects of interest were individual sequences, which were fixed points of a substitution. In this chapter, by contrast, we consider complete forward limit sets of substitution semigroups. We recall from Chapter 2 that a substitution semigroup S is a semigroup generated by a family \mathcal{F} of substitutions of an alphabet \mathcal{A} under functional composition. We recall also that the forward limit set $\Lambda(A)$ of a subset A of \mathcal{A} for S is $\overline{S(A)} \setminus S(A)$, and the forward limit set Λ of S is $\Lambda(\mathcal{A})$ (see Definition 2.5.14).

The notion of forward limit set is richer for substitution semigroups than for individual substitutions, for which only the periodic points of the substitution populate the forward limit set (see Lemma 2.4.12). By definition, Λ is the boundary of $S(\mathcal{A})$ and, as such, contains all the fixed points of elements of S and, in general, many other points. The main objective of this chapter is to characterise forward limit sets and to determine the size of such limit sets.

We show that Λ typically coincides with the set of all possible s -adic limits of \mathcal{F} (see Theorem 5.4.1). Next, we characterise forward limit sets by invariant sets. We show that a necessary and sufficient condition for a set of infinite words to be closed and strongly S -invariant is that it is the forward limit set of some subset of the alphabet (see Theorem 5.4.16). This implies that Λ is the unique maximal closed and strongly S -invariant set of infinite words. We also prove that Λ is the closure of the image under S of the set of all fixed points of S (see Theorem 5.4.24).

Having characterised forward limit sets, we move towards determining their size. We first give certain assumptions under which a forward limit set is uncountable (see Theorem 5.5.2). Therefore, Λ typically cannot be too small. We show that, nonetheless, it can neither be too large. More precisely, we give upper bounds on the size of Λ in terms of logarithmic Hausdorff dimension (see Theorem 5.5.7).

We finish the chapter with a characterisation of the hull of S by its invariant properties. We prove that, under mild assumptions, the hull is the smallest possible closed, S -invariant and shift-invariant non-empty set of infinite words (see Theorem 5.6.5). We also show that, if S is primitive, its hull is uniquely determined by the set of fixed points of S (see Theorem 5.6.6).

The chapter is organised as follows. In Section 5.2 we give the growing condition which is equivalent to S being fixed-letter-free. In Section 5.3 we study some basic properties of Λ . In Section 5.4 we provide the several characterisations of Λ , first by s -adic limits (Section 5.4.1), next by invariant sets (Section 5.4.2), and finally by fixed points of S (Section 5.4.3). In Section 5.5 we study the size of Λ , first showing that it is typically uncountable (Section 5.5.1) and next, giving upper bounds on its size in terms of logarithmic Hausdorff dimension (Section 5.5.2). In Section 5.6, we characterise the hull of S .

5.1 Preliminaries

Before diving into the contents of this chapter, we recall some definitions from Chapter 2 that will be used in the subsequent sections. In this chapter we index the letters of words starting by 1; accordingly we denote the set of infinite words over \mathcal{A} by $\mathcal{A}^{\mathbb{N}}$. We write $\pi_k(w)$ for the k th letter of a word w (see Section 2.2.2). In particular, the first letter of w is $\pi_1(w)$. For a substitution semigroup S generated by a family \mathcal{F} of substitutions, we use the map $F : \mathcal{F}^+ \longrightarrow S$ that sends $f_1 f_2 \dots f_n$ to $f_1 \circ f_2 \circ \dots \circ f_n$ (see Section 2.5.3). We obtain an action of S on \mathcal{A} by defining $f[a] = \pi_1(f(a))$, for $f \in S$ and $a \in \mathcal{A}$ (see Section 2.5.4).

5.2 Fixed-letter-free substitution semigroups

A substitution semigroup S of the alphabet \mathcal{A} is *fixed-letter-free* if each substitution f in S satisfies $f(a) \neq a$, for all $a \in \mathcal{A}$. In this section we prove that the fixed-letter-free property for a substitution semigroup is equivalent to a growth condition for images of letters under the semigroup (Theorem 5.2.5).

We begin with a lemma that later on we will apply to the alphabet \mathcal{A} and to the alphabet \mathcal{F} . For this reason, we state the lemma using a different notation for the alphabet altogether.

Lemma 5.2.1. *Let \mathcal{X} be a finite alphabet and let (u_n) be an infinite sequence of words over \mathcal{X} for which $|u_n| \rightarrow \infty$ as $n \rightarrow \infty$. Then there is a subsequence (v_n) of (u_n) of the form*

$$v_n = x_1 x_2 \dots x_n w_n, \quad n = 1, 2, \dots,$$

where x_1, x_2, \dots are letters of \mathcal{X} and w_1, w_2, \dots are words over \mathcal{X} .

Proof. We will define a chain $I_0 \supseteq I_1 \supseteq I_2 \supseteq \dots$ of infinite subsets of \mathbb{N} (where $I_0 = \mathbb{N}$) and a sequence of letters x_1, x_2, \dots of \mathcal{X} with the property that, for each $k \in I_n$, we have $|u_k| > n$ and $\pi_i(u_k) = x_i$, for $i = 1, 2, \dots, n$.

To do this, suppose that I_0, I_1, \dots, I_{n-1} and x_1, x_2, \dots, x_{n-1} have been constructed with this property, where $n \geq 1$. Let I_{n-1}^* be the infinite subset of I_{n-1} of those integers k for which $|u_k| > n$. Now, there are only finitely many choices for the letter $\pi_n(u_k)$, for $k \in I_{n-1}^*$. Since I_{n-1}^* is infinite, we can choose an infinite subset I_n of I_{n-1}^* and a letter x_n of \mathcal{X} for which $\pi_n(u_k) = x_n$, for all $k \in I_n$. Thus I_0, I_1, \dots, I_n and x_1, x_2, \dots, x_n have the required property, and the existence of the full chain I_1, I_2, \dots and sequence x_1, x_2, \dots follows from the axiom of dependent choices (see, for example, [65, 69]).

We now choose $i_n \in I_n$, for $n = 1, 2, \dots$, and define $v_n = u_{i_n}$. This sequence (v_n) is of the form specified in the lemma. \square

Remark 5.2.2. Sometimes we apply the reverse form of Lemma 5.2.1, in which $v_n = w_n x_n x_{n-1} \dots x_1$, for $x_i \in \mathcal{X}$ and $w_n \in \mathcal{X}^+$. This can be obtained quickly from Lemma 5.2.1 by judicious use of the operation that reverses the letters of a word. \diamond

The next lemma provides conditions under which a substitution must have a fixed letter.

Lemma 5.2.3. *Let f be a substitution of an alphabet \mathcal{A} and let u be a word over \mathcal{A} with $|f(u)| = |u|$ and $\pi_1(f(u)) = \pi_1(u)$. Then f fixes the letter $\pi_1(u)$.*

Proof. Let $u = a_1 a_2 \dots a_n$, where $a_i \in \mathcal{A}$. Then $a_1 = \pi_1(u)$ and

$$|f(a_1)| + |f(a_2)| + \dots + |f(a_n)| = |f(u)| = |u| = n.$$

Hence $|f(a_1)| = |f(a_2)| = \dots = |f(a_n)| = 1$; in particular, $|f(a_1)| = 1$. It follows that $f(a_1)$ is a single letter. Now, $\pi_1(f(a_1)) = \pi_1(f(u))$ (because $a_1 = \pi_1(u)$), so we see that

$$f(a_1) = \pi_1(f(a_1)) = \pi_1(f(u)) = \pi_1(u) = a_1,$$

as required. □

Corollary 5.2.4. *Let f be a substitution of an alphabet \mathcal{A} . Then f has a fixed letter in \mathcal{A} if, and only if, it has a fixed word in \mathcal{A}^+ .*

Proof. Suppose that f fixes a word w over \mathcal{A} . Then $f(w) = w$. Applying Lemma 5.2.3, we see that f fixes the letter $\pi_1(w)$. The converse implication is immediate. □

We can now prove the main theorem of this section.

Theorem 5.2.5. *Let S be a substitution semigroup with finite generating set \mathcal{F} . Then S has the fixed-letter-free property if, and only if,*

$$\min\{|f_1 \circ f_2 \circ \dots \circ f_n(a)| : f_i \in \mathcal{F}\} \rightarrow \infty \quad \text{as } n \rightarrow \infty,$$

for each $a \in \mathcal{A}$.

Proof. Suppose first that there is a substitution g in S and a letter a in \mathcal{A} with $g(a) = a$. We can find generators g_1, g_2, \dots, g_m in \mathcal{F} with $g = g_1 \circ g_2 \circ \dots \circ g_m$. Then

$$|(g_1 \circ g_2 \circ \dots \circ g_m)^n(a)| = |g^n(a)| = |a| = 1,$$

for all positive integers n . Consequently,

$$\min\{|f_1 \circ f_2 \circ \dots \circ f_n(a)| : f_i \in \mathcal{F}\} \not\rightarrow \infty \quad \text{as } n \rightarrow \infty.$$

Conversely, suppose that

$$\min\{|f_1 \circ f_2 \circ \dots \circ f_n(a)| : f_i \in \mathcal{F}\} \not\rightarrow \infty \quad \text{as } n \rightarrow \infty,$$

for some letter a in \mathcal{A} . Then there are a positive integer N and a sequence (u_n) in \mathcal{F}^+ with $|u_1| < |u_2| < \dots$ and

$$|F(u_n)(a)| \leq N,$$

for $n = 1, 2, \dots$. Since \mathcal{F} is finite, we can apply Lemma 5.2.1 (reverse form) to find a subsequence (v_n) of (u_n) with $v_n = w_n f_n f_{n-1} \dots f_1$, where $f_i \in \mathcal{F}$ and $w_n \in \mathcal{F}^+$. Let $F_n = f_n \circ f_{n-1} \circ \dots \circ f_1$. Then $F(v_n) = F(w_n) \circ F_n$, so

$$|F_n(a)| \leq |F(w_n)(F_n(a))| = |F(v_n)(a)| \leq N.$$

Additionally, $|F_{n+1}(a)| = |f_{n+1}(F_n(a))| \geq |F_n(a)|$, so the sequence $|F_1(a)|, |F_2(a)|, \dots$ is eventually constant. Then, because \mathcal{A} is finite, we can find positive integers r and s (with $r > s$) for which $|F_r(a)| = |F_s(a)|$ and $\pi_1(F_r(a)) = \pi_1(F_s(a))$. We can now apply Lemma 5.2.3 with $f = f_r \circ f_{r-1} \circ \dots \circ f_{s+1}$ and $u = F_s(a)$ to see that f fixes the letter $\pi_1(u)$, as required. \square

Example 5.2.6. Consider a substitution semigroup S generated by a set \mathcal{F} of three substitutions f, g and h of the alphabet $\{a, b, c\}$, which satisfy $f(a) = b, g(b) = c$ and $h(c) = a$. Then $h \circ g \circ f(a) = a$ and since $(h \circ g \circ f)^n(a) \not\rightarrow \infty$ as $n \rightarrow \infty$, S does not have the fixed-letter-free property. Observe that none of the generators from \mathcal{F} needs to fix any letter in \mathcal{A} for S not to be a fixed-letter-free substitution semigroup. \diamond

A straightforward corollary of the previous theorem is that, given a finite set of substitutions \mathcal{F} , we can check in a finite number of steps whether the substitution semigroup generated by \mathcal{F} has the fixed-letter-free property.

Corollary 5.2.7. *A substitution semigroup S with finite generating set \mathcal{F} is fixed-letter-free if, and only if, no substitution in $\{f_1 \circ f_2 \circ \dots \circ f_n : f_i \in \mathcal{F}, n = 1, 2, \dots, |\mathcal{A}|\}$ fixes any letter in \mathcal{A} .*

Proof. If S is fixed-letter-free, no substitution of the form $f_1 \circ f_2 \circ \dots \circ f_n$ with $f_i \in \mathcal{F}$ can fix any letter in \mathcal{A} because, otherwise, there exists a letter $b \in \mathcal{A}$ such that $|(f_1 \circ f_2 \circ \dots \circ f_n)^m(b)| \not\rightarrow \infty$ as $m \rightarrow \infty$, which is incompatible with the fixed-letter-free property.

The converse proof is, essentially, the same as in Theorem 5.2.5. Observe that the positive integers s and r used in that proof satisfy $1 \leq r - s \leq |\mathcal{A}|$, by the pigeonhole principle. This implies that there exists a substitution $f = f_r \circ f_{r-1} \circ \dots \circ f_{s+1}$ with $f_i \in \mathcal{F}$ that fixes some letter $b \in \mathcal{A}$. We can rewrite f as $g_1 \circ g_2 \circ \dots \circ g_n$ with $g_i \in \mathcal{F}$, where $n = r - s \leq |\mathcal{A}|$, which completes the proof. \square

5.3 Properties of forward limit sets

In this section we explore some of the basic properties of forward limit sets. Let S be a semigroup generated by a finite set of substitutions \mathcal{F} of an alphabet \mathcal{A} . We recall that the forward limit set of a subset A of \mathcal{A} for S is $\Lambda(A) = \overline{S(A)} \setminus S(A)$. Since \mathcal{A}^+ has the discrete topology, $\overline{S(A)}$ does not accumulate in \mathcal{A}^+ , and so the set $\Lambda(A)$ is contained wholly within $\mathcal{A}^\mathbb{N}$. Evidently it is a closed subset of $\mathcal{A}^\mathbb{N}$ (it is the boundary of $S(A)$ in $\tilde{\mathcal{A}}$). We will prove that $\Lambda(A)$ is invariant under S , which, as we recall, means that $S(\Lambda(A)) \subseteq \Lambda(A)$.

Lemma 5.3.1. *The forward limit set $\Lambda(A)$ of a subset A of \mathcal{A} for a substitution semigroup S is invariant under S .*

Proof. Let $x \in \Lambda(A)$ and $g \in S$. Then there exist sequences (F_n) in S and (a_n) in A with $F_n(a_n) \rightarrow x$. Since \mathcal{A} is finite we can assume by passing to a subsequence that in fact all the letters a_n are equal, that is, $a_n = a$ for some letter a . Hence $F_n(a) \rightarrow x$. Observe that $(g \circ F_n)$ is also a sequence in S and $g \circ F_n(a) \rightarrow g(x)$ by continuity of g . Hence $g(x) \in \Lambda(A)$. Thus $\Lambda(A)$ is S -invariant, as required. \square

We record another elementary lemma, which is used often.

Lemma 5.3.2. *Let S be a substitution semigroup. Then*

$$\Lambda(A) = \bigcup_{a \in A} \Lambda(a),$$

for any subset A of \mathcal{A} .

Proof. We have $S(A) = \bigcup S(a)$, by definition. Hence $\overline{S(A)} = \overline{\bigcup S(a)}$ because \mathcal{A} is finite. Note also that $\overline{S(a)} \setminus S(a) = \overline{S(a)} \setminus S(A)$, for $a \in A$, because $S(A) \subseteq \mathcal{A}^+$. Hence

$$\bigcup_{a \in A} \Lambda(a) = \bigcup_{a \in A} \overline{S(a)} \setminus S(a) = \bigcup_{a \in A} \overline{S(a)} \setminus S(A) = \overline{S(A)} \setminus S(A) = \Lambda(A),$$

as required. \square

Thus we can describe all forward limit sets for S in terms of the forward limit sets $\Lambda(a)$, where $a \in \mathcal{A}$. We will explore how to use the first-letter graph $G_{\mathcal{F}}$ of \mathcal{F} to understand how the forward limit sets of individual letters are related (we introduced first-letter graphs of substitution systems in Section 2.5.5). The next two lemmas will assist us with this task.

Lemma 5.3.3. *Let g be a substitution of an alphabet \mathcal{A} . Let $x, y \in \tilde{\mathcal{A}}$, and suppose that $\pi_1(x) = \pi_1(y)$. Then*

$$d(g(x), g(y)) \leq \frac{1}{2^{|g(a)|}},$$

where $a = \pi_1(x)$.

Proof. Let $x = a_1 a_2 \dots$ and $y = b_1 b_2 \dots$, for $a_i, b_j \in \mathcal{A}$, where $a_1 = b_1 = a$. Then $g(x) = g(a_1)g(a_2) \dots$ and $g(y) = g(b_1)g(b_2) \dots$. Consequently, the first $|g(a)|$ letters of $g(x)$ and $g(y)$ coincide, so the inequality follows. \square

Lemma 5.3.4. *Let (x_n) and (y_n) be sequences in $\tilde{\mathcal{A}}$ with $\pi_1(x_n) = \pi_1(y_n)$, for $n = 1, 2, \dots$, and let $x \in \mathcal{A}^{\mathbb{N}}$. Suppose that (F_n) is a sequence of substitutions of \mathcal{A} for which $F_n(x_n) \rightarrow x$ and $|F_n(a_n)| \rightarrow \infty$, where $a_n = \pi_1(x_n)$. Then $F_n(y_n) \rightarrow x$.*

Proof. By Lemma 5.3.3, we have

$$d(F_n(x_n), F_n(y_n)) \leq d(F_n(x_n), F_n(a_n)) + d(F_n(a_n), F_n(y_n)) \leq \frac{2}{2^{|F_n(a_n)|}}.$$

Since $|F_n(a_n)| \rightarrow \infty$, we see that $F_n(y_n) \rightarrow x$, as required. \square

Now we return to the task of relating forward limit sets using the first-letter graph.

Lemma 5.3.5. *Let S be a substitution semigroup and let \mathcal{F} be a generating set of S . Suppose that there is a directed walk in $G_{\mathcal{F}}$ from one letter a to another letter b . Then $\Lambda(b) \subseteq \Lambda(a)$.*

Proof. That there is a directed walk in $G_{\mathcal{F}}$ from a to b implies that there is an element g of S with $g[a] = b$. We define $w = g(a)$, so $\pi_1(w) = b$. Suppose now that $x \in \Lambda(b)$. Then there is a sequence (F_n) in S with $F_n(b) \rightarrow x$. Since x is an infinite word, $|F_n(b)| \rightarrow \infty$, so we can apply Lemma 5.3.4 to see that $F_n(w) \rightarrow x$. Now, $F_n(w) = F_n \circ g(a)$, and $(F_n \circ g)$ is itself a sequence in S , so we see that $x \in \Lambda(a)$, as required. \square

An immediate corollary of Lemma 5.3.5 is that the forward limit sets of letters in the same strongly connected component of $G_{\mathcal{F}}$ coincide.

Corollary 5.3.6. *Let S be a substitution semigroup and let \mathcal{F} be a generating set of S . Suppose that letters a and b lie in the same strongly connected component of $G_{\mathcal{F}}$. Then $\Lambda(a) = \Lambda(b)$.*

Example 5.3.7. Considered the substitutions f and g of the alphabet $\{a, b, c, d, e\}$, given by

$$\begin{array}{ll} a \mapsto aa, & a \mapsto b, \\ b \mapsto c, & b \mapsto e, \\ f: c \mapsto d, & \text{and } g: c \mapsto cc, \\ d \mapsto dd, & d \mapsto cd, \\ e \mapsto ee, & e \mapsto d. \end{array}$$

In Figure 5.3.1 we see the first-letter graph for $\{f, g\}$ with labels for loops omitted, and the inclusions of the forward limit sets. Observe that vertices c and d form a strongly connected component and, by Corollary 5.3.6, $\Lambda(c) = \Lambda(d)$. By Lemma 5.3.5, $\Lambda(d) \subseteq \Lambda(e) \subseteq \Lambda(b) \subseteq \Lambda(a)$, but the second inclusion must be an equality because $f[e] = g[b] = e$, and $f[b] = c$, $g[e] = d$ and $\Lambda(c) = \Lambda(d)$.

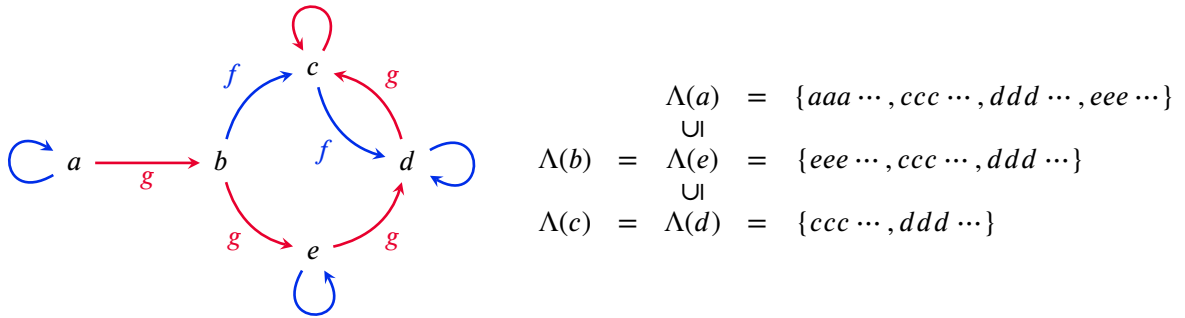


Figure 5.3.1: First-letter graph for $\{f, g\}$ and inclusions of forward limit sets.

❖

One could establish further properties of the relationships between forward limit sets of strongly connected components of $G_{\mathcal{F}}$ in terms of the graph $G_{\mathcal{F}}$. For example, the forward limit sets of two strongly connected components intersect if, and only if, there is a directed walk from both of these components to a common vertex. We explore these relationships no further here.

We finish this section with one final theorem on forward limit sets. In this theorem we use the notation $\pi_1(X)$ for the set $\{\pi_1(x) : x \in X\}$.

Theorem 5.3.8. *Let S be a fixed-letter-free substitution semigroup, let \mathcal{F} be a generating set of S , and let X be a forward limit set of some subset of \mathcal{A} for S . Then $X = \Lambda(A)$, where $A = \pi_1(X)$.*

Proof. First we show that $\Lambda(A) \subseteq X$. To this end, choose $x \in \Lambda(A)$. Then there exists $a \in A$ and a sequence (F_n) in S with $F_n(a) \rightarrow x$. Since $A = \pi_1(X)$, we can find $y \in X$ with $\pi_1(y) = a$. Then $F_n(y) \rightarrow x$ by Lemma 5.3.4. Observe that $F_n(y) \in X$, by S -invariance of X , and then $x \in X$, by closure of X . Hence $\Lambda(A) \subseteq X$.

Next we show that $X \subseteq \Lambda(A)$. Observe that $X = \Lambda(B)$, for some subset B of \mathcal{A} . Choose $x \in X$. Then there exists $b \in B$ and a sequence (w_n) of words over \mathcal{F} for which $F(w_n)(b) \rightarrow x$. Note that $|w_n| \rightarrow \infty$. Choose further sequences (u_n) and (v_n) in \mathcal{F}^+ with $w_n = u_n v_n$ and $|u_n| \rightarrow \infty$ and $|v_n| \rightarrow \infty$. Since \mathcal{A} is finite we can assume by passing to a subsequence that in fact all the letters $F(v_n)[b]$, for $n = 1, 2, \dots$, are equal to some letter c in \mathcal{A} .

Now, because $(\tilde{\mathcal{A}}, d)$ is compact, there is a subsequence of $(F(v_n)(b))$ that converges to some limit $y \in \tilde{\mathcal{A}}$. Since $|v_n| \rightarrow \infty$, by Theorem 5.2.5, $|F(v_n)(b)| \rightarrow \infty$. Then $y \in \mathcal{A}^{\mathbb{N}}$, so $y \in \Lambda(B)$. Since $F(v_n)[b] = c$ for each n , it follows that $\pi_1(y) = c$. So $c \in A$.

We have $F(u_n)(F(v_n)(b)) \rightarrow x$ and $\pi_1(F(v_n)(b)) = c$ for each n . Observe that $|F(u_n)(c)| \rightarrow \infty$, by Theorem 5.2.5, because $|u_n| \rightarrow \infty$. Hence we can apply Lemma 5.3.4 with $x_n = F(v_n)(b)$, $y_n = c$, and $F_n = F(u_n)$ to see that $F(u_n)(c) \rightarrow x$. Hence $x \in \Lambda(A)$, so $X \subseteq \Lambda(A)$. Therefore $X = \Lambda(A)$, as required. \square

The theorem fails if S has fixed letters, as we can easily illustrate with examples.

Example 5.3.9. Consider the semigroup S generated by the pair of substitutions

$$f : \begin{array}{l} a \mapsto ba, \\ b \mapsto b, \end{array} \quad \text{and} \quad g : \begin{array}{l} a \mapsto bb, \\ b \mapsto b. \end{array}$$

For $X = \Lambda(a)$, which consists of the point $bbb \dots$ alone, $A = \pi_1(X) = \{b\}$. Consequently $\Lambda(A)$ is the empty set and therefore, $X \not\subseteq \Lambda(A)$. \diamond

Example 5.3.10. Consider the semigroup S generated by the pair of substitutions

$$\begin{array}{l} a \mapsto ac, \\ f : b \mapsto cb, \\ c \mapsto c, \end{array} \quad \text{and} \quad \begin{array}{l} a \mapsto aa, \\ g : b \mapsto cb, \\ c \mapsto c. \end{array}$$

Observe that $\Lambda(c)$ is empty and $\Lambda(b)$ consists of the point $ccc \dots$ alone. The forward limit set $\Lambda(a)$ contains infinitely many points but, importantly, all of them start with the letter a . For $X = \Lambda(\{a, b\})$, $A = \pi_1(X) = \{a, c\}$. Consequently $\Lambda(A) = \Lambda(a)$ and therefore, $X \not\subseteq \Lambda(A)$. \diamond

5.4 Characterisations of forward limit sets

In this section, we focus on characterising forward limit sets of substitution semigroups in terms of s-adic limits (Section 5.4.1), invariant sets (Section 5.4.2) and fixed points (Section 5.4.3).

5.4.1 Forward limit sets and s-adic limits

The main result of this section is Theorem 5.4.1, which says that for a fixed-letter-free substitution semigroup S generated by a finite set of substitutions \mathcal{F} , the forward limit set of S is equal to the set of all s-adic limits of \mathcal{F} . We recall from Section 2.5.6 in Chapter 2 that an infinite word x over \mathcal{A} is an s-adic limit of a family of substitutions \mathcal{F} if there exist sequences (f_n) in \mathcal{F} and (a_n) in \mathcal{A} with $f_1 \circ f_2 \circ \dots \circ f_n(a_n) \rightarrow x$ as $n \rightarrow \infty$.

Theorem 5.4.1. *Let S be a fixed-letter-free substitution semigroup with finite generating set \mathcal{F} . The forward limit set of S is equal to the set of all s-adic limits of \mathcal{F} .*

Proof. First, we prove that the set of all s-adic limits of \mathcal{F} is contained in Λ , the forward limit set of S . Suppose that x is an s-adic limit of \mathcal{F} . Then there are sequences (f_n) in \mathcal{F} and (a_n) in \mathcal{A} for which $F_n(a_n) \rightarrow x$ as $n \rightarrow \infty$, where $F_n = f_1 \circ f_2 \circ \dots \circ f_n$. Since \mathcal{A} is finite, we can find an increasing sequence of positive integers (n_k) and a letter $a \in \mathcal{A}$ with $a_{n_k} = a$, for $k = 1, 2, \dots$. Hence $F_{n_k}(a) \rightarrow x$ as $n_k \rightarrow \infty$. Consequently, x belongs to $\Lambda(a)$, the forward limit set of a for \mathcal{F} . So x belongs to Λ .

Conversely, we prove that Λ is contained in the set of all s-adic limits of \mathcal{F} . Suppose that $x \in \Lambda$. Then $x \in \Lambda(a)$, for some letter $a \in \mathcal{A}$. Hence there is a sequence of words (u_n) in \mathcal{F}^+ with $|u_n| \rightarrow \infty$ and $F(u_n)(a) \rightarrow x$. Since \mathcal{F} is finite, by Lemma 5.2.1, there is a subsequence (v_n) of (u_n) of the form $v_n = f_1 f_2 \dots f_n w_n$, for $n = 1, 2, \dots$, where $f_i \in \mathcal{F}$ and $w_n \in \mathcal{F}^+$. Let $F_n = f_1 \circ f_2 \circ \dots \circ f_n$, $x_n = F(w_n)(a)$, and $a_n = \pi_1(x_n)$, for $n = 1, 2, \dots$. Then $F_n(x_n) = F(v_n)(a)$, so $F_n(x_n) \rightarrow x$. Since $|F_n(a_n)| \rightarrow \infty$, by Theorem 5.2.5, we can apply Lemma 5.3.4 with $y_n = a_n$ to see that $F_n(a_n) \rightarrow x$. Therefore x is an s-adic limit of \mathcal{F} , as required. \square

Observe that the requirements that \mathcal{F} is finite and S is fixed-letter-free are only necessary in the second part of the previous proof. Hence, the set of all s-adic limits of a set of substitutions \mathcal{F} is always contained in the forward limit set of the substitution semigroup generated by \mathcal{F} .

An example where Theorem 5.4.1 applies is the substitution semigroup generated by the Thue–Morse substitution and the reversed Thue–Morse substitution considered in Example 2.5.16, which is a fixed-letter-free substitution semigroups. We recall that the forward limit set of this substitution semigroup consist of two points, the Thue–Morse word and its image under the exchange of the letters of the alphabet. Therefore, these are the only two s-adic limits of the considered pair of substitutions.

Another example where Theorem 5.4.1 applies is the substitution semigroup generated by the Fibonacci substitution and the reversed Fibonacci substitution considered in Example 2.5.8. In this case, the forward limit set is infinite, but as we mentioned in Example 2.5.22, it admits a simple description. To not interrupt the thread of the discussion, we postpone a detailed treatment of this example till the end of this section on forward limit sets and s-adic limits (see Section 5.4.1.1). Now, we consider an example showing that Theorem 5.4.1 fails if S has fixed letters.

Example 5.4.2. Consider the semigroup S generated by substitutions f and g of the alphabet $\{a, b\}$, given by

$$f : \begin{array}{l} a \mapsto a, \\ b \mapsto ab, \end{array} \quad \text{and} \quad g : \begin{array}{l} a \mapsto a, \\ b \mapsto bb. \end{array}$$

Then $g^n \circ f(b) \rightarrow x$, where $x = abbb \dots$ (and where $g^n = g \circ g \circ \dots \circ g$, the n -fold composition of g with itself), and so x belongs to the forward limit set of S . However, x is not an s-adic limit of $\{f, g\}$. This can be seen from a short argument by contradiction. We assume that $f_1 \circ f_2 \circ \dots \circ f_n(a_n) \rightarrow x$, where $f_i \in \{f, g\}$ and $a_i \in \{a, b\}$. Then $a_n = b$ for all but finitely many values of n , and the fact that there is only a single occurrence of a in x implies that none of the substitutions f_i can equal f , which gives the required contradiction. \diamond

Notice that if S is not fixed-letter-free, the situation not considered in Theorem 5.4.1, it is still possible that the forward limit set of S is equal to the set of s-adic limits of \mathcal{F} . We consider a particular example.

Example 5.4.3. Consider the semigroup S of Example 2.5.15, which recall is generated by the substitutions

$$f : \begin{array}{l} a \mapsto a, \\ b \mapsto ab, \end{array} \quad \text{and} \quad g : \begin{array}{l} a \mapsto a, \\ b \mapsto ba. \end{array}$$

We know that S consists of substitutions of the form

$$f^n \circ g^m : \begin{array}{l} a \mapsto a, \\ b \mapsto a^n b a^m, \end{array}$$

where n and m are non-negative integers that are not simultaneously equal to 0. Here we have a substitution semigroup S which is not fixed-letter-free, but whose forward limit set is equal to the set of all s-adic limits of $\{f, g\}$, as we will now prove.

Suppose that x is an s-adic limit of $\{f, g\}$. Then there exist a sequence of substitutions (f_n) in $\{f, g\}$ and a sequence of letters (a_n) in $\{a, b\}$ such that $F_n(a_n) \rightarrow x$ as $n \rightarrow \infty$, where $F_n = f_1 \circ f_2 \circ \dots \circ f_n$. Since the letter a is fixed by all the substitutions in S , there must exist an increasing sequence of positive integers (n_k) such that $a_{n_k} = b$, for $k = 1, 2, \dots$, so $F_{n_k}(b) \rightarrow x$ as $n_k \rightarrow \infty$. Hence $x \in \Lambda$.

Conversely, suppose that $x \in \Lambda$. In Example 2.5.15 we saw that $\Lambda = \{aaaa \dots, a^n baaa \dots : n \in \mathbb{N}_0\}$. If $x = aaa \dots$, choose the substitution $F_n = f^{n-1} \circ g$ and the letter $a_n = b$, for $n = 1, 2, \dots$, so that $F_n(a_n) = a^n ba$. If $x = a^k baa \dots$, where k is a non-negative integer, choose the substitution $F_n = f^k \circ g^{n-k}$ and the letter $a_n = b$, for $n > k$, so that $F_n(b) = a^k b a^{n-k}$. In either case, $F_n(b) \rightarrow x$ as $n \rightarrow \infty$, so x is an s-adic limit of $\{f, g\}$, as required. \diamond

Theorem 5.4.1 tells us that for each $x \in \Lambda$ we can find sequences (f_n) in \mathcal{F} and (a_n) in \mathcal{A} with $f_1 \circ f_2 \circ \dots \circ f_n(a_n) \rightarrow x$ as $n \rightarrow \infty$. The next theorem says that we can obtain a similar conclusion but with $f_n \in S$ (rather than $f_n \in \mathcal{F}$) and all letters a_n equal.

Theorem 5.4.4. *Let S be a fixed-letter-free substitution semigroup with finite generating set \mathcal{F} , and let $x \in \Lambda$. Then there exists a letter $a \in \mathcal{A}$ and a sequence (g_n) in S for which*

$$g_1 \circ g_2 \circ \dots \circ g_n(a) \rightarrow x \quad \text{as } n \rightarrow \infty.$$

Proof. By Theorem 5.4.1, x is an s-adic limit of \mathcal{F} . Hence there exist sequences (f_n) in \mathcal{F} and (a_n) in \mathcal{A} for which $F_n(a_n) \rightarrow x$, where $F_n = f_1 \circ f_2 \circ \dots \circ f_n$. Since \mathcal{A} is finite we can find a letter a in \mathcal{A} and an increasing sequence of positive integers (n_k) with $a_{n_k} = a$, for $k = 1, 2, \dots$. Let $n_0 = 0$ and $g_k = f_{n_{k-1}+1} \circ f_{n_{k-1}+2} \circ \dots \circ f_{n_k}$, for $k = 1, 2, \dots$, and define $G_k = g_1 \circ g_2 \circ \dots \circ g_k$. Then $G_k = F_{n_k}$. Hence

$$G_k(a) = F_{n_k}(a) = F_{n_k}(a_{n_k}) \rightarrow x$$

as $k \rightarrow \infty$, as required. □

We finish this section on forward limit sets and s-adic limits with a detailed description of the forward limit set generated by the Fibonacci substitution and the reversed Fibonacci substitution.

5.4.1.1 The Fibonacci substitution semigroup

Consider the Fibonacci substitution f and the reversed Fibonacci substitution g , which we recall are given by

$$f : \begin{array}{lcl} a & \mapsto & ab, \\ b & \mapsto & a, \end{array} \quad \text{and} \quad g : \begin{array}{lcl} a & \mapsto & ba, \\ b & \mapsto & a. \end{array}$$

Throughout this Section 5.4.1.1, f and g will be these substitutions, and S will be the substitution semigroup generated by f and g , which we call the *Fibonacci substitution semigroup*. Furthermore, Λ will be the forward limit set of S , Ω will be the hull of S and \mathbb{X} will be the subshift of S .

In Example 2.5.22 we mentioned that $\Lambda = \Omega = \mathbb{X}$ and that they are given by the closure of the shift-orbit of the Fibonacci word, the fixed point of f . We will prove these assertions in Theorems 5.4.8 and 5.4.10. The following two lemmas will be used to prove the subsequent results.

Lemma 5.4.5. *For every finite word w over $\{a, b\}$, the Fibonacci substitution f and the reversed Fibonacci substitution g satisfy $f(wb) = g(bw)$.*

Proof. It is immediate to check that the claim holds for $w = a$ and $w = b$. Now, suppose that the claim holds for every word of length n , for some positive integer n . Then, for every word $w = a_1 a_2 \dots a_{n+1}$,

where $a_i \in \{a, b\}$ for $i = 1, 2, \dots, n+1$, we have

$$\begin{aligned} f(wb) &= f(a_1) f(a_2 a_3 \cdots a_{n+1} b) = f(a_1) g(b a_2 a_3 \cdots a_{n+1}) = \\ &= f(a_1) a g(a_2 a_3 \cdots a_{n+1}) = f(a_1 b) g(a_2 a_3 \cdots a_{n+1}) = \\ &= g(b a_1) g(a_2 a_3 \cdots a_{n+1}) = g(b a_1 a_2 a_3 \cdots a_{n+1}) = g(bw). \end{aligned}$$

The proof follows by mathematical induction. \square

Lemma 5.4.6. *For every infinite word w over $\{a, b\}$, the Fibonacci substitution f and the reversed Fibonacci substitution g satisfy $f(w) = g(bw)$.*

Proof. For every positive integer n , let x_n be the prefix of w of length n . For every n , $f(x_n b) = g(bx_n)$, by Lemma 5.4.5. Since $x_n \rightarrow w$ as $n \rightarrow \infty$,

$$f(x_n b) \rightarrow f(w) \quad \text{and} \quad g(bx_n) \rightarrow g(bw),$$

by continuity of f and g . Therefore $f(w) = g(bw)$, as required. \square

Using Lemma 5.4.5 it is easy to show that both substitutions f and g have the same language.

Lemma 5.4.7. *The language of the Fibonacci substitution f is equal to the language of the reversed Fibonacci substitution g .*

Proof. We have to look at subwords of $f^n(c)$ and $g^n(c)$, for all positive integers n and letters c in $\{a, b\}$. Without loss of generality, we can assume that $c = a$ because $f^n(a) = f^{n+1}(b)$ and $g^n(a) = g^{n+1}(b)$. By direct inspection, we see that all the subwords of $f(a)$ are subwords of $g^2(a)$ and that all the subwords of $g(a)$ are subwords of $f^2(a)$. Similarly, we verify that the language of $f^2(a)$ is equal to the language of $g^2(a)$, or in other words, $\mathcal{L}(f^2(a)) = \mathcal{L}(g^2(a))$. Now, let us suppose that, for a positive integer $n > 2$, we have $\mathcal{L}(f^n(a)) = \mathcal{L}(g^n(a))$. Any subword x of $f^{n+1}(a)$ is a subword of $f(f^n(a)b)$ and, by Lemma 5.4.5, a subword of $g(bf^n(a))$. Then x is a subword of $g(bg^n(a))$, and so of $g^{n+1}(a)$. Therefore $\mathcal{L}(f^{n+1}(a)) = \mathcal{L}(g^{n+1}(a))$, and the proof follows by induction. \square

Now, we can prove the equality of Ω and \mathbb{X} .

Theorem 5.4.8. *The hull Ω and the subshift \mathbb{X} of the Fibonacci substitution semigroup are equal, and they are given by the closure of the shift-orbit of the Fibonacci word, the fixed point of the Fibonacci substitution.*

Proof. Since f is a primitive substitution, by Theorem 2.4.35, its hull Ω_f and its subshift \mathbb{X}_f are equal. The same happens for g . Moreover, since the language of f is equal to the language of g , by Lemma 5.4.7, their subshifts are equal. In short, $\Omega_f = \Omega_g = \mathbb{X}_f = \mathbb{X}_g$. From the equality of the languages of f and g , it also follows that the language of S is equal to the language of f and g . Consequently, $\mathbb{X} = \mathbb{X}_f = \mathbb{X}_g$. Furthermore, it can easily be shown that $\Omega_f \subseteq \Omega \subseteq \mathbb{X}$. Then, we have that $\mathbb{X} \subseteq \Omega \subseteq \mathbb{X}$ and therefore,

$\Omega = \mathbb{X}$. That the sets Ω and \mathbb{X} are equal to the closure of the shift-orbit of the Fibonacci word is a straightforward consequence of Theorem 2.4.35. \square

Since the dynamical system (Ω, σ) is minimal and Λ is a non-empty closed subset of Ω , to show that $\Lambda = \Omega$ it suffices to show that Λ is σ -invariant. In the following lemma we show that Λ is, in fact, strongly σ -invariant.

Lemma 5.4.9. *The forward limit set Λ of the Fibonacci substitution semigroup is strongly invariant under the shift map σ . In other words, $\Lambda = \sigma(\Lambda)$.*

Proof. Suppose that $x \in \Lambda$. It can be easily verified that S is fixed-letter-free, so Λ is strongly S -invariant, by Theorem 5.4.16 (result to come on page 121). In other words, $\Lambda = S(\Lambda)$. So there exists $y \in \Lambda$ such that $x = g(y)$. Since $g(y) = \sigma(ag(y)) = \sigma(g(by))$, we can use Lemma 5.4.6 to write $x = \sigma(f(y))$, so $x \in \sigma(\Lambda)$. Hence $\Lambda \subseteq \sigma(\Lambda)$.

Conversely, suppose that $x \in \Lambda$. Since $\Lambda = S(\Lambda)$, there exists $y \in \Lambda$ such that $x = f(y)$. By Lemma 5.4.6, $f(y) = g(by) = ag(y)$, so $\sigma(x) = g(y)$. Hence $\sigma(\Lambda) \subseteq \Lambda$. Consequently, $\Lambda = \sigma(\Lambda)$, as required. \square

Now, we can prove the equality of Λ and Ω .

Theorem 5.4.10. *The forward limit set Λ and the hull Ω of the Fibonacci substitution semigroup are equal.*

Proof. Since (Ω, σ) is a minimal dynamical system and Λ is a non-empty closed and σ -invariant subset of Ω , $\Lambda = \Omega$, as required. \square

Therefore, by Theorems 5.4.8 and 5.4.10, Λ , Ω and \mathbb{X} are equal to each other and they are given by the closure of the shift-orbit of the Fibonacci word, as we wanted to show. Since S is fixed-letter-free and, by Theorem 5.4.1, Λ is equal to the set of all s-adic limits of $\{f, g\}$, we have a precise description of this family of s-adic sequences.

5.4.2 Invariant sets

In this section we turn to means for classifying forward limit sets by means of the action of S on $\mathcal{A}^{\mathbb{N}}$. Recall that a subset X of $\mathcal{A}^{\mathbb{N}}$ is S -invariant if $S(X) \subseteq X$, and strongly S -invariant if $S(X) = X$. The main result of this section is Theorem 5.4.16 which says that, given a finitely-generated fixed-letter-free substitution semigroup S , a subset of $\mathcal{A}^{\mathbb{N}}$ is closed and strongly S -invariant if, and only if, it is the forward limit set of some subset of \mathcal{A} for S . A consequence of this result is another characterisation of the forward limit set of S , which turns out to be the greatest element in the poset of closed and strongly S -invariant subsets of $\mathcal{A}^{\mathbb{N}}$ (this is Corollary 5.4.17). Furthermore, we characterise the minimal closed and S -invariant subsets of $\mathcal{A}^{\mathbb{N}}$, which turn out to be the forward limit sets of the terminal components of the corresponding first-letter graph (this is Theorem 5.4.19).

A first step towards these goals is the following lemma.

Lemma 5.4.11. *Let S be a fixed-letter-free substitution semigroup with finite generating set \mathcal{F} . The forward limit set $\Lambda(a)$ of a letter $a \in \mathcal{A}$ is strongly S -invariant.*

Proof. We already know that $\Lambda(a)$ is S -invariant, by Lemma 5.3.1, so it remains to show that if $y \in \Lambda(a)$, then there exists $g \in S$ and $x \in \Lambda(a)$ with $g(x) = y$. To prove this, observe that since $y \in \Lambda(a)$ there is a sequence (w_n) in \mathcal{F}^+ with $F(w_n)(a) \rightarrow y$. Note that $|w_n| \rightarrow \infty$. Since \mathcal{F} is finite, by restricting to a subsequence of (w_n) , we can assume that in fact $w_n = gv_n$, for $n = 1, 2, \dots$, where $g \in \mathcal{F}$ and $v_n \in \mathcal{F}^+$. Now, $(F(v_n)(a))$ is a sequence in the compact metric space $(\tilde{\mathcal{A}}, d)$, so there is an increasing sequence of positive integers (n_k) for which $F(v_{n_k})(a) \rightarrow x$, for some point $x \in \tilde{\mathcal{A}}$. In fact, $x \in \mathcal{A}^{\mathbb{N}}$ because $|F(v_{n_k})(a)| \rightarrow \infty$ by Theorem 5.2.5. Hence, by continuity of g ,

$$F(w_{n_k})(a) = g \circ F(v_{n_k})(a) \rightarrow g(x),$$

so $g(x) = y$, as required. \square

It follows immediately from Lemma 5.4.11 that the forward limit set of any subset of \mathcal{A} for S is strongly S -invariant.

Lemma 5.4.12. *Let S be a fixed-letter-free substitution semigroup, let \mathcal{F} be a generating set of S , and let X be a subset of $\mathcal{A}^{\mathbb{N}}$. Suppose that for some $x \in X$ there are sequences (f_n) in S and (x_n) in X with $x_{n-1} = f_n(x_n)$, for $n = 1, 2, \dots$, where $x_0 = x$. Then $x \in \Lambda(A)$, where $A = \pi_1(X)$.*

Proof. Choose sequences (f_n) and (x_n) as specified in the lemma. Let $F_n = f_1 \circ f_2 \circ \dots \circ f_n$. Then we have $F_n(x_n) = x$. Define $a_n = \pi_1(x_n)$, and note that $a_n \in \pi_1(X)$. Since $|F_n(a_n)| \rightarrow \infty$, by Theorem 5.2.5, we can apply Lemma 5.3.4 with $y_n = a_n$ to see that $F_n(a_n) \rightarrow x$. Hence $x \in \Lambda(A)$, so $X \subseteq \Lambda(A)$, as required. \square

Using Lemma 5.4.12 we obtain another characterisation of Λ .

Theorem 5.4.13. *Let S be a fixed-letter-free substitution semigroup with generating set \mathcal{F} , and let $x \in \mathcal{A}^{\mathbb{N}}$. Then $x \in \Lambda$ if, and only if, there are sequences (f_n) in S and (x_n) in $\mathcal{A}^{\mathbb{N}}$ with $x_{n-1} = f_n(x_n)$, for $n = 1, 2, \dots$, where $x_0 = x$.*

Proof. Suppose first that $x \in \Lambda$. Since Λ is strongly S -invariant, we can find a substitution f_1 in S and an infinite word x_1 in $\mathcal{A}^{\mathbb{N}}$ with $f_1(x_1) = x$. By repeating this argument (and applying the axiom of dependent choices) we obtain the required sequences (f_n) and (x_n) .

Conversely, suppose there are sequences (f_n) in S and (x_n) in $\mathcal{A}^{\mathbb{N}}$ with $x_{n-1} = f_n(x_n)$, for $n = 1, 2, \dots$, where $x_0 = x$. Applying Lemma 5.4.12 with $X = \mathcal{A}^{\mathbb{N}}$, we see that $x \in \Lambda(A)$, where $A = \pi_1(X) = \mathcal{A}$. Consequently, $x \in \Lambda$, as required. \square

The concept ‘stable set’ of a set of self-maps, in particular a set of substitutions, was defined in [59] and it was studied in [97], for Sturmian and Episturmian substitutions, and in [10], for random compositions of substitutions with the same matrix (in the latter the term ‘stable set’ is not explicitly mentioned).

Let \mathcal{F} be a set of substitutions of an alphabet \mathcal{A} . We say that a word x over \mathcal{A} can be *indefinitely desubstituted using substitutions from \mathcal{F}* if there exist sequences (f_n) in \mathcal{F} and (x_n) in $\tilde{\mathcal{A}}$ with $x_{n-1} = f_n(x_n)$, for $n = 1, 2, \dots$, where $x_0 = x$. The *stable set* of \mathcal{F} is the set of all words over \mathcal{A} that can be indefinitely desubstituted using substitutions from \mathcal{F} . Thus, we obtain the following characterisation of Λ as a corollary of Theorem 5.4.13.

Corollary 5.4.14. *The forward limit set of a fixed-letter-free substitution semigroup generated by a set \mathcal{F} of substitutions is equal to the stable set of \mathcal{F} .*

Proof. Let S be the substitution semigroup generated by \mathcal{F} and let Λ be the forward limit set of S . If $x \in \Lambda$, then x belongs to the stable set of \mathcal{F} , by Theorem 5.4.13. Conversely, suppose that x belongs to the stable set of \mathcal{F} . Since S is fixed-letter-free, no finite word can be indefinitely desubstituted using substitutions from \mathcal{F} , by Theorem 5.2.5, so x must be an infinite word. Hence $x \in \Lambda$, by Theorem 5.4.13. \square

The next lemma features in the proof of Theorem 5.4.16.

Lemma 5.4.15. *Let S be a substitution semigroup, let \mathcal{F} be a generating set of S , and let X be a closed and S -invariant subset of $\mathcal{A}^{\mathbb{N}}$. Then $\Lambda(A) \subseteq X$, where $A = \pi_1(X)$.*

Proof. Let $y \in \Lambda(A)$. There exists $a \in A$ and a sequence (F_n) in S with $F_n(a) \rightarrow y$. Choose $x \in X$ with $\pi_1(x) = a$. Then $F_n(x) \rightarrow y$ by Lemma 5.3.4. Observe that $F_n(x) \in X$, by S -invariance of X , and then $y \in X$, by closure of X . Hence $\Lambda(A) \subseteq X$, as required. \square

We can now prove the main result of this section.

Theorem 5.4.16. *Let S be a fixed-letter-free substitution semigroup with finite generating set \mathcal{F} , and let $X \subseteq \mathcal{A}^{\mathbb{N}}$. Then X is closed and strongly S -invariant if, and only if, $X = \Lambda(A)$, where $A = \pi_1(X)$.*

Proof. Suppose that $X = \Lambda(A)$, where $A = \pi_1(X)$. Then X is closed, and it is strongly S -invariant, by Lemma 5.4.11.

Conversely, suppose that X is closed and strongly S -invariant. Let $x \in X$. By the strongly S -invariant property, there are sequences (f_n) in S and (x_n) in X with $f_n(x_n) = x_{n-1}$, for $n = 1, 2, \dots$, where $x_0 = x$. Applying Lemma 5.4.12, we find that $x \in \Lambda(A)$, where $A = \pi_1(X)$. Thus $X \subseteq \Lambda(A)$. Next, $\Lambda(A) \subseteq X$, by Lemma 5.4.15. Hence $X = \Lambda(A)$, as required. \square

A consequence of this theorem is another characterisation of Λ , which says that Λ is the greatest element in the poset of closed and strongly S -invariant subsets of $\mathcal{A}^{\mathbb{N}}$.

Corollary 5.4.17. *Let S be a fixed-letter-free substitution semigroup with finite generating set \mathcal{F} . Every closed and strongly S -invariant subset of $\mathcal{A}^{\mathbb{N}}$ is contained in the forward limit set of S .*

We finish this section with a result (Theorem 5.4.19) characterising closed and S -invariant sets (rather than closed and strongly S -invariant sets) in terms of forward limit sets. A *minimal* closed and S -invariant subset of $\mathcal{A}^{\mathbb{N}}$ is a closed and S -invariant subset of $\mathcal{A}^{\mathbb{N}}$ that contains no other such sets besides itself (and the empty set). The next lemma facilitates proving Theorem 5.4.19.

Lemma 5.4.18. *Let S be a substitution semigroup of the alphabet \mathcal{A} , and let $x \in \Lambda(A)$, for some subset A of \mathcal{A} . Then there exists $a \in A$ and $g \in S$ with $g[a] = \pi_1(x)$.*

Proof. Since $x \in \Lambda(A)$, there exists $a \in A$ and a sequence (F_n) in S with $F_n(a) \rightarrow x$. Thus there exists a positive integer m with $\pi_1(F_n(a)) = \pi_1(x)$, for $n \geq m$. Hence we can choose $g = F_m$, to give $g[a] = F_m[a] = \pi_1(F_m(a)) = \pi_1(x)$, as required. \square

Here is the promised result on closed and S -invariant sets. We recall that the first-letter graph for a set of substitutions \mathcal{F} is denoted by $G_{\mathcal{F}}$.

Theorem 5.4.19. *Let S be a substitution semigroup with generating set \mathcal{F} . A subset of $\mathcal{A}^{\mathbb{N}}$ is a minimal closed and S -invariant subset if, and only if, it is the forward limit set of a terminal component of $G_{\mathcal{F}}$.*

Proof. Let T be a terminal component of $G_{\mathcal{F}}$. Then $\Lambda(T)$ is closed and S -invariant. Let X be a closed and S -invariant subset of $\mathcal{A}^{\mathbb{N}}$ with $X \subseteq \Lambda(T)$. Observe that $\Lambda(A) \subseteq X$, where $A = \pi_1(X)$, by Lemma 5.4.15. We will prove that $\Lambda(A) = \Lambda(T)$, from which it follows that $\Lambda(T)$ is minimal.

To do this, choose $a \in A$. Then $a = \pi_1(x)$, for some $x \in X$, so $x \in \Lambda(T)$ because $X \subseteq \Lambda(T)$. By Lemma 5.4.18, there exists $b \in T$ and $g \in S$ with $g[b] = a$. But T is a terminal component, so there exists $h \in S$ with $h[a] = b$. Hence $\Lambda(b) \subseteq \Lambda(a)$, by Lemma 5.3.5. Observe that $\Lambda(b) = \Lambda(T)$, by Corollary 5.3.6, and of course $\Lambda(a) \subseteq \Lambda(A)$, so we see that $\Lambda(T) \subseteq \Lambda(A)$. Hence $\Lambda(A) = \Lambda(T)$, as required.

Conversely, let X be a minimal closed and S -invariant subset of $\mathcal{A}^{\mathbb{N}}$. Then $\Lambda(A) \subseteq X$, where $A = \pi_1(X)$, by Lemma 5.4.15. Choose $a \in A$. Then $\Lambda(a) \subseteq \Lambda(A)$. Since $\Lambda(a)$ is closed and S -invariant, we must have $X = \Lambda(a)$, by minimality of X .

Now choose $x \in X$ with $\pi_1(x) = a$. There exists $f \in S$ with $f[a] = a$, by Lemma 5.4.18. Hence the vertex a belongs to some strongly connected component B of $G_{\mathcal{F}}$.

Let $g \in S$ and define $b = g[a]$. To show that B is a terminal component of $G_{\mathcal{F}}$ we must prove that $b \in B$. Observe that $\Lambda(b) \subseteq \Lambda(a)$, by Lemma 5.3.5, so $X = \Lambda(a) = \Lambda(b)$ by minimality of X . Then, by Lemma 5.4.18, there exists $h \in S$ with $h[b] = a$. Therefore $b \in B$, as required. \square

Example 5.4.20. Consider the set $\mathcal{F} = \{f, g\}$, where f and g are given by

$$\begin{array}{ll} a \mapsto b, & a \mapsto c, \\ f: b \mapsto c, & \text{and } g: b \mapsto ba, \\ c \mapsto ca, & c \mapsto cb. \end{array}$$

The substitution semigroup S generated by \mathcal{F} is fixed-letter-free, which can be easily checked. The only terminal component of the first-letter graph for \mathcal{F} , shown in Figure 5.4.1, is the set $\{c\}$. Therefore, the unique minimal closed and S -invariant set of infinite words over $\{a, b, c\}$ is $\Lambda(c)$, the forward limit set of the letter c .

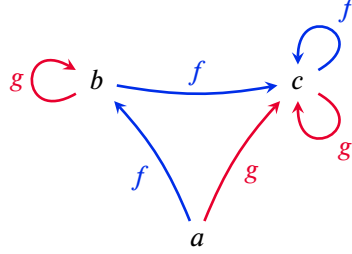


Figure 5.4.1: First-letter graph for $\mathcal{F} = \{f, g\}$.

◆

5.4.3 Fixed points of substitution semigroups

We recall that a fixed point of a substitution f is a word x (finite or infinite) with $f(x) = x$. In this section we characterise the forward limit set of a finitely-generated fixed-letter-free substitution semigroup S in terms of the fixed points of S , by showing that it is equal to $\overline{S(X)}$, where $X = \text{fix}(S)$ is the set of all fixed points of substitutions from S . This is Theorem 5.4.24, but three preliminary results are required before we prove the theorem itself.

The first lemma is a particular case of Lemma 2.4.6, but re-stated in more convenient words for this chapter. In the proof we use the well-known contraction mapping theorem, which we recall here. Let (Y, d) be a non-empty complete metric space. A map $f : Y \rightarrow Y$ is called a *contraction mapping* on Y if there exists a real number $0 \leq k < 1$ such that $d(f(x), f(y)) \leq k d(x, y)$, for all $x, y \in Y$. Let f be a contraction mapping on Y . The *contraction mapping theorem*, or *Banach fixed-point theorem*, says that f has a unique fixed point x in Y and that $f^n(y) \rightarrow x$ as $n \rightarrow \infty$, for all $y \in Y$.

Lemma 5.4.21. *Let f be a substitution that has no fixed letters and that satisfies $f[a] = a$, for some letter a . Then f has a unique fixed point x in $\mathcal{A}^{\mathbb{N}}$ with first letter a . Furthermore, $f^n(a) \rightarrow x$ as $n \rightarrow \infty$.*

Proof. Let X denote the set of all words over \mathcal{A} with first letter a . Observe that f maps X into itself. For any two distinct words y and z from X , there exist distinct words u and v over \mathcal{A} such that $y = au$ and $z = av$. Let w be the longest common prefix of u and v , and let $m = |w|$. Then

$$|f(aw)| = |f(a)| + |f(w)| \geq 2 + |w| = 2 + m,$$

since $|f(a)| \geq 2$ (because f has no fixed letters). Consequently,

$$d(y, z) = \frac{1}{2^{m+1}} \quad \text{and} \quad d(f(y), f(z)) \leq \frac{1}{2^{m+2}},$$

and we see that

$$d(f(y), f(z)) \leq \frac{1}{2}d(y, z).$$

Therefore, f is a contraction mapping on X , so it has a unique fixed point x and $f^n(a) \rightarrow x$, by the contraction mapping theorem. \square

Lemma 5.4.22. *Let S be a fixed-letter-free substitution semigroup, let \mathcal{F} be a generating set of S , and let $a \in \mathcal{A}$. Let (f_n) be a sequence in S and let $F_n = f_1 \circ f_2 \circ \dots \circ f_n$. Suppose that some subsequence of $(F_n(a))$ converges to an infinite word x in $\mathcal{A}^{\mathbb{N}}$, where $\pi_1(x) = a$. Then $x \in \overline{\text{fix}(S)}$.*

Proof. Let us choose a sequence of positive integers (n_k) for which $F_{n_k}(a) \rightarrow x$. Since $\pi_1(x) = a$ it follows that $\pi_1(F_{n_k}(x)) = a$ for sufficiently large values of k ; in fact, after relabelling the sequence we can assume that $\pi_1(F_{n_k}(x)) = a$, for $k = 1, 2, \dots$.

By Lemma 5.4.21, F_{n_k} has a unique fixed point x_k in $\mathcal{A}^{\mathbb{N}}$ with $\pi_1(x_k) = a$. And by Lemma 5.3.4, $F_{n_k}(x_k) \rightarrow x$. Since $F_{n_k}(x_k) = x_k$, we deduce that $x \in \overline{\text{fix}(S)}$, as required. \square

Lemma 5.4.23. *Let (w_n) be a sequence in \mathcal{A}^+ with $|w_1| < |w_2| < \dots$. Then, there exist a pair $(r, a) \in \mathbb{N} \times \mathcal{A}$ and two increasing sequences of positive integers (n_k) and (l_k) with $r + l_k \leq |w_{n_k}|$ and*

$$\pi_r(w_{n_k}) = \pi_{r+l_k}(w_{n_k}) = a,$$

for $k = 1, 2, \dots$.

Proof. We prove the lemma by induction on the size m of \mathcal{A} . Suppose that $m = 1$. Then we choose a to be the unique element of \mathcal{A} , and we choose $r = 1$, $n_k = k + 1$, and $l_k = |w_{k+1}| - 1$, for $k = 1, 2, \dots$. This pair and these sequences satisfy the required properties.

Suppose now that the lemma is true for alphabets of size m , where m is a positive integer. Let \mathcal{A} be an alphabet of size $m + 1$. Since \mathcal{A} is finite, there is an element e of \mathcal{A} and an infinite subset E of \mathbb{N} with $\pi_1(w_n) = e$, for all $n \in E$.

Now, there may be increasing sequences of positive integers (n_k) and (l_k) with (n_k) in E and with $1 + l_k \leq |w_{n_k}|$ and $\pi_1(w_{n_k}) = \pi_{1+l_k}(w_{n_k}) = e$, for $k = 1, 2, \dots$. If that is so, then the pair $(1, e)$ and the sequences (n_k) and (l_k) satisfy the required properties.

If there are no such sequences, then there is an integer s for which $\pi_j(w_n) \neq e$, for $j > s$ and $n \in E$. Let E' denote the infinite subset of E of those integers n in E with $|w_n| > s$. Let p_1, p_2, \dots be the elements of E' , in increasing order, and define v_n to be the word obtained from w_{p_n} by removing the first s letters from w_{p_n} . Then (v_n) is a sequence in $(\mathcal{A} - \{e\})^+$ with $|v_1| < |v_2| < \dots$. Since $\mathcal{A} - \{e\}$ has size m we can apply the inductive hypothesis to obtain a pair $(r, a) \in \mathbb{N} \times (\mathcal{A} - \{e\})$ and two increasing sequences of positive integers (n_k) and (l_k) with $r + l_k \leq |v_{n_k}|$ and $\pi_r(v_{n_k}) = \pi_{r+l_k}(v_{n_k}) = a$, for $k = 1, 2, \dots$. Hence $(r + s, a) \in \mathbb{N} \times \mathcal{A}$ and $(r + s) + l_k \leq |w_{p_{n_k}}|$ and $\pi_{r+s}(w_{p_{n_k}}) = \pi_{(r+s)+l_k}(w_{p_{n_k}}) = a$, for $k = 1, 2, \dots$. Therefore the pair $(r + s, a)$ and the sequences (p_{n_k}) and (l_k) satisfy the properties required by the lemma. This completes the proof by induction. \square

We can now prove Theorem 5.4.24.

Theorem 5.4.24. *The forward limit set of a finitely-generated fixed-letter-free substitution semigroup S is equal to $\overline{S(X)}$, where $X = \text{fix}(S)$.*

Proof. Since S has no fixed letters, it also has no fixed finite words, by Corollary 5.2.4. Suppose now that $x \in X$. Then x is an infinite word fixed by some substitution $f \in S$. Lemma 5.4.21 tells us that $f^n(a) \rightarrow x$, where $a = \pi_1(x)$. Hence $x \in \Lambda$. It follows that $X \subseteq \Lambda$, and since Λ is closed and S -invariant, we see that $\overline{S(X)}$ is contained in Λ .

Conversely, take $x \in \Lambda$. Then by Theorem 5.4.4 we can find $b \in \mathcal{A}$ and substitutions g_1, g_2, \dots in S for which $G_n(b) \rightarrow x$, where $G_n = g_1 \circ g_2 \circ \dots \circ g_n$. Let us define $G_{m,n} = g_m \circ g_{m+1} \circ \dots \circ g_n$, where $1 \leq m \leq n$. We also define the n -letter word

$$w_n = G_n[b] G_{2,n}[b] \cdots G_{n,n}[b],$$

for $n = 1, 2, \dots$. By Lemma 5.4.23, there exists a pair $(r, a) \in \mathbb{N} \times \mathcal{A}$ and two increasing sequences of positive integers (n_k) and (l_k) with $r + l_k \leq |w_{n_k}|$ and $\pi_r(w_{n_k}) = \pi_{r+l_k}(w_{n_k}) = a$. Notice that this implies

$$G_{r,n_k}[b] = G_{r+l_k,n_k}[b] = a.$$

We define $g = G_{r-1}$ (possibly $r = 1$ in which case instead we define g to be the identity substitution) and $h_n = g_{n+r-1}$ and $H_n = h_1 \circ h_2 \circ \dots \circ h_n$, for $n = 1, 2, \dots$. Then

$$H_{l_k}[a] = H_{l_k}[G_{r+l_k,n_k}[b]] = G_{r,n_k}[b] = a,$$

for $k = 1, 2, \dots$.

Since (\mathcal{A}, d) is compact, we can find a convergent subsequence $(H_{p_k}(a))$ of $(H_{l_k}(a))$. The limit y of this sequence must have first letter a because $H_{l_k}[a] = a$, for all k . By Lemma 5.4.22, $y \in \overline{X}$. Hence $g \circ H_{p_k}(a) \rightarrow g(y)$, by continuity of g , and $g(y) \in \overline{S(X)}$.

Next, by applying Lemma 5.3.4 with $x_k = a$, $y_k = G_{r+p_k,n_k}(b)$, and $F_k = H_{p_k}$, we see that $H_{p_k}(G_{r+p_k,n_k}(b)) \rightarrow y$. But $H_{p_k} \circ G_{r+p_k,n_k} = G_{r,n_k}$, so $G_{r,n_k}(b) \rightarrow y$. Therefore $G_{n_k}(b) = g \circ G_{r,n_k}(b) \rightarrow g(y)$. However, $G_n(b) \rightarrow x$, which implies that $x = g(y)$, so $x \in \overline{S(X)}$. Thus, we see that Λ is contained in $\overline{S(X)}$. Therefore, $\Lambda = \overline{S(X)}$, as required. \square

If S is generated by a single substitution f , the set $S(X)$, where $X = \text{fix}(S)$, is precisely the finite set of all periodic points of f . This implies that the forward limit set of S is equal to the set of all periodic points of f , so we recover Lemma 2.4.12.

Example 5.4.25. Let S be the substitution semigroup generated by the Thue–Morse substitution and the reversed Thue–Morse substitution, and let Λ be the forward limit set of S . We know from Example 2.5.16 that $\Lambda = \{x, h(x)\}$, where x is the Thue–Morse word and h the substitution exchanging the two letters of the alphabet. It is immediate to see that, in this case, $\Lambda = \text{fix}(S)$. \diamond

Example 5.4.26. Let S be the substitution semigroup generated by the Fibonacci substitution and the reversed Fibonacci substitution, and let Λ be the forward limit set of S . From Section 5.4.1.1 we know that Λ is given by the closure of the shift-orbit of the Fibonacci word, which, by Theorem 5.4.24, is equal to the closure of $S(X)$, where $X = \text{fix}(S)$. \diamond

5.5 Size of forward limit sets

The results stated so far concern characterisations of forward limit sets. This section is about the size of forward limit sets, which typically are not too small (see Section 5.5.1) nor too large (see Section 5.5.2).

5.5.1 Cardinality of forward limit sets

In this section we show that, under certain assumptions, the forward limit set of a substitution semigroup is uncountable. Recall that a word a is a *prefix* of another word b if $b = ac$, where c is either another word or the empty word. With this description on hand, the main theorem we prove in this section (Theorem 5.5.2) says that if S is a fixed-letter-free substitution semigroup generated by $\mathcal{F} = \{f, g\}$ for which $\text{fix}(f)$ and $\text{fix}(g)$ are disjoint and for which $h(a)$ is not a prefix of $h(b)$, for any distinct $a, b \in \mathcal{A}$ and $h \in \mathcal{F}$, then the forward limit set of S is uncountable.

The first step in proving this is to show that, with this prefix property, f and g are injective on infinite words.

Lemma 5.5.1. *Let f be a substitution of \mathcal{A} for which $f(a)$ is not a prefix of $f(b)$, for any distinct $a, b \in \mathcal{A}$. Then f is injective on $\tilde{\mathcal{A}}$.*

Proof. First, consider two infinite words $u = a_1a_2 \dots$ and $v = b_1b_2 \dots$ over \mathcal{A} , where a_i and b_j are letters of \mathcal{A} . Suppose that $f(u) = f(v)$. Then

$$f(a_1)f(a_2) \dots = f(b_1)f(b_2) \dots,$$

so one of $f(a_1)$ and $f(b_1)$ must be a prefix of the other. Consequently, $a_1 = b_1$. Now let $u' = a_2a_3 \dots$ and $v' = b_2b_3 \dots$. Then $f(u') = f(v')$, and we obtain $a_2 = b_2$. This is the basis for an inductive argument to show that $a_i = b_i$, for each positive integer i , so $u = v$. Thus f is injective on infinite words. The argument used can be immediately modified to show that f is also injective on finite words, a result that also follows from Lemma 2.4.1. Hence, f is injective on $\tilde{\mathcal{A}}$, as required. \square

We can now prove the promised theorem.

Theorem 5.5.2. *Let S be a fixed-letter-free substitution semigroup with finite generating set \mathcal{F} . Suppose that $\text{fix}(S)$ contains two words with the same first letter and suppose also that $f(a)$ is not a prefix of $f(b)$, for any distinct $a, b \in \mathcal{A}$ and $f \in \mathcal{F}$. Then the forward limit set of S is uncountable.*

Proof. We begin by observing that each substitution from S is injective in its action on $\mathcal{A}^{\mathbb{N}}$, because the generators from \mathcal{F} are injective, by Lemma 5.5.1.

Next, let a be a letter from \mathcal{A} for which there are at least two words in $\text{fix}(S)$ with first letter a . We denote by $\Sigma(a)$ the set of those infinite words x with first letter a for which there is a sequence of substitutions (g_n) in S with $G_n(a) \rightarrow x$, where $G_n = g_1 \circ g_2 \circ \cdots \circ g_n$.

The set $\Sigma(a)$ contains all fixed points of S with first letter a . Indeed, if x is a fixed point of some element h of S with $h[a] = a$, then $h^n(a) \rightarrow x$ (by Lemma 5.4.21), so $x \in \Sigma(a)$. Hence $\Sigma(a)$ has size at least two.

Observe that $\Sigma(a)$ is invariant under those elements h of S that satisfy $h[a] = a$. Indeed, if $x \in \Sigma(a)$ and (g_n) is a sequence in S with $G_n(a) \rightarrow x$, and if $h \in S$ with $h[a] = a$, then $h \circ G_n(a) \rightarrow h(x)$, so $h(x) \in \Sigma(a)$.

Choose any infinite word x in $\Sigma(a)$. Let y be another infinite word in $\Sigma(a)$ and let ε be any positive number that satisfies $\varepsilon < d(x, y)$. Observe that $d(x, y) < 1$, since $\pi_1(x) = \pi_1(y) = a$. Let (g_n) be a sequence in S with $G_n(a) \rightarrow x$. By Lemma 5.4.22, we have $x \in \overline{\text{fix}(S)}$. Hence there is an infinite word z that is fixed by some substitution $h \in S$ and that satisfies $d(x, z) < \varepsilon$. Since $\varepsilon < d(x, y) < 1$, it follows that $\pi_1(z) = a$ (so $z \in \Sigma(a)$) and $z \neq y$.

Notice that $h^n(a) \rightarrow z$, by Lemma 5.4.21, so $h^n(y) \rightarrow z$, by Lemma 5.3.4. Each iterate $h^n(y)$ lies in $\Sigma(a)$, by invariance of $\Sigma(a)$ under h . Also, none of the iterates equal z , because h is injective and $h(z) = z$. Consequently, $\Sigma(a)$ accumulates at z . Since ε can be chosen to be arbitrarily small, we see that $\Sigma(a)$ also accumulates at x . It follows that every point in $\overline{\Sigma(a)}$ is an accumulation point, so $\overline{\Sigma(a)}$ is a perfect set, hence uncountable. Since $(\mathcal{A}^{\mathbb{N}}, d)$ is complete, and the forward limit set Λ of S contains $\overline{\Sigma(a)}$, we deduce that Λ is uncountable, as required. \square

The scope of application of Theorem 5.5.2 is broader than it might first appear.

Example 5.5.3. The Fibonacci substitution f and the reversed Fibonacci substitution g , illustrated in Figure 2.5.3 in Example 2.5.12, do not satisfy the hypotheses of the theorem because f fails the prefix property (since $f(b) = a$ is a prefix of $f(a) = ab$). However, the pair of substitutions g and $h = f \circ g$, given by

$$g: \begin{array}{l} a \mapsto ba, \\ b \mapsto a, \end{array} \quad \text{and} \quad h: \begin{array}{l} a \mapsto aab, \\ b \mapsto ab, \end{array}$$

do satisfy the hypotheses, from which it follows that the semigroup generated by this pair has an uncountable forward limit set. Consequently, the forward limit set of the semigroup generated by f and g is also uncountable. \diamond

The hypothesis that $\text{fix}(S)$ contains two words with the same first letter rules out semigroups generated by a single substitution – such semigroups have finite forward limit sets. The prefix hypothesis rules out semigroups generated by substitutions that are not injective.

Example 5.5.4. Consider the substitution semigroup S of the two-letter alphabet $\{a, b\}$ generated by substitutions f and g , where

$$f: \begin{array}{l} a \mapsto aa, \\ b \mapsto aa, \end{array} \quad \text{and} \quad g: \begin{array}{l} a \mapsto ab, \\ b \mapsto ab. \end{array}$$

The forward limit set of S consists of the two fixed points of f and g . ❖

There are more complex substitution semigroups with countable forward limit sets.

Example 5.5.5. Consider the semigroup S generated by the substitutions

$$\begin{array}{l} a \mapsto ac, \\ b \mapsto cb, \\ c \mapsto cba, \end{array} \quad \text{and} \quad \begin{array}{l} a \mapsto bac, \\ b \mapsto c, \\ c \mapsto cba, \end{array}$$

illustrated in Figure 5.5.1, which fail the prefix condition of Theorem 5.5.2.

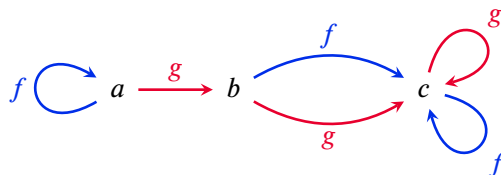


Figure 5.5.1: First-letter graph for $\{f, g\}$.

One can check that $f \circ g = g^2$ and from this it follows that the semigroup S generated by $\mathcal{F} = \{f, g\}$ comprises all substitutions of the form $g^m \circ f^n$, where m and n are positive integers or 0 (and they are not both 0). From this it can be shown that Λ consists of the fixed point x of f with first letter c (also a fixed point of g) as well as all points $g^m(y)$, for $m = 0, 1, 2, \dots$, where y is the fixed point of f with first letter a . Thus Λ is infinite and countable. ❖

5.5.2 Hausdorff dimension of forward limit sets

The main result proved in this section is Theorem 5.5.7, which is framed using logarithmic Hausdorff dimension, which can be used to quantify the size of sets for which the usual Hausdorff dimension is zero. We begin with some background material on Hausdorff dimension, which can be found in [47, 64, 99].

We work in the metric space $(\mathcal{A}^{\mathbb{N}}, d)$. For a non-empty subset U of $\mathcal{A}^{\mathbb{N}}$, the *diameter* of U , denoted $\text{diam } U$, is defined as $\sup\{d(u, v) : u, v \in U\}$; the diameter of the empty set is defined to be 0. For $\varepsilon > 0$, an ε -cover of a subset X of $\mathcal{A}^{\mathbb{N}}$ is a sequence (U_n) of subsets of $\mathcal{A}^{\mathbb{N}}$ for which $X \subseteq \bigcup_n U_n$, and such that, for each n , $\text{diam } U_n$ does not exceed ε . A *dimension function* is a function $\phi : [0, +\infty) \rightarrow [0, +\infty)$

that is increasing, continuous, and satisfies $\lim_{x \rightarrow 0} \phi(x) = \phi(0) = 0$. Let

$$H_\epsilon^\phi(X) = \inf \left\{ \sum_{n=1}^{\infty} \phi(\text{diam } U_n) : (U_n) \text{ is an } \epsilon\text{-cover of } X \right\}$$

and

$$H^\phi(X) = \lim_{\epsilon \rightarrow 0} H_\epsilon^\phi(X).$$

The function H^ϕ is an outer measure on $\mathcal{A}^\mathbb{N}$ known as *Hausdorff measure* with respect to ϕ (see, for example, [99, Section 2.1, Definition 1]).

Given two dimension functions ϕ and ψ such that $\phi(x)/\psi(x) \rightarrow 0$ as $x \rightarrow 0$ it is straightforward to show that if $H^\psi(X) < +\infty$ then $H^\phi(X) = 0$. The dimension functions most widely used are the collection $\phi_t(x) = x^t$, for $t > 0$. For $t_1 < t_2$ we have $\phi_{t_2}(x)/\phi_{t_1}(x) \rightarrow 0$ as $x \rightarrow 0$, so there is a unique value d in $[0, +\infty]$ such that $H^{\phi_{t_1}}(X) = +\infty$, for $t < d$, and $H^{\phi_{t_1}}(X) = 0$, for $t > d$. This value d is the *Hausdorff dimension* of X .

An alternative collection of dimension functions is

$$\psi_t(x) = \begin{cases} 1/\left(\log \frac{1}{x}\right)^t & \text{if } 0 < x \leq 1/e, \\ ex & \text{otherwise,} \end{cases} \quad (5.5.1)$$

for $t > 0$ (see Figure 5.5.2). It is only the value of ψ_t near 0 that matters; the extension to $[0, +\infty)$ is chosen for convenience. For $t_1 < t_2$ we have $\psi_{t_2}(x)/\psi_{t_1}(x) \rightarrow 0$ as $x \rightarrow 0$, so there is a unique value d in $[0, +\infty]$ such that $H^{\psi_{t_1}}(X) = +\infty$, for $t < d$, and $H^{\psi_{t_1}}(X) = 0$ for $t > d$ (see Figure 5.5.3). This value d is the *logarithmic Hausdorff dimension* of X . Notice that, for any positive numbers t_1 and t_2 , $\phi_{t_2}(x)/\psi_{t_1}(x) \rightarrow 0$ as $x \rightarrow 0$, which implies that if X has finite logarithmic Hausdorff dimension, then it has Hausdorff dimension zero.

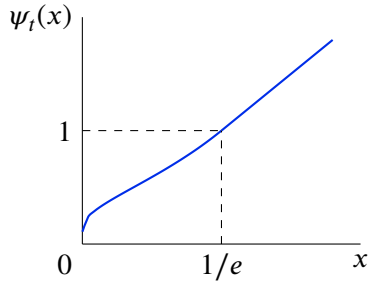


Figure 5.5.2: Dimension function ψ_t with $t = 1$.

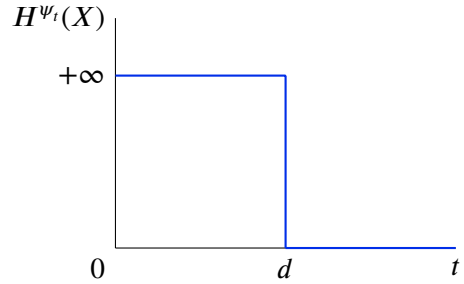


Figure 5.5.3: Hausdorff measure of X for ψ_t .

In the following lemma and thereafter, the *length* of a set \mathcal{F} of substitutions of \mathcal{A} is the least length (number of letters) of $f(a)$, among all substitutions $f \in \mathcal{F}$ and letters $a \in \mathcal{A}$.

Lemma 5.5.6. *Let S be a substitution semigroup generated by a set of substitutions \mathcal{F} of length r . Then, for any word w over \mathcal{F} of length n and any letter a in \mathcal{A} , $|F(w)(a)|$ has length at least r^n .*

Proof. For all $f \in \mathcal{F}$ and $a \in \mathcal{A}$, $|f(a)| \geq r$, and so, for any $f \in \mathcal{F}$ and $a_1, a_2, \dots, a_m \in \mathcal{A}$, $|f(a_1 a_2 \dots a_m)| = \sum_{i=1}^m |f(a_i)| \geq mr$. Since $|w| = n$, there exist $f_1, f_2, \dots, f_n \in \mathcal{F}$ for which $w = f_n \dots f_2 f_1$. It is immediate to prove by induction that $|F_k(a)| \geq r^k$, for $k = 1, 2, \dots, n$, where $F_k = f_k \circ \dots \circ f_2 \circ f_1$. Indeed, $|f_1(a)| \geq r$ and suppose that, for $1 \leq k < n$, $|F_k(a)| \geq r^k$. Then $|F_{k+1}(a)| \geq r|F_k(a)|$, so $|F_{k+1}(a)| \geq r^{k+1}$. \square

Now, we state the main result of this section as follows.

Theorem 5.5.7. *The forward limit set of a substitution semigroup S of \mathcal{A} generated by a finite set of substitutions \mathcal{F} of length r and size s , where $r > 1$, has logarithmic Hausdorff dimension at most $\log_r s$.*

Furthermore, given any pair of positive integers r and s with $r > 1$ and $s \leq |\mathcal{A}|^{r-1}$, there exists a substitution semigroup S with these parameters for which the bound $\log_r s$ is attained.

We start by proving the first part of Theorem 5.5.7, namely, that for a substitution semigroup generated by a finite set of substitutions \mathcal{F} of length r and size s , where $r > 1$, the forward limit set of S has logarithmic Hausdorff dimension at most $\log_r s$.

Proof of Theorem 5.5.7: Part 1. We recall that \mathcal{F}^n denotes the collection of words over \mathcal{F} of length n . Given a word w in \mathcal{F}^n and a letter $a \in \mathcal{A}$, we define the cylinder set

$$X(w, a) = \{x \in \mathcal{A}^{\mathbb{N}} : x \text{ has prefix } F(w)(a)\},$$

which is both closed and open. Let ℓ_n be the maximal possible length of $F(w)(a)$, among all words w in \mathcal{F}^n and letters $a \in \mathcal{A}$.

We will prove that the collection $\mathcal{X}_n = \{X(w, a) : w \in \mathcal{F}^n, a \in \mathcal{A}\}$ covers Λ . To see this, choose $x \in \Lambda$. Then we can find a letter b in \mathcal{A} and a word u over \mathcal{F} for which x and $F(u)(b)$ share a common prefix of length ℓ_n . Let w be the truncation of u after n letters (so $w \in \mathcal{F}^n$) and let v be a word over \mathcal{F} , or the empty word, such that $u = wv$. If v is the empty word, we consider that $F(v)(b) = b$. Define $a = \pi_1(F(v)(b))$. Then $F(w)(a)$ and $F(w)(F(v)(b))$ share a common prefix $F(w)(a)$, which has length equal to or less than ℓ_n . But $F(w)(F(v)(b)) = F(u)(b)$, so x and $F(w)(a)$ share a common prefix $F(w)(a)$. Hence $x \in X(w, a)$.

Next, observe that $\text{diam } X(w, a) \leq 1/2^{r^n}$. Therefore, for any $\varepsilon > 0$, the collection \mathcal{X}_n is an ε -cover of Λ , for sufficiently large values of n . Using the dimension functions ψ_t defined earlier in this section, we see that

$$\psi_t(\text{diam } X(w, a)) \leq \frac{1}{(\log 2)^t r^{nt}}.$$

Since $|\mathcal{X}_n| \leq |\mathcal{A}|s^n$, we then have that

$$\sum_{X(w, a) \in \mathcal{X}_n} \psi_t(\text{diam } X(w, a)) \leq \frac{|\mathcal{A}|}{(\log 2)^t} \left(\frac{s}{r^t}\right)^n.$$

If $s/r^t < 1$, or equivalently $t > \log_r s$, then $H^{\psi_t}(\Lambda) = 0$. Therefore the logarithmic Hausdorff dimension of Λ is less than or equal to $\log_r s$, as required. \square

We now turn to the other part of Theorem 5.5.7, which says that, given any pair of positive integers r and s with $r > 1$ and $s \leq |\mathcal{A}|^{r-1}$, there exists a substitution semigroup S generated by a set of substitutions of minimal length r and size s for which the logarithmic Hausdorff dimension attains the bound $\log_r s$. In proving this we use the following lemma.

Lemma 5.5.8. *Let \mathcal{F} be a set of s substitutions for which $f[a] = a$, $|f(a)| = |g(a)|$, and $f(a) \neq g(a)$, for each $a \in \mathcal{A}$ and each distinct pair $f, g \in \mathcal{F}$. Then, for each positive integer n and $a \in \mathcal{A}$, the s^n words $f_1 \circ f_2 \circ \dots \circ f_n(a)$, where $f_i \in \mathcal{F}$, are distinct.*

Proof. Let $a \in \mathcal{A}$. We assert that, for each positive integer n , the s^n words $f_1 \circ f_2 \circ \dots \circ f_n(a)$, for $f_i \in \mathcal{F}$, are distinct.

This assertion is true for $n = 1$ (one of the hypotheses of the lemma). Suppose that the assertion is true for $n = m-1$, where $m > 1$. Now assume that $f_1 \circ f_2 \circ \dots \circ f_m(a) = g_1 \circ g_2 \circ \dots \circ g_m(a)$, for $f_i, g_i \in \mathcal{F}$. Observe that $f_2 \circ f_3 \circ \dots \circ f_m[a] = a$, so $f_1(a)$ is a prefix of $f_1 \circ f_2 \circ \dots \circ f_m(a)$ of length $|f_1(a)|$. Likewise $g_1(a)$ is a prefix of $g_1 \circ g_2 \circ \dots \circ g_m(a)$ of length $|g_1(a)|$. Since $|f_1(a)| = |g_1(a)|$, we see that $f_1(a) = g_1(a)$, so $f_1 = g_1$. Now, f_1 is injective on \mathcal{A}^+ by Lemma 5.5.1, so $f_2 \circ f_3 \circ \dots \circ f_m(a) = g_2 \circ g_3 \circ \dots \circ g_m(a)$. It follows from the inductive hypothesis that $f_i = g_i$, for $i = 2, 3, \dots, m$, as required. \square

Now we prove the second part of Theorem 5.5.7.

Proof of Theorem 5.5.7: Part 2. Recall that $r > 1$ and $s \leq |\mathcal{A}|^{r-1}$. Observe that there are $|\mathcal{A}|^{r-1}$ words over \mathcal{A} of length r with first letter a . Consequently, we can choose a set \mathcal{F} of s substitutions that satisfy $f[a] = a$, $|f(a)| = |g(a)| = r$ and $f(a) \neq g(a)$, for each $a \in \mathcal{A}$ and each distinct pair $f, g \in \mathcal{F}$. Let S be the substitution semigroup generated by \mathcal{F} , with forward limit set Λ .

We now define a probability measure μ on Λ using the following standard procedure. Let \mathcal{X}_n be the cover of Λ introduced earlier (for $n = 1, 2, \dots$) and let $\mathcal{X}_0 = \mathcal{A}^{\mathbb{N}}$. Observe that, by Lemma 5.5.8, any two members of \mathcal{X}_n are disjoint. Also, $|\mathcal{X}_n| = |\mathcal{A}|s^n$. Each set U in \mathcal{X}_n is contained in one set from \mathcal{X}_{n-1} and contains s sets from \mathcal{X}_{n+1} . The diameter of U is $1/2^n$. Observe that the intersection of any nested sequence of sets (U_n) , with $U_n \in \mathcal{X}_n$, comprises a single infinite word in $\mathcal{A}^{\mathbb{N}}$.

For U in \mathcal{X}_n , we define

$$\mu(U) = \frac{1}{|\mathcal{A}|s^n}$$

and $\mu(E) = 0$, where E is the complement in $\mathcal{A}^{\mathbb{N}}$ of the union of all the members of \mathcal{X}_n . So $\mu(\mathcal{A}^{\mathbb{N}}) = 1$. By [47, Proposition 1.7], μ can be extended to a probability measure on $\mathcal{A}^{\mathbb{N}}$ that is supported on

$$\Delta = \bigcap_{n=1}^{\infty} \bigcup_{U \in \mathcal{X}_n} U.$$

Note that $\Delta \supseteq \Lambda$, since \mathcal{X}_n is a cover of Λ . Conversely, if $x \in \Delta$, then there is a sequence of cylinder sets (U_n) , where $U_n = X(w_n, a)$ with $w_n \in \mathcal{F}^n$ and $a \in \mathcal{A}$, such that $x \in U_n$, for $n = 1, 2, \dots$. Since each element of U_n has prefix $F(w_n)(a)$ and $\bigcap_{n=1}^{\infty} U_n$ comprises a single point, we see that $F(w_n)(a) \rightarrow x$ as $n \rightarrow \infty$. Hence $x \in \Lambda$. Therefore $\Delta = \Lambda$, so μ is supported on Λ .

Suppose now that (U_n) is any ε -cover of Λ , where $\varepsilon = 1/2^r$. Consider some particular set U in this cover, and let k be the positive integer such that

$$\frac{1}{2^{r^{k+1}}} \leq \text{diam } U < \frac{1}{2^{r^k}}.$$

Then U can intersect at most one of the sets from \mathcal{X}_k . Consequently,

$$\mu(U) \leq \frac{1}{|\mathcal{A}|s^k}.$$

Also,

$$\psi_t(\text{diam } U) \geq \psi_t(1/2^{r^{k+1}}) = \frac{1}{(r \log 2)^t r^{kt}}.$$

Let $t = \log_r s$. Then

$$\psi_t(\text{diam } U) \geq \frac{1}{(r \log 2)^t s^k}.$$

Combining these inequalities gives

$$\mu(U) \leq c \psi_t(\text{diam } U), \quad \text{where } c = \frac{(r \log 2)^t}{|\mathcal{A}|}.$$

Thus

$$\sum_{n=1}^{\infty} \psi_t(\text{diam } U_n) \geq \frac{1}{c} \sum_{n=1}^{\infty} \mu(U_n) \geq \frac{1}{c} \mu\left(\bigcup_{n=1}^{\infty} U_n\right) > 0.$$

Thus $H^{\psi_t}(\Lambda) > 0$, so Λ has logarithmic Hausdorff dimension at least $t = \log_r s$. By applying the first part of the proof we see that in fact Λ has logarithmic Hausdorff dimension exactly $\log_r s$, as required. \square

Example 5.5.9. Let S be the substitution semigroup generated by the substitutions

$$f: \begin{array}{l} a \mapsto a b a, \\ b \mapsto b b b, \end{array} \quad \text{and} \quad g: \begin{array}{l} a \mapsto a a a, \\ b \mapsto b a b. \end{array}$$

We call f and g *Cantor substitutions* (see, for example, [57, Section 2.4]). Let $x \in \mathcal{A}^{\mathbb{N}}$ be the fixed point of f with $\pi_1(x) = a$, and let $y \in \mathcal{A}^{\mathbb{N}}$ be the fixed point of g with $\pi_1(y) = b$. For any positive integer n , $\pi_n(x) = a$ (equivalently $\pi_n(y) = b$) if, and only if, the base-3 representation of $n-1$ does not contain any digit equal to 1. We observe that the hypothesis of Theorem 5.5.2 are satisfied, and so the forward limit set Λ of S is uncountable. We also observe that the set $\{f, g\}$ has exactly the form considered in the proof of the second part of Theorem 5.5.7. Hence, the logarithmic Hausdorff dimension of Λ is equal to $\log_3 2$, which coincides with the usual Hausdorff dimension of the ternary Cantor set. \blacklozenge

The assumption that $r > 1$ in Theorem 5.5.7 is not as prohibitive as it may seem, for fixed-letter-free substitution semigroups at least. To justify this claim we present the following example.

Example 5.5.10. Consider the Fibonacci substitution f and the reversed Fibonacci substitution g considered in Section 5.4.1.1. This pair of substitutions has length 1. However, the semigroup generated by f and g has the same forward limit set Λ as the similar semigroup generated by the collection

$\{f^2, f \circ g, g \circ f, g^2\}$, which has length 2 and size 4. Then, by Theorem 5.5.7, the logarithmic Hausdorff dimension of Λ is less than or equal to $\log_2 4 = 2$. More generally, for any positive integer n , the semigroup generated by the collection

$$\mathcal{F}_n = \{f_1 \circ f_2 \circ \cdots \circ f_n : f_i \in \{f, g\}\}$$

has the same forward limit set Λ and therefore, the logarithmic Hausdorff dimension of Λ is equal to or less than $\log_{r_n} s_n$, where r_n and s_n are the length and the size of \mathcal{F}_n , respectively.

It is well known that r_n is equal to c_{n+1} , the $(n+1)$ th Fibonacci number (see, for example, [17, Example 4.6]). The Fibonacci numbers are defined by $c_0 = 0$, $c_1 = 1$ and, for $n = 2, 3, \dots$, $c_n = c_{n-2} + c_{n-1}$. On the other hand, since $f^2 \circ g = g^2 \circ f$, we see that s_n is less than 2^n , for $n = 3, 4, \dots$. Though we can also obtain the value of s_n explicitly using the properties of the Fibonacci numbers.

We will prove that $s_n = c_{n+3} - 1$ by induction. Obviously, $s_1 = c_4 - 1 = 2$ and $s_2 = c_3 - 1 = 4$. Now, suppose that $s_k = c_{k+3} - 1$, for $k = 3, 4, \dots, n$, for a positive integer $n \geq 3$. Among the s_n words over $\{f, g\}$ representing the elements of \mathcal{F}_n , there are s_{n-2} words ending in f^2 and s_{n-2} words ending in g^2 ; hence, the number of words not ending in f^2 or g^2 is $s_n - 2s_{n-2}$. By Example 2.5.8, the only defining relation for the substitution semigroup generated by $\{f, g\}$ is $f^2 \circ g = g^2 \circ f$. Using this fact, we see that the number of words over $\{f, g\}$ representing the elements of \mathcal{F}_{n+1} is

$$\begin{aligned} s_{n+1} &= 2(s_n - 2s_{n-2}) + 2s_{n-2} + 2s_{n-2} - s_{n-2} = 2s_n - s_{n-2} = \\ &= 2c_{n+3} - c_{n+1} - 1 = c_{n+1} + 2c_{n+2} - 1 = c_{n+2} + c_{n+3} - 1 = c_{n+4} - 1, \end{aligned}$$

which completes the inductive proof.

Then, by Theorem 5.5.7, the logarithmic Hausdorff dimension of Λ is less than or equal to

$$\log_{r_n} s_n = \frac{\log(c_{n+3} - 1)}{\log c_{n+1}},$$

for $n = 1, 2, \dots$. Notice that

$$\lim_{n \rightarrow \infty} \log_{r_n} s_n = \lim_{n \rightarrow \infty} \frac{\log c_{n+3}}{\log c_{n+1}}$$

and that $c_{n+3} = c_{n+1} + c_{n+2} = 2c_{n+1} + c_n \leq 3c_{n+1}$, so $\log c_{n+3} \leq \log 3 + \log c_{n+1}$. This directly implies that $\lim_{n \rightarrow \infty} \log_{r_n} s_n = 1$. Hence, the logarithmic Hausdorff dimension of Λ is less than or equal to 1. ♦

5.6 Hulls of substitution semigroups

Central to the study of substitution dynamics is the concept of the hull of a substitution, introduced in Section 2.4.9, and more generally, the hull of a substitution semigroup, introduced in Section 2.5.7. Here we characterise the hull of a substitution semigroup S by its invariant properties, proving that, with some assumptions, it is the least element in the poset of closed, S -invariant and shift-invariant non-empty subsets of $\mathcal{A}^{\mathbb{N}}$.

We recall from Section 2.4.9 that the shift map is the map σ that satisfies $\pi_k(\sigma(w)) = \pi_{k+1}(w)$, for $w \in \tilde{\mathcal{A}}$ and $k \in \mathbb{N}$ (with $k < |w|$ if w is finite). Also, we recall from Section 2.5.7 that the hull $\Omega(a)$ of a letter $a \in \mathcal{A}$ for a substitution semigroup S is given by the closure of $\bigcup_{n=0}^{\infty} \sigma^n(\Lambda(a))$, and the hull Ω of S is given by $\bigcup_{a \in \mathcal{A}} \Omega(a)$.

The hull $\Omega(a)$ is closed and shift-invariant, as can easily be verified. We will prove shortly that it is S -invariant. For this we need the next lemma.

Lemma 5.6.1. *Let h be a substitution of an alphabet \mathcal{A} and let y be an infinite word over \mathcal{A} . Then for any positive integer k there exists a positive integer ℓ for which*

$$h(\sigma^k(y)) = \sigma^\ell(h(y)).$$

Proof. We can write $y = xz$, where x is a finite word of length k and z is an infinite word. Let $\ell = |h(x)|$. Then

$$\sigma^\ell(h(y)) = h(z) = h(\sigma^k(y)),$$

as required. □

Now we can prove that every hull $\Omega(a)$ is S -invariant.

Lemma 5.6.2. *Let S be a substitution semigroup of an alphabet \mathcal{A} and let $a \in \mathcal{A}$. The hull $\Omega(a)$ is S -invariant.*

Proof. Let $x \in \bigcup_n \sigma^n(\Lambda(a))$. Then $x \in \sigma^k(\Lambda(a))$, for some non-negative integer k . Hence there exists a sequence (F_n) in S and a word $y \in \Lambda(a)$ such that $F_n(a) \rightarrow y$ and $\sigma^k(y) = x$.

Let $h \in S$. By Lemma 5.6.1, there is a positive integer ℓ such that

$$h(\sigma^k(y)) = \sigma^\ell(h(y)).$$

That is, $h(x) = \sigma^\ell(h(y))$. Now, we know that $h(y) \in \Lambda(a)$, because $\Lambda(a)$ is S -invariant. Therefore $h(x) \in \sigma^\ell(\Lambda(a))$.

This argument shows that $\bigcup_n \sigma^n(\Lambda(a))$ is S -invariant. By continuity of the action of S , the set $\Omega(a)$ is also S -invariant. □

We recall from Section 2.5.2 that a substitution semigroup S is irreducible if, for any two letters a and b of \mathcal{A} , there exists an element f of S for which the word $f(a)$ contains the letter b .

Lemma 5.6.3. *Let S be an irreducible substitution semigroup and let X be a closed subset of $\mathcal{A}^{\mathbb{N}}$ that is both S -invariant and shift-invariant. Then X contains $\Omega(a)$, for any $a \in \mathcal{A}$.*

Proof. Choose $x \in X$. Since S is irreducible, there is a substitution $h \in S$ for which the word $h(x)$ contains the letter a . Hence there is a non-negative integer k for which $\pi_1(y) = a$, where $y = \sigma^k(h(x))$. Observe that $y \in X$, by S -invariance and shift-invariance of X .

Now choose $u \in \Lambda(a)$. Then there exists a sequence (F_n) in S with $F_n(a) \rightarrow u$. By applying Lemma 5.3.4 we see that $F_n(y) \rightarrow u$ also. Then $u \in X$ by S -invariance and closure of X . Consequently $\Lambda(a) \subseteq X$. Therefore $\Omega(a) \subseteq X$, by shift-invariance, as required. \square

An immediate corollary of Lemma 5.6.3 is that there is only one hull for an irreducible substitution semigroup.

Corollary 5.6.4. *Let S be an irreducible substitution semigroup. Then $\Omega(a) = \Omega(b)$, for all $a, b \in \mathcal{A}$.*

Proof. The hull $\Omega(b)$ is closed and shift-invariant, and it is S -invariant by Lemma 5.6.2. Hence $\Omega(a) \subseteq \Omega(b)$, by Lemma 5.6.3. The roles of a and b can be reversed to give $\Omega(a) = \Omega(b)$. \square

Therefore the hull Ω of an irreducible substitution semigroup S is equal to $\Omega(a)$, for any $a \in \mathcal{A}$.

Next, we prove another corollary of Lemma 5.6.3, which characterises the hull in terms of the actions of S and σ on $\mathcal{A}^{\mathbb{N}}$.

Theorem 5.6.5. *The hull of an irreducible substitution semigroup S is the smallest closed subset of $\mathcal{A}^{\mathbb{N}}$ that is both S -invariant and shift-invariant.*

Proof. We know that the hull Ω is a closed subset of $\mathcal{A}^{\mathbb{N}}$ that is shift-invariant, and it is S -invariant by Lemma 5.6.2.

Now let X be any closed subset of $\mathcal{A}^{\mathbb{N}}$ that is both S -invariant and shift-invariant. Then X contains $\Omega(a)$, by Lemma 5.6.3, and $\Omega(a) = \Omega$, by Corollary 5.6.4, so Ω is the smallest closed subset of $\mathcal{A}^{\mathbb{N}}$ that is both S -invariant and shift-invariant. \square

We recall from Section 2.5.2 that a substitution semigroup S with generating set \mathcal{F} is primitive if there is a positive integer n such that, for all letters a and b of \mathcal{A} , all the words $f_1 \circ f_2 \circ \cdots \circ f_n(a)$ with f_i in \mathcal{F} contain the letter b . We recall from Section 2.5.7 that the subshift \mathbb{X} of a substitution semigroup S is the set of those infinite words for which all the subwords are included in the language of S . In other words, the subshift of S is the set $\mathbb{X} = \{w \in \mathcal{A}^{\mathbb{N}} : \mathcal{L}(w) \subseteq \mathcal{L}\}$, where \mathcal{L} is the language of S .

We finish this section with an extension of a well-known result for single primitive substitutions to primitive substitution semigroups. In Theorem 2.4.35 we learnt that the hull and the subshift of a primitive substitution are equal, and they are uniquely determined by any fixed point of the substitution. The following theorem gives the analogous result for substitution semigroups.

Theorem 5.6.6. *The hull and the subshift of a finitely-generated primitive substitution semigroup S are equal to each other, and they are given by the closure of the shift-orbit of $S(X)$, where $X = \text{fix}(S)$.*

Proof. Let S be a finitely-generated primitive substitution semigroup with forward limit set Λ , hull Ω and subshift \mathbb{X} . Observe that, since S is primitive, it is fixed-letter-free. Indeed, if there is a letter $a \in \mathcal{A}$ and a substitution $f \in S$ with $f(a) = a$, then $f^n(a) = a$, for all positive integers n , so S is not primitive.

The hull of S can be written as the closure of the shift-orbit of Λ , or, in other words, $\Omega = \overline{\bigcup_n \sigma^n(\Lambda)}$. It is then easy to show that Ω is the closure of the shift-orbit of $S(X)$, or, in other words,

$$\Omega = \overline{\bigcup_{n=0}^{\infty} \sigma^n(S(X))}.$$

Let x be a point in Ω . Then there are a sequence (k_n) of non-negative integers and a sequence (y_n) in Λ with $\sigma^{k_n}(y_n) \rightarrow x$ as $n \rightarrow \infty$. Since S is fixed-letter-free, by Theorem 5.4.24, $\Lambda = \overline{S(X)}$, where $X = \text{fix}(S)$ is the set of all fixed points of substitutions from S . Hence, for each non-negative integer n , there are sequences (z_i) in X and (F_i) in S with $F_i(z_i) \rightarrow y_n$ as $i \rightarrow \infty$. So, by continuity of the shift map, $\sigma^{k_n}(F_n(z_n)) \rightarrow x$ as $n \rightarrow \infty$. Since $(F_n(z_n))$ is a sequence in $S(X)$, we see that $x \in \overline{\bigcup_n \sigma^n(S(X))}$. Conversely, let $x \in \overline{\bigcup_n \sigma^n(S(X))}$. Since $S(X)$ is a subset of Λ , we see that x is a point in Ω .

Next, we prove that Ω and \mathbb{X} are equal. Let x be a point in Ω . Then there is an infinite word y in Λ and a sequence (k_n) of non-negative integers such that $\sigma^{k_n}(y) \rightarrow x$ as $n \rightarrow \infty$. Since $y \in \Lambda$, there is a letter $a \in \mathcal{A}$ and a sequence (F_n) in S such that $F_n(a) \rightarrow y$. Consequently, any subword w of x , which is therefore also a subword of y , appears in $F_n(a)$, for sufficiently large values of n . So w belongs to the language of S , hence x is a point in \mathbb{X} . Therefore $\Omega \subseteq \mathbb{X}$.

Conversely, let x be a point in \mathbb{X} . Then, for each positive integer n , there is a letter $a_n \in \mathcal{A}$ and a substitution $F_n \in S$ such that the word $\pi_1(x)\pi_2(x) \cdots \pi_n(x)$ occurs in $F_n(a_n)$. Note that the set of fixed points X cannot be empty. So, for each n , we can choose an infinite word $y_n \in X$ and define $z_n = F_n(y_n) \in S(X)$. Since S is primitive, y_n contains the letter a_n . So z_n contains the word $F_n(a_n)$, hence it also contains the word $\pi_1(x)\pi_2(x) \cdots \pi_n(x)$. So there is a sequence (k_n) of non-negative integers such that the infinite word $\sigma^{k_n}(z_n)$ has the finite word $\pi_1(x)\pi_2(x) \cdots \pi_n(x)$ as a prefix, so $\sigma^{k_n}(z_n) \rightarrow x$ as $n \rightarrow \infty$. Note that $z_n \in \Lambda$ because, since S is fixed-letter-free, $\Lambda = \overline{S(X)}$. Hence $(\sigma^{k_n}(z_n))$ is a sequence in Ω and, since Ω is a closed subset of $\mathcal{A}^{\mathbb{N}}$, x is a point in Ω . So $\mathbb{X} \subseteq \Omega$. Therefore $\Omega = \mathbb{X}$, as required. \square

Example 5.6.7. Consider the substitution semigroup S generated by the substitutions

$$\begin{array}{ll} a \mapsto ab, & a \mapsto ab, \\ f: b \mapsto aa, & \text{and} \quad g: b \mapsto ba, \\ c \mapsto ca, & c \mapsto ca. \end{array}$$

Clearly S is not a primitive substitution semigroup (notice that the letter c does not appear in any of the images of the letters a and b under any element of S). It is easy to see that the letter b appears infinitely many times in every point of the forward limit set Λ of S . Then, since the hull of S is given by the closure of $\bigcup_n \sigma^n(\Lambda)$, the infinite word $x = aaa \cdots$ is not an element of the hull. However, x is a point of the subshift of S because the word aa belongs to the language of S , since $f(b) = aa$. Therefore, the hull and the subshift of S are not equal. \blacklozenge

6. DIRECTIONS FOR FURTHER RESEARCH

The results obtained in the previous chapters invite further research on the topics discussed in this thesis. In this chapter we set out some of the new ideas that we want to address in the future. Section 6.1 is about monochromatic arithmetic progressions in infinite words and Section 6.2 is about forward limit sets of substitution semigroups.

6.1 Monochromatic arithmetic progressions

In this section we present the ideas on which we will work in the future concerning monochromatic arithmetic progressions in infinite words. In Sections 6.1.1 and 6.1.2 we consider monochromatic arithmetic progressions in automatic sequences which arise from constant-length substitutions that are bijective and non-bijective, respectively. In Section 6.1.3 we consider monochromatic arithmetic progressions in higher-dimensional automatic sequences.

6.1.1 Bijective constant-length substitutions

In Chapter 3 we studied the length of the longest monochromatic arithmetic progressions appearing in the Thue–Morse sequence (Section 3.2) and in some generalised Thue–Morse sequences (Section 3.3). In the future, we will continue this work.

In the case of the Thue–Morse sequence, we want to obtain a better understanding of the plot of Figure 3.2.1, which displays the exact value of $A(d)$, for $d = 1, 2, \dots, 1100$, obtained experimentally using the algorithm described in Appendix A. Our main goal is to obtain a complete description of the symmetric distribution of the values of $A(d)$ that we can see in this figure around some particular differences d .

The “peaks” observed around differences of the form 2^n can be explained from our results. More precisely, observe that these peaks occur for differences of the form $d = 2^n \pm 2^k$, for $0 \leq k < n$ (see, for example, the “zoom” made in Figure 3.2.1 around the difference 2^9). By Lemma 3.2.4, for $1 \leq k < n$, $A(2^n \pm 2^k) = A(2^{n-k} \pm 1)$, so these values follow from Proposition 3.2.13 and Theorem 3.2.12. This implies that $|A(2^n + 2^k) - A(2^n - 2^k)| = 2$, or more precisely,

$$A(2^n + 2^k) - A(2^n - 2^k) = \begin{cases} 2, & \text{if } n \text{ and } k \text{ have the same parity,} \\ -2, & \text{otherwise,} \end{cases}$$

which explains the symmetric distribution of the values of $A(d)$ around differences of the form 2^n .

We do not know of an expression that gives the values taken by $A(d)$, for differences d others than 2^n and $2^n \pm 2^k$. The values taken by $A(d)$ in most of these cases are small compared to $A(2^n \pm 2^k)$. Nonetheless, there are some exceptions, which correspond to some of the peaks in Figure 3.2.1, such as the values taken by $A(d)$ for differences d around $3 \cdot 2^n$, for $n = 1, 2, \dots$. Observe that, by Lemma 3.2.4, $A(3 \cdot 2^n) = A(3) = 8$. One can check that $A(d)$ is significantly larger than 8 (corresponding to the peaks) at $d = 3(2^n \pm 2^k)$, for $k = 1, 2, \dots, n-4$. Experimental data also reveals that $|A(3(2^n + 2^k)) - A(3(2^n - 2^k))| = 1$, or, more precisely,

$$A(3(2^n + 2^k)) - A(3(2^n - 2^k)) = \begin{cases} -1, & \text{if } n \text{ and } k \text{ have the same parity,} \\ 1, & \text{otherwise.} \end{cases}$$

Not only are we interested in the peaks of Figure 3.2.1, but also in the set of values taken by $A(d)$, that is, $\{A(1), A(2), \dots\}$. In Section 3.2.6, in particular, we wondered whether 3 is the smallest positive integer that is not in this set (this is Conjecture 42 in [2]). We will try to answer this question too.

In the case of the generalised Thue–Morse sequences of Section 3.3, the goal is similar. We will try to prove Conjecture 3.3.11 and, more generally, to obtain a complete description of the distribution of $A(d)$ (consider, for instance, the two examples of Figures 3.3.1 and 3.3.2).

6.1.2 General constant-length substitutions

We recall from Section 2.4.5 that an automatic sequence is the fixed point, under a coding, of a constant-length substitution. Many of the automatic sequences we have considered, such as the Thue–Morse sequence and the generalised Thue–Morse sequences, arise from bijective constant-length substitutions. We will call them *bijective automatic sequences*. A natural extension to our work that we want to tackle in the future is the case of automatic sequences arising from non-bijective constant-length substitutions. We will call them *non-bijective automatic sequences*. In Chapter 4 we obtained some results for some such sequences, however we aim to obtain more general results which are valid for any non-bijective automatic sequence.

Some bijective automatic sequences admit alternative descriptions using mathematical tools from other areas of mathematics, such as number theory. For example, the Thue–Morse sequence can be described as the sum of the binary digits of the non-negative integers (modulo 2) [6]. Another example is the Rudin–Shapiro sequence which can be described as the number of (possibly overlapping) occurrences of the string 11 in the binary digits of the non-negative integers (modulo 2) [8]. For non-bijective automatic sequences, these kinds of descriptions are rarely known (an exception can be found, for example, in [103, Theorem 58]), which motivates us to study these sequences further.

In this section we introduce the column semigroup of a constant-length substitution and the graph of sets for that substitution, two tools that we suspect we will find useful to explore questions regarding non-bijective automatic sequences, and to gather more information on the behaviour of $A(d)$.

The columns of a bijective substitution are permutations of the alphabet, making it possible to define the group generated by these columns. If a constant-length substitution fails to be bijective, the aforementioned group can be replaced by a semigroup of letter-to-letter substitutions, which has only recently received attention [77, 83].

Definition 6.1.1. Let ϱ be a substitution of \mathcal{A} of constant length L . The *column semigroup* S of ϱ is the semigroup generated by the columns of ϱ under composition of functions. In other words,

$$S = \left\{ f_1 \circ f_2 \circ \cdots \circ f_n : f_i \in \{[\varrho]_0, \dots, [\varrho]_{L-1}\}, n \in \mathbb{N} \right\}.$$

The elements of S are letter-to-letter substitutions (codings), so the natural action of S is on \mathcal{A} . This action can be visualised using a directed graph. In the following definition, for a substitution $s \in S$, we write the set $\{s(a) : a \in \mathcal{A}\}$ as $s(\mathcal{A})$.

Definition 6.1.2. Let ϱ be a substitution of \mathcal{A} of constant length L , and let S be its column semigroup. The *graph of sets* for ϱ , denoted G_ϱ , is the directed graph with vertex set $V = \{s(\mathcal{A}) : s \in S \cup \text{id}\}$ and, for each $k \in \{0, 1, \dots, L-1\}$ and $v \in V$, a directed edge, labelled k , from vertex v to the vertex $[\varrho]_k(v)$.

Similar directed graphs to the graph of sets considered here can be found in [36]. If \mathcal{A} is finite, then S is finite and consequently, G_ϱ is finite too. Notice that, if there exists a directed edge from a vertex u to a vertex v of V , then $|v| \leq |u|$, where $|x|$ is the size of the set x . One can prove that G_ϱ has a unique terminal component. The sets of this terminal component are called the *minimal sets* of G_ϱ . When ϱ has height 1, the size of any minimal set, denoted C_ϱ , is called the *column number* of G_ϱ [77]. The column number satisfies $1 \leq C_\varrho \leq |\mathcal{A}|$, where the upper bound is attained for bijective substitutions and the lower bound is attained for substitutions admitting coincidences.

It is customary to draw G_ϱ with the vertices ordered in levels according to their sizes, with all vertices of the same size in the same level. The vertex \mathcal{A} , which is the largest vertex, is on the highest level and the minimal sets, which are the smallest vertices, are on the lowest level.

Example 6.1.3. The graph of sets for a bijective substitution of \mathcal{A} of length L consists always of the single vertex \mathcal{A} and L loops. For example,

$$\begin{array}{lcl} a & \mapsto & a b b, \\ \varrho: b & \mapsto & b c a, \\ c & \mapsto & c a c. \end{array} \qquad \begin{array}{c} 0,1,2 \\ \curvearrowright \\ \{a, b, c\} \end{array}$$

Figure 6.1.1: Graph of sets for ϱ .

❖

Example 6.1.4. Consider the substitution ϱ given by

$$\begin{aligned} \varrho: \quad a &\mapsto ab, \\ b &\mapsto cb, \\ c &\mapsto ad, \\ d &\mapsto cd, \end{aligned}$$

which is primitive and has height 1. The graph of sets for ϱ , shown in Figure 6.1.2, has three levels and the lowest level contains four minimal sets, each of size 1. So the column number is $C_\varrho = 1$ and consequently, ϱ admits coincidences. The shortest walks in G_f from \mathcal{A} to a minimal set have length 2 and

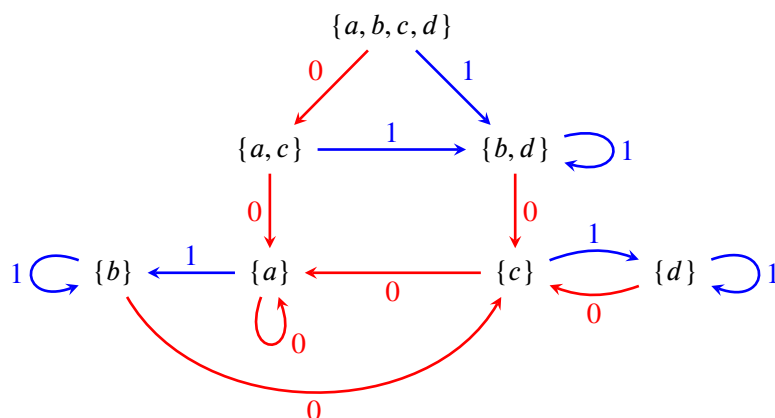


Figure 6.1.2: Graph of sets for ϱ .

there are two such walks. This implies that ϱ admits two coincidences at order 2. To be more precise, one of these two walks is labelled $[0, 0]$ and terminates in the minimal set $\{a\}$ and the other walk is labelled $[1, 0]$ and terminates in the minimal set $\{c\}$. Since $[0, 0]$ and $[1, 0]$ are the binary representations of 0 and 2, respectively, we see that the 0th column of ϱ^2 is a coincidence column of a letters and the 2nd column of ϱ^2 is a coincidence column of c letters. Indeed,

$$\begin{aligned} \varrho^2: \quad a &\mapsto abcb, \\ b &\mapsto adcb, \\ c &\mapsto abcd, \\ d &\mapsto adcd. \end{aligned}$$

This implies that the fixed points of ϱ^2 contain infinitely long monochromatic arithmetic progressions of difference 4. More generally, every infinite word that is a fixed point of a substitution of constant length L which admits coincidences at order n always contain infinitely long monochromatic arithmetic progressions of difference L^n . \diamond

Example 6.1.5. Consider the substitution ρ of $\mathcal{A} = \{a, b, c, d\}$ given by

$$\begin{aligned} \rho: \quad a &\mapsto ac, \\ b &\mapsto bd, \\ c &\mapsto ad, \\ d &\mapsto bc, \end{aligned}$$

which is primitive and has height 1. By the graph of sets for ρ , shown in Figure 6.1.3, the column number is $C_\rho = 2$, so $1 < C_\rho < |\mathcal{A}|$. This implies that ρ does not admit any coincidence, but it admits partial coincidences. \blacklozenge

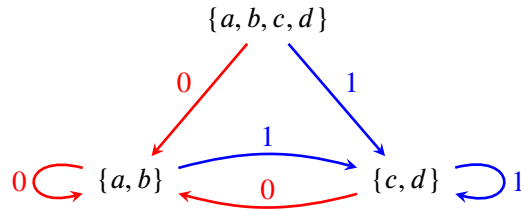


Figure 6.1.3: Graph of sets for ρ .

Example 6.1.6. Consider the following six-letter substitution ρ

$$\rho: \quad \begin{array}{lll} a &\mapsto ad, & c &\mapsto ea, & e &\mapsto bf, \\ b &\mapsto bc, & d &\mapsto ab, & f &\mapsto ba. \end{array}$$

The graph of sets for ρ is shown in Figure 6.1.4.

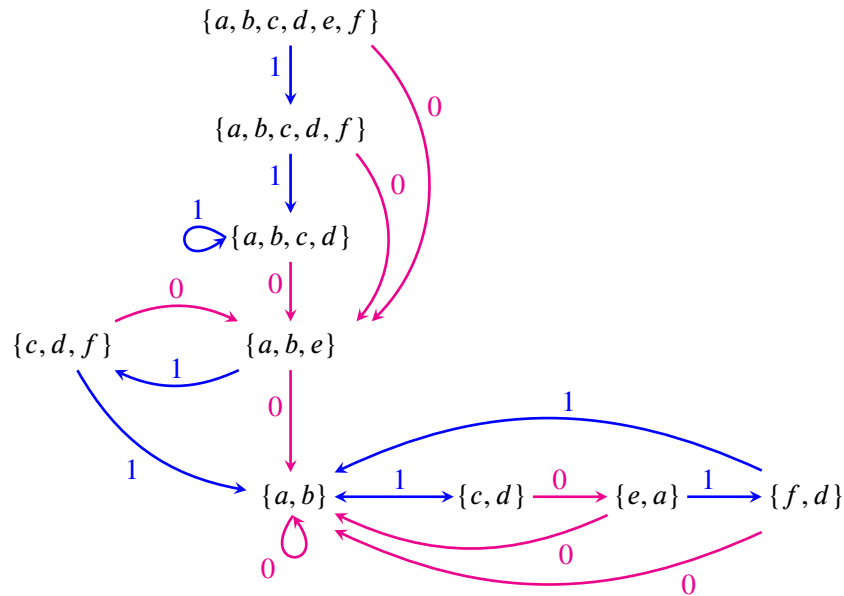


Figure 6.1.4: Graph of sets for ρ .

Minimal sets may be good candidates to look for long monochromatic arithmetic progressions within the fixed points of ρ because, since they all belong to the terminal component of G_ρ , we can consider

directed walks over this terminal component that return to the same minimal set every d steps, which may yield long monochromatic arithmetic progressions of difference d . The difficulty, however, is that a minimal set may contain two letters, and so the arithmetic progressions found may be bichromatic (two-coloured). This nonetheless could help to narrow down the scope of suitable differences d for which long monochromatic arithmetic progression may be found.

For this particular example, computer experiments suggests that $A(d)$ grows polynomially along differences of the form $2^n + 2$ (see Figure 6.1.5 and the experimental data underlying this thesis). Notice that, for $n > 3$, the binary representation of $2^n + 2$ is of the form $[1, 0, 0, \dots, 0, 1, 0]$, and tracing this path from $\{a, b\}$ or $\{e, a\}$ leads to $\{e, a\}$.

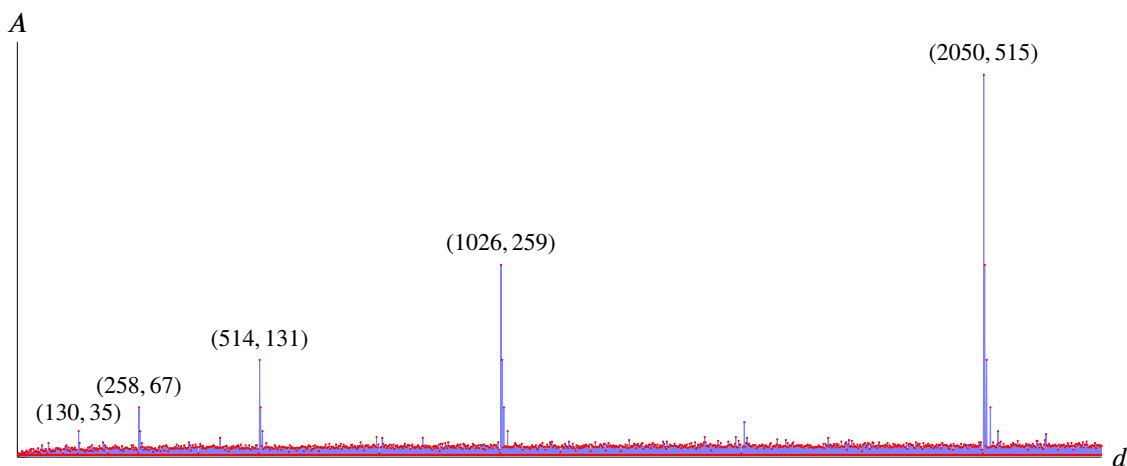


Figure 6.1.5: $A(d)$, for $d = 1, 2, \dots, 2300$, for the fixed point of ρ starting with the letter a .

❖

6.1.3 Higher-dimensional monochromatic arithmetic progressions

In Chapter 3 we obtained results for monochromatic arithmetic progressions in one-dimensional automatic sequences. In the future, we will also consider generalising monochromatic arithmetic progressions to higher-dimensional words. In this section we give the definitions of the higher-dimensional counterparts of the mathematical objects used in Chapter 3, such as words, substitutions and monochromatic arithmetic progressions, and we prove some preliminary results. In particular, we prove the generalisation of Proposition 4.2.2 to higher dimensions.

For simplicity, we will only consider substitutions of “rectangular” words (see, for example, [50,55]). In particular, we will look at substitutions of constant size, which are a generalisation of one-dimensional constant-length substitutions. Loosely speaking, a substitutions of constant size in p dimensions substitutes every letter of an alphabet \mathcal{A} with a word over \mathcal{A} with certain p -dimensional “rectangular” shape. The iteration of a letter under the substitution produces rectangular word of increasing size and generates infinite p -dimensional words with no holes.

Let \mathcal{A} be a finite alphabet and let p be a positive integer. A p -dimensional (rectangular) word w over \mathcal{A} with length vector $L_w = (L_1, L_2, \dots, L_p)$ is a subset of $\mathcal{A} \times X_w$, where

$$X_w = \{(x_1, x_2, \dots, x_p) \in \mathbb{N}_0^p : x_i \in \{0, 1, \dots, L_i - 1\}, i \in \{1, 2, \dots, p\}\}.$$

We say that X_w is the *support* of w . We denote the set of all non-empty p -dimensional words over \mathcal{A} by \mathcal{A}^+ . Given a p -dimensional word w with support X_w , for every $x \in X_w$, the letter of w located at x is denoted by w_x .

Example 6.1.7. An example of a two-dimensional word over the alphabet $\{\blacksquare, \blacksquare\}$ is

$$w = \begin{array}{|c|c|c|} \hline \blacksquare & \blacksquare & \blacksquare \\ \hline \blacksquare & \blacksquare & \blacksquare \\ \hline \end{array}.$$

The length vector of w is $(3, 2)$ and its support is $\{(0, 0), (1, 0), (2, 0), (2, 1)\}$. ❖

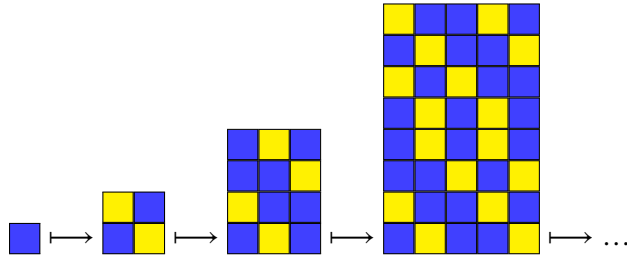
A p -dimensional infinite word w over \mathcal{A} is a subset of $\mathcal{A} \times \mathbb{N}_0^p$, which can be considered as tiling of the first quadrant of the plane. We denote the set of all p -dimensional infinite words over \mathcal{A} by $\mathcal{A}^{\mathbb{N}_0^p}$.

Let \mathcal{A} be a finite alphabet and let p be a positive integer. Similar to the one-dimensional case, a *substitution* ρ of p -dimensional words over \mathcal{A} is a map $\mathcal{A} \rightarrow \mathcal{A}^+$. A substitution ρ is said to be *primitive* if there exists a positive integer n such that, for all $a \in \mathcal{A}$, all the letters of \mathcal{A} appear in the word $\rho^n(a)$.

Example 6.1.8. An example of a primitive substitution of two-dimensional words over $\mathcal{A} = \{\blacksquare, \blacksquare\}$ is

$$\rho: \blacksquare \mapsto \begin{array}{|c|c|} \hline \blacksquare & \blacksquare \\ \hline \blacksquare & \blacksquare \\ \hline \end{array}, \quad \blacksquare \mapsto \begin{array}{|c|} \hline \blacksquare \\ \hline \blacksquare \\ \hline \end{array}.$$

Notice that the support of $\rho(\blacksquare)$ is $\{(0, 0), (0, 1), (1, 0), (1, 1)\}$, while the support of $\rho(\blacksquare)$ is $\{(0, 0), (0, 1)\}$. This substitution extended to a map $\mathcal{A}^+ \rightarrow \mathcal{A}^+$ and also to a map $\mathcal{A}^{\mathbb{N}_0^p} \rightarrow \mathcal{A}^{\mathbb{N}_0^p}$. Consequently, a word from \mathcal{A}^+ can be iterated under this substitution in the usual way. For example,



Notice that each iteration step generates an element of \mathcal{A}^+ . ❖

Not every substitution extends to a map $\mathcal{A}^+ \rightarrow \mathcal{A}^+$, as in the previous example. The iteration of an element from \mathcal{A}^+ may generate p -dimensional words with holes, which do not belong to \mathcal{A}^+ . To ensure a good behaviour under iteration, one needs an expansive map that leads to an inflate-and-subdivide rule. We do not develop the theory here, which can be found, for example, in [50–52]. Here, we will always

assume that the substitutions considered extend to a map $\mathcal{A}^+ \longrightarrow \mathcal{A}^+$ and hence, to a map $\mathcal{A}^{\mathbb{N}_0^p} \longrightarrow \mathcal{A}^{\mathbb{N}_0^p}$, so they generate p -dimensional infinite words.

Let ρ be a substitution of p -dimensional words over \mathcal{A} . We say that ρ has *constant length* if the images of the letters of \mathcal{A} under ρ all have the same length vector and hence same support, that is, $L_{\rho(a)} = L_{\rho(b)}$ and $X_{\rho(a)} = X_{\rho(b)}$, for all $a, b \in \mathcal{A}$. In such a case, we say that the *length vector* and the *support* of ρ are $L_{\rho(a)}$ and $X_{\rho(a)}$, respectively, for any $a \in \mathcal{A}$, and we denote them by L and X , respectively. We say that ρ is *bijective* if $\rho(a)_x \neq \rho(b)_x$, for all different letters $a, b \in \mathcal{A}$ and all $x \in X$. The substitution in Example 6.1.8 is not a constant-length substitution.

Example 6.1.9. An example of a primitive, constant-length substitution of two-dimensional words is

$$\rho: \begin{array}{c} \text{blue square} \end{array} \mapsto \begin{array}{cc} \text{yellow} & \text{yellow} \\ \text{blue} & \text{yellow} \end{array}, \quad \begin{array}{c} \text{yellow square} \end{array} \mapsto \begin{array}{cc} \text{blue} & \text{blue} \\ \text{yellow} & \text{blue} \end{array}.$$

This substitution is bijective. ❖

Similar to the one-dimensional case, a constant-length substitution ρ is determined by its columns. Let ρ be a substitution of p -dimensional words over \mathcal{A} with support X . For every $x \in X$, the substitution given, for all $a \in \mathcal{A}$, by $a \mapsto \rho(a)_x$ is a *column* of ρ ; we denote it by $[\rho]_x$. Since $\{\rho(a)_x : a \in \mathcal{A}\}$ is a subset of the alphabet, every column is a letter-to-letter substitution. The semigroup generated by the columns of a uniform substitution ρ is called the *column semigroup* of ρ . If ρ is bijective it becomes a group and we call it the *column group* of ρ .

The following result is an extension of Proposition 4.1.2 for constant-length substitutions in one dimension to constant-length substitutions in higher dimensions. We omit the proof which is similar to the one-dimensional case. Notice that the result does not require the substitution to be bijective. Here and hereafter, for a vector $V \in \mathbb{N}_0^p$, the i th entry of V is denoted by V_i .

Proposition 6.1.10. *Let ρ be a constant-length substitution of p -dimensional words with length vector L and let n be a positive integer. For every (x_1, \dots, x_p) in the support of ρ^n , the column of ρ^n at position (x_1, \dots, x_p) is given by*

$$[\rho^n]_{(x_1, \dots, x_p)} = [\rho]_{(x_0^{(1)}, \dots, x_0^{(p)})} \circ [\rho]_{(x_1^{(1)}, \dots, x_1^{(p)})} \circ \dots \circ [\rho]_{(x_{n-1}^{(1)}, \dots, x_{n-1}^{(p)})},$$

with $[x_{n-1}^{(1)}, \dots, x_1^{(1)}, x_0^{(1)}]$ the representation of x_i in base L_i , for $i = 1, \dots, p$.

Example 6.1.11. Consider the substitution

$$\rho: \begin{array}{c} \text{blue square} \end{array} \mapsto \begin{array}{ccc} \text{yellow} & \text{blue} & \text{yellow} \\ \text{blue} & \text{yellow} & \text{blue} \end{array}, \quad \begin{array}{c} \text{yellow square} \end{array} \mapsto \begin{array}{ccc} \text{blue} & \text{yellow} & \text{yellow} \\ \text{yellow} & \text{blue} & \text{blue} \end{array}.$$

The length vector of ρ is $L = (3, 2)$ and its support is $X = \{(0, 0), (1, 0), (2, 0), (0, 1), (1, 1), (2, 1)\}$. The

columns of ϱ are the letter-to-letter substitutions

$$\begin{aligned} [\varrho]_{(0,0)} = [\varrho]_{(1,1)} : & \begin{array}{c} \blacksquare \mapsto \blacksquare, \\ \blacksquare \mapsto \blacksquare, \end{array} & [\varrho]_{(2,0)} : & \begin{array}{c} \blacksquare \mapsto \blacksquare, \\ \blacksquare \mapsto \blacksquare, \end{array} \\ [\varrho]_{(1,0)} = [\varrho]_{(0,1)} : & \begin{array}{c} \blacksquare \mapsto \blacksquare, \\ \blacksquare \mapsto \blacksquare, \end{array} & [\varrho]_{(2,1)} : & \begin{array}{c} \blacksquare \mapsto \blacksquare, \\ \blacksquare \mapsto \blacksquare. \end{array} \end{aligned}$$

Now, for example, we can determine the column of ϱ^2 located at position $(6, 3)$, which belongs to the support of ϱ^2 . Since the representation of 6 in base $L_1 = 3$ is $[2, 0]$ and the representation of 3 in base $L_2 = 2$ is $[1, 1]$, we will need the vectors $x_0 = (0, 1)$ and $x_1 = (2, 1)$. Then, by Proposition 6.1.10,

$$[\varrho^2]_{(6,3)} = [\varrho]_{(0,1)} \circ [\varrho]_{(2,1)} : \begin{array}{c} \blacksquare \mapsto \blacksquare, \\ \blacksquare \mapsto \blacksquare. \end{array}$$

Similarly, we can see that the column of ϱ^2 located at position $(0, 3)$ is given by

$$[\varrho^2]_{(0,3)} = [\varrho]_{(0,1)}^2 : \begin{array}{c} \blacksquare \mapsto \blacksquare, \\ \blacksquare \mapsto \blacksquare, \end{array}$$

that is, it is the identity substitution. One can verify that these are correct using the substitution

$$\varrho^2 : \begin{array}{c} \blacksquare \mapsto \begin{array}{cccccccc} \blacksquare & \blacksquare & \blacksquare & \blacksquare & \blacksquare & \blacksquare & \blacksquare & \blacksquare \\ \blacksquare & \blacksquare & \blacksquare & \blacksquare & \blacksquare & \blacksquare & \blacksquare & \blacksquare \\ \blacksquare & \blacksquare & \blacksquare & \blacksquare & \blacksquare & \blacksquare & \blacksquare & \blacksquare \\ \blacksquare & \blacksquare & \blacksquare & \blacksquare & \blacksquare & \blacksquare & \blacksquare & \blacksquare \end{array}, \\ \blacksquare \mapsto \begin{array}{cccccccc} \blacksquare & \blacksquare & \blacksquare & \blacksquare & \blacksquare & \blacksquare & \blacksquare & \blacksquare \\ \blacksquare & \blacksquare & \blacksquare & \blacksquare & \blacksquare & \blacksquare & \blacksquare & \blacksquare \\ \blacksquare & \blacksquare & \blacksquare & \blacksquare & \blacksquare & \blacksquare & \blacksquare & \blacksquare \\ \blacksquare & \blacksquare & \blacksquare & \blacksquare & \blacksquare & \blacksquare & \blacksquare & \blacksquare \end{array}. \end{array}$$

❖

Next, we define the analogs of arithmetic progressions and monochromatic arithmetic progressions in p dimensions.

Definition 6.1.12. For a positive integer p , a (finite) p -dimensional arithmetic progression is a set

$$\{s + n_1 d_1 + \dots + n_p d_p : 0 \leq n_i < M_i \text{ for all } 1 \leq i \leq p\},$$

where s is a fixed vector in \mathbb{N}_0^p , d_1, \dots, d_p are linearly independent fixed vectors in \mathbb{N}^p , and M_1, \dots, M_p are fixed positive integers. We call the elements d_1, \dots, d_p the *differences* and $M = (M_1, \dots, M_p)$ the *size vector* of the progression. If we allow $M_i = \infty$, for some $1 \leq i \leq p$, we say that the arithmetic progression has infinite size.

Definition 6.1.13. For a positive integer p , let w be a p -dimensional word over \mathcal{A} and q a positive integer not larger than p . We say that w contains a (finite) q -dimensional monochromatic arithmetic progression if there exist a letter $a \in \mathcal{A}$ and a q -dimensional arithmetic progression R such that $w_r = a$, for all $r \in R$. The monochromatic progression inherits the differences, size vector and starting position of R . In other words, w contains a q -dimensional monochromatic arithmetic progression of differences d_1, \dots, d_q , size

vector M , and starting position s , if

$$w_s = w_{s+n_1d_1+\dots+n_qd_q},$$

for all $0 \leq n_i < M_i$ and all $1 \leq i \leq q$. If $M_i = \infty$ is allowed, for some $1 \leq i \leq q$, the monochromatic arithmetic progression is said to be of infinite size.

Here, for p -dimensional words, we will only consider p -dimensional monochromatic arithmetic progressions, also called *monochromatic arithmetic progressions of full rank*. Similar to the one-dimensional case, we can consider the largest p -dimensional monochromatic arithmetic progressions within a p -dimensional word. Since we now have p linearly independent differences, we need to consider p contributions.

Definition 6.1.14. For a p -dimensional word w over \mathcal{A} and linearly independent vectors d_1, \dots, d_p in \mathbb{N}^p , we define $A_w(d_1, \dots, d_p)$ as the maximum size of the grid spanned by the vectors such that the letters of w at the positions determined by the grid are all equal to a fixed letter $a \in \mathcal{A}$. More precisely, $A_w(d_1, \dots, d_p)$ is the maximum product $\prod_{i=1}^p M_i$ of positive integers such that

$$w_s = w_{s+n_1d_1+\dots+n_pd_p}$$

for all $0 \leq n_i < M_i$ and $1 \leq i \leq p$, and some s in the defining set of w .

Notice that the previous definition does not consider monochromatic arithmetic progressions of infinite size. To consider finite as well as infinite progressions we would need to allow $M_i = \infty$, for some $1 \leq i \leq p$. However, we will not need this, as we will work only with finite arithmetic progressions.

The results given in Section 3.1 in Chapter 3 for dimension one extend to higher dimensions, since [84] and [38] also have higher dimensional extensions. In particular, Propositions 3.1.3 and 3.1.4 and Corollary 3.1.5 in that chapter hold in higher dimensions. Similarly, since [76] also extend to higher dimensions, Proposition 4.2.1 in Chapter 4 also holds in higher dimensions. As a consequence, we have the following result.

Proposition 6.1.15. *Let ϱ be an aperiodic, primitive, bijective substitution of p -dimensional words. Every p -dimensional monochromatic arithmetic progression occurring in a fixed point of any power of ϱ has finite size vector. Consequently, $A(d_1, \dots, d_p) < \infty$, for all linearly independent vectors d_1, \dots, d_p in \mathbb{N}^p .*

The following result is a generalisation of Proposition 4.2.2 to the p -dimensional scenario. It shows that, for aperiodic, primitive and bijective substitutions, $A(d)$ grows at least polynomially in d for an specific form of the differences d_1, \dots, d_p .

Proposition 6.1.16. *Let ϱ be an aperiodic, primitive, bijective substitution of p -dimensional words, which has a column equal to the identity, length vector $L = (L_1, \dots, L_p)$, and column group G . Then, for any fixed point of a power of ϱ ,*

$$\prod_{i=1}^p L_i^n \leq A(d_1, \dots, d_p) < \infty,$$

where

$$d_i = |d_i| \cdot e_i = \frac{L_i^{n|G|} - 1}{L_i^n - 1} \cdot e_i,$$

with

$$e_i = (\overbrace{0, 0, \dots, 0}^{i-1}, 1, \overbrace{0, 0, \dots, 0}^{p-i}),$$

for $i = 1, \dots, p$.

Proof. The finiteness of $A(d_1, \dots, d_p)$ follows by Proposition 6.1.15, for all positive integers n . To prove the lower bound, for any positive integer n , we consider the substitution $\varphi^{n|G|}$, which has length vector $(L_1^{n|G|}, \dots, L_p^{n|G|})$. Since for all $1 \leq i \leq p$ and $0 \leq k_i \leq L_i^n - 1$, the representation of $k_i |d_i|$ in base L_i^n is $[k_i, k_i, \dots, k_i]$, the column of $\varphi^{n|G|}$ at position $(k_1 |d_1|, \dots, k_p |d_p|)$ is given by

$$[\varphi^{n|G|}]_{(k_1 |d_1|, \dots, k_p |d_p|)} = [\varphi^n]_{(k_1, \dots, k_p)}^{|G|},$$

by Proposition 6.1.10. Here G is the column group of φ , but it is also the column group of φ^n , for all positive integers n . This is because φ has a column equal to the identity (see [28]). Consequently, the column in the previous equation is the identity, since $g^{|G|} = \text{id}$, for every group element $g \in G$. So, $\varphi^{n|G|}$ has $\prod_{i=1}^p L_i^n$ columns equal to the identity located at the positions determined by a p -dimensional arithmetic progression of differences d_1, \dots, d_p and size vector L . Consequently, every fixed point of φ^n contains a p -dimensional monochromatic arithmetic progression of the same differences and the same or larger size vector. In other words, $A(d_1, \dots, d_p) \geq \prod_{i=1}^p L_i^n$, as required. \square

Corollary 6.1.17. *Let φ be an aperiodic, primitive, bijective substitution of p -dimensional words, which has a column equal to the identity, length vector (L_1, \dots, L_p) , and column group G . For any fix point of a power of φ ,*

$$A(d_1, \dots, d_p) \gtrsim (|d_1| \cdot \dots \cdot |d_p|)^\alpha,$$

where

$$\alpha = \frac{1}{|G| - 1} \quad \text{and} \quad d_i = |d_i| \cdot e_i = \frac{L_i^{n|G|} - 1}{L_i^n - 1} \cdot e_i,$$

with

$$e_i = (\overbrace{0, 0, \dots, 0}^{i-1}, 1, \overbrace{0, 0, \dots, 0}^{p-i}),$$

for $i = 1, \dots, p$.

Proof. We know that $A(d_1, \dots, d_p) \geq (L_1 \cdot \dots \cdot L_p)^n$, by Proposition 6.1.16. Then it suffices to show that the limit

$$\lim_{n \rightarrow \infty} \frac{(L_1 \cdot \dots \cdot L_p)^n}{(|d_1| \cdot \dots \cdot |d_p|)^\alpha}$$

is equal to 1. Noticing that

$$|d_i| = \frac{L_i^{n|G|} - 1}{L_i^n - 1} = L_i^{n(|G|-1)} + \dots + L_i^n + 1,$$

for $i = 1, \dots, p$, we see that

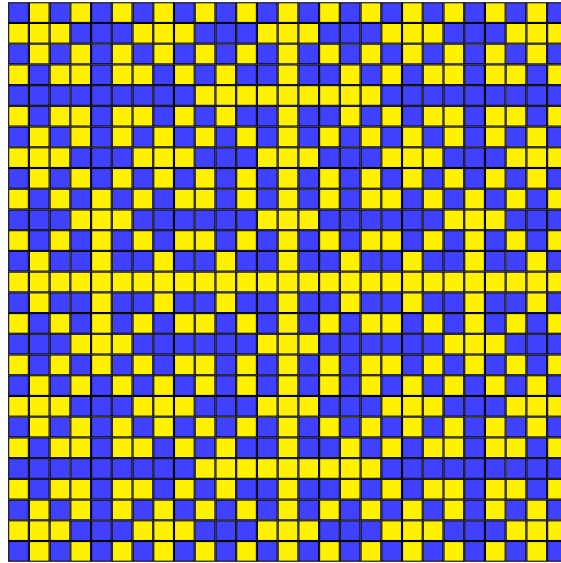
$$\lim_{n \rightarrow \infty} \frac{(L_1 \cdot \dots \cdot L_p)^n}{(|d_1| \cdot \dots \cdot |d_p|)^\alpha} = \lim_{n \rightarrow \infty} \frac{(L_1 \cdot \dots \cdot L_p)^n}{(L_1^{n(|G|-1)} \cdot \dots \cdot L_p^{n(|G|-1)})^\alpha} = \lim_{n \rightarrow \infty} \frac{(L_1 \cdot \dots \cdot L_p)^n}{(L_1 \cdot \dots \cdot L_p)^n} = 1,$$

as required. □

Example 6.1.18. The two-dimensional aperiodic, primitive, bijective substitution

$$\varphi: \begin{array}{c} \text{blue square} \end{array} \mapsto \begin{array}{|c|c|c|} \hline \text{blue} & \text{yellow} & \text{blue} \\ \hline \text{yellow} & \text{blue} & \text{yellow} \\ \hline \text{blue} & \text{yellow} & \text{blue} \\ \hline \end{array}, \quad \begin{array}{c} \text{yellow square} \end{array} \mapsto \begin{array}{|c|c|c|} \hline \text{yellow} & \text{blue} & \text{yellow} \\ \hline \text{blue} & \text{yellow} & \text{blue} \\ \hline \text{yellow} & \text{blue} & \text{yellow} \\ \hline \end{array}.$$

is called the *squirrel* substitution. In [53], it was proved that the hull of φ cannot be realised as a model set, which made it a good candidate to have a continuous spectral component. This was later proved in [18] and φ became one of the first substitutions of two-dimensional words known to have this property. We can iterate a letter under φ to see how a patch of an element of the hull looks like. For example, iterating the blue letter under φ^3 we obtain



Consider any of the two fixed points of φ^2 (or, in fact, any element of the hull). By Proposition 6.1.16, since the length vector of φ is $L = (3, 3)$ and its column group is $G = C_2$, we see that $A(d_1, d_2) \geq 9^n$, for all positive integers n , where

$$d_1 = (d, 0) \quad \text{and} \quad d_2 = (0, d) \quad \text{with} \quad d = \frac{3^{2n} - 1}{3^n - 1} = 3^n + 1.$$

By Corollary 6.1.17, $A(d_1, d_2) \gtrsim d^2$. This result is similar to the result for the Thue–Morse substitution, which shares certain properties with the squiral substitution. We recall that, for the Thue–Morse substitution, we have $A(2^n + 1) = 2^n + 2$, for all positive integers n . \blacklozenge

6.2 Forward limit sets of substitution semigroups

In Chapter 5 we introduced forward limit sets of substitution semigroups and studied many of their properties. We would like to develop further this theory and also to consider new examples that may be of general interest. So in the future we will continue investigating substitution semigroups, their forward limit sets and their hulls.

In this section we make some preliminary notes on these lines. In Section 6.2.1 we show our intention to extend our results for fixed-letter-free substitution semigroups to general substitution semigroups, and in Section 6.2.2 we make a connection between the logarithmic Hausdorff dimension of a set of infinite words and its complexity.

6.2.1 Forward limit sets of substitution semigroups with fixed letters

In Section 5.4, we characterised forward limit sets of fixed-letter-free substitution semigroups in terms of s-adic limits, invariant sets and fixed points. Considering that there are interesting families of substitutions which do not satisfy the fixed-letter-free property, one task that we will address in the future is the characterisation of forward limit sets of general substitution semigroups.

We will start by considering particular examples, such as the Sturmian substitution semigroup S , introduced in Example 2.5.9, and which can be generated by the three substitutions

$$f: \begin{array}{lcl} 0 & \mapsto & 01, \\ 1 & \mapsto & 0, \end{array} \quad g: \begin{array}{lcl} 0 & \mapsto & 10, \\ 1 & \mapsto & 0, \end{array} \quad h: \begin{array}{lcl} 0 & \mapsto & 1, \\ 1 & \mapsto & 0. \end{array}$$

Notice that h^2 is equal to the identity substitution, so it fixes both letters 0 and 1. Hence S is not fixed-letter-free. In a future preprint that we plan to submit for publication, as explained in (vi) in the Declaration of Authorship on page i, we will show that the forward limit set of S is equal to the set of all balanced infinite words over $\{0, 1\}$; these are infinite words x over $\{0, 1\}$ with the property that the numbers of 0s (or 1s) in any two subwords of x of the same length differ by at most one.

6.2.2 Hausdorff dimension and complexity of sets of infinite words

In Section 5.5.2 we quantified the size of the forward limit sets of a substitution semigroup using logarithmic Hausdorff dimension. In this section we prove Lemma 6.2.1, which relates the logarithmic Hausdorff dimension of a subset X of $\mathcal{A}^{\mathbb{N}}$ with the complexity function of X .

We recall from Section 2.2.1 that, for a positive integer n , the set of all subwords of elements of X that has length n is denoted by $\mathcal{L}_n(X)$, the language of X is $\mathcal{L}(X) = \bigcup_{n=1}^{\infty} \mathcal{L}_n(X)$, and the complexity function $p_X: \mathbb{N} \rightarrow \mathbb{N}$ of X is given by $p_X(n) = |\mathcal{L}_n(X)|$.

We also recall the dimension function ψ_t defined in Equation (5.5.1), which is given, for $t > 0$, by

$$\psi_t(x) = \begin{cases} 1/\left(\log \frac{1}{x}\right)^t & \text{if } 0 < x \leq 1/e, \\ ex & \text{otherwise.} \end{cases}$$

In addition, we recall from Section 2.1 the following definitions. Let $f, g : \mathbb{N} \rightarrow \mathbb{R}$ be non-zero functions. We write $f(n) \succ g(n)$ if $|f(n)/g(n)| \rightarrow \infty$ as $n \rightarrow \infty$. We write $f(n) = O(g(n))$ if there exists a positive real constant C such that $|f(n)| < C|g(n)|$ for all but finitely many values of n .

Lemma 6.2.1. *Let X be a subset of $\mathcal{A}^{\mathbb{N}}$ with complexity function p_X and let ℓ be a positive real number. If $p_X(n) = O(n^\ell)$, then the logarithmic Hausdorff dimension of X is equal to or less than ℓ . If the logarithmic Hausdorff dimension of X is equal to ℓ , then $p_X(n) \succ n^{\ell-\delta}$, for any positive real number δ .*

Proof. For a word u in \mathcal{A}^n , we define the cylinder set

$$C(u) = \{x \in \mathcal{A}^{\mathbb{N}} : x \text{ has prefix } u\}$$

and for each positive integer n , we define the set

$$\mathcal{T}_n = \{C(u) : u \in \mathcal{L}_n(X)\}.$$

Observe that, for each n , the collection \mathcal{T}_n covers X . Indeed, for every $x \in X$, $x \in C(u)$ and $u \in \mathcal{L}_n(X)$, where u is the prefix of x of length n , so $x \in \mathcal{T}_n$. Observe also that, for $u \in \mathcal{L}_n(X)$, $\text{diam } C(u) = 1/2^n$. Therefore, for any $\varepsilon > 0$, the collection \mathcal{T}_n is an ε -cover of X , for sufficiently large values of n . Using the previous dimension functions ψ_t , we have that

$$\psi_t(\text{diam } C(u)) = \frac{1}{(\log 2)^t n^t}.$$

Since $|\mathcal{T}_n| = p(n)$, where $p = p_X$ is the complexity function of X , we see that

$$\sum_{C(u) \in \mathcal{T}_n} \psi_t(\text{diam } C(u)) = \frac{1}{(\log 2)^t} \frac{p(n)}{n^t}.$$

Then the Hausdorff measure of X satisfies

$$H^{\psi_t}(X) \leq \frac{1}{(\log 2)^t} \lim_{n \rightarrow \infty} \frac{p(n)}{n^t}.$$

If $p(n) = O(n^\ell)$, then $H^{\psi_\ell}(X) \leq \lim_{n \rightarrow \infty} p(n)/n^\ell < \infty$, which implies that the logarithmic Hausdorff dimension of X is less than or equal to ℓ , as required. If the logarithmic Hausdorff dimension of X is equal to ℓ , then $H^{\psi_{\ell-\delta}}(X) = \infty \leq \lim_{n \rightarrow \infty} p(n)/n^{\ell-\delta}$, which implies that $p_X(n) \succ n^{\ell-\delta}$, as required. \square

Example 6.2.2. Let u be the substitutive sequence obtained as the limit of $g \circ f^n(a)$ as $n \rightarrow \infty$, where f

and g are substitutions given by

$$f: \begin{array}{l} a \mapsto ab, \\ b \mapsto bc, \\ c \mapsto cd, \\ d \mapsto d, \end{array} \quad \text{and} \quad g: \begin{array}{l} a \mapsto a, \\ b \mapsto b, \\ c \mapsto c, \\ d \mapsto c. \end{array}$$

The hull arising from u , defined as $\mathbb{X} = \overline{\bigcup_{n=0}^{\infty} \sigma^n u}$, has complexity function $p_{\mathbb{X}}(n) = O(n^{3/2})$, by [39]. Hence, by Lemma 6.2.1, the logarithmic Hausdorff dimension of \mathbb{X} is less than or equal to $3/2$. \diamond

Example 6.2.3. Consider the forward limit set Λ of the semigroup generated by the Fibonacci substitution and the reverse Fibonacci substitution. In Example 5.5.10 we did a detailed analysis and showed that the logarithmic Hausdorff dimension of Λ is less than or equal to 1. Using Lemma 6.2.1 we obtain the same result directly because, since Λ consists of Sturmian sequences, its complexity function is $n + 1$, which implies the claim. \diamond

Let f be a substitution of \mathcal{A} , $x \in \mathcal{A}^{\mathbb{N}}$ be a fixed point of f , and p_x be the complexity function of x . It is known from Pansiot [88] that p_x is one of $O(1)$, $O(n)$, $O(n \log \log n)$, $O(n \log n)$, or $O(n^2)$. Notice that the complexity function of the shift-orbit of x is equal to p_x , as no new subword arise by shifting x . Consequently, if x is the unique fixed point of f , or if f is primitive (see Theorem 2.4.35), the complexity function of the hull Ω_f of f is equal to p_x . Then, by Pansiot's result and Lemma 6.2.1, the logarithmic Hausdorff dimension of Ω_f cannot be larger than 2. Notice that, for large values of n ,

$$\frac{1}{n^2} < \frac{1}{n \log n} < \frac{1}{n \log \log n} < \frac{1}{n} < \frac{1}{1}.$$

In the future, we will try to strengthen Lemma 6.2.1 to help determine the complexity function of given word sets for which the logarithmic Hausdorff dimension can be obtained or estimated.

A. COMPUTER EXPERIMENTS WITH LINEAR RECURRENT SEQUENCES

Let φ be an aperiodic and primitive substitution that is linearly recurrent for the constant R , and let w be a fixed point of φ . Theorem 4.2.16 from Chapter 4 provides direct access to calculating the exact value of $A_w(d)$, for any given difference d , using a computer. Obviously the infinite word w cannot be generated experimentally, but we can generate a finite prefix of w which is long enough to be sure that it contains all the monochromatic arithmetic progressions of difference d . By linear recurrence, this can always be done.

First, we generate the prefix $w_{[0,k)}$ of w of length k , for some positive integer k . Next, we look for the longest monochromatic arithmetic progressions of difference d within $w_{[0,k)}$, and compute their length, which we denote by $B_k(d)$. This length is our first candidate for $A_w(d)$. But it may happen that $A_w(d) > B_k(d)$. Suppose that w contains a monochromatic arithmetic progression of difference d and length $B_k(d) + 1$. This arithmetic progression lays within a word of length $d \cdot B_k(d) + 1$ which, by Theorem 4.2.16, must appear in all the words of length $\ell = (R + 1)(d \cdot B_k(d) + 1)$. This implies that, if $k \geq \ell$, then $A_w(d) = B_k(d)$. Otherwise, we generate the prefix $w_{[0,\ell)}$ of w of length ℓ . If $w_{[0,\ell)}$ does not contain any monochromatic arithmetic progressions of difference d and length $B_k(d) + 1$, then $A_w(d) = B_k(d)$. Otherwise, we compute $B_\ell(d)$ and repeat the process.

The algorithm described in the previous paragraph finishes always in a finite number of steps. It can be described with the diagram in Figure A.0.1, where k_0 is the length of the prefix initially generated.

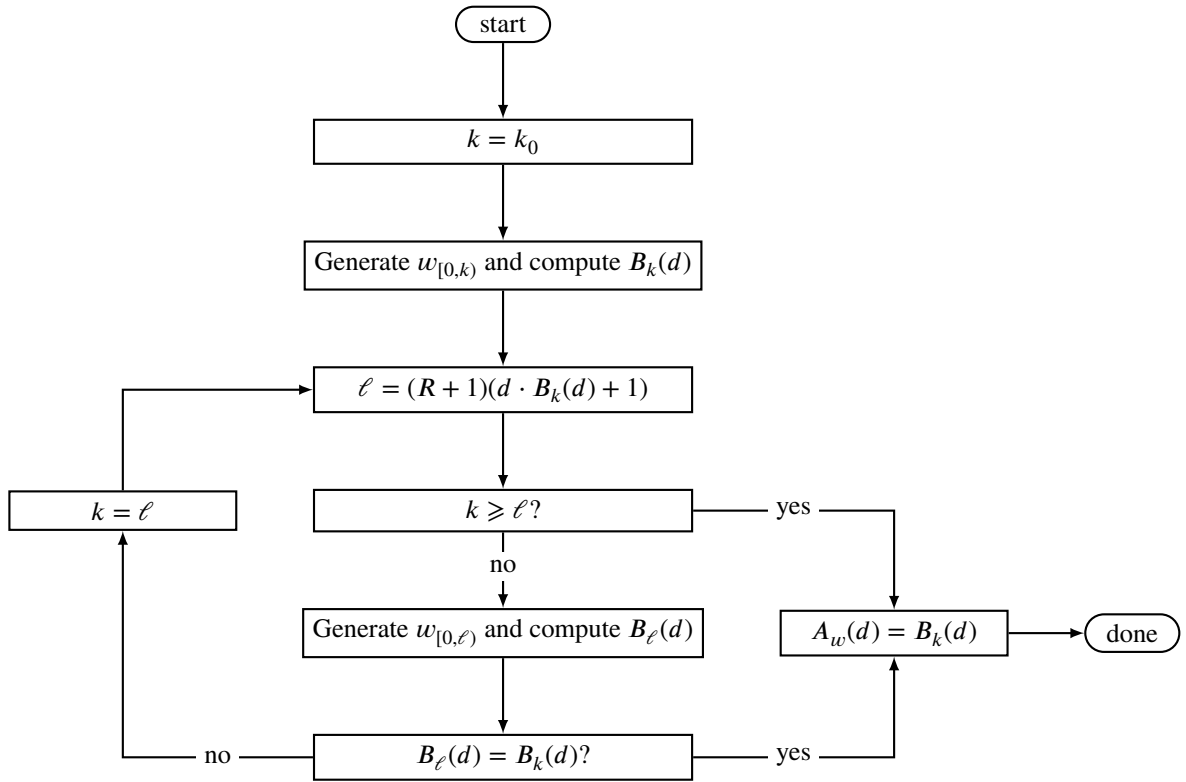


Figure A.0.1: Algorithm for computing $A_w(d)$, for any d .

REFERENCES

- [1] I. Aedo, U. Grimm, N. Mañibo, Y. Nagai, P. Staynova. Monochromatic arithmetic progressions in automatic sequences with group structure. Preprint arXiv:2302.12908 (2023).
- [2] I. Aedo, U. Grimm, Y. Nagai, P. Staynova. Monochromatic arithmetic progressions in binary Thue–Morse-like words. *Theor. Comput. Sci.* 934 (2022), 65–80.
- [3] I. Aedo, U. Grimm, I. Short. Forward limit sets of semigroups of substitutions. Preprint arXiv:2305.00078 (2023).
- [4] J.P. Allouche, P. Liardet. Generalized Rudin–Shapiro sequences. *Acta Arith.* 60 (1991), 1–27.
- [5] J.-P. Allouche, M. Mendès France. Automata and automatic sequences. In: F. Axel, D. Gratias (Eds.), *Beyond quasicrystals*, Springer, Berlin–Heidelberg, 1994, 293–367.
- [6] J.-P. Allouche, J. Shallit. The ubiquitous Prouhet–Thue–Morse sequence. In: C. Ding, T. Helleseht, H. Niederreiter (Eds.), *Sequences and Their Applications*, Springer, London, 1999, 1–16.
- [7] J.-P. Allouche, J. Shallit. Sums of digits, overlaps, and palindromes. *DMTCS* (2000) 4 (1), 1–10.
- [8] J.-P. Allouche, J. Shallit. *Automatic Sequences: Theory, Applications, Generalizations*. Cambridge University Press, Cambridge, 2003.
- [9] J.-P. Allouche, J. Shallit. Automatic sequences are also non-uniformly morphic. In: A. M. Raigorodskii, M. Th. Rassias (Eds.), *SOIA, Discrete Mathematics and Applications Vol. 165*, Springer, Cham, 2020, 1–6.
- [10] P. Arnoux, M. Mizutani, T. Sellami. Random product of substitutions with the same incidence matrix. *Theor. Comput. Sci.* 543 (2014), 68–78.
- [11] S. V. Avgustinovich, J. Cassaigne, A. E. Frid. Sequences of low arithmetical complexity. *RAIRO – Theor. Inf. Appl.* 40 (2006), 569–582.
- [12] A. Avila, J. Bochi, J.-C. Yoccoz. Uniformly hyperbolic finite-valued $SL(2, \mathbb{R})$ -cocycles. *Comment. Math. Helv.* 85 (2010), 813–884.
- [13] M. Baake, F. Gähler. Pair correlations of aperiodic inflation rules via renormalisation: some interesting examples. *Topology & Appl.* 205 (2016), 4–27.

- [14] M. Baake, F. Gähler, U. Grimm. Spectral and topological properties of a family of generalised Thue–Morse sequences. *J. Math. Phys.* 53 (2012), 032701.
- [15] M. Baake, F. Gähler, N. Mañibo. Renormalisation of pair correlation measures for primitive inflation rules and absence of absolutely continuous diffraction. *Commun. Math. Phys.* 370 (2019), 591–635.
- [16] M. Baake, U. Grimm. Surprises in aperiodic diffraction. *J. Physics: Conf. Ser.* 226 (2010), 012023.
- [17] M. Baake, U. Grimm. *Aperiodic Order Vol. 1: A Mathematical Invitation*. *Encyclopedia of Mathematics and its Applications Vol. 149*. Cambridge University Press, Cambridge, 2013.
- [18] M. Baake, U. Grimm. Squirals and beyond: substitution tilings with singular continuous spectrum. *Ergod. Th. & Dynam. Sys.* 34 (2014), 1077–1102.
- [19] M. Baake, J. A. G. Roberts, R. Yassawi. Reversing and extended symmetries of shift spaces. *Discrete Contin. Dyn. Syst.* 38 (2018), 835–866.
- [20] M.-P. Béal, D. Perrin, A. Restivo. Recognizability of morphisms. *Ergodic Th. & Dynam. Syst.* (2023), 25 pp.
- [21] M. Beeler. A new van der Waerden number. *Discrete Appl. Math.* 6 (1983), 207.
- [22] M. Beeler, P. O’Neil. Some new van der Waerden numbers. *Discrete Math.* 28 (1979), 135–146.
- [23] V. Berthé, V. Delecroix. Beyond substitutive dynamical systems: S -adic expansions. *RIMS Lecture note ‘Kôkyûroku Bessatsu’ B46* (2014), 81–123.
- [24] V. Berthé, M. Rigo. *Combinatorics, Automata and Number Theory*. *Encyclopedia of Mathematics and its Applications Vol. 135*. Cambridge University Press, Cambridge, 2010.
- [25] V. Berthé, W. Steiner, J. M. Thuswaldner, R. Yassawi. Recognizability for sequences of morphisms. *Ergodic Th. & Dynam. Syst.* 39 (2019), 2896–2931.
- [26] J. Brestel. Sur la construction de mots sans carré. *Séminaire de Théorie des Nombres (1978–1979) exposé n° 18* pages 01–15, Université de Bordeaux I.
- [27] T. C. Brown. Some new van der Waerden numbers (preliminary report). *Notices Amer. Math. Soc.* 21 (1974), A–432.
- [28] A. Bustos, D. Luz, N. Mañibo. Admissible reversing and extended symmetries for bijective substitutions. *Discrete Comput. Geom.* (2022).
- [29] R. V. Chacon. Weakly mixing transformations which are not strongly mixing. *Proc. Amer. Math. Soc.* 22 (1969), 559–562.
- [30] D. G. Champernowne. The construction of decimals normal in the scale of ten. *J. London Math. Soc.* 8 (1933), 254–260.

- [31] L. Chan, U. Grimm, I. Short. Substitution-based structures with absolutely continuous spectrum. *Indag. Math.* 29 (2018), 1072–1086.
- [32] V. Chvátal. Some unknown van der Waerden numbers. In: R. Guy et al. (Eds.), *Combinatorial Structures and their Applications*, Gordon and Breach, New York, 1970, 31–33.
- [33] A. Cobham. On the base-dependence of sets of numbers recognizable by finite automata. *Math. Systems Theory* 3 (1969), 186–192.
- [34] A. Cobham. Uniform tag sequences. *Math. Systems Theory* 6 (1972), 164–192.
- [35] J. Coquet, T. Kamae, M. Mendès France. Sur la mesure spectrale de certaines suites arithmétiques. *Bull. Soc. Math. France* 105 (1977), 369–384.
- [36] E. Coven, A. Quas, R. Yassawi. Computing automorphism groups of shifts using atypical equivalence classes. *Discrete Anal.* 611 (2016), 24 pp.
- [37] D. Damanik, D. Lenz. Substitution dynamical systems: Characterization of linear repetitivity and applications. *J. Math. Anal. Appl.* 321 (2006), 766–780.
- [38] F. M. Dekking. The spectrum of dynamical systems arising from substitutions of constant length. *Z. Wahrscheinlichkeitstheorie und verw. Geb.* 41 (1978), 221–239.
- [39] R. Deviatov. On subword complexity of morphic sequences. In: E. A. Hirsch, A. A. Razborov, A. Semenov, A. Slissenko (Eds.), *Computer Science - Theory and Applications*, Lect. Notes in Comput. Sci., Vol. 5010, Springer, 2008, 146–157.
- [40] F. Durand. A characterization of substitutive sequences using return words. *Discrete Math.* 179 (1998), 89–101.
- [41] S. Dulucq, D. Gouyou-Beauchamps. Sur les facteurs des suites de Sturm. *Theor. Comput. Sci.* 71 (1990), 381–400.
- [42] F. Durand, B. Host, C. Skau. Substitutive dynamical systems, Bratteli diagrams and dimension groups. *Ergod. Th. & Dynam. Sys.* 19 (1999), 953–993.
- [43] F. Durand, J. Leroy. Decidability of isomorphism and factorization between minimal substitution subshifts. *Discrete Anal.* (2022), 65 pp.
- [44] S. Dworkin. Spectral theory and X-ray diffraction. *J. Math. Phys.* 34 (1993), 2965–2967.
- [45] S. Eilenberg. *Automata, Languages and Machines Vol. A. Pure and Applied Mathematics*. Academic Press, London–New York, 1974.
- [46] P. Erdős, P. Turán. On some sequences of integers. *J. London Math. Soc.* 11 (1936), 261–264.
- [47] K. Falconer. *Fractal Geometry – Mathematical foundations and applications*. John Wiley & Sons Inc., Hoboken–NJ, 2003.

- [48] N. P. Frank. Substitution sequences in \mathbb{Z}^d with a nonsimple Lebesgue component in the spectrum. *Ergodic Th. & Dynam. Syst.* 23 (2003), 519–532.
- [49] N. P. Frank. Multidimensional constant-length substitution sequences. *Topol. Appl.* 152 (2005), 44–69.
- [50] N. P. Frank. A primer of substitution tilings of the Euclidean plane. *Expo. Math.* 26 (2008), 295–326.
- [51] N. P. Frank. Introduction to hierarchical tiling dynamical systems. In: S. Akiyama, P. Arnoux (Eds.), *Substitution and Tiling Dynamics: Introduction to Self-inducing Structures*, CIRM Jean–Morlet Chair, Lecture Notes in Mathematics Vol. 2273, Springer, Cham, 2017, 33–95.
- [52] N. P. Frank, N. Mañibo. Spectral theory of spin substitutions. *Discrete Contin. Dyn. Syst.* 42 (2022), 5399–5435.
- [53] D. Frettlöh, B. Sing. Computing modular coincidences for substitution tilings and point sets. *Discrete Comput. Geom.* 37 (2007), 381–407.
- [54] A. E. Frid. Arithmetical complexity of symmetric D0L words. *Theor. Comput. Sci.* 306 (2003), 535–542.
- [55] A. E. Frid. Sequences of linear arithmetic complexity. *Theor. Comput. Sci.* 339 (2005), 68–87.
- [56] D. Fried, S. M. Marotta, R. Stankewitz. Complex dynamics of Möbius semigroups. *Ergod. Th. & Dynam. Sys.* 32 (2012), 1889–1929.
- [57] P. N. Fogg. Substitutions in Dynamics, Arithmetics and Combinatorics. In: V. Berthé, S. Ferenczi, C. Mauduit, A. Siegel (Eds.), *Lecture Notes in Mathematics Vol. 1794*, Springer, Berlin, 2002.
- [58] A. O. Gelfond. Sur les nombres qui ont des propriétés additives et multiplicatives données. *Acta Arith.* 13 (1968), 259–265.
- [59] E. Godelle. The stable set of a self-map. *Adv. Appl. Math.* 45 (2010), 438–448.
- [60] I. Goldstein. Asymptotic subword complexity of fixed points of group substitutions. *Theor. Comput. Sci.* 410 (2009), 2084–2098.
- [61] W. T. Gowers. A new proof of Szemerédi’s theorem. *Geom. Funct. Anal.* 11 (2001), 465–588.
- [62] B. Green, T. Tao. The primes contain arbitrarily long arithmetic progressions. *Ann. of Math.* 167 (2008), 481–547.
- [63] G. H. Hardy, E. M. Wright. *An Introduction to Number Theory*. Oxford University Press, Oxford, 1960.
- [64] W. K. Hayman, P. B. Kennedy. *Subharmonic functions Vol. I*. London Mathematical Society Monographs No. 9. Academic Press Inc., London–New York, 1976.

- [65] H. Herrlich. Axiom of Choice. Lecture Notes in Mathematics Vol. 1876. Springer, Berlin–Heidelberg, 2006.
- [66] A. Hinkkanen, G. J. Martin. The dynamics of semigroups of rational functions I. Proc. London Math. Soc. 73 (1996), 358–384.
- [67] K. Jacobs, M. Keane. 0 – 1 sequences of Toeplitz type. Z. Wahrscheinlichkeitsth. verw. Geb. 13 (1969), 123–131.
- [68] M. Jacques, I. Short. Semigroups of isometries of the hyperbolic plane. Int. Math. Res. Not. N° 9 (2022), 6403–6463.
- [69] T. J. Jech. The Axiom of Choice. North-Holland Publishing Company, Amsterdam–London, 1973.
- [70] M. Keane. Generalized Morse sequences. Z. Wahrscheinlichkeitsth. verw. Geb. 10 (1968), 335–353.
- [71] J. Kellendonk, R. Yassawi. The Ellis semigroup of bijective substitutions. Groups Geom. Dyn. 16 (2022), 29–73.
- [72] M. Kouril. Computing the van der Waerden number $W(3, 4) = 293$. Integers 12 (2012), 13 pp.
- [73] M. Kouril, J. L. Paul. The van der Waerden Number $W(2, 6)$ is 1132. Exp. Math. 17 (2008), 53–61.
- [74] P. Kůrka. Topological and Symbolic Dynamics. Cours Spécialisés 11, Société Mathématique de France, Paris, 2003.
- [75] B. M. Landman, A. Robertson. Ramsey Theory on the Integers. Student Mathematical Library Vol. 24. American Mathematical Society, USA, 2004.
- [76] J.-Y. Lee, R. V. Moody, B. Solomyak. Consequences of pure point diffraction spectra for multiset substitution systems. Discrete Comput. Geom. 29 (2003), 525–560.
- [77] M. Lemańczyk, C. Müllner. Automatic sequences are orthogonal to aperiodic multiplicative functions. Discrete Contin. Dynam. Syst. 40 (2020), 6877–6918.
- [78] M. Lothaire. Algebraic Combinatorics on Words. Cambridge University Press, Cambridge, 2002.
- [79] P. Michel. Stricte ergodicité d’ensembles minimaux de substitutions. C. R. Acad. Sci. Paris 278 (1974), 811–813.
- [80] J. F. Morgenbesser, J. Shallit, T. Stoll. Thue–Morse at multiples of an integer. J. Number Theory 131 (2011), 1498–1512.
- [81] M. Morse. Recurrent geodesics on a surface of negative curvature. Trans. Amer. Math. Soc. 22 (1921), 84–100.
- [82] H. Mousavi. Automatic theorem proving in Walnut. Preprint arXiv:1603.06017v2 (2021).

- [83] C. Müllner, R. Yassawi. Automorphisms of automatic shifts. *Ergod. Th. & Dynam. Sys.* 41 (2021), 1530–1559.
- [84] Y. Nagai, S. Akiyama, J.-Y. Lee. On arithmetic progressions in non-periodic self-affine tilings. *Ergod. Th. & Dynam. Sys.* (2021), 1–33.
- [85] OEIS Foundation Inc. (2021). Entry A010051 in The On-Line Encyclopedia of Integer Sequences. <https://oeis.org/A010051>.
- [86] OEIS Foundation Inc. (2021). Entry A020985 in The On-Line Encyclopedia of Integer Sequences. <https://oeis.org/A020985>.
- [87] OEIS Foundation Inc. (2021). Entry A342818 in The On-Line Encyclopedia of Integer Sequences. <https://oeis.org/A342818>.
- [88] J.-J. Pansiot. Complexité des facteurs des mots infinis engendrés par morphismes itérés. In J. Paredaens (Ed.), *Proc. 11th Int’l Conf. on Automata, Languages, and Programming (ICALP)*, Lecture Notes in Computer Science Vol. 172. Springer-Verlag, 1984, 380–389.
- [89] O. G. Parshina. Homogeneous arithmetic progressions in the Thue–Morse word. *International Scientific Student Conference*, Novosibirsk, Russia, April 2015.
- [90] O. G. Parshina. On arithmetic progressions in the generalized Thue–Morse word. In: F. Manea, D. Nowotka (Eds.), *WORDS 2015*, Lecture Notes in Computer Science 9304, Springer, Cham, 2015, 191–196.
- [91] O. G. Parshina. On arithmetic index in the generalized Thue–Morse word. In: S. Brlek, F. Dolce, C. Reutenauer, É. Vandomme (Eds.), *WORDS 2017*, Lecture Notes in Computer Science 10432, Springer, Cham, 2017, 121–131.
- [92] O. G. Parshina. ПЕРИОДИЧЕСКИЕ СТРУКТУРЫ В МОРФИЧЕСКИХ СЛОВАХ И РАСКРАСКАХ БЕСКОНЕЧНЫХ ЦИРКУЛЯНТНЫХ ГРАФОВ. PhD thesis, Université de Lyon and Sobolev Institute of Mathematics, 2019.
- [93] D. Perrin, J.-E. Pin. *Infinite Words: Automata, Semigroups, Logic and Games*. Pure and Applied Mathematics Series Vol. 141. Elsevier, Amsterdam, 2004.
- [94] V. Prasolov. *Problems and Theorems in Linear Algebra*. Translations of Mathematical Monographs Vol. 134. American Mathematical Society, Providence, 1994.
- [95] E. Prouhet. Mémoire sur quelques relations entre les puissances des nombres. *C. R. Acad. Sci. Paris* 33 (1851), 225.
- [96] M. Queffélec. *Substitution Dynamical Systems-Spectral Analysis*. 2nd edition. Lecture Notes in Mathematics Vol. 1294. Springer, Berlin, 2010.
- [97] G. Richomme. On sets of indefinitely desubstitutable words. *Theor. Comput. Sci.* 857 (2021), 97–113.

- [98] M. Rigo. Formal Languages, Automata and Numeration Systems Vol. 1: Introduction to Combinatorics on Words. Wiley–ISTE, London–Hoboken, 2014.
- [99] C. A. Rogers. Hausdorff measures. Cambridge University Press, Cambridge, 1998.
- [100] H. Schneider. Wielandt’s proof of the exponent inequality for primitive nonnegative matrices. *Linear Algebra Appl.* 353 (2002), 5–10.
- [101] P. Séébold. Fibonacci morphisms and Sturmian words. *Theor. Comput. Sci.* 88 (1991), 365–384.
- [102] B. Sobolewski. On monochromatic arithmetic progressions in binary words associated with block-counting functions. Preprint arXiv:2204.05287 (2022).
- [103] P. Staynova. The Ellis semigroup of certain constant-length substitutions. *Ergod. Th. & Dynam. Sys.* 41 (2021), 935–960.
- [104] R. Stevens, R. Shantaram. Computer-generated van der Waerden partitions. *Math. Comput.* 32 (1978), 635–636.
- [105] E. Szemerédi. On sets of integers containing no k elements in arithmetic progression. *Acta Arith.* 27 (1975), 199–245.
- [106] A. Thue. Über unendliche Zeichenreihen. *Norske vid. Selsk. Skr. Mat. Nat. Kl.* 7 (1906), 1–22. Reprinted in: T. Nagell (Ed.), *Selected Mathematical Papers of Axel Thue*, Universitetsforlaget, Oslo, 1977, 139–158.
- [107] A. Thue. Über die gegenseitige Lage gleicher Teile gewisser Zeichenreihen. *Norske vid. Selsk. Skr. Mat. Nat. Kl.* 1 (1912), 1–67. Reprinted in: T. Nagell (Ed.), *Selected Mathematical Papers of Axel Thue*, Universitetsforlaget, Oslo, 1977, 413–478.
- [108] J. M. Thuswaldner. S-adic sequences: a bridge between dynamics, arithmetic and geometry. In: S. Akiyama, P. Arnoux (Eds.), *Substitution and Tiling Dynamics: Introduction to Self-inducing Structures*, CIRM Jean–Morlet Chair, Lecture Notes in Mathematics Vol. 2273, Springer, Cham, 2017, 97–191.
- [109] B. L. van der Waerden. Beweis einer Baudetschen Vermutung. *Nieuw. Arch. Wisk.* 15 (1927), 212–216.
- [110] H. Wielandt. Unzerlegbare, nicht negative Matrizen. *Math. Z.* 52 (1950), 642–648.
- [111] C. Wojcik, L. Q. Zamboni. Colouring problems for infinite words. In V. Berthé, M. Rigo (Eds.), *Sequences, Groups, and Number Theory*. Birkhäuser, Basel, 2018, 213–231.