1 2 9 0

UNIVERSIDADE Đ COIMBRA

Herman Goulet-Ouellet

Schützenberger groups of minimal shift spaces

Tese no âmbito do Programa Interuniversitário de Doutoramento em Matemática, orientada pelos Professores Doutores Jorge Almeida e Alfredo Costa e apresentada ao Departamento de Matemática da Faculdade de Ciências e Tecnologia da Universidade de Coimbra.

Agosto de 2022

Schützenberger groups of minimal shift spaces

Herman Goulet-Ouellet

1 2 9 0 UNIVERSIDADE D COIMBRA

U. PORTO

UC|UP Joint PhD Program in Mathematics

Programa Interuniversitário de Doutoramento em Matemática

PhD Thesis | Tese de Doutoramento

August 2022

À la mémoire de Desneiges et Lionel.

Acknowledgements

I would like to dedicate some special words to some of the persons who touched my life in these past four years. Each of you contributed, in your own way, to the making of this thesis.

To my advisors, Jorge and Alfredo. For your patience, generosity and support. You provided me with focus and direction while I took my first steps in the world of mathematical research. The semigroup community owes both of you a great deal, and so do I. Thank you Jorge for sharing your deep knowledge and your unique insights into semigroup theory. Thank you Alfredo for your contagious curiosity and enthusiasm, and for suggesting more inspired ideas than I can count.

To Ana with all my love. For being a truly wonderful person. During those years, I could always count on your support, from helping with all sorts of mundane problems to proofreading my work, and everything in between. Your presence made my life so much brighter. You made me feel loved, special and safe. I can only hope I made you feel the same.

To my uprooted friends, Hugo, Carla and Igor. For the many evenings and nights spent laughing, talking, eating, drinking, complaining, sometimes in excess but always in good taste. These years would not have been the same without our little adventures. This feels like the end of a chapter.

To my friend Pedro. Thank you for making me feel so welcome in Portugal and for all your help in navigating the intricacies of day-to-day life here. I will miss our captivating discussions, mathematical or otherwise, on which I could always count to break the monotony of everyday life.

To other friends and colleagues I met along the way. David, Leonardo and Simon first come to mind. Thank you for many lunches, beers, coffees and interesting conversations. Meeting you was a great pleasure which made studying abroad all the more worthwhile.

To my Czech friends, Ondřej and Jonatan. For your generosity and hospitality. Thank you for giving me the opportunity to come work with you in Brno. It was a great pleasure to visit your beautiful city. I hope this planted the seed for many future collaborations and exchanges.

À mes parents, Joanne et Louis-Marie. Pour votre soutien inconditionel, vos encouragements, votre confiance, et tellement d'autres choses. Merci d'avoir été à mes côtés pendant ces quatre années, malgré la distance et malgré une pandémie mondiale. Cette thèse, c'est un peu la vôtre.

Aux amis de toujours, Charlie et Ghyslain. Pour votre amitié qui ne veut pas mourir et qui grandit avec les saisons. Ce fut toujours un plaisir de passer avec vous des soirées à parler, à travailler, et plus souvent qu'à notre tour, à flâner.

À Dominique. Pour ton enthousiasme contagieux, ta curiosité et ta générosité. Merci pour les encouragements et pour les échanges inspirants.

I gratefully acknowledge financial support from the FCT (scholarship PD/BD/150350/2019), as well as from the Centre for Mathematics of the University of Coimbra (under FCT grant UIDB/00324/2020) and the Centre for Mathematics of the University of Porto (under FCT grant UIDB/00144/2020).

Abstract

This thesis aims to shed some light on the structure of maximal subgroups of free profinite monoids corresponding to minimal shift spaces. These groups, which came to be known as *Schützenberger groups* in the literature, were first studied by Almeida in the early 2000s. They provide a fruitful connection between semigroup theory and symbolic dynamics. But despite many significant advances taking place in the last two decades, our understanding of these groups remains sparse. This thesis proposes a number of contributions on different aspects of this topic, organized in three parts.

The first part is concerned with the freeness question: when are these groups free, be it in the category of profinite groups, or relative to some pseudovariety of finite groups? This part of the thesis focuses in particular on the maximal subgroups corresponding to primitive substitutions. One of the main results is a criterion for absolute freeness which uses a special kind of profinite presentations introduced by Almeida and Costa, which we call *ω-presentations*. The criterion is used to exhibit a primitive invertible substitution with a non-free Schützenberger group, disproving a result proposed by Almeida. Some early results are also obtained on the topic of relative freeness.

The second part of the thesis examines the pronilpotent quotients of Schützenberger groups of primitive substitutions. The main result is a description of the maximal pronilpotent quotients of ω-presented groups, of which Schützenberger groups of primitive substitutions are special cases. We show that all the information about the pronilpotent quotients of a given ω-presented group can be extracted from the characteristic polynomial of a certain matrix. This can be used, for instance, to show that ω-presented groups are never pro-p groups (partially answering a question of Zalesskii), and that they are perfect only under strict conditions which exclude Schützenberger groups of primitive substitutions. These results also lead to a number of necessary conditions for absolute and relative freeness of ω-presented groups. We deduce that Schützenberger groups of primitive aperiodic substitutions of constant length are never absolutely free.

The last part of the thesis is devoted to a study of the subgroups generated by return words in minimal shift spaces. In 2016, Almeida and Costa showed that the collective behaviour of these subgroups can be used to gather information about the Schützenberger group. Their results were motivated in part by a series of papers initiated in 2015 by Berthé et al., which developed a number of ideas centred around the notion of *extension graphs*. Under certain assumptions, Berthé et al.'s results allowed for a complete understanding of the subgroups generated by return words. Our main contribution on this topic is a new condition called *suffix-connectedness*, which allows to generalize some of these results. Various applications of suffix-connectedness to the study of Schützenberger groups are also highlighted.

Resumo

Esta tese visa esclarecer a estrutura dos subgrupos maximais dos monoides profinitos livres que correspondem aos sistemas dinâmicos simbólicos minimais. Esses grupos, agora chamados *grupos de Schützenberger* na literatura, foram estudados pela primeira vez por Almeida no início dos anos 2000. Eles revelam uma conexão frutuosa entre a teoria dos semigrupos e a dinâmica simbólica. Mas, apesar de vários desenvolvimentos importantes nas últimas duas décadas, a nossa compreensão desses grupos permanece incompleta. Esta tese propõe uma série de contribuições sobre diferentes aspectos do assunto, organizadas em três partes.

A primeira parte trata da questão da liberdade: em que condições esses grupos são livres, seja na categoria de grupos profinitos, seja em relação a alguma pseudovariedade de grupos finitos? Concentramos a nossa atenção nos subgrupos maximais correspondentes às substituições primitivas. Um dos principais resultados é um critério de liberdade absoluta usando um tipo de apresentações profinitas introduzidas por Almeida e Costa, que são chamadas de *ω-apresentações*. Este critério permite destacar um exemplo de substituição primitiva invertível cujo grupo de Schützenberger não é livre, refutando um resultado proposto por Almeida. Alguns resultados preliminares sobre a liberdade relativa também são apresentados.

A segunda parte da tese examina os quocientes pronilpotentes dos grupos de Schützenberger das substituições primitivas. O principal resultado é uma descrição dos quocientes pronilpotentes maximais dos grupos ω-apresentados, entre os quais se contam os grupos de Schützenberger de substituições primitivas. Mostramos que todas as informações sobre os quocientes pronilpotentes de um grupo ω-apresentado podem ser extraídas do polinómio característico de uma certa matriz. Podemos usar isso para provar, por exemplo, que os grupos ω-apresentados nunca são pro-p (o que responde parcialmente a uma pergunta de Zalesskii), e que eles são perfeitos apenas sob condições estritas que excluem os grupos de Schützenberger das substituições primitivas. Esses resultados também levam a uma série de condições necessárias para a liberdade absoluta e relativa dos grupos ω-apresentados. Deduzimos que os grupos de Schützenberger das substituições primitivas aperiódicas de comprimento uniforme nunca são absolutamente livres.

A última parte da tese é dedicada ao estudo dos subgrupos gerados por palavras de retorno nos sistemas dinâmicos simbólicos minimais. Em 2016, Almeida e Costa demonstraram que o comportamento colectivo desses subgrupos permite compreender melhor o grupo de Schützenberger. Os seus resultados são motivados em parte por uma série de artigos publicados a partir de 2015 por Berthé et al., desenvolvendo certas ideias centradas em torno da noção de *grafos de extensões*. Sob certas condições, os resultados de Berthé et al. permitem obter um conhecimento completo dos subgrupos gerados pelas palavras de retorno. A nossa principal contribuição neste assunto é uma nova condição, a *conectividade por sufixos*, permitindo generalizar alguns desses resultados. Várias aplicações da conectividade por sufixos para o estudo dos grupos de Schützenberger também são destacadas.

Résumé

Cette thèse vise à faire la lumière sur la structure des sous-groupes maximaux des monoïdes profinis libres qui correspondent aux systèmes dynamiques symboliques minimaux. Ces groupes, maintenant appelés *groupes de Schützenberger* dans la littérature, furent d'abord étudiés par Almeida au début des années 2000. Ils révèlent une fructueuse connection entre la théorie des semi-groupes et la dynamique symbolique. Mais malgré plusieurs progrès importants au cours des deux dernières décennies, notre compréhension de ces groupes demeure incomplète. Cette thèse propose une série de contributions sur différents aspects du sujet, organisées en trois parties.

La première partie porte sur la question de la liberté : sous quelles conditions ces groupes sont-ils libres, soit dans la catégorie des groupes profinis, ou relativement à une certaine pseudo-variété de groupes finis ? On s'y concentre en particulier sur les sous-groupes maximaux correspondant aux substitutions primitives. L'un des principaux résultats est un critère pour la liberté absolue utilisant un type de présentations profinies introduit par Almeida et Costa, que l'on appelle ω-*présentations*. Ce critère permet de mettre en évidence un exemple de substitution primitive inversible dont le groupe de Schützenberger est non-libre, réfutant un résultat proposé par Almeida. Quelques résultats préliminaires sur la liberté relative sont aussi présentés.

La deuxième partie de la thèse examine les quotients pronilpotents des groupes de Schützenberger des substitutions primitives. Le résultat principal est une description des quotients pronilpotents maximaux des groupes ω-présentés, dont les groupes de Schützenberger des substitutions primitives font partie. On y démontre que toute l'information sur les quotients pronilpotents d'un groupe ω-présenté peut être prélevée à même le polynôme caractéristique d'une certaine matrice. On peut utiliser ceci pour démontrer, par exemple, que les groupes ω-présentés ne sont jamais pro-p (ce qui répond en partie à une question de Zalesskii), et qu'ils sont parfaits seulement sous des conditions strictes qui excluent les groupes de Schützenberger des substitutions primitives. Ces résultats mènent aussi à un certain nombre de conditions nécessaires à la liberté, absolue et relative, des groupes ω-présentés. On en déduit que les groupes de Schützenberger des substitutions primitives apériodiques de longueur uniforme ne sont jamais absolument libres.

La dernière partie de la thèse est dédiée à l'étude des sous-groupes engendrés par les mots de retour dans les systèmes dynamiques symboliques minimaux. En 2016, Almeida et Costa démontrent que le comportement collectif de ces sous-groupes permet de mieux comprendre le groupe de Schützenberger. Leurs résultats sont motivés en partie par une série d'articles publiés à partir de 2015 par Berthé et al., développant des idées centrées autour de la notion de *graphes d'extensions*. Sous certaines conditions, les résultats de Berthé et al. permettent d'obtenir une connaissance complète des sous-groupes engendrés par les mots de retour. Notre principale contribution sur ce sujet est une nouvelle condition, la *connectivité par suffixes*, permettant de généraliser certains de ces résultats. Plusieurs applications de la connectivité par suffixes pour l'étude des groupes de Schützenberger sont aussi soulignées.

Table of contents

List of Figures

Figures in Paper 1

Figures in Paper 2

Figures in Paper 3

Figures in Appendix B

List of Tables

Tables in Paper 1

Tables in Appendix B

Introduction

Relatively free profinite monoids and semigroups play an important role in modern semigroup theory. Almeida made this clear in his landmark book on finite semigroups and universal algebra [2]; and so did Rhodes and Steinberg, more than a decade later, in their book on q-theory [65]. This fact is further evidenced by the many survey papers that have been written on the topic [7, 13, 15, 63, 73]. Moreover, the relevance of these objects is not limited to semigroup theory: free profinite groups in particular have had a profound impact on Galois theory [41, 46, 67, 69, 75]. In many specific instances, the structure of relatively free profinite semigroups and monoids is well understood. Examples include: free pro-aperiodic monoids [17, 72]; free profinite $\mathcal{J}$-trivial and $\mathcal{R}$-trivial semigroups [1, 16]; free profinite local semilattices [31]; or free profinite semigroups relative to **DA**, the pseudovariety consisting of finite semigroups whose $\mathcal{D}$-classes are aperiodic semigroups [58, 59].

The case of absolutely free profinite monoids has proven particularly difficult, and indeed many aspects of their structure are yet to be understood. In the early 2000s, Almeida proposed a systematic program to study them, which relied on a newly discovered connection with symbolic dynamics [5, 6, 8]. His ideas served as the impetus for a whole body of work, leading to an overall better understanding of the structure of free profinite monoids. We can cite, for instance: the work of Costa [28] and Costa and Steinberg [30] deepening Almeida's connection; the joint work of Almeida and Costa [9–12], providing various tools to further study the maximal subgroups and regular $\mathcal{J}$-classes corresponding to minimal shift spaces; or results of Costa and Steinberg [29] on maximal subgroups corresponding to irreducible sofic shift spaces. Other related work includes a paper of Rhodes and Steinberg [64] whose title, *Closed Subgroups of Free Profinite Monoids Are Projective Profinite Groups*, speaks for itself; a paper of Almeida et al. [18] drawing relations with the theory of codes; the work of Almeida [3] and Almeida and Volkov [14] on dynamical properties of implicit operators; or a paper by Almeida et al. [17] about the linear nature of pseudowords, which contains some results about chains of $\mathcal{J}$-classes in free profinite monoids. Further cementing the importance of Almeida's approach to the study of free profinite monoids, a monograph written by Almeida et al. [19] was recently published, providing a comprehensive treatment of the subject matter.

This thesis examines a particular structural aspect of free profinite monoids which has been the focus of much of the work on the topic, namely their maximal subgroups. In his 2007 paper [8], Almeida showed that to each minimal shift space $X \subseteq A^{\mathbb{Z}}$ corresponds a regular $\mathcal{J}$-class $J(X)$ in the free profinite monoid $\widehat{A^*}$, which is given by $\overline{L(X)} \setminus A^*$. In other words, $J(X)$ is obtained by taking the infinite part of the topological closure of the language of X inside $\widehat{A^*}$. By standard semigroup theory, the maximal subgroups contained in $J(X)$ define, up to isomorphism, a single profinite group $G(X)$, which came to be known as the *Schützenberger group* of the shift space. The core of this thesis is a collection of three single-authored papers [43–45] presenting several contributions to our understanding of these groups. From now on, these papers will be referred to as Paper 1 [45], Paper 2 [44] and Paper 3 [43], respectively. Papers 1 and 2 focus on the specific case of shift spaces defined by primitive substitutions, and use as a starting point a collection of results published in 2013 by Almeida and Costa [11]. Paper 3 generalizes some combinatorial results from Berthé et al. [23] about the subgroups of free groups generated by return sets in minimal shift spaces, which were shown by Almeida and Costa [12] to be tightly related with Schützenberger groups of minimal shift spaces. The thesis also contain two appendices which complement Paper 3: Appendix A presents some unpublished applications of the third paper to the study of Schützenberger groups, while Appendix B presents an example which answers some natural questions regarding the scope of these applications.

The *freeness question*, that is whether or not these groups are free, either in the category of profinite groups (absolute freeness) or in a subcategory determined by a pseudovariety of finite groups (relative freeness), has been a recurring theme in the study of Schützenberger groups [8, 11, 12, 14, 29]. This thesis is no exception; indeed, most of the results presented here relate to this question in one way or another. Its near ubiquity is perhaps not so surprising when considering the rich history of similar questions in different areas of algebra. A classical example is of course the Nielsen–Schreier theorem, which states that in free groups, all subgroups are free. Several results of this form are also known within the setting of profinite groups: for instance, clopen subgroups of free profinite groups are free profinite, while by a famous theorem of Tate, all closed subgroups of free pro-p groups are free pro-p (see [67]). However, closed subgroups of free profinite groups are not always free, though they are projective objects in the category of profinite groups. A similar situation occurs for maximal subgroups of free profinite monoids: they were shown by Rhodes and Steinberg to be projective [64], but they are not necessarily free, not even relatively so. A first example of a maximal subgroup lacking absolute freeness, realized as the Schützenberger group of a primitive substitution, was given by Almeida in 2007 [8]. A second example, the Schützenberger group of the Thue–Morse substitution, was established later by Almeida and Costa [11].[1] In fact, they showed that in both cases, the Schützenberger group is not relatively free.

On the other hand, absolute freeness has been observed in many instances, most notably in maximal subgroups corresponding to irreducible sofic shift spaces [29] and minimal dendric shift spaces [12]. The dendric case in particular comprises a few well-known families of minimal shift spaces, such as Arnoux–Rauzy shift spaces [22] and the shift spaces defined by regular interval exchanges [24]. Among the first attempts at a general investigation of the freeness question, we also find the following positive result proposed by Almeida: the Schützenberger group of a primitive invertible substitution is absolutely free [8]. We noticed however a gap in Almeida's proof, which resisted all of our attempts at fixing it. Then, we found an intriguing example: a primitive invertible substitution with a Schützenberger group whose freeness, or lack thereof, could not be deduced from any existing result. Fortunately, some of the earlier work of Almeida and Costa [11] could be leveraged to settle the question, confirming that the Schützenberger group of this invertible substitution is indeed not absolutely free. This counterexample is featured in Paper 1; and the argument we used was generalized and turned into a criterion for absolute freeness which is also presented there. This criterion relies heavily on the notion, central in this thesis, of ω-*presentations*, a kind of profinite presentations introduced in 2013 by Almeida and Costa [11] to study Schützenberger groups of primitive substitutions. While our criterion established

[1] Almeida already had a look at the Schützenberger group of the Thue–Morse substitution in [8], where he showed that it could not be free on 3 or more generators. Subsequent work of Almeida and Costa [11] shows it is not 2-generated.

failure of *absolute* freeness for the Schützenberger group of our counterexample, the question of its *relative* freeness remained unclear. We answered this by showing that proper relative freeness (that is, relative freeness without absolute freeness) is in fact always impossible for Schützenberger groups of primitive invertible substitutions. This follows from a correlation between relative invertibility of a primitive aperiodic substitution and relative freeness of its Schützenberger group. In particular, when absolute invertibility is achieved, only absolute freeness is possible.

The arguments used in the aforementioned counterexample are mostly combinatorial in nature, but another, more algebraic approach has proved effective in other cases. Almeida and Costa's proof that the Schützenberger group of the Thue–Morse substitution is not relatively free is an edifying example. The core of their argument lies in characterizing its finite elementary Abelian quotients, a task which is made relatively straightforward with the help of their notion of ω-presentations. In [11], they observed that in the case of the Thue–Morse substitution, a finite elementary Abelian p-group is a quotient of the Schützenberger group precisely when it has dimension 2 or less if p is an odd prime, but that the dimension could only be at most 1 for $p = 2$. This discrepancy alone suffices to infer failure of relative freeness. Computing these bounds on the dimensions of the finite elementary Abelian quotients involves looking at the long term behaviour of powers of an appropriate matrix, namely the composition matrix of a *return substitution*. (This is an important concept in symbolic dynamics, popularized in part by Durand's work in the late 90s [35, 36].) In essence, Almeida and Costa's argument consists of two steps: first, compute a return substitution; second, determine the long-term behaviour of the powers of its composition matrix (more precisely of its reductions mod p for different primes p). This is the starting point of the work presented in Paper 2, and it led to a few unexpected conclusions.

We can in fact apply similar ideas to the wider setting of ω-presented groups: in that case, all the information about the finite elementary Abelian quotients can in fact be extracted directly from a characteristic polynomial (this is the *dimension formula* of Paper 2). And this can be taken one step further: with a few standard results from profinite group theory, we can show that this polynomial contains enough information to understand all finite nilpotent quotients. In particular, we can tell easily whether these quotients witness such things as failure of absolute or relative freeness. This has some interesting corollaries, including the fact that Schützenberger groups of primitive aperiodic substitutions of constant length (like the Thue–Morse substitution) are never absolutely free. This description of the finite nilpotent quotients also sheds some light on other properties of Schützenberger groups. For instance, it answers partially a question of Zalesskii reported in [11]: can free pro-p groups be realized as maximal subgroups of free profinite monoids? The answer is negative for maximal subgroups corresponding to primitive substitutions, because their maximal pronilpotent quotients have non-trivial Sylow components for cofinitely many primes. However, Zalesskii question remains open for non-substitutive minimal shift spaces. In light of recent work by Costa and Steinberg [30], the finite nilpotent quotients also provide a number of dynamical invariants for shift spaces defined by primitive substitutions. Indeed, Costa and Steinberg proved that the Schützenberger group is invariant under *flow equivalence*, and therefore so is the corresponding maximal pronilpotent quotient. Since this quotient is completely and transparently determined by the characteristic polynomial of the return substitutions, certain properties of these polynomials, and even of the characteristic polynomial of the original substitution, must also be invariants of the suspension flow. These invariants, though clearly weaker than the Schützenberger group itself, have the advantage of being finite in nature and easily computable. For example, one such invariant is the set of primes dividing the pseudodeterminant (the product with multiplicity of the non-zero eigenvalues) of the composition matrix of the substitution.

Paper 3 is somewhat of an outlier in this thesis. It contains a number of combinatorial results regarding subgroups generated by return words in minimal shift spaces. The connection with Schützenberger groups, which is not mentioned in the paper itself, is provided by a series of results of Almeida and Costa [12]. These results are surveyed in Appendix A, where we also explain in detail the relevance of Paper 3 within the context of this thesis. One of the main findings of Almeida and Costa is that the return sets, taken collectively, provide a criterion for absolute freeness: roughly speaking, when *enough* return sets are bases of the same subgroup (say of rank n) then the Schützenberger group must be a free profinite group (also of rank n). While this criterion is in general difficult to apply, it has the advantage of also working for non-substitutive minimal shift spaces, as opposed to the various criteria relying on ω-presentations. For a while, the only cases where this criterion could be conclusively applied were the minimal dendric shift spaces, which we mentioned earlier in passing. This family of shift spaces was introduced in 2015, under the name *tree sets*,[2] by Berthé et al. [23], and they all share a remarkable property: all of their return sets form bases of the free group over the alphabet of the shift space, a result known as the *Return Theorem* [23]. The initial motivation behind Paper 3 was to find weaker conditions under which the subgroups generated by return sets could be kept under tight control, with the hope of finding non-dendric examples where Almeida and Costa's freeness criterion could be applied. The main contribution of Paper 3 is *suffix-connectedness*, a new condition that does precisely this. In a minimal suffix-connected shift space, all return sets generate essentially the same subgroup of the free group. But suffix-connectedness is more flexible than dendricity: return sets can have varying cardinalities and they can generate proper subgroups. Paper 3 contains an example of the former, while Appendix B presents an example showcasing both properties at once. Appendix A also contains a variation of Almeida and Costa's freeness criterion which was suggested to the author of this thesis by Costa. The suffix-connected example of Paper 3 fulfils this criterion, while the example from Appendix B fails it. Another interesting feature of suffix-connected shift spaces is that they behave similarly to primitive invertible substitutions when it comes to relative freeness. That is, proper relative freeness is simply impossible for Schützenberger groups of suffix-connected minimal shift spaces.

Notes to the reader

An effort has been made to keep the three papers that constitute the core of this thesis as close as possible to their published form. As such, figures, sections, theorems, lemmas, etc., are numbered independently in each paper. For the sake of coherence, the same goes for the conclusion and the appendices. However, it seemed more convenient that references be numbered globally and collected in a single reference list, which the reader will find right after the conclusion. Lists of figures and tables are given at the beginning of the thesis, and indices of subjects and notations are given at the end.

[2]We warn the reader that the precise definition of *tree sets* varies across the literature. For instance, in Paper 3 and in Dolce and Perrin's 2017 paper [33], the term takes on a less restrictive meaning than in the paper where it was introduced [23].

Paper 1

Freeness of Schützenberger groups of primitive substitutions

International Journal of Algebra and Computations, 2022. In press.

doi:10.1142/S0218196722500473

Freeness of Schützenberger groups of primitive substitutions

Herman Goulet-Ouellet

Received 23 September 2021
Accepted 8 April 2022
Communicated by B. Steinberg

Abstract. Our main goal is to study the freeness of Schützenberger groups defined by primitive substitutions. Our findings include a simple freeness test for these groups, which is applied to exhibit a primitive invertible substitution with corresponding non-free Schützenberger group. This constitutes a counterexample to a result of Almeida dating back to 2005. We also give some early results concerning relative freeness of Schützenberger groups, a question which remains largely unexplored.

Keywords. Profinite groups, Invertible substitutions, Schützenberger groups, Return words

Mathematics subject classification 2010. 20E18, 37B10, 20E05, 20M05

1 Introduction

In [8], Almeida unveiled a connection between symbolic dynamical systems, or shift spaces, and maximal subgroups of free profinite monoids. More precisely, he proved that the topological closure inside the free profinite monoid of the language of a minimal shift space contains a unique regular $\mathcal{J}$-class. By standard results from semigroup theory, all the maximal subgroups contained in a regular $\mathcal{J}$-class define the same group up to isomorphism, known as its *Schützenberger group*. In a profinite monoid, the Schützenberger group of a regular $\mathcal{J}$-class is a profinite group. Thus, Almeida's correspondence associates to each minimal shift space a profinite group, and this defines a conjugacy invariant [28].

In the study of Schützenberger groups corresponding to minimal shift spaces, the freeness question has been a recurring theme [8, 11, 12, 29]. These groups are known to be free for the family of dendric shift spaces, also known as tree sets [12, Theorem 6.5]. Notably, these include Arnoux–Rauzy shift spaces [22, Example 3.2], as well as shift spaces defined by regular interval exchange [24, Theorem 4.3]. On the other hand, failure of freeness was also observed, for instance in the shift space defined by the Thue–Morse substitution [11, Theorem 7.6]. This raises the general question: when is the Schützenberger group defined by a minimal shift space free? At time of writing, this question remains largely open. A partial answer was proposed early on by Almeida, which argued that the Schützenberger group of a primitive invertible substitution must be free [8, Corollary 5.7]. However, upon closer inspection, we noticed some gaps in the proof. This prompted us to investigate more closely the freeness question for Schützenberger groups of primitive substitutions, with an eye on the specific case of invertible substitutions. This paper aims to present the results of this investigation, which include a counterexample to [8, Corollary 5.7].

The paper is organized as follows. In Section 2, we review some relevant background. In Section 3, we discuss the notion of ω-presentation (a type of profinite presentation introduced in [11]) and we give a number of technical results. In Section 4, we examine the link between freeness and ω-presentations. The main result of this section, Theorem 4.1, provides a simple test for freeness of Schützenberger groups of primitive substitutions. Several examples are presented for which the test can be successfully applied. In Section 5, we study the Schützenberger groups of relatively invertible primitive substitutions, and more precisely the pseudovarieties generated by the finite quotients of such Schützenberger groups. The main result of this section has two consequences that are of particular interest to us. First, if a primitive substitution is invertible, then its Schützenberger group is relatively free if and only if it is absolutely free. Second, if a primitive substitution is unimodular and its Schützenberger group is relatively free, then it must be free with respect to a pseudovariety containing at least all finite nilpotent groups. Finally, Section 6 presents our counterexample to [8, Corollary 4.7], which consists of a primitive invertible substitution whose Schützenberger group is not free, and in fact not relatively free by the results of Section 5.

2 Preliminaries

This section aims to provide some context and present most of the relevant background. Additional notions will be introduced in the course of the paper as they are needed. The monograph [19] contains an in-depth treatment of most of the material we need. Here is a list of more specialized documents that may also be useful: on profinite groups and profinite presentations, [51, 67]; on profinite semigroups and Schützenberger groups of primitive substitutions, [7, 8, 11]; on return sets and return substitutions, [35, 39].

By an *alphabet*, we mean a finite set A whose elements are called *letters*. We use A_n as a shorthand for the alphabet $\{0,\dots,n-1\}$, $n \in \mathbb{N}$. Let $F(A)$ be the free group on the alphabet A and $\widehat{F}(A)$ be the free profinite group on A. We use the notation ε to denote the identity element of both $F(A)$ and $\widehat{F}(A)$, as well as the empty word. We denote by $\mathrm{End}(F(A))$ the set of endomorphisms of $F(A)$, and by $\mathrm{End}(\widehat{F}(A))$ the set of continuous endomorphisms of $\widehat{F}(A)$. An endomorphism $\phi \in \mathrm{End}(F(A))$ admits a unique continuous extension $\widehat{\phi} \in \mathrm{End}(\widehat{F}(A))$, called the *profinite extension* of ϕ.

In this paper, we deal with profinite presentations in the sense of [51]. Formally, a *presentation* of a profinite group G is a pair formed by a set A and a subset $R \subseteq \widehat{F}(A)$ such that $G \cong \widehat{F}(A)/N$, where N is the closed normal subgroup of $\widehat{F}(A)$ generated by R. We call A the set of *generators* and R the set of *relators*. The notation $G \cong \langle A \mid R\rangle$ means that (A,R) is a presentation of G. The minimal number of generators in a presentation of G is denoted $d(G)$. A presentation realizing this minimum is called a *minimal presentation*.

A *substitution* is an endomorphism φ of the free monoid A^* over an alphabet A. Assuming A has at least two letters, we say that φ is *primitive* if there exists $n \in \mathbb{N}$ such that b occurs in $\varphi^n(a)$, for all $a,b \in A$. On the other hand, if A is a one-letter alphabet, then we say that φ is *primitive* if $\varphi(a) = a^n$ with $n > 1$. A substitution $\varphi\colon A^* \to A^*$ is called *invertible* if its natural extension to an endomorphism of $F(A)$ is an automorphism. Note that, if A is a singleton, the only invertible substitution is the identity mapping, which is not primitive according to our definition. Thus, a primitive invertible substitution is always defined on at least two letters.

Following [19, Section 5.5], a primitive substitution $\varphi\colon A^* \to A^*$ defines a minimal shift space $X(\varphi) \subseteq A^{\mathbb{Z}}$. The language of this shift space, which we denote $L(\varphi)$, is the subset of A^* formed by the factors of the words $\varphi^n(a)$ for all $n \in \mathbb{N}$ and $a \in A$. Minimality of $X(\varphi)$ means that $L(\varphi)$ must be *uniformly recurrent*. That is, $L(\varphi)$ is infinite, closed under taking factors, and satisfies the *bounded gap property*: for all $u \in L(\varphi)$, there exists $n \in \mathbb{N}$ such that u is a factor of every word $w \in L(\varphi)$ with $|w| \geq n$. We say that φ is *periodic* if $X(\varphi)$ is a periodic shift space, or equivalently if $L(\varphi)$ is the language of factors in the powers of a given word $w \in A^+$. Otherwise, we say that φ is *aperiodic*.

Let $\widehat{A^*}$ be the free profinite monoid over an alphabet A. A result of Almeida shows that if $L \subseteq A^*$ is uniformly recurrent, then $\overline{L} \setminus A^*$ is a $\mathcal{J}$-maximal regular $\mathcal{J}$-class of $\widehat{A^*}$, where $\overline{L}$ is the topological closure of L in $\widehat{A^*}$ [19, Propositon 5.6.14]. This in fact gives a bijective correspondence between uniformly recurrent languages (and thus minimal shift spaces) and $\mathcal{J}$-maximal regular $\mathcal{J}$-classes of $\widehat{A^*}$ [19, Proposition 5.6.12]. Standard results from semigroup theory imply that the maximal subgroups contained in $\overline{L} \setminus A^*$ are all isomorphic to the same profinite group, which is called the *Schützenberger group* of the $\mathcal{J}$-class (see for instance [19, Section 3.6]). In case $L = L(\varphi)$ is the language of a primitive substitution, we denote this group by $G(\varphi)$ and we call it the *Schützenberger group of* φ. Note that if φ is periodic, then $G(\varphi)$ is a free profinite group of rank 1 [19, Exercise 5.20], so from now on we focus on the aperiodic case.

Two-sided return substitutions, introduced in [39], play an important role in the study of Schützenberger groups of primitive substitutions [11]. This notion is based on the concept of return word, which we recall now. Let φ be a primitive substitution and $u, v \in L(\varphi)$ be such that $uv \in L(\varphi)$. By a *return word* to (u, v) in $L(\varphi)$, we mean a word $r \in A^*$ that separates two consecutive occurrences of (u, v) in $L(\varphi)$. More precisely, it is a word $r \in A^*$ such that urv is in $L(\varphi)$, starts and ends with uv, and contains exactly two occurrences of uv. The set of such words is denoted $\mathcal{R}_{u,v}$, and we call this a *return set* of φ. For primitive substitutions, the return sets are always finite and non-empty (by uniform recurrence of $L(\varphi)$, see [23, Proposition 4.2]). Moreover, they generate free submonoids of A^*, for which they form bases. In other words, the return sets of primitive substitutions are *codes* [39, Lemma 17]. A further property worth mentioning is that a primitive substitution is periodic if and only if one of its return sets is a singleton, if and only if all but finitely many of its return sets are singletons (see [35, Proposition 2.8] and [23, Proposition 4.4]).

By a *connection*[1] of a primitive substitution φ, we mean a pair of non-empty words (u, v) such that $uv \in L(\varphi)$ and, for some positive integer l, $\varphi^l(u)$ ends with u and $\varphi^l(v)$ starts with v. The least positive integer l with that property is called the *order* of the connection. If (u, v) is a connection of φ of order k, then φ^k restricts to a primitive substitution of the free submonoid generated by $\mathcal{R}_{u,v}$ [39, Lemma 21]. This substitution, which we denote $\varphi_{u,v}$, is said to be a *return substitution* of φ. All primitive substitutions have at least one connection, hence at least one return substitution [19, Proposition 5.5.10].

Following the convention used in [35], we relabel return substitutions using the natural ordering of return words induced by leftmost occurrences. This ordering may be defined as follows. Let (u, v) be a connection of order k of a primitive substitution φ. First, by uniform recurrence of $L(\varphi)$, there exists $n \in \mathbb{N}$ such that the word $u\varphi^{nk}(v)$ contains every word of the form urv, $r \in \mathcal{R}_{u,v}$. For $r, s \in \mathcal{R}_{u,v}$, we

[1] The term *connection* was coined by Almeida in [8], where it was used under the condition $|u| = |v| = 1$.

say that r *precedes* s *in the leftmost occurrence ordering* if the leftmost occurrence of urv in $u\varphi^{nk}(v)$ is located to the left of every occurrence of usv. Because $u\varphi^{nk}(v)$ is a prefix of $u\varphi^{mk}(v)$ whenever $m \geq n$, this ordering is independent of n. We view this as a bijection

$$\theta_{u,v} \colon A_{u,v} \to \mathcal{R}_{u,v}, \qquad \text{where } A_{u,v} = \{0, \ldots, \mathrm{Card}(\mathcal{R}_{u,v}) - 1\}.$$

The return substitution $\varphi_{u,v}$ can be defined as the unique substitution of $A_{u,v}^*$ satisfying the relation

$$\theta_{u,v} \circ \varphi_{u,v} = \varphi^k \circ \theta_{u,v},$$

where $\theta_{u,v}$ is extended to an homomorphism $\theta_{u,v} \colon A_{u,v}^* \to A^*$.

3 ω-presentations

We recall that the continuous endomorphisms of a finitely generated profinite group form a profinite monoid (see for instance [19, Section 3.12]).[2] This implies that for every such continuous endomorphism ψ, the closure of $\{\psi^n : n \in \mathbb{N}\}$ contains a unique idempotent element, which is denoted ψ^ω. More information about ω-powers, including basic properties, can be found in [19, Section 3.7]. We now give the eponymous definition of this section. Recall that, for an endomorphism ϕ of a free group $F(A)$, we denote by $\widehat{\phi}$ its profinite extension, which is a continuous endomorphism of $\widehat{F}(A)$.

Definition 3.1. Let G be a profinite group. An ω*-presentation* of G is a profinite presentation of the form

$$G \cong \langle A \mid \widehat{\phi}^\omega(a)a^{-1} : a \in A \rangle,$$

where A is a finite set and $\phi \in \mathrm{End}(F(A))$. We then say that ϕ *defines an* ω*-presentation* of G.

The number of generators of an ω-presentation of G defined by an endomorphism of $F(A)$ is equal to $\mathrm{Card}(A)$. Hence, such an ω-presentation is minimal as a presentation of G precisely when $\mathrm{Card}(A) = d(G)$. We call this a *minimal* ω*-presentation*. We also note that the following alternative notation is sometimes used for ω-presentations, using relations instead of relators, for instance in [11]:

$$G \cong \langle A \mid \widehat{\phi}^\omega(a) = a \ (a \in A) \rangle.$$

The next lemma gives a different way to interpret ω-presentations. We use essentially the same argument as [51, Proposition 1.1], where it was attributed to Kovács.

Lemma 3.2. *If* $\phi \in \mathrm{End}(F(A))$ *defines an* ω*-presentation of a profinite group* G*, then* $G \cong \mathrm{Im}(\widehat{\phi}^\omega)$.

Proof. Let $\psi = \widehat{\phi}$. It suffices to show that the closed normal subgroup K of $\widehat{F}(A)$ generated by $\{\psi^\omega(a)a^{-1} : a \in A\}$ is equal to $\ker(\psi^\omega)$. Since ψ^ω is an idempotent endomorphism, the following equalities hold:

$$\psi^\omega(\psi^\omega(a)a^{-1}) = \psi^\omega(\psi^\omega(a))\psi^\omega(a^{-1}) = \psi^\omega(a)\psi^\omega(a^{-1}) = \psi^\omega(aa^{-1}) = \varepsilon.$$

Therefore, K is contained in $\ker(\psi^\omega)$.

[2] For historical context, Hunter proved in [47] that the monoid of continuous endomorphisms of a finitely generated profinite semigroup is profinite for the compact-open topology. This result was rediscovered by Almeida [7] and generalized by Steinberg [71].

To prove the reverse inclusion, we show that K contains every element of the form $\psi^{\omega}(x)x^{-1}$ with $x \in \widehat{F}(A)$. The desired inclusion clearly follows since $x \in \ker(\psi^{\omega})$ implies $x^{-1} = \psi^{\omega}(x)x^{-1}$. Consider the following subset of $\widehat{F}(A)$:

$$\{x \in \widehat{F}(A) : \psi^{\omega}(x)x^{-1} \in K\}.$$

Routine arguments show that this set forms a closed subgroup of $\widehat{F}(A)$ which contains A. Hence, it must be equal to $\widehat{F}(A)$, and this finishes the proof. □

Our motivation for introducing ω-presentations is a key result due to Almeida and Costa, which is stated below. It allows to effectively compute an ω-presentation for the Schützenberger group of every primitive aperiodic substitution, and will serve as our starting point in Section 6. The original statement is restricted to connections (u,v) satisfying $|u| = |v| = 1$, but the proof works as long as $u, v \neq \varepsilon$.

Theorem 3.3 ([11, Theorem 6.2])**.** *Let φ be a primitive aperiodic substitution and (u,v) be a connection of φ. Then $G(\varphi)$ has the following ω-presentation:*

$$G(\varphi) \cong \langle A_{u,v} \mid \widehat{\varphi_{u,v}}^{\omega}(a)a^{-1} : a \in A_{u,v}\rangle.$$

In other words, every return substitution of φ defines an ω-presentation of $G(\varphi)$.

Remark 3.4. Assume that φ is also *proper*, meaning that there are $a_1, a_2 \in A$ and $n \in \mathbb{N}$ such that $\varphi^n(b) \in a_1A^* \cup A^*a_2$ for all $b \in A$. Then $G(\varphi)$ has the more straightforward ω-presentation $G(\varphi) \cong \langle A \mid \widehat{\varphi}^{\omega}(a)a^{-1} : a \in A\rangle$ [11, Theorem 6.4]. That is to say, φ defines an ω-presentation of its own Schützenberger group. Further noting that return substitutions are always proper [39, Lemma 21], it follows that a return substitution $\varphi_{u,v}$ defines an ω-presentation of both $G(\varphi)$ and $G(\varphi_{u,v})$. Hence, the two Schützenberger groups are isomorphic.

Example 3.5. The *Thue–Morse substitution* is the binary substitution τ defined by

$$\tau\colon 0 \mapsto 01,\ 1 \mapsto 10.$$

This substitution is clearly primitive and it is well known to be aperiodic. Moreover, it is easily verified that the pairs $(0,1)$, $(0,10)$ are connections of τ of order 2. Computing the corresponding return substitutions (for instance using the algorithm described in Section 6), one obtains the following substitutions, both defined on the alphabet $A_4 = \{0,1,2,3\}$:

$$\tau_{0,1}\colon 0 \mapsto 0123,\ 1 \mapsto 013,\ 2 \mapsto 02123,\ 3 \mapsto 0213,$$
$$\tau_{0,10}\colon 0 \mapsto 01,\ 1 \mapsto 023132,\ 2 \mapsto 0232,\ 3 \mapsto 0131.$$

By Theorem 3.3, the substitutions $\tau_{0,1}$ and $\tau_{0,10}$ define ω-presentations of the Schützenberger group $G(\tau)$, which means

$$G(\tau) \cong \langle A_4 \mid \widehat{\tau_{0,1}}^{\omega}(a)a^{-1} : a \in A_4\rangle \cong \langle A_4 \mid \widehat{\tau_{0,10}}^{\omega}(a)a^{-1} : a \in A_4\rangle.$$

As it was observed in [11], the ω-presentations given by return substitutions (or indeed by the substitution itself in the proper case) are not always minimal. We now introduce a simple method for reducing the number of generators in ω-presentations. Let ϕ be an element of $\mathrm{End}(F(A))$. We denote by $r_n(\phi)$ the restriction of ϕ to an endomorphism of $\mathrm{Im}(\phi^n)$.

Proposition 3.6. *If $\phi \in \mathrm{End}(F(A))$ defines an ω-presentation of a profinite group G, then, for every non-negative integer n, the endomorphism $r_n(\phi)$ defines an ω-presentation of G with at most* $\mathrm{Card}(A)$ *generators.*

Proof. By the Nielsen–Schreier theorem, $\mathrm{Im}(\phi^n) = F(B)$ for some finite set B. Moreover, since $F(B)$ is generated by $\phi^n(A)$, we have $\mathrm{Card}(B) \leq \mathrm{Card}(A)$. It remains to show that $r_n(\phi)$ defines an ω-presentation of G, which by Lemma 3.2 amounts to showing that $\mathrm{Im}(\widehat{r_n(\phi)}^{\omega}) \cong \mathrm{Im}(\widehat{\phi}^{\omega})$.

Let $\eta\colon F(B) \to F(A)$ be the homomorphism induced by the inclusion $F(B) \subseteq F(A)$ and let $\widehat{\eta}\colon \widehat{F}(B) \to \widehat{F}(A)$ be its profinite extension. Since η is injective, so is $\widehat{\eta}$ by [19, Theorem 4.6.7]. Moreover, from the equality $\phi \circ \eta = \eta \circ r_n(\phi)$, we deduce that the following diagram is commutative:

$$\begin{tikzcd}
\widehat{F}(B) \arrow[r, "\widehat{\eta}"] \arrow[d, "\widehat{r_n(\phi)}"] & \widehat{F}(A) \arrow[d, "\widehat{\phi}"] \\
\widehat{F}(B) \arrow[r, "\widehat{\eta}"] & \widehat{F}(A).
\end{tikzcd}$$

Hence, $\widehat{\eta}$ restricts to a continuous isomorphism $\mathrm{Im}(\widehat{r_n(\phi)}^{\omega}) \cong \widehat{\phi}^{\omega}(\mathrm{Im}(\widehat{\eta}))$. Noting the equalities

$$\mathrm{Im}(\widehat{\eta}) = \overline{\mathrm{Im}(\eta)} = \overline{\mathrm{Im}(\phi^n)} = \mathrm{Im}(\widehat{\phi}^n),$$

it then suffices to show that $\widehat{\phi}^{\omega}(\mathrm{Im}(\widehat{\phi}^n)) = \mathrm{Im}(\widehat{\phi}^{\omega})$. And indeed, we have

$$\widehat{\phi}^{\omega}(\mathrm{Im}(\widehat{\phi}^n)) \subseteq \mathrm{Im}(\widehat{\phi}^{\omega}) = \widehat{\phi}^{\omega}(\mathrm{Im}(\widehat{\phi}^{\omega})) \subseteq \widehat{\phi}^{\omega}(\mathrm{Im}(\widehat{\phi}^n)). \qquad \square$$

Note that the restriction operation satisfies $r_k(r_n(\phi)) = r_{n+k}(\phi)$. Therefore, $\{r_n(\phi)\}_{n\in\mathbb{N}}$ gives a sequence of ω-presentations of the same profinite group with weakly decreasing numbers of generators. The next result tells us exactly when the number of generators stabilizes. The proof mostly boils down to the well-known fact that free groups of finite rank enjoy the *Hopfian property*, which can be stated as follows: every surjective homomorphism between two free groups of the same finite rank is an isomorphism. See for instance [61, Theorem 41.52].

Proposition 3.7. *Let ϕ define an ω-presentation of a profinite group G. For every two non-negative integers $m, n \in \mathbb{N}$ with $n < m$, the ω-presentations of G defined by $r_n(\phi)$ and $r_m(\phi)$ have the same number of generators if and only if $r_n(\phi)$ is injective.*

Proof. We start by noting that $r_n(\phi)^{m-n}$ is a continuous surjective homomorphism from $\mathrm{Im}(\phi^n)$ to $\mathrm{Im}(\phi^m)$. If $r_n(\phi)$ and $r_m(\phi)$ define ω-presentations with the same number of generators, then $\mathrm{Im}(\phi^n)$ and $\mathrm{Im}(\phi^m)$ are free groups of the same rank, and by the Hopfian property, $r_n(\phi)^{m-n}$ is an isomorphism. In particular, $r_n(\phi)^{m-n}$ is injective, and since $m-n \geq 1$ so is $r_n(\phi)$.

Conversely, if $r_n(\phi)$ is injective, then $r_n(\phi)^{m-n}\colon \mathrm{Im}(\phi^n) \to \mathrm{Im}(\phi^m)$ is an isomorphism. Thus, $\mathrm{Im}(\phi^n)$ and $\mathrm{Im}(\phi^m)$ are free groups of the same rank and the ω-presentations defined by $r_m(\phi)$ and $r_n(\phi)$ have the same number of generators. $\square$

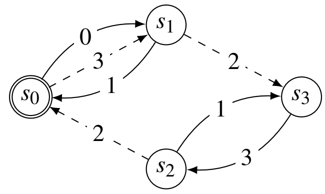


Fig. 1 Stallings automaton of the image of the return substitution $\tau_{0,10}$ viewed as an endomorphism of $F(A_4)$. The distinguished state is identified by a double circle and the dashed edges form a spanning tree.

We immediately deduce the following.

Corollary 3.8. *Let ϕ define an ω-presentation of a profinite group G. If ϕ is not injective, then there exists an ω-presentation of G with strictly less generators. In particular, if ϕ defines a minimal ω-presentation of G, then ϕ must be injective.*

The following example shows that injective endomorphisms can also define non-minimal ω-presentations.

Example 3.9 (Continued from Example 3.5). One can show that the endomorphism of $F(A_4)$ induced by the return substitution $\tau_{0,1}$ is not injective. For instance,

$$02^{-1}02^{-1}31^{-1}20^{-1} \in \ker(\tau_{0,1}).$$

Hence, by Corollary 3.8, the ω-presentation defined by $\tau_{0,1}$ is not minimal.

On the other hand, $\tau_{0,10}$ extends to an injective endomorphism of $F(A_4)$. One way to see this is to show that the set $\{03^{-1}, 31^{-1}, 3232, 2^{-1}12^{-1}3^{-1}\}$ is a basis of $\mathrm{Im}(\tau_{0,10})$. More precisely, it is the basis determined (as in [48, Lemma 6.1]) by the spanning tree of the Stallings automaton of $\mathrm{Im}(\tau_{0,10})$ given in Fig. 1. Even though $\tau_{0,10}$ is injective, it does not define a minimal ω-presentation of $G(\tau)$, since it has the same number of generators as the non-minimal ω-presentation defined by $\tau_{0,1}$.

According to Proposition 3.6, a shorter ω-presentation of $G(\tau)$ is defined by the restriction $r_1(\tau_{0,1})$. Here is the endomorphism $r_1(\tau_{0,1})$ expressed in the basis $\{020^{-1}, 3^{-1}23, 02^{-1}12^{-1}3\}$ of $\mathrm{Im}(\tau_{0,1})$:

$$r_1(\tau_{0,1})\colon 0 \mapsto 02110,\ 1 \mapsto 10021,\ 2 \mapsto 2.$$

Another ω-presentation of $G(\tau)$ with 3 generators was obtained, by other means, in [11], where it is also shown that $d(G(\tau)) = 3$ [11, Theorem 7.7]. Therefore, the ω-presentation defined by $r_1(\tau_{0,1})$ is minimal.

4 Freeness via ω-presentations

In this section, we present a few key results concerning freeness of profinite groups with ω-presentations. Given an endomorphism ϕ of $F(A)$, the *incidence matrix* of ϕ is the matrix $M(\phi) \in \mathbb{Z}^{A\times A}$ defined by $M(\phi)_{a,b} = |\phi(a)|_b$, where $|-|_b\colon F(A) \to \mathbb{Z}$ is the unique group homomorphism extending the Kronecker delta function $\delta_b\colon A \to \mathbb{Z}$. The main result of the section is the following theorem, which provides a simple freeness test for Schützenberger groups of primitive substitutions. We will make use of this test in Section 6 to exhibit a primitive invertible substitution whose Schützenberger group is not free. Two examples where this test can be applied are also presented at the end of the current section.

Theorem 4.1. *Let G be a profinite group with an ω-presentation defined by an endomorphism ϕ such that* $\det(M(\phi)) \neq 0$. *Then G is a free profinite group if and only if ϕ is an automorphism.*

The following example shows why the theorem may fail without the assumption that $\det(M(\phi)) \neq 0$.

Example 4.2. Let A be an alphabet and b a letter not in A. Consider the endomorphism ϕ of $F(A \cup \{b\})$ defined by

$$\phi(a) = \begin{cases} a & \text{if } a \neq b \\ \varepsilon & \text{if } a = b. \end{cases}$$

It is straightforward to check that ϕ defines an ω-presentation of $\widehat{F}(A)$, but it is clearly not an automorphism.

We split the proof of Theorem 4.1 into two propositions. The first one relates freeness with minimal ω-presentations. The proof uses the fact that free profinite groups of finite ranks satisfy a topological version of the Hopfian property: every continuous surjective homomorphism between two free profinite groups of the same rank is an isomorphism [67, Proposition 2.5.2]. Also note the following straightforward consequence of the Hopfian property, which is used in the proof: the free profinite group over a finite set A cannot be generated by strictly less than $\mathrm{Card}(A)$ elements, and therefore $d(\widehat{F}(A)) = \mathrm{Card}(A)$.

Proposition 4.3. *Let $\phi \in \mathrm{End}(F(A))$ define a minimal ω-presentation of a profinite group G. Then G is a free profinite group if and only if ϕ is an automorphism.*

Proof. Suppose that ϕ is an automorphism. Noting that the profinite completion is functorial [67, Lemma 3.2.3], it follows that $\widehat{\phi}$ is also an automorphism, and by [19, Proposition 3.7.4], $\widehat{\phi}^{\omega}$ is the identity. Since ϕ defines an ω-presentation of G, we see that

$$G \cong \langle A \mid \widehat{\phi}^{\omega}(a)a^{-1} : a \in A \rangle = \langle A \mid aa^{-1} : a \in A \rangle = \langle A \mid \varepsilon \rangle = \widehat{F}(A).$$

Conversely, suppose that G is a free profinite group. Since the ω-presentation of G defined by ϕ is minimal, we have $d(G) = \mathrm{Card}(A)$ and it follows that G is isomorphic to $\widehat{F}(A)$. Moreover, by Lemma 3.2, G is isomorphic to $\mathrm{Im}(\widehat{\phi}^{\omega})$. Therefore, $\widehat{\phi}^{\omega} \colon \widehat{F}(A) \to \mathrm{Im}(\widehat{\phi}^{\omega})$ is a continuous surjective homomorphism between free profinite groups of the same rank. By the Hopfian property, it follows that $\widehat{\phi}^{\omega}$ is injective. Since it is idempotent, we conclude that $\widehat{\phi}^{\omega}$ is the identity. By [19, Proposition 3.7.4], $\widehat{\phi}$ is an automorphism and by [19, Proposition 4.6.8], so is ϕ. $\square$

Remark 4.4. At time of writing, we are not aware of any reliable way to find minimal ω-presentations for Schützenberger groups of primitive substitutions. Example 3.9 gives some clues as to why this might be a difficult problem.

The second proposition, which completes the proof of Theorem 4.1, gives a sufficient condition for an ω-presentation to be minimal. The minimal ω-presentation of $G(\tau)$ given at the end of Example 3.9 shows that this condition is not necessary.

Proposition 4.5. *Let $\phi \in \mathrm{End}(F(A))$ define an ω-presentation of a profinite group G such that $\det(M(\phi)) \neq 0$. Then the ω-presentation defined by ϕ is a minimal presentation of G.*

The proof relies on a result from [11] which is recalled in the next proposition. Given ψ in $\mathrm{End}(\widehat{F}(A))$ and a finite group H, we define an operator $\psi_H\colon H^A \to H^A$ as follows. A tuple $t \in H^A$, viewed as a map $A \to H$, extends uniquely to a continuous homomorphism $\widehat{t}\colon \widehat{F}(A) \to H$. We define $\psi_H(t) \in H^A$ by

$$\psi_H(t)(a) = \widehat{t}(\psi(a)), \qquad a \in A.$$

This construction gives a contravariant continuous action of the profinite monoid $\mathrm{End}(\widehat{F}(A))$ on H^A [11, Lemma 3.1].

Let H be a finite group and $t \in H^A$ be a tuple. We say that t *generates* H if its components form a generating set of H.

Proposition 4.6 ([11, Proposition 3.2])**.** *Let $\phi \in \mathrm{End}(F(A))$ define an ω-presentation of a profinite group G and H be a finite group. Then the following are equivalent:*

(1) H is a continuous homomorphic image of G.
(2) There exist $t \in H^A$ and $n \geq 1$ such that t generates H and $\widehat{\phi}^n_H(t) = t$.

With this, we are ready for the proof of Proposition 4.5, which also completes the proof of Theorem 4.1.

Proof of Proposition 4.5. Since every continuous homomorphic image H of G satisfies $d(H) \leq d(G)$, it suffices to show that one such image exists satisfying $d(H) = \mathrm{Card}(A)$. To this end, fix a prime p that does not divide $\det(M(\phi))$ and let $H = (\mathbb{Z}/p\mathbb{Z})^A$. Clearly, $d(H) = \mathrm{Card}(A)$. Let $M_p(\phi)$ be the reduction modulo p of the incidence matrix $M(\phi)$. Then, a direct computation shows that for all $t \in H^A$ and $a \in A$,

$$\widehat{\phi}_H(t)(a) = \sum_{b \in A} \varepsilon_b(\phi(a))t(b) = (M_p(\phi)t)(a),$$

where t is viewed as a column vector in the rightmost expression. By our choice of p, the determinant of $M_p(\phi)$ is an invertible element of $\mathbb{Z}/p\mathbb{Z}$, hence $M_p(\phi)$ is an invertible matrix over $\mathbb{Z}/p\mathbb{Z}$. Since invertible matrices of order $\mathrm{Card}(A)$ over $\mathbb{Z}/p\mathbb{Z}$ form a finite group, $M_p(\phi)^n$ is an identity matrix for some $n \geq 1$. It follows that

$$\widehat{\phi}^n_H(t) = M_p(\phi)^n t = t.$$

Hence, we may apply Proposition 4.6 with any tuple that generates H (for instance, a tuple formed by a basis of H as a vector space over $\mathbb{Z}/p\mathbb{Z}$), and we conclude that H is a continuous homomorphic image of G. $\square$

We finish this section by pointing out some interesting applications of Theorem 4.1, starting with the following corollary.

Corollary 4.7. *Let G be a profinite group with an ω-presentation defined by an endomorphism ϕ such that $|\det(M(\phi))| > 1$. Then G is not a free profinite group.*

Proof. Suppose that G is a free profinite group. By Theorem 4.1, ϕ is an automorphism of $F(A)$. But note that the incidence matrix defines a monoid homomorphism from $\mathrm{End}(F(A))$ equipped with reversed composition, to the monoid of matrices of order $\mathrm{Card}(A)$ over $\mathbb{Z}$. In particular, it follows that the matrix $M(\phi)$ is invertible over $\mathbb{Z}$. Therefore, $|\det(M(\phi))|$ equals 1, a contradiction. $\square$

Next, we present two examples of primitive substitutions where the previous corollary may be used to show that the Schützenberger group is not free. The first example is due to Almeida, who proved that the Schützenberger group is non-free back in 2005 [8, Example 7.2].

Example 4.8 (Almeida's example). Let α be the primitive binary substitution defined by

$$\alpha\colon 0 \mapsto 01,\ 1 \mapsto 0001.$$

This substitution is aperiodic (using for instance [19, Exercise 5.15]) and proper. It follows that α defines an ω-presentation of $G(\alpha)$ (see Remark 3.4). A quick computation shows that $\det(M(\alpha)) = -2$, hence $G(\alpha)$ is not a free profinite group by Corollary 4.7.

The second example is another well-known primitive substitution, although it appears as though its Schützenberger group has not been studied.

Example 4.9. The *period doubling substitution* is the binary substitution ρ defined as follows:

$$\rho\colon 0 \mapsto 01,\ 1 \mapsto 00.$$

It is a primitive substitution which is also aperiodic (using again [19, Exercise 5.15]). It admits $(1,0)$ as a connection of order 2. The return substitution $\rho_{1,0}$ is given by

$$\rho_{1,0}\colon 0 \mapsto 010,\ 1 \mapsto 01110.$$

The incidence matrix of $\rho_{1,0}$ has determinant 4. By Theorem 3.3, $\rho_{1,0}$ defines an ω-presentation of $G(\rho)$, hence we may apply Corollary 4.7 to conclude that $G(\rho)$ is not free.

5 Schützenberger groups of relatively invertible substitutions

In this section, we examine the Schützenberger groups of relatively invertible primitive substitutions, that is primitive substitutions that extend to automorphisms of some relatively free profinite group. To this end, it is useful to first recall a few basic things about pseudovarieties. A *pseudovariety of groups*, or *pseudovariety* for short, is a class $\mathbf{H}$ of finite groups closed under taking subgroups, quotients and finite direct products. Here are a few common examples:

- the pseudovariety $\mathbf{G}$ of all finite groups;
- the pseudovariety $\mathbf{G}_p$ of finite p-groups, where p is a given prime;
- the pseudovariety $\mathbf{G}_{\mathrm{nil}}$ of finite nilpotent groups;
- the pseudovariety $\mathbf{G}_{\mathrm{sol}}$ of finite solvable groups;
- the pseudovariety $\mathbf{Ab}$ of finite Abelian groups.

A pseudovariety $\mathbf{H}$ is called *extension-closed* if for each $N,K \in \mathbf{H}$, all extensions of K by N are in $\mathbf{H}$. Among the examples given above, $\mathbf{G}$, $\mathbf{G}_p$ and $\mathbf{G}_{\mathrm{sol}}$ are extension-closed, while $\mathbf{G}_{\mathrm{nil}}$ and $\mathbf{Ab}$ are not.

We denote by $\widehat{F}_{\mathbf{H}}(A)$ the free pro-$\mathbf{H}$ group on a set A. As the name suggests, these are the free objects in the category of *pro-*$\mathbf{H}$ *groups* (residually $\mathbf{H}$ compact groups). A detailed construction of free pro-**H** groups can be found in [67, Section 3]. We call groups of the form $\widehat{F}_{\mathbf{H}}(A)$, where **H** is a non-trivial pseudovariety, *relatively free* profinite groups. For emphasis, we say that the groups $\widehat{F}(A) = \widehat{F}_{\mathbf{G}}(A)$ are *absolutely free*. It was shown in [11, Theorems 7.2 and 7.6] that the Schützenberger groups of the substitutions τ and α presented in Examples 3.5 and 4.8 are not relatively free. In fact, at time of writing, there is no known example of a primitive substitution whose Schützenberger group is relatively free but not absolutely free. Part of our conclusion for this section, which is presented in Corollary 5.10, states that the Schützenberger group of a primitive invertible substitution is absolutely free if and only if it is relatively free.

Let $\varphi\colon A^* \to A^*$ be a primitive substitution and **H** be a pseudovariety of groups. We denote by $\widehat{\varphi}_{\mathbf{H}}$ the continuous endomorphism of $\widehat{F}_{\mathbf{H}}(A)$ naturally induced by φ. We say that φ is **H**-*invertible* if $\widehat{\varphi}_{\mathbf{H}}$ is an automorphism, or equivalently if $\widehat{\varphi}_{\mathbf{H}}^{\omega}$ is the identity [19, Proposition 3.7.4]. Note that **G**-invertibility is equivalent to invertibility in the usual sense. More explicitly, a primitive substitution extends to an automorphism of $F(A)$ if and only if it extends to an automorphism of $\widehat{F}(A)$ [19, Proposition 4.6.8].

Primitive substitutions also determine pseudovarieties of their own, which have been introduced in [11]: let $\mathbf{V}(\varphi)$ be the pseudovariety generated by the finite quotients of $G(\varphi)$, that is, by the finite groups that are continuous homomorphic images of $G(\varphi)$. Here is the main result of this section.

Theorem 5.1. *Let* **H** *be a non-trivial extension-closed pseudovariety and* φ *be a primitive, aperiodic and* **H**-*invertible substitution. Then,* **H** *is contained in* $\mathbf{V}(\varphi)$.

The proof of this theorem relies on a number of intermediate results, starting with the technical lemma stated below. If **H** is a non-trivial extension-closed pseudovariety, then free groups are residually **H** [67, Proposition 3.3.15], hence there is a natural embedding $F(A) \hookrightarrow \widehat{F}_{\mathbf{H}}(A)$ for every alphabet A. The induced topology on $F(A)$ is called the *pro-***H** *topology*. If X is a subset of $F(A)$, then we denote its topological closure in $\widehat{F}_{\mathbf{H}}(A)$ by $\overline{X}_{\mathbf{H}}$. On the other hand, we denote by $\mathrm{Cl}_{\mathbf{H}}(X)$ the closure of X in the pro-**H** topology of $F(A)$.

The proof of the next lemma is mostly a matter of combining several known results. We provide a proof for the sake of completeness. We chose to rely on [54, 66, 67], but let us mention that results from [32] could be used as well. Alternatively, one could adapt the proof of [19, Proposition 4.6.5], which can be partly traced back to [3, Lemma 4.2].

Lemma 5.2. *Let A be a finite set, K be a finitely generated subgroup of $F(A)$ and* **H** *be a non-trivial extension-closed pseudovariety. Then, $\overline{K}_{\mathbf{H}}$ is a free pro-***H** *group of rank at most that of K.*

Proof. By [66, Proposition 3.4], $\mathrm{Cl}_{\mathbf{H}}(K)$ is a subgroup of $F(A)$ of rank at most that of K, so we may write $\mathrm{Cl}_{\mathbf{H}}(K) = F(B)$, where $\mathrm{Card}(B) \leq \mathrm{Card}(A)$. Let $\iota\colon F(B) \hookrightarrow F(A)$ be the inclusion, and denote by $\widehat{\iota}_{\mathbf{H}}$ its extension to a continuous homomorphism between the respective pro-**H** completions. By [67, Proposition 3.3.6], the pro-**H** completion of a free group of finite rank is a free profinite group of the same rank, hence we have $\widehat{\iota}_{\mathbf{H}}\colon \widehat{F}_{\mathbf{H}}(B) \to \widehat{F}_{\mathbf{H}}(A)$. Moreover, note that

$$\mathrm{Im}(\widehat{\iota}_{\mathbf{H}}) = \overline{\mathrm{Im}(\iota)}_{\mathbf{H}} = \overline{\mathrm{Cl}_{\mathbf{H}}(K)}_{\mathbf{H}} = \overline{K}_{\mathbf{H}},$$

where the leftmost equality follows from [67, Lemma 3.2.4]. Therefore, it suffices to show that the pro-**H** extension $\widehat{\iota}_{\mathbf{H}}$ is injective. By [67, Lemma 3.2.6], this is equivalent to showing that the pro-**H** topology of $\mathrm{Cl}_{\mathbf{H}}(K)$ coincides with the subspace topology induced by the pro-**H** topology of $F(A)$. This last statement holds by the last part of [54, Proposition 2.9]. □

We now turn to the following proposition, which is one of the main ingredients in the proof of Theorem 5.1.

Proposition 5.3. *Let* $\mathbf{H}$ *be a non-trivial extension-closed pseudovariety and* φ *be a primitive, aperiodic and* $\mathbf{H}$*-invertible substitution. Then,* $G(\varphi)$ *has a continuous homomorphic image isomorphic to a free pro-*$\mathbf{H}$ *group of rank at least 2.*

Proof. Fix a connection (u,v) of φ. By Theorem 3.3, $\varphi_{u,v}$ defines an ω-presentation of $G(\varphi)$ and by Lemma 3.2, it follows that $G(\varphi) \cong \mathrm{Im}(\widehat{\varphi_{u,v}}^{\omega})$. Let $\widetilde{\theta_{u,v}}$ be the natural extension of $\theta_{u,v}$ to a continuous homomorphism $\widetilde{\theta_{u,v}}\colon \widehat{F}(A_{u,v}) \to \widehat{F}_{\mathbf{H}}(A)$. Recall that $\theta_{u,v} \circ \varphi_{u,v} = \varphi^k \circ \theta_{u,v}$, where k is the order of the connection (u,v), hence the following diagram is commutative:

$$\begin{tikzcd} \widehat{F}(A_{u,v}) \arrow[r, "\widetilde{\theta_{u,v}}"] \arrow[d, "\widehat{\varphi_{u,v}}^{\omega}"] & \widehat{F}_{\mathbf{H}}(A) \arrow[d, "\widehat{\varphi}_{\mathbf{H}}^{\omega}"] \\ \widehat{F}(A_{u,v}) \arrow[r, "\widetilde{\theta_{u,v}}"] & \widehat{F}_{\mathbf{H}}(A). \end{tikzcd}$$

Since φ is $\mathbf{H}$-invertible, $\widehat{\varphi}_{\mathbf{H}}^{\omega}$ is the identity, hence $\mathrm{Im}(\widetilde{\theta_{u,v}})$ is a continuous homomorphic image of $G(\varphi)$. But notice that $\mathrm{Im}(\widetilde{\theta_{u,v}}) = \overline{\mathrm{Im}(\theta_{u,v})}_{\mathbf{H}} = \overline{K}_{\mathbf{H}}$, where K is the subgroup of $F(A)$ generated by the return set $\mathcal{R}_{u,v}$. By Lemma 5.2, $\overline{K}_{\mathbf{H}}$ is free pro-$\mathbf{H}$ group of finite rank. It remains only to show that this group has rank at least 2, or alternatively that this group is not commutative. But notice that $\overline{K}_{\mathbf{H}}$ contains the submonoid of A^* generated by $\mathcal{R}_{u,v}$, of which $\mathcal{R}_{u,v}$ itself forms a basis by [39, Lemma 17]. Since φ is aperiodic, $\mathcal{R}_{u,v}$ must have at least 2 elements, and therefore it generates a non-commutative submonoid of A^*, thus concluding the proof. □

Next is another lemma, which all but completes the proof of our main result. This lemma is a consequence of an embedding result, due to Neumann and Neumann, dating back to 1959 [60].

Lemma 5.4. *Let* $\mathbf{H}$ *be a non-trivial extension-closed pseudovariety. Then* $\mathbf{H}$ *is generated, as a pseudovariety, by its 2-generated members.*

Proof. Let $L \in \mathbf{H}$ be generated by non-identity elements $x_1,\dots,x_d$ of respective order $n_1,\dots,n_d$. The main construction of [60] implies that for all integers m,n such that $m \geq 4d$ and $\mathrm{lcm}(n_1,\dots,n_d) \mid n$, we may embed L in a 2-generated subgroup of the following wreath product:

$$(L \wr \mathbb{Z}/n\mathbb{Z}) \wr \mathbb{Z}/m\mathbb{Z}.$$

Since $\mathbf{H}$ is extension-closed, such a wreath product is in $\mathbf{H}$ provided all the factors are in $\mathbf{H}$. Therefore, it suffices to show that m and n can be chosen so that $\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z} \in \mathbf{H}$. For n, we may simply take $n = \mathrm{lcm}(n_1,\dots,n_d)$. Indeed, it then follows that $\mathbb{Z}/n\mathbb{Z}$ is a subgroup of $\mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_d\mathbb{Z}$. This last group in turn lies in $\mathbf{H}$ because, for $i = 1,\dots,d$, the subgroup of L generated by x_i is isomorphic to $\mathbb{Z}/n_i\mathbb{Z}$. For m, choose some prime p such that $\mathbb{Z}/p\mathbb{Z} \in \mathbf{H}$, for instance a prime that divides one of the n_i. Since $\mathbf{H}$ is extension-closed, it contains the extension-closed pseudovariety generated by $\mathbb{Z}/p\mathbb{Z}$, which is in fact $\mathbf{G}_p$. In particular, $\mathbf{H}$ contains $\mathbb{Z}/p^k\mathbb{Z}$ for all positive integers k. Taking $k \geq \log_p(4d)$, we find that $m = p^k$ fulfils all the required conditions. □

The proof of Theorem 5.1 is now a straightforward matter.

Proof of Theorem 5.1. By Proposition 5.3, $\mathbf{V}(\varphi)$ contains all 2-generated members of $\mathbf{H}$. But by Lemma 5.4, these groups generate $\mathbf{H}$, hence $\mathbf{H} \subseteq \mathbf{V}(\varphi)$. □

Next, we proceed to highlight some consequences of our main result. A result of Almeida implies that a substitution is $\mathbf{G}_p$-invertible if and only if $\det(M(\varphi))$ is not divisible by p [4, Proposition 5.2]. Combining this with Theorem 5.1, we immediately obtain the following:

Corollary 5.5. *Let φ be a primitive aperiodic substitution. Then $\mathbf{G}_p$ is contained in $\mathbf{V}(\varphi)$ for every prime p that does not divide* $\det(M(\varphi))$. *In particular, if* $\det(M(\varphi))$ *is not 0, this must be the case for cofinitely many primes.*

We now wish to show that Theorem 5.1 also holds for $\mathbf{G}_{\mathrm{nil}}$, even though it is not extension-closed. By [4, Corollary 5.3], a substitution φ is $\mathbf{G}_{\mathrm{nil}}$-invertible if and only if $\det(M(\varphi)) = \pm 1$. Substitutions satisfying the latter condition are called *unimodular*. It turns out that for primitive substitutions, unimodularity implies aperiodicity, as we now proceed to show.

Proposition 5.6. *A primitive unimodular substitution φ is aperiodic.*

Proof. We argue by contradiction and suppose that φ is periodic. Let φ be defined on an alphabet A. Then, all words in $L(\varphi)$ are factors of the powers of some word $w \in A^+$. Without loss of generality, we may assume that w is a primitive word (meaning there is no proper factorization $w = xy$ with $yx = w$), and that the pair (w,w) is a connection of φ of order 1. We claim that $\varphi(w) = w^n$ for some $n > 1$. Indeed, by assumption $\varphi(w) = sw^n t$ for some positive integer n and some words s, t such that s is a proper suffix, and t a proper prefix, of w. But as (w,w) is a connection of φ, w is both a prefix and suffix of $\varphi(w)$; and since w is a primitive word, this forces s and t to be empty. Thus, $\varphi(w) = w^n$, with $n > 1$ because φ is primitive. To conclude the proof, note that $(|w|_a)_{a\in A} \in \mathbb{Z}^A$ is an eigenvector of $M(\varphi)$ of eigenvalue n, which contradicts the unimodularity of φ. □

Tying up loose ends, we give a simple example showing that the conclusion of the previous proposition may not hold for substitutions that are $\mathbf{G}_p$-invertible for cofinitely many primes.

Example 5.7. Consider the following primitive substitution:

$$\varphi \colon 0 \mapsto 02,\ 1 \mapsto 21,\ 2 \mapsto 10.$$

It is straightforward to check that $\det(M(\varphi)) = -2$, hence φ is $\mathbf{G}_p$-invertible for all odd primes p. Yet, φ is periodic, as the language of φ consists of the factors in powers of the word 021.

In the next corollary of Theorem 5.1, we are able to omit the assumption of aperiodicity thanks to Proposition 5.6.

Corollary 5.8. *If φ is a primitive unimodular substitution, then $\mathbf{G}_{\mathrm{nil}}$ is contained in $\mathbf{V}(\varphi)$.*

Proof. Under our assumptions, φ is $\mathbf{G}_p$-invertible for all primes p, hence $\mathbf{V}(\varphi)$ contains $\mathbf{G}_p$ for all primes p by Corollary 5.5. Since $\mathbf{G}_{\mathrm{nil}}$ is the join (in the lattice of pseudovarieties ordered by inclusion) of the pseudovarieties $\mathbf{G}_p$, where p ranges over all primes, we find $\mathbf{G}_{\mathrm{nil}} \subseteq \mathbf{V}(\varphi)$. □

For the next corollary, which is just Theorem 5.1 with $\mathbf{H} = \mathbf{G}$, it is useful to note that invertible substitutions are unimodular. Indeed, recall from the proof of Corollary 4.7 that the incidence matrix of an automorphism must be invertible over $\mathbb{Z}$. In particular, we may again omit the aperiodicity assumption.

Corollary 5.9. *If φ is a primitive invertible substitution, then $\mathbf{V}(\varphi)$ equals $\mathbf{G}$.*

Finally, we give an application of Theorem 5.1 to the relative freeness question. For every pseudovariety $\mathbf{H}$, all finite continuous homomorphic images of a pro-$\mathbf{H}$ group lie in $\mathbf{H}$ [67, Theorem 2.1.3]. In particular, if $G(\varphi)$ is a free pro-$\mathbf{H}$ group, then $\mathbf{V}(\varphi) \subseteq \mathbf{H}$. Combining this observation with the three corollaries stated above yields the following corollary, which is our conclusion for this section.

Corollary 5.10. *Let $\mathbf{H}$ be a pseudovariety and φ be a primitive substitution such that $G(\varphi)$ is a free pro-$\mathbf{H}$ group.*

(1) If φ is aperiodic, then $\mathbf{G}_p \subseteq \mathbf{H}$ for every prime p that does not divide the determinant of $M(\varphi)$.
(2) If φ is unimodular, then $\mathbf{G}_{\mathrm{nil}} \subseteq \mathbf{H}$.
(3) If φ is invertible, then $\mathbf{H} = \mathbf{G}$ and therefore $G(\varphi)$ is absolutely free.

6 An invertible substitution with a non-free Schützenberger group

The aim of this section is to present a primitive invertible substitution whose Schützenberger group is not free, and thus not relatively free by Corollary 5.10. This constitutes a counterexample to [8, Corollary 5.7]. Let us formally state our conclusion.

Theorem 6.1. *There exists an invertible primitive substitution whose Schützenberger group is not a relatively free profinite group.*

Our example is the following substitution defined on $A_4 = \{0,1,2,3\}$:

$$\xi : 0 \mapsto 001,\ 1 \mapsto 02,\ 2 \mapsto 301,\ 3 \mapsto 320.$$

Showing that ξ is primitive amounts to a straightforward computation. Moreover, one can show that ξ is invertible by directly checking that

$$\xi^{-1} : 0 \mapsto 1^{-1}02^{-1}3,\ 1 \mapsto (3^{-1}20^{-1}1)^2 0,\ 2 \mapsto 3^{-1}20^{-1}11,\ 3 \mapsto 20^{-1}1^{-1}02^{-1}3.$$

Since invertible substitutions are unimodular, it follows from Proposition 5.6 that ξ is aperiodic.

We proceed to show that $G(\xi)$ is not a free profinite group. In light of Theorem 4.1, it suffices to show that $G(\xi)$ admits an ω-presentation defined by an endomorphism whose incidence matrix is invertible but which is not an automorphism. This boils down to a series of computations organized as follows:

Step 1. We compute the return substitution of ξ with respect to the connection $(1,0)$. This defines an ω-presentation of $G(\xi)$ with seven generators.
Step 2. We compute the restriction $r_1(\xi_{1,0})$. This defines an ω-presentation of $G(\xi)$ with five generators, and moreover the incidence matrix of $r_1(\xi_{1,0})$ has non-zero determinant.
Step 3. We show that $r_1(\xi_{1,0})$ is not an automorphism of $F(A_5)$.

Step 1

Let us compute the return substitution of ξ with respect to the connection $(1,0)$. Note that this connection has order 2. For this computation, we use an algorithm described by Durand in [37, p.5]. A detailed implementation of Durand's algorithm written in pseudocode may be found in Algorithm 1. Given a primitive substitution φ with a connection (u,v) of order k, Durand's algorithm simultaneously computes the return substitution $\varphi_{u,v}$ and the bijection $\theta_{u,v}\colon A_{u,v} \to \mathcal{R}_{u,v}$ satisfying $\theta_{u,v} \circ \varphi_{u,v} = \varphi^k \circ \theta_{u,v}$. In particular, it can also be used to compute the return set.

The first part of Algorithm 1 (lines 1-6) computes the value of $\theta_{u,v}(0)$. In the case at hand, we find that 001 is the leftmost return word in $1\xi^2(0) = 100100102$, so $\theta_{1,0}(0) = 001$. Carrying out the rest of the algorithm yields the following result (see Table 1 for details):

$$\theta_{1,0}\colon \begin{cases} 0 \mapsto 001,\ 1 \mapsto 02001,\ 2 \mapsto 02001301,\ 3 \mapsto 02320001, \\ 4 \mapsto 02001301320301,\ 5 \mapsto 02320301,\ 6 \mapsto 001320001; \end{cases}$$

$$\xi_{1,0}\colon \begin{cases} 0 \mapsto 00102,\ 1 \mapsto 00310102,\ 2 \mapsto 003101040002,\ 3 \mapsto 003561010102, \\ 4 \mapsto 00310104000461050002,\ 5 \mapsto 003561050002,\ 6 \mapsto 0010461010102. \end{cases}$$

We recall that ξ is primitive and unimodular (since it is invertible), hence it is aperiodic by Proposition 5.6. Therefore, Theorem 3.3 shows that $\xi_{1,0}$ defines an ω-presentation of $G(\xi)$. This ω-presentation has seven generators.

Step 2

We now compute $r_1(\xi_{1,0})$, which we recall is the restriction of $\xi_{1,0}$ to the subgroup $\mathrm{Im}(\xi_{1,0})$ of $F(A_7)$. First, we need to find a basis of $\mathrm{Im}(\xi_{1,0})$. To do this, it is convenient to recall some notions related with Stallings' algorithm. For a more exhaustive exposition of this topic, we point the reader to [48].

Let $\mathscr{A}$ be a non-deterministic automaton over the alphabet A with a distinguished state s_0, serving as both initial and final state. Let us also suppose that $\mathscr{A}$ is weakly connected. We allow $\mathscr{A}$ to also read words in $(A \cup A^{-1})^*$ in the natural way. More explicitly, if $a \in A$ acts partially on the states of $\mathscr{A}$ by $x \mapsto x \cdot a$, then we let a^{-1} act partially on the states of $\mathscr{A}$ by

$$x \cdot a^{-1} = \{y : x \in y \cdot a\}.$$

We say that $\mathscr{A}$ is *folded* if no two distinct transitions exist that share the same label as well as the same origin or terminus. When $\mathscr{A}$ is folded, it defines a subgroup $H_{\mathscr{A}}$ of $F(A)$ as follows: $x \in F(A)$ belongs to $H_{\mathscr{A}}$ if and only if the reduced word of $(A \cup A^{-1})^*$ representing x is accepted by $\mathscr{A}$ [48, Lemma 3.2]. Furthermore, we can obtain a basis for the subgroup $H_{\mathscr{A}}$ as follows. Let T be a spanning tree of $\mathscr{A}$. Given two states $x,y \in \mathscr{A}$, we denote by $[x,y]_T$ the unique path between x and y in T. Let T' be the set of transitions of $\mathscr{A}$ that do not belong to T. For each $e \in T'$, let b_e be the label of the path $[s_0,x]_T e[y,s_0]_T$, where x and y are respectively the origin and terminus of e. Then, the set $X_T = \{b_e : e \in T'\}$ is a basis of $H_{\mathscr{A}}$ [48, Lemma 6.1].

Let us use this to obtain a basis of $\mathrm{Im}(\xi_{1,0})$. First, note the two following equalities, which can be checked with direct computations:

$$\xi_{1,0}(6) = \xi_{1,0}(02^{-1}45^{-1}3), \quad \xi_{1,0}(4) = \xi_{1,0}(21^{-1}25^{-1}31^{-1}5).$$

It follows that $\mathrm{Im}(\xi_{1,0})$ is generated by $\xi_{1,0}(B)$, where $B = \{0,1,2,3,5\}$. Let

$$Y = \{0,\ 10^{-1},\ 1^{-1}2,\ 1^{-1}25^{-1}31^{-1}30^{-1},\ 03^{-1}52^{-1}1\}.$$

Data: A primitive substitution φ and a connection (u,v) of φ of order k.
Result: The ordering $\theta_{u,v}$ and the return substitution $\varphi_{u,v}$.

begin
 $w \leftarrow v$;
 repeat
  $w \leftarrow \varphi^k(w)$;
 until *uv occurs twice in uw*;
 let $\theta_{u,v}(0) =$ leftmost return word in uw;
 $i \leftarrow 1$; `// least undefined letter of` $\theta_{u,v}$
 $j \leftarrow 0$; `// least undefined letter of` $\varphi_{u,v}$
 while $j<i$ **do**
  foreach *return word r in* $u\varphi^k(\theta_{u,v}(j))v$ **do**
   if *r is not in* $\mathrm{Im}(\theta_{u,v})$ **then**
    let $\theta_{u,v}(i) = r$;
    $i \leftarrow i+1$;
   end if
  end foreach
  let $\varphi_{u,v}(j) = \theta_{u,v}^{-1}(\varphi^k(r))$;
  $j \leftarrow j+1$;
 end while
end

Algorithm 1 Durand's algorithm for computing return substitutions.

$\theta_{1,0}^{-1}(r)$	r	$1\xi^2(r)0$
0	001	1.001.001.02001.001.02001301.0
1	02001	1.001.001.02320001.02001.001.02001.001.02001301.0
2	02001301	1.001.001.02320001.02001.001.02001.001.02001301320301.001.001.001.02001301.0
3	02320001	1.001.001.02320001.02320301.001320001.02001.001.02001.001.02001.001.02001301.0
4	02001301320301	1.001.001.02320001.02001.001.02001.001.02001301320301.001.001.001.02001301320301.001320001.02001.001.02320301.001.001.001.02001301.0
5	02320301	1.001.001.02320001.02320301.001320001.02001.001.02320301.001.001.001.02001301.0
6	001320001	1.001.001.02001.001.02001301320301.001320001.02001.001.02001.001.02001.001.02001301.0

Table 1 Factorization of the words $1\xi^2(r)0$, $r \in \mathcal{R}_{1,0}$, used during the computation of the return substitution $\xi_{1,0}$.

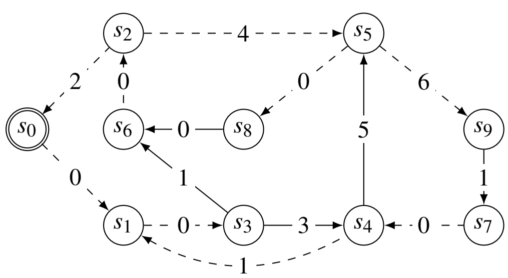


Fig. 2 An automaton over the alphabet A_7. The distinguished state is identified by a double circle and a spanning tree is highlighted with dashed edges.

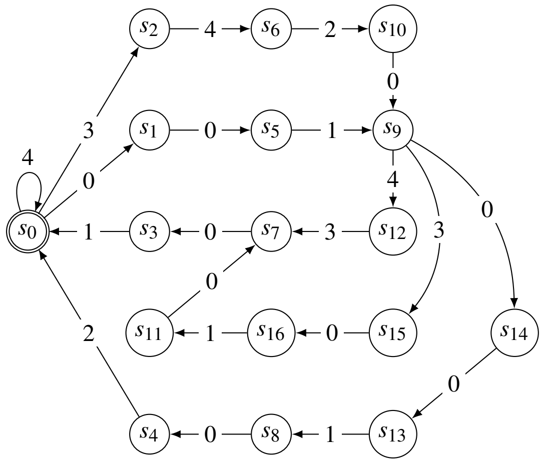


Fig. 3 An automaton over the alphabet A_5. The distinguished state is identified by a double circle.

It is not hard to see that Y generates $F(B)$ (it is even a basis of $F(B)$ since Y and B have the same number of elements). Therefore, $\mathrm{Im}(\xi_{1,0})$ is generated by the set

$$\xi_{1,0}(Y) = \{00102,\ 00310^{-1},\ 2^{-1}40002,\ 2^{-1}461010^{-1},\ 01^{-1}54^{-1}2\}.$$

Let $X = \xi_{1,0}(Y)$. We claim that X is a basis of $\mathrm{Im}(\xi_{1,0})$. Indeed, consider the automaton $\mathscr{A}$ over the alphabet A_7 presented in Fig. 2, where a spanning tree T is highlighted. A direct verification reveals that $\mathscr{A}$ is folded and that $X = X_T$, so X is a basis of $\mathrm{Im}(\xi_{1,0})$ by [48, Lemma 6.1]. The restriction $r_1(\xi_{1,0})$, written in the basis X ordered as above, is (see Table 2 for details):

$$r_1(\xi_{1,0})\colon 0 \mapsto 00100102,\ 1 \mapsto 0014301,\ 2 \mapsto 342000102,\ 3 \mapsto 3420301001,\ 4 \mapsto 4.$$

By Proposition 3.6, we conclude that $r_1(\xi_{1,0})$ defines an ω-presentation of $G(\xi)$. The incidence matrix of $r_1(\xi_{1,0})$, which has determinant 1, is given by

$$M(r_1(\xi_{1,0})) = \begin{pmatrix} 5&2&1&0&0\\ 3&2&0&1&1\\ 4&1&2&1&1\\ 4&2&1&2&1\\ 0&0&0&0&1 \end{pmatrix}.$$

Step 3

To conclude the proof of Theorem 6.1, it remains only to show that $r_1(\xi_{1,0})$ is not an automorphism of $F(A_5)$. Consider the automaton $\mathscr{A}$ over the alphabet A_5 presented in Fig. 3. A simple inspection of each of its 17 states shows that $\mathscr{A}$ is folded, hence it defines a proper subgroup $H_{\mathscr{A}}$ of $F(A_5)$. Moreover, the words $r_1(\xi_{1,0})(a)$ for $a \in A_5$ are all accepted by $\mathscr{A}$, hence $\mathrm{Im}(r_1(\xi_{1,0})) \leq H_{\mathscr{A}}$. Therefore, $\mathrm{Im}(r_1(\xi_{1,0}))$ is also a proper subgroup of $F(A_5)$ and $r_1(\xi_{1,0})$ is not an automorphism of $F(A_5)$.

Note, interestingly, that our counterexample ξ is not tame (in the sense of [23]). On the other hand, if an invertible substitution defines a dendric shift space, then it must be tame [23, Theorem 5.19]. But recall that the Schützenberger groups of dendric shift spaces are free [12, Theorem 6.5], hinting at the following question.

b	$\xi_{1,0}(b)$
00102	$00102.00102.00310^{-1}.00102.00102.00310^{-1}.00102.2^{-1}40002$
00310^{-1}	$00102.00102.00310^{-1}.01^{-1}54^{-1}2.2^{-1}461010^{-1}.00102.00310^{-1}$
$2^{-1}40002$	$2^{-1}461010^{-1}.01^{-1}54^{-1}2.2^{-1}40002.00102.00102.00102.00310^{-1}.00102.2^{-1}40002$
$2^{-1}461010^{-1}$	$2^{-1}461010^{-1}.01^{-1}54^{-1}2.2^{-1}40002.00102.2^{-1}461010^{-1}.00102.00310^{-1}.00102.00102.00310^{-1}$
$01^{-1}54^{-1}2$	$01^{-1}54^{-1}2$

Table 2 Factorization of the elements $\xi_{1,0}(b)$, $b \in X$, used to compute the restriction $r_1(\xi_{1,0})$.

Question 6.2. Is the Schützenberger group of a primitive, invertible and tame substitution a free profinite group?

Acknowledgements

I am indebted to Alfredo Costa for many helpful comments which greatly simplified Section 6 and overall made this paper much clearer. I also wish to thank Jorge Almeida for insightful discussions and for numerous suggestions, some of which led to more general results in Section 5. Finally, I would like to thank the referee for pointing out a more direct proof of Proposition 5.6 and for suggesting Question 6.2.

This work was conducted with the support of the Centre for Mathematics of the University of Coimbra (UIDB/00324/2020, funded by the Portuguese Government through FCT/MCTES) and the Centre for Mathematics of the University of Porto (UIDB/00144/2020, funded by the Portuguese Government through FCT/MCTES). I wish to also acknowledge the financial support of the Portuguese Government through a PhD grant (PD/BD/150350/2019).

Paper 2

Pronilpotent quotients associated with primitive substitutions

Journal of Algebra, 606 (2022) 341–370.

doi:10.1016/j.jalgebra.2022.05.021

Pronilpotent quotients associated with primitive substitutions

Herman Goulet-Ouellet

Received 12 April 2022
Accepted 17 May 2022
Communicated by V. Mazorchuk

Abstract. We describe the pronilpotent quotients of a class of projective profinite groups, that we call ω-presented groups, defined using a special type of presentations. The pronilpotent quotients of an ω-presented group are completely determined by a single polynomial, closely related with the characteristic polynomial of a matrix. We deduce that ω-presented groups are either perfect or admit the p-adic integers as quotients for cofinitely many primes. We also find necessary conditions for absolute and relative freeness of ω-presented groups. Our main motivation comes from semigroup theory: the maximal subgroups of free profinite monoids corresponding to primitive substitutions are ω-presented (a theorem due to Almeida and Costa). We are able to show that the composition matrix of a primitive substitution carries partial information on the pronilpotent quotients of the corresponding maximal subgroup. We apply this to deduce that the maximal subgroups corresponding to primitive aperiodic substitutions of constant length are not absolutely free.

Keywords. Profinite groups, Pseudovarieties of groups, Pronilpotent groups, Primitive substitutions, Schützenberger groups

Mathematics subject classification 2010. 20E18, 20F05, 37B10, 68R15

1 Introduction

In the early 2000s, Almeida established a connection between symbolic dynamics and free profinite monoids [5, 6, 8]. He showed that to each minimal shift space corresponds a maximal subgroup of a free profinite monoid, later named the *Schützenberger group* of the shift space. This group is obtained by taking the topological closure of the language of the shift space inside the corresponding free profinite monoid, and it defines an invariant of the shift space: two conjugate shift spaces have isomorphic Schützenberger groups [28] (as do, even, flow equivalent shift spaces [30]).

In 2013, Almeida and Costa showed how to obtain presentations for the Schützenberger groups corresponding to substitutive minimal shift spaces using return substitutions and ω-powers [11]. Using a similar process, every endomorphism of a free group of finite rank yields a presentation for some profinite group. Groups thus defined are called *ω-presented* and they are formally introduced in

Section 3.1. The main goal of this paper is to describe the pronilpotent quotients of ω-presented groups and apply this knowledge to study Schützenberger groups of primitive substitutions. In order to do this, we rely on several properties of maximal quotient functors which are presented in Section 2. Since ω-presented groups are projective (Section 3.1), their maximal pronilpotent quotients are products of free pro-p groups (Section 2.2). The ranks of these pro-p components are completely determined, in a very straightforward way, by a single polynomial: the reciprocal of the characteristic polynomial of the composition matrix of the free group endomorphism used in the ω-presentation (Section 3.2). In particular, for a given ω-presented group, all the information about its pronilpotent quotients is contained in this single polynomial.

Using all of this, we draw a number of conclusions. We show in Section 3.3 that these groups are either perfect, or have *prime-rich* Abelianizations, in the sense that they admit the p-adic integers as quotients for cofinitely many primes. In Section 3.4, we give necessary conditions for absolute and relative freeness of ω-presented groups (on this topic, other results may also be found in a recent paper by the author [45]). This may be viewed as a contribution toward a solution to a problem proposed in 2013 by Almeida and Costa [11, Problem 8.3].

In Section 4, we specialize these results to maximal subgroups of free profinite monoids corresponding to primitive substitutions. In this case, an ω-presentation can be obtained using a return substitution [11]. Our first observation is that these groups are neither perfect nor pro-p, partially answering a question of Zalesskii reported by Almeida and Costa [11]. Extending an idea of Durand (Section 4.3), we show that the structure of the pronilpotent quotients of the maximal subgroup corresponding to a primitive aperiodic substitution is partially reflected in the characteristic polynomial of the substitution itself (Section 4.4). The section culminates with one of our main results: the Schützenberger group of a primitive aperiodic substitution of constant length is not absolutely free (Theorem 4.12). We conclude with a series of examples that illustrate various aspects of our results (Section 4.5).

2 Maximal pronilpotent quotients

The aim of this section is to collect some general facts about maximal quotient functors, and more specifically about the pronilpotent one. We also recall along the way some definitions and set up some notation for the next sections. The first subsection is concerned with general properties of maximal quotient functors, while the second one focuses on the pronilpotent case.

2.1 Maximal quotient functors

By a *pseudovariety*, we mean a class of finite groups $\mathbf{H}$ closed under taking quotients and subgroups, and forming finite direct products. For the definition and basic properties of so-called *pro-*$\mathbf{H}$ *groups*, the reader may wish to consult Ribes and Zalesskii's book on the topic [67]. (Note that they use the term *variety* instead of *pseudovariety*.) Let

- $\mathbf{G}$ be the pseudovariety of all finite groups;
- $\mathbf{G}_p$ be the pseudovariety of finite p-groups (p a prime);
- $\mathbf{G}_{\mathrm{nil}}$ be the pseudovariety of finite nilpotent groups.

Pro-$\mathbf{H}$ groups are respectively called *profinite* when $\mathbf{H} = \mathbf{G}$, *pro-p* when $\mathbf{H} = \mathbf{G}_p$ or *pronilpotent* when $\mathbf{H} = \mathbf{G}_{\mathrm{nil}}$.

Given a profinite group G and a pseudovariety $\mathbf{H}$, we let $R_{\mathbf{H}}(G)$ be the intersection of all clopen normal subgroups $N \trianglelefteq G$ such that $G/N \in \mathbf{H}$. We further define $Q_{\mathbf{H}}(G) = G/R_{\mathbf{H}}(G)$, and we denote by $\mu_G^{\mathbf{H}} \colon G \to Q_{\mathbf{H}}(G)$ the corresponding canonical epimorphism, $\mu_G^{\mathbf{H}}(x) = xR_{\mathbf{H}}(G)$. Note that $Q_{\mathbf{H}}(G)$ is pro-$\mathbf{H}$: it is a subdirect product of the groups G/N, where N ranges over all clopen normal subgroups $N \trianglelefteq G$ such that $G/N \in \mathbf{H}$, and every subdirect product of pro-$\mathbf{H}$ groups is also pro-$\mathbf{H}$ [67, Proposition 2.2.1(c)].

Let $\mathsf{Pro}(\mathbf{H})$ be the category of pro-$\mathbf{H}$ groups equipped with continuous group homomorphisms, and consider the inclusion functor $I_{\mathbf{H}} \colon \mathsf{Pro}(\mathbf{H}) \to \mathsf{Pro}(\mathbf{G})$. The next result is standard, although not usually stated in those terms. We include a proof for the reader's convenience. For more details on adjunctions, we refer to Mac Lane's book [53, Chapter IV]. The reader will also find there the definition of universal arrows used in the proof below [53, Section III.1].

Proposition 2.1 (cf. [67, Lemma 3.4.1(a)])**.** *For every pseudovariety* $\mathbf{H}$*,* $Q_{\mathbf{H}}$ *is a functor which is a left adjoint of* $I_{\mathbf{H}}$*. Moreover,* $\mu^{\mathbf{H}}$ *is a natural transformation which is the unit of this adjunction.*

Proof. It suffices to show that for every profinite group G, the pair $(Q_{\mathbf{H}}(G), \mu_G^{\mathbf{H}})$ is a universal arrow from G to $I_{\mathbf{H}}$ [53, Section IV.1, Theorem 2].

Let H be a pro-$\mathbf{H}$ group and $\varphi \colon G \to H$ be a continuous group homomorphism. The set B of all clopen normal subgroups $N \trianglelefteq H$ such that $H/N \in \mathbf{H}$ forms a neighbourhood basis of the identity element of H [67, Theorem 2.1.3]. Hence, $\ker(\varphi)$ is the intersection $\bigcap_{N \in B} \varphi^{-1}(N)$ and $G/\varphi^{-1}(N) \cong H/N \in \mathbf{H}$. Thus, $R_{\mathbf{H}}(G) \subseteq \ker(\varphi)$ and by standard properties of quotients, the map $\bar{\varphi} \colon Q_{\mathbf{H}}(G) \to H$ defined by $\bar{\varphi}(xR_{\mathbf{H}}(G)) = \varphi(x)$ is a well-defined morphism of profinite groups. In particular, it satisfies $\bar{\varphi}\mu_G^{\mathbf{H}} = \varphi$, as required. $\square$

Note that $Q_{\mathbf{H}}$ acts on morphisms as follows: if $\varphi \colon G \to G'$ is a morphism of profinite groups, then $Q_{\mathbf{H}}(\varphi)$ is the unique morphism satisfying $Q_{\mathbf{H}}(\varphi)\mu_G^{\mathbf{H}} = \mu_{G'}^{\mathbf{H}}\varphi$. The group $Q_{\mathbf{H}}(G)$ is called the *maximal pro-*$\mathbf{H}$ *quotient* of G, and when $\mathbf{H} = \mathbf{G}_{\mathrm{nil}}$ or $\mathbf{G}_p$, the *maximal pronilpotent quotient* or *maximal pro-p quotient* of G. Moreover, we abbreviate $Q_{\mathbf{G}_{\mathrm{nil}}}$ by Q_{nil} and $Q_{\mathbf{G}_p}$ by Q_p.

Left adjoints are unique up to natural isomorphism [53, Section IV.1, Corollary 1]. We make use of this fact to establish the next lemma. The proof uses a characterization of pro-$\mathbf{H}$ groups which already appeared in the previous proof: a profinite group G is pro-$\mathbf{H}$ if and only if its identity element admits a neighbourhood basis consisting of clopen normal subgroups $N \trianglelefteq G$ such that $G/N \in \mathbf{H}$ [67, Theorem 2.1.3].

Lemma 2.2. *Let* $\mathbf{H}$ *and* $\mathbf{K}$ *be pseudovarieties. There is a natural isomorphism*

$$Q_{\mathbf{H}}Q_{\mathbf{K}} \cong Q_{\mathbf{H}\cap\mathbf{K}}.$$

Proof. Let $\mathbf{L} = \mathbf{H} \cap \mathbf{K}$. We claim that a profinite group G which is both pro-$\mathbf{H}$ and pro-$\mathbf{K}$ must also be pro-$\mathbf{L}$. Let B and B' be neighbourhood bases of the identity element of G consisting of clopen normal subgroups $N \trianglelefteq G$ satisfying respectively $G/N \in \mathbf{H}$ (for $N \in B$) and $G/N \in \mathbf{K}$ (for $N \in B'$). Given $N \in B$, there is $N' \in B'$ such that $N' \subseteq N$, hence G/N is a quotient of G/N'. In particular, $G/N \in \mathbf{L}$ which proves the claim.

By the previous paragraph, $Q_{\mathbf{H}}Q_{\mathbf{K}}$ is a functor $\mathsf{Pro}(\mathbf{G}) \to \mathsf{Pro}(\mathbf{L})$. By the uniqueness of left adjoints, it suffices to show that $Q_{\mathbf{H}}Q_{\mathbf{K}}$ is a left adjoint of $I_{\mathbf{L}}$, or equivalently that for every profinite group G, the pair $(Q_{\mathbf{H}}(K), \mu_K^{\mathbf{H}}\mu_G^{\mathbf{K}})$, where $K = Q_{\mathbf{K}}(G)$, is a universal arrow from G to $I_{\mathbf{L}}$ [53, Section IV.1, Theorem 2].

Let $\varphi\colon G \to H$ be a morphism of profinite groups, where H is pro-$\mathbf{H}$. The universal properties of $Q_{\mathbf{K}}(G)$ and $Q_{\mathbf{H}}(K)$ give morphisms $\varphi'\colon Q_{\mathbf{K}}(G) \to H$ and $\varphi''\colon Q_{\mathbf{H}}(K) \to H$ such that $\varphi'\mu_G^{\mathbf{K}} = \varphi$ and $\varphi''\mu_K^{\mathbf{H}} = \varphi'$, as in the diagram below.

$$\begin{tikzcd}
G \arrow[r, "\mu_G^{\mathbf{K}}"] \arrow[dr, "\varphi"'] & Q_{\mathbf{K}}(G) \arrow[r, equal] \arrow[d, dashed, "\varphi'"] & K \arrow[r, "\mu_K^{\mathbf{H}}"] \arrow[d, "\varphi'"'] & Q_{\mathbf{H}}(K) \arrow[dl, dashed, "\varphi''"] \\
& H \arrow[r, equal] & H &
\end{tikzcd}$$

Finally, we find that $\varphi''\mu_K^{\mathbf{H}}\mu_G^{\mathbf{K}} = \varphi'\mu_G^{\mathbf{K}} = \varphi$, as required. □

Let us denote by $\widehat{F}_{\mathbf{H}}(X,*)$ the free pro-$\mathbf{H}$ group over a pointed Stone space $(X,*)$. Free pro-$\mathbf{H}$ groups have the universal property determined by the fact that $\widehat{F}_{\mathbf{H}}$ is the left adjoint of $U_{\mathbf{H}}$, where $U_{\mathbf{H}}$ is the forgetful functor from the category of pro-$\mathbf{H}$ groups to that of pointed Stone spaces (with the identity element of a group acting as basepoint). See [67, Chapter 3] for more details. We abbreviate $\widehat{F}_{\mathbf{G}}$ by $\widehat{F}$, $\widehat{F}_{\mathbf{G}_{\mathrm{nil}}}$ by $\widehat{F}_{\mathrm{nil}}$, and $\widehat{F}_{\mathbf{G}_p}$ by $\widehat{F}_p$ for every prime p. Groups of the form $\widehat{F}(X,*)$, $\widehat{F}_p(X,*)$ and $\widehat{F}_{\mathrm{nil}}(X,*)$ are respectively called *free profinite groups*, *free pro-p groups* and *free pronilpotent groups*. Next is a slightly stronger version of a well-known result.

Lemma 2.3. *Let* $\mathbf{H}$ *and* $\mathbf{K}$ *be pseudovarieties. There is a natural isomorphism*

$$Q_{\mathbf{H}}\widehat{F}_{\mathbf{K}} \cong \widehat{F}_{\mathbf{H}\cap\mathbf{K}}.$$

Proof. The case $\mathbf{K} = \mathbf{G}$ is handled by [67, Proposition 3.4.2]. To deduce the general case, use the first case together with Lemma 2.2, as follows:

$$Q_{\mathbf{H}}\widehat{F}_{\mathbf{K}} \cong Q_{\mathbf{H}}Q_{\mathbf{K}}\widehat{F} \cong Q_{\mathbf{H}\cap\mathbf{K}}\widehat{F} \cong \widehat{F}_{\mathbf{H}\cap\mathbf{K}}.$$ □

2.2 Pronilpotent quotients of projective profinite groups

Recall that a profinite group G is projective when, for all profinite groups H and K, and all morphisms of profinite groups $\varphi\colon G \to H$ and $\psi\colon K \to H$, with ψ surjective, there exists a morphism $\varphi'\colon K \to H$ such that $\psi\varphi' = \varphi$.

$$\begin{tikzcd}
& G \arrow[dl, dashed, "\varphi'"'] \arrow[d, "\varphi"] \\
K \arrow[r, "\psi"] & H
\end{tikzcd}$$

Our main result for this section, Proposition 2.6 below, is a decomposition of the maximal pronilpotent quotient for projective profinite groups. Bearing in mind the properties of maximal quotient functors presented in Section 2.1, it is a mostly straightforward consequence of Tate's characterization of projective pro-p groups, which we now recall.

Let A be a set (possibly infinite) equipped with its discrete topology, and $\mathbf{H}$ be a pseudovariety. Consider the pointed Alexandroff extension $(A \cup \{*\}, *)$ of A. We stress that $A \cup \{*\}$ has an extra point even when A is finite, so the term *compactification* would be a misnomer. We write $\widehat{F}_{\mathbf{H}}(A)$ as a shorthand for $\widehat{F}_{\mathbf{H}}(A \cup \{*\}, *)$, the free pro-$\mathbf{H}$ group over the pointed Alexandroff extension of A. Groups of the form $F_{\mathbf{H}}(A)$ are sometimes known as *free pro-*$\mathbf{H}$ *groups on sets converging to 1*. Observe that if two sets A and B are in bijection, then $(A \cup \{*\}, *)$ and $(B \cup \{*\}, *)$ are homeomorphic. Hence, up to isomorphism, $\widehat{F}_{\mathbf{H}}(A)$ depends only on $\mathrm{Card}(A)$.

Let G be a profinite group and A be a set. Recall that a map $f\colon A \to G$ *converges to 1* when, for every clopen neighbourhood U of the identity element of G, the preimage $f^{-1}(U)$ contains all but finitely many elements of A. If G is a pro-$\mathbf{H}$ group, then the pro-$\mathbf{H}$ group morphisms $\widehat{F}_{\mathbf{H}}(A) \to G$ are in bijection with the maps $f\colon A \to G$ converging to 1. A result of Melnikov states that every free pro-$\mathbf{H}$ group is isomorphic to $\widehat{F}_{\mathbf{H}}(\mathfrak{m})$ for some cardinal $\mathfrak{m}$, called its *rank* [67, Proposition 3.5.12]. In particular, every profinite group G admits a map $A \to G$ converging to 1 for some set A, and we denote by $\mathrm{d}(G)$ the smallest cardinality of such a set. Here is a statement for Tate's theorem extracted from the proof found in Fried and Jarden's book [41, Proposition 22.7.6].

Theorem 2.4 (Tate)**.** *Let G be a projective pro-p group. Then, G is isomorphic to $\widehat{F}_p(\mathrm{d}(G))$, the free pro-$p$ group of rank* $\mathrm{d}(G)$.

Let G be a profinite group and p be a prime. A *p-Sylow subgroup* of G is a closed pro-p subgroup $H \leq G$ such that $[G : H]$ is coprime to p. (The definition of the index $[G : H]$ may be recalled in [67, Section 2.3]). It is well known that G is pronilpotent if and only if it has, for every prime p, a unique p-Sylow subgroup, which we denote G_p [67, Proposition 2.3.8]. Moreover, in that case, $G = \prod_p G_p$ where p ranges over all primes. In the next lemma, we record a simple observation which will prove useful in the sequel. Let us write R_p in place of $R_{\mathbf{G}_p}$ for every prime p (so $R_p(G)$ denotes the intersection of the clopen normal subgroups $N \trianglelefteq G$ such that $G/N \in \mathbf{G}_p$).

Lemma 2.5. *Let G be a pronilpotent group. For every prime p, the p-Sylow subgroup G_p is isomorphic to $Q_p(G)$. In particular, G is isomorphic to $\prod_p Q_p(G)$ where p ranges over all primes.*

Proof. Fix a prime p and let N be the kernel of the component projection $G \to G_p$. Since $G/N \cong G_p$ is pro-p, we have $R_p(G) \subseteq N$. Let $M \trianglelefteq G$ be a clopen normal subgroup such that G/M is a finite p-group. Then, $N/(N \cap M) \cong (MN)/M$ is a subgroup of G/M, hence it is also a finite p-group. Note however that $N \cong G/G_p$, so the order of N is coprime to p. Hence, $N/(N \cap M)$ is trivial and $N \subseteq M$. This shows that $N \subseteq R_p(G)$, finishing the proof. □

We now give our main result for this section. Let $\mathbf{Ab}_p$ be the pseudovariety of finite elementary Abelian p-groups. Given a profinite group G, we abbreviate $\mathrm{d}(Q_{\mathbf{Ab}_p}(G))$ by $\mathrm{d}_p(G)$.

Proposition 2.6. *For every projective profinite group G, we have*

$$Q_{\mathrm{nil}}(G) \cong \prod_p \widehat{F}_p(\mathrm{d}_p(G)),$$

where p ranges over all primes.

Proof. By Lemmas 2.2 and 2.5, we have that $Q_{\mathrm{nil}}(G)$ is isomorphic to the product $\prod_p Q_p(G)$ for p ranging over all primes. Fix a prime p and let H stand for $Q_p(G)$; it suffices to show that $H \cong \widehat{F}_p(\mathrm{d}_p(G))$. Since G is projective, so is H [41, Proposition 22.4.8]. By Tate's theorem (Theorem 2.4), it follows that $H \cong \widehat{F}_p(\mathrm{d}(H))$. On the one hand, we have $\mathrm{d}(H) = \mathrm{d}(Q_{\mathbf{Ab}_p}(H))$ [41, Lemma 22.7.4], while on the other hand, Lemma 2.2 implies that $Q_{\mathbf{Ab}_p}(H) \cong Q_{\mathbf{Ab}_p}(G)$, hence $\mathrm{d}(Q_{\mathbf{Ab}_p}(H)) = \mathrm{d}_p(G)$. $\square$

Remark 2.7. A further consequence of [41, Lemma 22.7.4] is that $Q_{\mathbf{Ab}_p}(G)$ and $(\mathbb{Z}/p\mathbb{Z})^{\mathrm{d}_p(G)}$ are isomorphic as elementary Abelian p-groups. If G is finitely generated, then $\mathrm{d}_p(G)$ is finite for every p and it also gives the dimension of $Q_{\mathbf{Ab}_p}(G)$ as a vector space over $\mathbb{Z}/p\mathbb{Z}$. This fails when $\mathrm{d}_p(G)$ is infinite [41, Remark 22.7.5].

The decomposition of the maximal pronilpotent quotient above leads to the characterization of pronilpotent quotients below. Let us say that a profinite group G is $\mathfrak{m}$-*generated*, for a cardinal $\mathfrak{m}$, if there is a map $\mathfrak{m} \to G$ converging to 1 whose image generates a dense subgroup of G.

Corollary 2.8. *Let G be a projective profinite group and H be a pronilpotent group. Then, H is a continuous homomorphic image of G if and only if for every prime p, the p-Sylow subgroup of H is $\mathrm{d}_p(G)$-generated.*

Proof. If $\psi\colon G \to H$ is a surjective morphism of profinite groups, then so is $Q_p(\psi)\colon Q_p(G) \to Q_p(H)$, for every prime p. By the proof of the previous proposition, $\mathrm{d}(Q_p(G)) = \mathrm{d}_p(G)$, while by Lemma 2.5, $Q_p(H)$ is isomorphic to the p-Sylow subgroup H_p, hence H_p is indeed $\mathrm{d}_p(G)$-generated.

On the other hand, assume that for every prime p, H_p is $\mathrm{d}_p(G)$-generated. Then, the proof of the previous proposition shows that $Q_p(G) \cong \widehat{F}(\mathrm{d}_p(G))$, hence there is a surjective morphism of profinite groups $\psi_p\colon Q_p(G) \to H_p$. Since H is the product of its Sylow subgroups, $\psi = \prod_p \psi_p$ gives a surjective morphism $\prod_p Q_p(G) \to H$. The result follows since $\prod_p Q_p(G) \cong Q_{\mathrm{nil}}(G)$ is itself a continuous homomorphic image of G. $\square$

3 ω-presented groups

In this section, we introduce ω-presented groups (Section 3.1) and give a formula for the dimensions of the vector spaces $Q_{\mathbf{Ab}_p}(G)$, where G is an ω-presented group (Section 3.2). We then proceed to deduce a number of things about the structure of ω-presented groups in Sections 3.3 and 3.4.

3.1 ω-presentations

Let A be a set and R be a subset of $\widehat{F}(A)$. Denote by $N(R)$ the closed normal subgroup of $\widehat{F}(A)$ generated by R. A *presentation* of a profinite group G is a pair (A,R) with A and R as above and $\widehat{F}(A)/N(R) \cong G$. We write $G \cong \langle A \mid R\rangle$. We call A the set of *generators* and R the set of *relators*.

Projective profinite groups are also characterized by a special kind of presentation (Proposition 3.2). This was first noticed by Lubotzky [51, Proposition 1.1] and later extended by Almeida and Costa to the setting of profinite semigroups [11, Proposition 2.4]. Both sources work with finitely generated objects, but for profinite groups, the characterization holds in full generality. We start with a lemma.

Lemma 3.1. *Let A be a set and ψ be a continuous endomorphism of $\widehat{F}(A)$. If ψ is idempotent, then* $\mathrm{Im}(\psi) \cong \langle A \mid \psi(a)a^{-1} : a \in A\rangle$.

Proof. Letting $R = \{\psi(a)a^{-1} : a \in A\}$, it is enough to show that $N(R) = \ker(\psi)$. It follows from the idempotence of ψ that $\ker(\psi) = \{\psi(x)x^{-1} : x \in \widehat{F}(A)\}$, hence $N(R) \subseteq \ker(\psi)$. Showing that the remaining inclusion holds amounts to establishing that $H = \{x \in \widehat{F}(A) : \psi(x)x^{-1} \in N(R)\}$ is the whole of $\widehat{F}(A)$. Equivalently, we have to show that H is a closed subgroup of $\widehat{F}(A)$ that contains A. That H is closed follows readily from the fact that so is $N(R)$, together with the continuity of ψ and basic properties of compact groups. That H contains A follows from its definition. Finally, for $x, y \in H$, we find that

$$\psi(x^{-1}y)(x^{-1}y)^{-1} = \psi(x^{-1})\psi(y)y^{-1}x = x^{-1}(\psi(x)x^{-1})^{-1}(\psi(y)y^{-1})x,$$

and since $N(R)$ is a normal subgroup of $\widehat{F}(A)$, we have $x^{-1}y \in H$. $\square$

Proposition 3.2. *Let A be a set of cardinality $\mathfrak{m}$ and G be an $\mathfrak{m}$-generated profinite group. Then, G is projective if and only if $G \cong \langle A \mid \psi(a)a^{-1} : a \in A\rangle$, where ψ is a continuous idempotent endomorphism of $\widehat{F}(A)$.*

Proof. Suppose that $G \cong \langle A \mid \psi(a)a^{-1} : a \in A\rangle$ for some continuous idempotent endomorphism ψ of $\widehat{F}(A)$. By the previous lemma, this means that $G \cong \mathrm{Im}(\psi)$, hence G is isomorphic to a closed subgroup of $\widehat{F}(A)$. Therefore, it must be projective [67, Lemma 7.6.3]. Conversely, assume that G is projective. Since G is A-generated, there is a surjective morphism of profinite groups $\alpha\colon \widehat{F}(A) \to G$. By projectivity, there is a morphism of profinite groups $\beta\colon G \to \widehat{F}(A)$ such that $\alpha\beta = id_G$. Let ψ be the composite $\beta\alpha$. Plainly, ψ is an idempotent endomorphism and $\ker(\psi) = \ker(\alpha)$. Hence, $G = \mathrm{Im}(\alpha) \cong \mathrm{Im}(\psi)$ and the previous lemma concludes the proof. $\square$

We now restrict our attention to an even more specialized form of presentation. First, recall that if G is a finitely generated profinite group, then $\mathrm{End}(G)$, the space of continuous endomorphisms of G equipped with composition and the pointwise topology, is a profinite monoid [47, Proposition 1]. In particular, for every endomorphism $\psi \in \mathrm{End}(G)$, the sequence $(\psi^n)_{n\geq 1}$ has a unique idempotent accumulation point given by $\psi^\omega = \lim_n \psi^{n!}$ [19, Proposition 3.7.2 and 3.9.2]. Given a finite set A, let $F(A)$ denote the free group over A and $\mathrm{End}(F(A))$ be the set of endomorphisms of $F(A)$. Viewing $F(A)$ as a subgroup of $\widehat{F}(A)$, it follows from the universal property of $\widehat{F}(A)$ that every $\varphi \in \mathrm{End}(F(A))$ admits a continuous extension $\widehat{\varphi} \in \mathrm{End}(\widehat{F}(A))$.

Definition 3.3 (ω-presented groups)**.** A profinite group G is called *ω-presented* when it admits a presentation of the form $G \cong \langle A \mid \widehat{\varphi}^\omega(a)a^{-1} : a \in A\rangle$, where A is a finite set and $\varphi \in \mathrm{End}(F(A))$. We then say that φ *defines an ω-presentation of G.*

We emphasize that ω-presented groups are finitely generated by definition. While it clearly follows from Proposition 3.2 above that every ω-presented group is projective, it does not hold that every projective profinite group is ω-presented. First, because not all projective profinite groups are finitely generated, as ω-presented groups must be. But second and perhaps more interestingly, no ω-presented group is a pro-p group (Section 3.3).

3.2 Dimension formula

Following Section 2.2, the maximal pronilpotent quotient of a projective profinite group G is completely determined by the cardinals $\mathrm{d}_p(G)$, which in the finitely generated case agree, for each prime p, with the dimension of $Q_{\mathbf{Ab}_p}(G)$ as a vector space over $\mathbb{Z}/p\mathbb{Z}$. Proposition 3.5 below gives a simple formula for these dimensions in case G is ω-presented, which we call the *dimension formula*.

Before stating this proposition, we need to set up some notation. Let φ be an endomorphism of $F(A)$, where A is a finite set. For every $a \in A$, let $|-|_a \colon F(A) \to \mathbb{Z}$ be the group homomorphism defined on $b \in A$ by $|b|_a = 1$ if $a = b$ and $|b|_a = 0$ otherwise. The *composition matrix* of φ is the $A \times A$ matrix over $\mathbb{Z}$ defined by

$$M_\varphi(a,b) = |\varphi(b)|_a, \quad a,b \in A.$$

Given a prime p, we denote by $M_{p,\varphi}$ the matrix over $\mathbb{Z}/p\mathbb{Z}$ obtained by reducing modulo p the coefficients of M_φ. We define the characteristic polynomial of a square matrix M by $\chi(x) = \det(x - M)$, with the convention that $\chi = 1$ when M is the empty matrix. We denote by χ_φ and $\chi_{p,\varphi}$ respectively the characteristic polynomial of M_φ and $M_{p,\varphi}$. Given a polynomial ξ of degree n, we let ξ^* be its *reciprocal polynomial*, defined by $\xi^*(x) = x^n \xi(x^{-1})$. We also call χ_φ and χ_φ^* the *characteristic polynomial* and *reciprocal characteristic polynomial* of φ. We record the following observations for future use.

Remark 3.4. Let $\mathbb{K}$ be an algebraically closed field and M be a square matrix over $\mathbb{K}$. Let χ be the characteristic polynomial of M. Recall that χ splits over $\mathbb{K}$ and that its roots are precisely the eigenvalues of M in $\mathbb{K}$. By Vieta's formulas, the degree of χ^* is the number of non-zero eigenvalues of M counted with multiplicity. Moreover, up to a sign, the leading coefficient of χ^* is the product, taken with multiplicities, of the non-zero eigenvalues of M. This quantity is sometimes known as the *pseudodeterminant* of M, and we denote it by $\operatorname{pdet}(M)$.

Proposition 3.5 (Dimension formula)**.** *Let $\varphi \in \operatorname{End}(F(A))$ define an ω-presentation of a profinite group G. The dimension of $Q_{\mathbf{Ab}_p}(G)$ over $\mathbb{Z}/p\mathbb{Z}$ is $\deg(\chi_{p,\varphi}^*)$.*

Proof. For convenience, we write $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. By Lemma 3.1, we have $G \cong \operatorname{Im}(\widehat{\varphi}^\omega)$, thus what we need is to compute the dimension of the image of $Q_{\mathbf{Ab}_p}(\widehat{\varphi})^\omega$. Note that $Q_{\mathbf{Ab}_p}(\widehat{\varphi})$ is a linear transformation of $\mathbb{F}_p^A$ which may be identified with the matrix $M_{p,\varphi}$. Moreover, $\operatorname{End}(\mathbb{F}_p^A)$ is a finite monoid, so $M_{p,\varphi}^\omega = M_{p,\varphi}^n$ for infinitely many positive integers n, and it follows that

$$\ker(M_{p,\varphi}^\omega) = \{x \in \mathbb{F}_p^A : \exists n \geq 1, M_{p,\varphi}^n(x) = 0\}.$$

But this is the generalized eigenspace of $M_{p,\varphi}$ of eigenvalue 0, which has dimension $\operatorname{mul}_0(\chi_{p,\varphi})$, the multiplicity of 0 as a root of $\chi_{p,\varphi}$ [74, Corollary 7.5.3(2)]. By the rank-nullity theorem,

$$\dim(\operatorname{Im}(M_{p,\varphi}^\omega)) = \deg(\chi_{p,\varphi}) - \operatorname{mul}_0(\chi_{p,\varphi}) = \deg(\chi_{p,\varphi}^*). \qquad \square$$

In light of Section 2.2, we then have the following.

Theorem 3.6. *If $\varphi \in \operatorname{End}(F(A))$ defines an ω-presentation of a profinite group G, then $Q_{\mathrm{nil}}(G) \cong \prod_p \widehat{F}_p(\deg(\chi_{p,\varphi}^*))$. Moreover, a pronilpotent group H is a continuous homomorphic image of G if and only if for every prime p, the p-Sylow subgroup of H is $\deg(\chi_{p,\varphi}^*)$-generated.*

Proof. By Proposition 2.6, the first part follows if we show that $\mathrm{d}_p(G) = \deg(\chi_{p,\varphi}^*)$ for every prime p. Since G is finitely generated, $\mathrm{d}_p(G)$ is the dimension of $Q_{\mathbf{Ab}_p}(G)$ over $\mathbb{Z}/p\mathbb{Z}$ (Remark 2.7), which is indeed $\deg(\chi_{p,\varphi}^*)$ by the dimension formula. The second part is proved in a similar way, using Corollary 2.8. $\square$

3.3 Perfect ω-presented groups

We now characterize perfect ω-presented groups and describe what happens otherwise. We deduce that ω-presented groups are never pro-p, and this includes the maximal subgroups of free profinite monoids defined by primitive substitutions (the topic of Section 4). The material in this section partially answers a question of Zalesskii reported in [11, Section 8]: can free pro-p groups be realized as maximal subgroups of free profinite monoids? The answer is negative at least for the maximal subgroups corresponding to primitive substitutions (as we shall see in Corollary 4.2). At time of writing, the question remains open for arbitrary minimal shift spaces.

Let us start with a characterization. By a *perfect profinite group*, we mean a profinite group G whose commutator subgroup is dense in G. Equivalently, the maximal pro-Abelian quotient of G is trivial. This extends the usual notion of perfect finite group.

Proposition 3.7. *Let φ define an ω-presentation of a profinite group G. Then, G is perfect if and only if M_φ is nilpotent, i.e. $M_\varphi^n = 0$ for some $n \geq 1$.*

Proof. Note that non-trivial pronilpotent groups are not perfect (they are prosolvable), hence G is perfect if and only if its maximal pronilpotent quotient is trivial. Then, by Theorem 3.6, G is perfect if and only if $\deg(\chi^*_{p,\varphi}) = 0$ for all primes. However, for cofinitely many primes, $\deg(\chi^*_{p,\varphi}) = \deg(\chi^*_\varphi)$. The latter is zero if and only if $\chi_\varphi(x) = x^n$, and this is equivalent to M_φ being nilpotent by the Cayley–Hamilton theorem. □

We deduce immediately the following result.

Corollary 3.8. *If G is ω-presented, then either G is a perfect profinite group, or the group $\mathbb{Z}_p$ of p-adic integers is a continuous homomorphic image of G for cofinitely many primes p. In particular, non-trivial pro-p groups are not ω-presented.*

Proof. If G is not perfect, then M_φ is not nilpotent and $\deg(\chi^*_\varphi) > 0$. As previously noted, $\deg(\chi^*_\varphi) = \deg(\chi^*_{p,\varphi})$ for cofinitely many primes p. But by Theorem 3.6, the product $\mathbb{Z}_p^n$ where $n = \deg(\chi^*_{p,\varphi})$ is the Abelianization of $Q_p(G)$, hence it is a continuous homomorphic image of G. The last part follows by recalling that non-trivial prosolvable groups are not perfect. □

Both alternatives occur in a non-trivial way. In Section 3.5, we exhibit a non-trivial perfect ω-presented group. As for the other alternative, plenty of non-trivial examples are found among maximal subgroups of free profinite monoids (Section 4).

3.4 Freeness

We give necessary conditions for absolute and relative freeness of ω-presented groups. These results partially address [11, Problem 8.3].

Let $\mathbf{H}$ be a pseudovariety. We say that a profinite group is *free with respect to* $\mathbf{H}$ if it is isomorphic to $\widehat{F}_{\mathbf{H}}(A)$ for some set A. A profinite group is called *relatively free* if it is free with respect to some pseudovariety $\mathbf{H}$, and *absolutely free* if moreover $\mathbf{H} = \mathbf{G}$, the pseudovariety of all finite groups. The next proposition characterizes relative freeness of maximal pronilpotent quotients of ω-presented groups. Let π be a set of primes. We let $\mathbf{G}_{\mathrm{nil},\pi}$ be the pseudovariety of finite nilpotent groups whose p-Sylow subgroups are trivial for all primes $p \notin \pi$.

Proposition 3.9. *Let $\varphi \in \mathrm{End}(F(A))$ define an ω-presentation of a profinite group G. Let π be the set of all primes p such that $\deg(\chi^*_{p,\varphi}) \neq 0$. Then, the following are equivalent.*

(1) $Q_{\mathrm{nil}}(G)$ is relatively free.
(2) For every prime p, $\deg(\chi^*_{p,\varphi})$ equals $\deg(\chi^*_{\varphi})$ or 0.
(3) $Q_{\mathrm{nil}}(G)$ is free with respect to the pseudovariety $\mathbf{G}_{\mathrm{nil},\pi}$.

In particular, $Q_{\mathrm{nil}}(G)$ is a free pronilpotent group if and only if the pseudodeterminant of M_φ is ± 1.

Proof. *(1) implies (2).* Suppose that $Q_{\mathrm{nil}}(G)$ is free with respect to a pseudovariety $\mathbf{H}$, say $Q_{\mathrm{nil}}(G) = \widehat{F}_{\mathbf{H}}(A)$ where A is a finite set of cardinality n. The case $n = 0$ is trivial: the only substitution on the empty alphabet has an empty composition matrix, so then $\chi^*_\varphi = 1$ and (2) holds trivially. We may assume from now on that $n > 0$. Fix a prime $p \in \pi$ and let $k = \deg(\chi^*_{p,\varphi})$. Theorem 3.6 implies that $\widehat{F}_p(k)$ is a continuous homomorphic image of G, hence so is $(\mathbb{Z}/p\mathbb{Z})^k$. Since $p \in \pi$, we have $k > 0$, hence $\mathbb{Z}/p\mathbb{Z} \in \mathbf{H}$ and $\mathbf{Ab}_p \subseteq \mathbf{H}$. It follows from Lemma 2.3 that $Q_{\mathbf{Ab}_p}(G) \cong (\mathbb{Z}/q\mathbb{Z})^n$. In particular, n is the dimension of $Q_{\mathbf{Ab}_p}(G)$ over $\mathbb{Z}/p\mathbb{Z}$, so the dimension formula (Proposition 3.5) implies that $n = k$. But recall that $\deg(\chi^*_{p,\varphi}) = \deg(\chi^*_\varphi)$ for all sufficiently large $p \in \pi$, hence $n = \deg(\chi^*_\varphi)$ and the result follows.

(2) implies (3). Writing $d = \deg(\chi^*_\varphi)$, we have by assumption $\deg(\chi^*_{p,\varphi}) = 0$ whenever $p \notin \pi$ and $\deg(\chi^*_{p,\varphi}) = d$ otherwise. Applying Theorem 3.6 then gives

$$Q_{\mathrm{nil}}(G) \cong \prod_p \widehat{F}_p(\deg(\chi^*_{p,\varphi})) \cong \prod_{p\in\pi} \widehat{F}_p(d),$$

which is indeed the free pro-$\mathbf{G}_{\mathrm{nil},\pi}$ group of rank d (e.g. by Lemmas 2.3 and 2.5).

That (3) implies (1) is trivial, so it remains only to prove the last part of the statement. Recall that the leading coefficient of χ^*_φ is equal, up to a sign, to the pseudodeterminant of M_φ (Remark 3.4). Thus, if $\mathrm{pdet}(M_\varphi) = \pm 1$, then (2) is satisfied, π is the set of all primes and by (3), $Q_{\mathrm{nil}}(G)$ is free pronilpotent. Conversely, suppose that $Q_{\mathrm{nil}}(G)$ is free pronilpotent and that moreover there is a prime p that divides $\mathrm{pdet}(M_\varphi)$. In particular, $\deg(\chi^*_{p,\varphi}) < \deg(\chi^*_\varphi)$ and $Q_{\mathrm{nil}}(G)$ is non-trivial. Since $Q_{\mathrm{nil}}(G)$ is relatively free, (2) must hold, thus $\deg(\chi^*_{p,\varphi}) = 0$. But then, (3) implies that the p-Sylow subgroup of $Q_{\mathrm{nil}}(G)$ is trivial, contradicting the fact that $Q_{\mathrm{nil}}(G)$ is a non-trivial free pronilpotent group. □

We proceed to deduce necessary conditions for an ω-presented group to be relatively or absolutely free. We think of these two results as quick tests for relative and absolute freeness. The second one extends a recent result of the author [45, Corollary 4.7].

Corollary 3.10. *Let φ define an ω-presentation of a profinite group G. If there is a prime p such that $0 < \deg(\chi^*_{p,\varphi}) < \deg(\chi^*_\varphi)$, then G is not relatively free.*

Proof. If G is relatively free, then so is $Q_{\mathrm{nil}}(G)$ by Lemma 2.3. But the assumption that $0 < \deg(\chi^*_{p,\varphi}) < \deg(\chi^*_\varphi)$ contradicts (2) from Proposition 3.9. □

Corollary 3.11. *Let φ define an ω-presentation of a profinite group G. If $\mathrm{pdet}(M_\varphi)$ is not ± 1, then G is not absolutely free.*

Proof. We prove the contrapositive. If G is absolutely free, then it follows from Lemma 2.3 that $Q_{\mathrm{nil}}(G)$ is a free pronilpotent group, hence $\mathrm{pdet}(M_\varphi) = \pm 1$ by the last part of Proposition 3.9. □

3.5 A perfect example

We conclude this section with an example of a perfect ω-presented group. Consider the following endomorphism of the free group $F(\{0,1\})$:

$$\psi\colon 0 \mapsto 010^{-1}1^{-1},\ 1 \mapsto 0.$$

Let $P = \mathrm{Im}(\widehat{\psi}^{\omega})$ be the corresponding ω-presented group. Plainly, M_ψ is nilpotent, so Proposition 3.7 ensures that P is perfect. We now show that P is non-trivial.

Consider a finite set A and a finite group H. Let $\mathrm{End}(\widehat{F}(A))$ act on the right of H^A as follows: an element $t \in H^A$, viewed as a map $t\colon A \to H$, naturally corresponds to a morphism of profinite groups $\widehat{t}\colon \widehat{F}(A) \to H$. For $\varphi \in \mathrm{End}(\widehat{F}(A))$, define

$$t^{\varphi} = (\widehat{t} \circ \varphi)|_A.$$

This gives a continuous right monoid action of $\mathrm{End}(\widehat{F}(A))$ on H^A [11, Lemma 3.1]. Moreover, H is a continuous homomorphic image of $\mathrm{Im}(\varphi^{\omega})$ if and only if there exists $t \in H^A$ and $k \geq 1$ such that $\{t(a) : a \in A\}$ generates H and $t^{\varphi^k} = t$ [11, Proposition 3.2]. Let $\mathbb{F}_4$ be the field with 4 elements. We consider below the special linear group $\mathrm{SL}_2(\mathbb{F}_4)$, which is isomorphic to the alternating group A_5.

Proposition 3.12. $\mathrm{SL}_2(\mathbb{F}_4)$ *is a continuous homomorphic image of* P.

Proof. Let g be a generator of the multiplicative group $\mathbb{F}_4^{\times}$, and consider the following 2×2 matrices over $\mathbb{F}_4$:

$$u = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \quad v = \begin{pmatrix} 0 & 1 \\ 1 & g \end{pmatrix}.$$

One checks, via explicit computations, that

$$(u,v)^{\psi^2} = (wuw^{-1}, wvw^{-1}),\ \text{where } w = \begin{pmatrix} g & 1 \\ 0 & 1 \end{pmatrix}.$$

It follows that $(u,v)^{\psi^{2k}} = (u,v)$, where k is the order of the matrix w in $\mathrm{GL}_2(\mathbb{F}_4)$, the general linear group of dimension 2 over $\mathbb{F}_4$. Let H be the subgroup of $\mathrm{SL}_2(\mathbb{F}_4)$ generated by $\{u,v\}$. By the aforementioned result [11, Proposition 3.2], it follows that H is a continuous homomorphic image of P. As P is perfect, so is H. But then H is a non-trivial perfect subgroup of $\mathrm{SL}_2(\mathbb{F}_4)$, and since the latter is the smallest non-trivial perfect group, we conclude that $H = \mathrm{SL}_2(\mathbb{F}_4)$. □

Question 3.13. We wonder whether the above argument can be generalized to show that $\mathrm{SL}_2(\mathbb{F}_{2^n})$ is a continuous homomorphic image of P for every $n \geq 2$, where $\mathbb{F}_{2^n}$ is the field with 2^n elements.

Using GAP and SageMath [42, 68], we were able to verify that the answer is positive for $2 \leq n \leq 12$. Our computations involved matrices u, v similar to the ones given above, with g a generator of the multiplicative group $\mathbb{F}_{2^n}^{\times}$.

Remark 3.14. Let us say that an endomorphism of $F(A)$ is *positive* when it restricts to an endomorphism of the free monoid A^*, which is viewed as a submonoid of $F(A)$ in the usual way. We observe that for a positive endomorphism φ, the matrix M_φ is nilpotent exactly when $\mathrm{Im}(\varphi^n)$ is trivial for all sufficiently large $n \in \mathbb{N}$. This, in turn, forces the corresponding ω-presented group to be trivial. In particular, by Proposition 3.7, non-trivial examples of perfect ω-presented groups cannot be obtained using positive endomorphisms.

4 Maximal subgroups of free profinite monoids

We further study examples of ω-presented groups arising from Almeida's correspondence between shift spaces and maximal subgroups of free profinite monoids (recalled in Section 4.1). We will focus on such maximal subgroups corresponding to primitive aperiodic substitutions. These groups are projective profinite groups by the main result of [64], and are in fact ω-presented by the main result of [11]. This last result is of particular interest to us, so additional details are given in Section 4.2. In Section 4.3, we revisit a result of Durand about eigenvalues of return substitutions. (By an eigenvalue of a substitution, we simply mean an eigenvalue of its composition matrix.) In Section 4.4, using this result, we relate more directly the characteristic polynomial of a primitive aperiodic substitution with the pronilpotent quotients of its Schützenberger group. We proceed to deduce specialized forms of the freeness tests of Section 3.4 and finally that the ω-presented groups corresponding to primitive aperiodic substitutions of constant length cannot be free (Theorem 4.12, our main result of this section). We finish, in Section 4.5, with a series of examples.

4.1 Almeida's correspondence

We give a brief account of Almeida's correspondence, which associates to each minimal shift space a maximal subgroup in a free profinite monoid. For a more collected presentation of the topic, see Almeida et al.'s recent monograph [19]. Given a finite discrete set A, consider the space $A^{\mathbb{Z}}$ equipped with the product topology. The map $\sigma\colon A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ defined by $\sigma(x)_n = x_{n+1}$ defines a self-homeomorphism of $A^{\mathbb{Z}}$ called the *shift map*. A *shift space* is a closed, non-empty subset $X \subseteq A^{\mathbb{Z}}$ satisfying $\sigma(X) = X$. Define the *language of a shift space* X to be the subset $L(X)$ of the free monoid A^* formed by all words appearing as finite, contiguous subsequences in the elements $x \in X$. A shift space is called *minimal* if it contains no shift space besides itself. It is well-known that a shift space is minimal if and only if $L(X)$ is uniformly recurrent: this is essentially [19, Proposition 5.2.3]. (The definition of uniform recurrence may recalled e.g. in [19, p.140].)

Almeida showed in [8] that if X is a minimal shift space, then the topological closure of $L(X)$ in the free profinite monoid $\widehat{A^*}$ intersects $\widehat{A^*} \setminus A^*$ in a regular $\mathcal{J}$-class. By standard semigroup theory, this $\mathcal{J}$-class contains maximal subgroups of $\widehat{A^*}$ that are (continuously) isomorphic to one another. We may think of these maximal subgroups as one single group, sometimes known as the *Schützenberger group of* X. We say that a minimal shift space is *periodic* if it is finite, or equivalently if its points have finite orbit under the shift map σ. Otherwise, by minimality, all points of X have infinite orbit under σ and we say that X is *aperiodic*. If X is periodic, then its Schützenberger group is easily described: it is simply a free profinite group of rank 1 [14, Theorem 7.5]. Hence, we restrict our attention to the aperiodic case.

Let now φ be a primitive substitution over a finite alphabet A. That is, φ is an endomorphism of A^* whose composition matrix M_φ is a primitive matrix. Equivalently, there is $n \in \mathbb{N}$ such that, for all $a, b \in A$, the letter b occurs in $\varphi^n(a)$. Such a substitution defines a shift space $X_\varphi \subseteq A^{\mathbb{Z}}$, whose language consists of all factors of the words $\varphi^n(a)$ for $n \geq 1$, $a \in A$ (see [19, Section 5.5]). Going forward, we denote the language of X_φ by $L(\varphi)$. Note that this language is uniformly recurrent (a proof may be found in [19, Proposition 5.5.4]), hence X_φ is minimal. We say that φ is *aperiodic* if X_φ is aperiodic in the above sense; otherwise, we say that φ is *periodic*. We denote the Schützenberger group of X_φ by $G(\varphi)$ and by extension, we call it the *Schützenberger group of* φ.

4.2 Return substitutions

Return substitutions are one of the key tools for studying Schützenberger groups of primitive substitutions: they were used in [11] to obtain ω-presentations for these groups. We give below the precise statement and reference for this result. But before, let us briefly recall what are return substitutions. Further details may be found for instance in [38, 39].

Let φ be a primitive substitution over a finite alphabet A. A pair of non-empty words (u,v) is called a *connection* of φ when $uv \in L(\varphi)$ and there exists $n \geq 1$ such that $\varphi^n(u) \in A^*u$ and $\varphi^n(v) \in vA^*$. The least such n is known as the *order* of the connection. Consider the *return set* $\mathcal{R}_{u,v}$, consisting of all words $r \in A^*$ such that $urv \in L(\varphi)$ and urv starts and ends with consecutive occurrences of uv. Such a word is called a *return word* to (u,v). Recall that, by primitivity of φ, the language $L(\varphi)$ is uniformly recurrent. Hence, every long enough word in $L(\varphi)$ has an occurrence of uv, and the return set $\mathcal{R}_{u,v}$ must be finite.

For convenience, we adopt a consistent ordering for return sets. By uniform recurrence of $L(\varphi)$, there exists $l \in \mathbb{N}$ such that for all $r \in \mathcal{R}_{u,v}$, urv occurs in $u\varphi^{nl}(v)$, where n is the order of (u,v). We order $\mathcal{R}_{u,v}$ according to the leftmost occurrence of each urv in $u\varphi^{nl}(v)$. Letting $A_{u,v} = \{0,\dots,\mathrm{Card}(\mathcal{R}_{u,v})-1\}$, this ordering induces a monoid homomorphism $\theta_{u,v} \colon A_{u,v}^* \to A^*$, which moreover does not depend on l. Note that $\mathcal{R}_{u,v}$ is the basis of a free submonoid of A^* [39, Lemma 17], so $\theta_{u,v}$ is injective. If $r \in \mathcal{R}_{u,v}$, then $u\varphi^n(r)v$ starts and ends with uv and it follows that $\varphi^n(r)$ is uniquely a concatenation of elements of $\mathcal{R}_{u,v}$. In particular, we may define a substitution $\varphi_{u,v}$ of $A_{u,v}^*$ by $\varphi^n\theta_{u,v} = \theta_{u,v}\varphi_{u,v}$. We call $\varphi_{u,v}$ the *return substitution* of φ with respect to (u,v). It is again a primitive substitution [39, Lemma 21].

We now recall a key result of Almeida and Costa implying that Schützenberger groups of primitive substitutions are ω-presented. We stress that this is only valid for aperiodic substitutions. We also warn the reader that the original statement of the result is restricted to connections (u,v) satisfying $|u| = |v| = 1$, but this assumption is in fact never used in the proof. Relaxing this assumption can be convenient because it may happen that longer connections have less return words (e.g. the substitution $\varphi\colon 0 \mapsto 01,\ 1 \mapsto 21,\ 1 \mapsto 20$).

Theorem 4.1 ([11, Theorem 6.2])**.** *Let φ be a primitive aperiodic substitution and (u,v) be a connection of φ. Then, $\varphi_{u,v}$, viewed as an endomorphism of $F(A_{u,v})$, defines an ω-presentation of $G(\varphi)$, that is*

$$G(\varphi) \cong \langle A_{u,v} \mid \widehat{\varphi_{u,v}}^{\omega}(a)a^{-1} : a \in A_{u,v} \rangle.$$

Since all primitive substitutions have at least one connection (see [19, Proposition 5.5.10]), Schützenberger groups of primitive aperiodic substitutions are indeed ω-presented. We further deduce the following.

Corollary 4.2. *Schützenberger groups of primitive substitutions are neither perfect nor pro-p.*

Proof. Let φ be a primitive substitution. If φ is periodic, then the result is an easy consequence of [14, Theorem 7.5]. From now on, we assume that φ is aperiodic. By Theorem 4.1, the group $G(\varphi)$ is ω-presented, hence it cannot be pro-p (Corollary 3.8). Moreover, note that the ω-presentation given by Theorem 4.1 is defined by an endomorphism with a primitive composition matrix. Of course, primitive matrices are never nilpotent. In light of Proposition 3.7, $G(\varphi)$ cannot be perfect. $\square$

Remark 4.3. Let $\varphi\colon A^* \to A^*$ be a primitive aperiodic substitution. It is called *proper* when for some $a,b \in A$ and $k \geq 1$, $\varphi^k(c) \in aA^* \cap A^*b$ for all $c \in A$. In the proper case, there is a simpler version of the above theorem, which is sometimes more convenient: φ itself defines an ω-presentation of $G(\varphi)$ [11, Theorem 6.4].

In any case, return substitutions may be effectively computed, for instance using the algorithm described in [37, p.205], and as a result, the pronilpotent quotients of Schützenberger groups of primitive substitutions are quite transparent. Indeed, by Theorems 3.6 and 4.1, all is needed is a quick look at the reciprocal characteristic polynomial of any return substitution. However, computing return substitutions can be very tedious, as the example below shows. This motivates the results of Section 4.3.

Example 4.4. Consider the following primitive substitution

$$\varphi\colon 0 \mapsto 12,\ 1 \mapsto 22,\ 2 \mapsto 33,\ 3 \mapsto 00.$$

The pair of 1-letter words $(2,3)$ is a connection of φ of order 12. The set $\mathcal{R}_{2,3}$ contains 12 return words with length ranging from 4 to 274. The return substitution $\varphi_{2,3}$ is thus defined on a 12-letter alphabet, and it is truly unwieldy: the images of the letters under $\varphi_{2,3}$ have lengths ranging from 821 to 97913. The other connections, which also have order 12, appear to give return substitutions that are comparable or even worse.

4.3 Characteristic polynomials of return substitutions

Thankfully, we may relate, for a primitive substitution φ with a connection (u,v) of order n, the two polynomials χ_{φ^n} and $\chi_{\varphi_{u,v}}$, and in turn the reciprocal polynomials $\chi^*_{\varphi^n}$ and $\chi^*_{\varphi_{u,v}}$. In [36, Proposition 9], Durand shows that (up to taking a power) a primitive substitution has the same eigenvalues as its one-sided return substitutions, except possibly for 0 and roots of 1. The main result of this subsection, Proposition 4.6, is slightly sharper, as it implies that the multiplicities must also be the same (again, except for 0 and roots of 1). We start with a technical lemma, also due to Durand. The lemma is outlined in the discussion preceding [36, Proposition 9]. Since Durand's version of this lemma is stated for *one-sided* return substitutions, we include a proof.

Let w,z be two words. An *occurrence* of z in w is an integer $i \geq 0$ such that $w = xzy$ and $|x| = i$. The number of occurrences of z in w is denoted $|w|_z$. (Note that there is no conflict with the similar-looking notation introduced in Section 3.2.) We also need to define composition matrices for homomorphisms between free monoids over possibly different alphabets, which is done as follows. If $\varphi\colon B^* \to A^*$ is a semigroup homomorphism where A and B are finite sets, then we let M_φ be the $A \times B$ matrix defined by

$$M_\varphi(a,b) = |\varphi(b)|_a, \quad a \in A, b \in B.$$

Note that the formation of composition matrices is compatible with composition, in the sense that $M_{\varphi\psi} = M_\varphi M_\psi$ whenever φ and ψ are composable homomorphisms.

Lemma 4.5. *Let $\varphi\colon A^* \to A^*$ be a primitive substitution and (u,v) be a connection of φ of order n. Then, there is a sequence of matrices $(K_l)_{l\in\mathbb{N}}$ with integer coefficients making the following sets finite:*

$$\{M^l_{\varphi^n} - M_{\theta_{u,v}}K_l : l \in \mathbb{N}\}, \quad \{M^l_{\varphi_{u,v}} - K_l M_{\theta_{u,v}} : l \in \mathbb{N}\}.$$

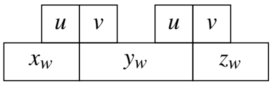


Fig. 1 Factorization of w used to define the map f in the proof of Lemma 4.5. The occurrences of uv represented above are the first and last of w. They might overlap and even coincide.

Proof. For simplicity, we replace φ by φ^n and assume that $n = 1$. We define a map $f\colon L(\varphi) \to L(\varphi_{u,v})$ as follows. If $w \in L(\varphi)$ has an occurrence of uv, then it has a factorization $w = x_w y_w z_w$ satisfying (and defined by) the following conditions:

$$\begin{cases} x_w \in A^*u, \\ x_w y_w \in A^*u, \\ |x_w v|_{uv} = 1, \end{cases} \qquad \begin{cases} z_w \in vA^*, \\ y_w z_w \in vA^*, \\ |uz_w|_{uv} = 1. \end{cases}$$

These conditions are depicted in Fig. 1. In this case, y_w is a concatenation of elements of $\mathcal{R}_{u,v}$ and we let $f(w) = \theta_{u,v}^{-1}(y_w)$, which is well-defined by injectivity of $\theta_{u,v}$ [39, Lemma 17]. Otherwise, let $f(w) = \varepsilon$, the empty word. The lemma is proved in 3 steps.

Step 1. Let us write

$$C_1 = \max\{|r| : r \in \mathcal{R}_{u,v}\}, \quad C_2 = \min\{|r| : r \in \mathcal{R}_{u,v}\}.$$

We claim that, for every $w \in L(\varphi)$ and $b \in A$,

$$0 \leq |w|_b - |\theta_{u,v} f(w)|_b \leq |w| - |\theta_{u,v} f(w)| \leq 2C_1 + |uv|. \tag{1}$$

If w has no occurrence of uv, then the claim holds trivially. If w has an occurrence of uv, then $|w| - |\theta_{u,v} f(w)| = |x_w| + |z_w|$ and the rightmost inequality of the claim follows from the upper bounds

$$|x_w| \leq C_1 + |u|; \quad |z_w| \leq C_1 + |v|. \tag{2}$$

To prove, say, the upper bound for $|x_w|$, note that $x_w v$ is a suffix of urv for some $r \in \mathcal{R}_{u,v}$, hence $|x_w| \leq |ur| \leq C_1 + |u|$. The upper bound for $|z_w|$ is obtained similarly. The two remaining inequalities of the claim are straightforward.

Step 2. Let $s \in L(\varphi_{u,v})$ and fix a factorization

$$\theta_{u,v}(s) = w_1 \dots w_k.$$

Assume further that each w_i has at least one occurrence of uv, that is $|w_i|_{uv} \geq 1$. We claim that, for every letter $c \in A_{u,v}$,

$$0 \leq |s|_c - \sum_{i=1}^{k} |f(w_i)|_c \leq |s| - \sum_{i=1}^{k} |f(w_i)| \leq \frac{k(2C_1 + |uv|)}{C_2}. \tag{3}$$

By assumption, we have for every $i = 1, \dots, k$ a factorization

$$w_i = x_{w_i} y_{w_i} z_{w_i},$$

as described at the beginning of the proof. Since the cutting points of these factorizations correspond to occurrences of uv in $\theta_{u,v}(s)$ shifted by $|u|$, we deduce from [35, Proposition 2.6(2)] that there must be a corresponding factorization $s = \tilde{x}_1\tilde{y}_1\dots\tilde{y}_k\tilde{x}_{k+1}$ such that

$$\theta_{u,v}(\tilde{y}_i) = y_{w_i}, \quad \theta_{u,v}(\tilde{x}_i) = \begin{cases} x_{w_1} & i = 1, \\ z_{w_{i-1}}x_{w_i} & 2 \leq i \leq k, \\ z_{w_k} & i = k+1. \end{cases}$$

For $i = 2,\dots,k$, we may use (2) to conclude that

$$|\tilde{x}_i| \leq \frac{C_1+|u|}{C_2} + \frac{C_1+|v|}{C_2} \leq \frac{2C_1+|uv|}{C_2}.$$

Similarly, we have $|\tilde{x}_1| + |\tilde{x}_{k+1}| \leq \frac{2C_1+|uv|}{C_2}$. Noting that $\tilde{y}_i = f(w_i)$ by definition of f, we may now deduce the rightmost inequality of (3),

$$|s| - \sum_{i=1}^{k}|f(w_i)| = |\tilde{x}_1| + |\tilde{x}_{k+1}| + \sum_{i=2}^{k}|\tilde{x}_i| \leq \frac{k(2C_1+|uv|)}{C_2}.$$

The two remaining inequalities are again straightforward.

Step 3. For $l \in \mathbb{N}$, define a homomorphism $\kappa_l \colon A^* \to A_{u,v}^*$ by

$$\kappa_l(a) = f(\varphi^l(a)), \quad a \in A.$$

Let $K_l = M_{\kappa_l}$. We finish the proof by showing that the matrices $(K_l)_{l\in\mathbb{N}}$ fulfil the requirements of the lemma. First, by (1), for all $a,b \in A$ and $l \in \mathbb{N}$, we have

$$0 \leq |\varphi^l(a)|_b - |\theta_{u,v}\kappa_l(a)|_b = |\varphi^l(a)|_b - |\theta_{u,v}f(\varphi^l(a))|_b \leq 2C_1 + |uv|.$$

Hence, the entries of the matrices $M_\varphi^l - M_{\theta_{u,v}}K_l$ can only take finitely many values, and this proves the first half of the statement. For the remaining half, we fix a letter $c \in A_{u,v}$ and we let $\theta_{u,v}(c) = a_1\dots a_k$, where $a_i \in A$. For every large enough l, the following factorization satisfies the condition of Step 2:

$$\theta_{u,v}(\varphi_{u,v}^l(c)) = \varphi^l(a_1)\dots\varphi^l(a_k).$$

Applying (3) while noting that $k \leq C_1$ yields, for every letter $d \in A_{u,v}$,

$$0 \leq |\varphi_{u,v}^l(c)|_d - |\kappa_l\theta_{u,v}(c)|_d = |\varphi_{u,v}^l(c)|_d - \sum_{i=1}^{k}|f(\varphi^l(a_i))|_d \leq \frac{C_1(2C_1+|uv|)}{C_2}.$$

This shows that the entries of the matrices $M_{\varphi_{u,v}}^l - K_lM_{\theta_{u,v}}$ can take only finitely many values, completing the proof of the lemma. □

This leads us to the following result, which is our main result for the subsection. Roughly speaking, it states that, up to powers of x and cyclotomic polynomials, a primitive substitution shares its characteristic polynomial with all of its return substitutions. As we already mentioned, this is a slightly sharpened version of a result of Durand [36, Proposition 9].

Proposition 4.6. *Let $\varphi\colon A^* \to A^*$ be a primitive aperiodic substitution and (u,v) be a connection of φ of order n. Then, there exists a unique pair of coprime polynomials $\xi_1, \xi_2 \in \mathbb{Z}[x]$ which are products of cyclotomic polynomials and satisfy*

$$\xi_1 \chi^*_{\varphi^n} = \pm \xi_2 \chi^*_{\varphi_{u,v}}.$$

Proof. We note that cyclotomic polynomials, and hence their products, satisfy the relation $\xi^* = \pm\xi$. Hence, the result follows if we can show that for some positive integers k_1, k_2, we have

$$x^{k_1}\xi_1(x)\chi_{\varphi^n}(x) = x^{k_2}\xi_2(x)\chi_{\varphi_{u,v}}(x), \tag{4}$$

where $\xi_1, \xi_2 \in \mathbb{Z}[x]$ are coprime and are both products of cyclotomic polynomials.

As in the proof of the previous lemma, we may assume that $n = 1$. Fix an eigenvalue $\lambda \in \mathbb{C}$ of M_φ which is not 0 or a root of 1, and let $E(\lambda)$ and $E'(\lambda)$ denote the respective generalized eigenspaces of M_φ and $M_{\varphi_{u,v}}$, that is

$$E(\lambda) = \{x \in \mathbb{C}^A : \exists k \geq 1,\ x(M_\varphi - \lambda)^k = 0\},$$
$$E'(\lambda) = \{x \in \mathbb{C}^{A_{u,v}} : \exists k \geq 1,\ x(M_{\varphi_{u,v}} - \lambda)^k = 0\}.$$

Note that we view the elements of $\mathbb{C}^A$ and $\mathbb{C}^{A_{u,v}}$ as row vectors, so matrices act on the right. Fix an element $x \in E(\lambda)$, so $x \in \ker(M_\varphi - \lambda)^k$ for some $k \geq 1$. Since $\varphi\theta_{u,v} = \theta_{u,v}\varphi_{u,v}$, we have $M_\varphi M_{\theta_{u,v}} = M_{\theta_{u,v}} M_{\varphi_{u,v}}$, and so

$$xM_{\theta_{u,v}}(M_{\varphi_{u,v}} - \lambda)^k = x(M_\varphi - \lambda)^k M_{\theta_{u,v}} = 0.$$

Therefore, $xM_{\theta_{u,v}}$ belongs to $E'(\lambda)$ and $M_{\theta_{u,v}}$ gives a linear map $E(\lambda) \to E'(\lambda)$. We claim that the kernel of this map is trivial. Indeed, fix $x \in E(\lambda) \cap \ker(M_{\theta_{u,v}})$, and let $k \in \mathbb{N}$ be minimal such that $x(M_\varphi - \lambda)^k = 0$. Clearly, $k = 0$ exactly when $x = 0$. Thus, we assume $k > 0$ and $x \neq 0$, and we argue by contradiction. Then, the vector $y = x(M_\varphi - \lambda)^{k-1}$ is an eigenvector of M_φ of eigenvalue λ which also belongs to $\ker(M_{\theta_{u,v}})$. For every $l \geq 1$, let $Q_l = M_\varphi^l - M_{\theta_{u,v}}K_l$, where K_l is the matrix from Lemma 4.5. It follows that

$$\lambda^l y = yM_\varphi^l = y(M_{\theta_{u,v}}K_l + Q_l) = yQ_l.$$

But Lemma 4.5 states that the set of matrices $\{Q_l : l \in \mathbb{N}\}$ is finite, so we may choose $1 \leq l_1 < l_2$ with $Q_{l_1} = Q_{l_2}$. Since $y \neq 0$, it follows that $\lambda^{l_1} = \lambda^{l_2}$, which contradicts the fact that λ is not 0 or a root of 1. Thus, $x = 0$ and $E(\lambda)$ is isomorphic to a subspace of $E'(\lambda)$. Using a similar argument, one proves that the left action of $M_{\theta_{u,v}}$ on $\mathbb{C}^{A_{u,v}}$, whose elements are now viewed as column vectors, induces an injective linear map $E'(\lambda) \to E(\lambda)$ (use instead $Q_l = M^l_{\varphi_{u,v}} - K_l M_{\theta_{u,v}}$). In particular, $\dim(E'(\lambda)) = \dim(E(\lambda))$ for every λ which is not 0 or a root of 1.

Next, recall that these dimensions give the algebraic multiplicities of λ as a root of χ_φ and $\chi_{\varphi_{u,v}}$ respectively [74, Corollary 7.5.3(2)]. Hence, for some polynomials ξ, ζ_1, ζ_2 in $\mathbb{C}[x]$ and some positive integers k_1, k_2, we have the following factorizations:

$$\chi_\varphi(x) = x^{k_2}\zeta_2(x)\xi(x), \quad \chi_{\varphi_{u,v}}(x) = x^{k_1}\zeta_1(x)\xi(x),$$

where ξ has no root equal to 0 or roots of 1, and all roots of ζ_1, ζ_2 are roots of 1. We claim that ζ_1 and ζ_2 are products of cyclotomic polynomials. Both cases being analogous, we argue only for ζ_2.

Choosing a root λ of ζ_2, we find that the minimal polynomial of λ over $\mathbb{Q}$, say γ, must divide χ_φ. But γ is a cyclotomic polynomial, thus its roots are all roots of 1. In particular, it follows that γ is coprime with both ξ and x^{l_2}. Hence, γ must divide ζ_2. Repeating this process until all roots of ζ_2 are accounted for proves the claim.

Let δ be the greatest common divisor of ζ_1 and ζ_2 in $\mathbb{Z}[x]$ and for $i=1,2$, let $\xi_i = \zeta_i/\delta$. Clearly we have $\xi_1\zeta_2 = \xi_1\xi_2\delta = \xi_2\zeta_1$, so ξ_1 and ξ_2 together with the integers k_1 and k_2 satisfy (4). That ξ_1 and ξ_2 are coprime and products of cyclotomic polynomials follows by construction. It remains to show that this is the only such pair. Suppose that ξ_1' and ξ_2' are products of cyclotomic polynomials satisfying (4) for some positive integers l_1, l_2. This readily implies $x^{l_1+k_2}\xi_1'\xi_2 = x^{l_2+k_1}\xi_2'\xi_1$. Since ξ_1 and ξ_2 are coprime, we deduce that ξ_1 divides ξ_1' and ξ_2 divides ξ_2', thus proving uniqueness. □

4.4 Pronilpotent quotients of Schützenberger groups

Let φ be a primitive aperiodic substitution. Recall that Theorem 3.6 together with Theorem 4.1 imply that all the information concerning the pronilpotent quotients of $G(\varphi)$ is contained within the reciprocal characteristic polynomial of any return substitution of φ. The main result of Section 4.3 means that the reciprocal characteristic polynomial of φ itself carries at least partial information about the pronilpotent quotients of its Schützenberger group. This allows us to specialize some results from Section 3, culminating with our main result (Theorem 4.12), which states that Schützenberger groups of primitive aperiodic substitutions of constant length are never free.

Proposition 4.7. *Let φ be a primitive aperiodic substitution and (u,v) be a connection of φ. Let m_φ be the difference $\deg(\chi^*_{\varphi_{u,v}}) - \deg(\chi^*_\varphi)$. Then, for every prime p, we have $m_\varphi = \deg(\chi^*_{p,\varphi_{u,v}}) - \deg(\chi^*_{p,\varphi})$. In particular, $Q_{\mathbf{Ab}_p}(G(\varphi))$ has dimension $m_\varphi + \deg(\chi^*_{p,\varphi})$ over $\mathbb{Z}/p\mathbb{Z}$.*

Proof. Let n be the order of the connection (u,v) and let ξ_1,ξ_2 be the pair of polynomials given by Proposition 4.6. Fix a prime p, and for $i=1,2$, let $\xi_{p,i}$ be the polynomial obtained by reducing the coefficients of ξ_i modulo p. It follows from Proposition 4.6 that $\deg(\chi^*_{p,\varphi_{u,v}}) - \deg(\chi^*_{p,\varphi^n}) = \deg(\xi_{p,1}) - \deg(\xi_{p,2})$. But observe that cyclotomic polynomials are monic, hence $\deg(\xi_{p,i}) = \deg(\xi_i)$ for $i=1,2$. We claim that $\deg(\chi^*_{p,\varphi^n}) = \deg(\chi^*_{p,\varphi})$. Indeed, let $\mathbb{K}$ be the algebraic closure of $\mathbb{Z}/p\mathbb{Z}$ and view $M_{p,\varphi}$ and M_{p,φ^n} as matrices over $\mathbb{K}$. Then, the eigenvalues of M_{p,φ^n} are the nth powers of the eigenvalues of $M_{p,\varphi}$ [50, Chapter XIV, Theorem 3.10], hence the two matrices must have the same number of non-zero eigenvalues over $\mathbb{K}$ counted with multiplicity. By Remark 3.4, their reciprocal characteristic polynomials must have the same degree, as claimed. Thus, for every prime p, we have

$$\deg(\chi^*_{p,\varphi_{u,v}}) - \deg(\chi^*_{p,\varphi}) = \deg(\xi_1) - \deg(\xi_2).$$

But for p large enough, the left-hand side of this equation is equal to m_φ, while the right-hand side is clearly independent of p. This completes the proof of the first part of the proposition. For the second part, recall that by Theorem 4.1, $\varphi_{u,v}$ defines an ω-presentation of $G(\varphi)$. Then, note that $m_\varphi + \deg(\chi^*_{p,\varphi}) = \deg(\chi^*_{p,\varphi_{u,v}})$ and apply the dimension formula (Proposition 4.7). □

We stress that m_φ need not be positive (Example 4.15). We also observe that the integer m_φ does not depend on the choice of (u,v). Indeed, we found it to be equal, for every prime p, to

$\mathrm{d}_p(G(\varphi)) - \deg(\chi^*_{p,\varphi})$, a quantity which clearly does not depend on (u,v). This can rephrased as follows.

Corollary 4.8. *Let φ be a primitive aperiodic substitution and (u,v) be a connection of φ. Let ξ_1, ξ_2 be the two polynomials given by Proposition 4.6. The difference $\deg(\xi_1) - \deg(\xi_2)$ does not depend on the connection (u,v).*

Remark 4.9. Let (u,v) and (u',v') be two connections of a primitive aperiodic substitution φ sharing the same middle letters (i.e., u and u' share their last letter while v and v' share their first letter). Then, using a two-sided analogue of [36, Proposition 7], one finds that $\chi^*_{\varphi_{u,v}} = \chi^*_{\varphi_{u',v'}}$. In particular, applying Proposition 4.6 with either (u,v) or (u',v') yields the same pair ξ_1, ξ_2. This might not be true for connections that do not share the same middle letters (Example 4.18).

Because the value of m_φ might be negative (Example 4.15), the relative freeness test of Corollary 3.10 cannot be applied directly using χ^*_φ in place of $\chi^*_{\varphi_{u,v}}$. However, we have the following weaker form.

Proposition 4.10. *Let φ be a primitive aperiodic substitution. If there are two primes p_1, p_2 such that*

$$\deg(\chi^*_{p_1,\varphi}) < \deg(\chi^*_{p_2,\varphi}) < \deg(\chi^*_\varphi),$$

then $G(\varphi)$ is not relatively free.

Proof. Let (u,v) be a connection of φ. By Proposition 4.7, adding m_φ to each term in the inequality above yields

$$0 \leq \deg(\chi^*_{p_1,\varphi_{u,v}}) < \deg(\chi^*_{p_2,\varphi_{u,v}}) < \deg(\chi^*_{\varphi_{u,v}}).$$

Since $\varphi_{u,v}$ defines an ω-presentation of $G(\varphi)$ (Theorem 4.1), we may apply Corollary 3.10 with p_2 to conclude that $G(\varphi)$ is not relatively free. □

Example 4.16 gives an example where the test above is conclusive. For the absolute freeness test of Corollary 3.11, the situation is more straightforward.

Proposition 4.11. *Let φ be a primitive aperiodic substitution. If $\mathrm{pdet}(M_\varphi)$ is not ± 1, then the Schützenberger group $G(\varphi)$ is not absolutely free.*

Proof. Let (u,v) be a connection of φ of order n. It follows from Proposition 4.6 that $\mathrm{pdet}(M_{\varphi^n}) = \pm\,\mathrm{pdet}(M_{\varphi_{u,v}})$. Moreover, we observe that $\mathrm{pdet}(M_{\varphi^n}) = \mathrm{pdet}(M_\varphi)^n$. Hence, $\mathrm{pdet}(M_\varphi)$ equals ± 1 if and only if so does $\mathrm{pdet}(M_{\varphi_{u,v}})$. Recall (Theorem 4.1) that $\varphi_{u,v}$ defines an ω-presentation of $G(\varphi)$ and apply Corollary 3.11 to conclude that $G(\varphi)$ is not absolutely free. □

A substitution $\varphi\colon A^* \to A^*$ is said to have *constant length* when there is some integer $k \in \mathbb{N}$ such that $|\varphi(a)| = k$, for all $a \in A$. Constant length primitive substitutions include the famous Thue–Morse substitution (Example 4.14), which was shown to have a non-free Schützenberger group in [11]. The next theorem generalizes this result.

Theorem 4.12. *Let φ be a primitive aperiodic substitution of constant length. Then $G(\varphi)$ is not absolutely free.*

Proof. Assume that $k = |\varphi(a)|$ for every letter a. In light of Proposition 4.11, it is enough to show that the leading coefficient of χ_φ^* is divisible by k. Note that the vector $(1,\dots,1)$ is a (left) eigenvector of M_φ of eigenvalue k with coefficients in $\mathbb{Z}$, hence there is a factorization in $\mathbb{Z}[x]$

$$\chi_\varphi(x) = (x-k)\gamma(x).$$

Plainly then, k divides the leading coefficient of χ_φ^*. □

Remark 4.13. We may contrast the last result with the case of unimodular substitutions. Recall that a substitution is called *unimodular* when its composition matrix is invertible over $\mathbb{Z}$, or equivalently when its determinant is ± 1. If φ is primitive, unimodular and aperiodic, then it follows from Propositions 3.9 and 4.6 that $Q_{\mathrm{nil}}(G(\varphi))$ is free pronilpotent. Therefore, $G(\varphi)$ is indistinguishable from a free profinite group in its finite nilpotent quotients. The same argument applies for all primitive aperiodic substitutions whose composition matrix has pseudodeterminant ± 1.

However, while unimodularity of φ guarantees that $Q_{\mathrm{nil}}(G(\varphi))$ is free pronilpotent, it does not, by any means, guarantee that $G(\varphi)$ itself is free, even relatively so. The reader can find in [45, Section 6] an example of a primitive substitution on 4 letters that induces an automorphism of the free group (hence is unimodular), but whose Schützenberger group is not relatively free.

In a recent paper [30], Costa and Steinberg proved that the Schützenberger groups (and, thus, their maximal pronilpotent quotients) of irreducible shift spaces are invariant under flow equivalence. In particular, this means that our results provide flow invariants for shift spaces of primitive aperiodic substitutions. Here are some low hanging fruits. Among shift spaces defined by primitive aperiodic substitutions, we found the following to be invariant under flow equivalence:

(1) the sequence of integers $(\deg(\chi^*_{p,\varphi_{u,v}}))_p$ indexed by prime numbers;
(2) the set of primes dividing $\mathrm{pdet}(\varphi)$.

These are reasonably easy to compute, especially the second one, but they are also fairly weak. For instance, (2) cannot distinguish primitive unimodular substitutions that are defined on the same alphabet. At least, these invariants suffice to separate, for instance, unimodular substitutions from substitutions of constant length.

4.5 Examples

Let us conclude with a series of examples chosen to illustrate different aspects of our results. All of them are primitive and aperiodic (aperiodicity can be checked using [19, Exercise 5.15], for instance). We use, without further mention, the fact that in these cases, every return substitution defines an ω-presentation of the Schützenberger group (Theorem 4.1). Return substitutions were computed using a Python implementation of an algorithm described in [37, p.205], and were labelled according to the ordering of return words defined in Section 4.2. In every example, we give also the relevant reciprocal characteristic polynomials, and (save for Example 4.19) the polynomials ξ_1, ξ_2 of Proposition 4.6 and the integer m_φ of Proposition 4.7. We then proceed, using Theorem 3.6, to describe the pronilpotent quotients of the Schützenberger group, and we draw conclusions regarding its freeness using our various tests (Sections 3.4, 4.4).

In what follows, we use the term *cyclic* as a synonym for 1-generated. We also recall the notation $\mathbb{Z}_p$, denoting for a prime p the additive group of the p-adic integers. For a set of primes π, we write $\widehat{F}_{\mathrm{nil},\pi}$ instead of $\widehat{F}_{\mathbf{G}_{nil,\pi}}$ (the definition of $\mathbf{G}_{\mathrm{nil},\pi}$ may be recalled at the beginning of Section 3.4). Our first example is a good contender for the title of "most studied substitution".

Example 4.14. The *Thue–Morse substitution* is the binary substitution τ defined by

$$\tau\colon 0 \mapsto 01,\ 1 \mapsto 10.$$

Since it has constant length, the group $G(\tau)$ is not absolutely free (Theorem 4.12). The reciprocal characteristic polynomial of τ is $-2x+1$, so the weak relative freeness test stated in Proposition 4.10 is inconclusive. Here is the return substitution corresponding to the connection $(0,1)$ of τ, which has order 2:

$$\tau_{0,1}\colon 0 \mapsto 0123,\ 1 \mapsto 013,\ 2 \mapsto 02123,\ 3 \mapsto 0213.$$

The reciprocal characteristic polynomial of $\tau_{0,1}$, together with the polynomials ξ_1, ξ_2 and the integer m_τ, are as follows:

$$\chi^*_{\tau_{0,1}}(x) = (4x-1)(x-1), \quad \xi_1(x) = x-1, \quad \xi_2(x) = 1, \quad m_\tau = 1.$$

Hence, we may apply Corollary 3.10 with $p = 2$ to conclude that $G(\tau)$ is not relatively free, thus recovering [11, Theorem 7.6]. (We note that the proof given in [11] is, in some sense, similar to ours: it relies on variations in the dimensions of the maximal pro-$\mathbf{Ab}_p$ quotients of $G(\tau)$ to reach a contradiction, much like what we do in Proposition 3.9.) Letting π be the set of all odd primes, we deduce from Theorem 3.6 that

$$Q_{\mathrm{nil}}(G(\varphi)) \cong \mathbb{Z}_2 \times \widehat{F}_{\mathrm{nil},\pi}(2).$$

A pronilpotent group is a quotient of $G(\tau)$ if and only if its 2-Sylow subgroup is cyclic and all other Sylow subgroups are 2-generated.

Next, we give an example of a substitution whose Schützenberger group has a cyclic maximal pronilpotent quotient. It also features a negative value for m_φ.

Example 4.15. Consider the following ternary substitution:

$$\varphi\colon 0 \mapsto 120,\ 1 \mapsto 121,\ 2 \mapsto 200.$$

Since it has constant length, its Schützenberger group is not absolutely free (Theorem 4.12). Its reciprocal characteristic polynomial is equal to $(3x-1)(x-1)$. The pair $(0,1)$ is a connection of φ of order 1, and the corresponding return substitution is the binary substitution

$$\varphi_{0,1}\colon 0 \mapsto 0011,\ 1 \mapsto 01.$$

We give below its reciprocal characteristic polynomial, the two polynomials ξ_1 and ξ_2 and the integer m_φ:

$$\chi^*_{\varphi_{0,1}}(x) = 3x-1, \quad \xi_1(x) = 1, \quad \xi_2(x) = x-1, \quad m_\varphi = -1.$$

Let π be the set of all primes distinct from 3. Following Proposition 3.9, the maximal pronilpotent quotient of $G(\varphi)$ is free of rank 1 with respect to $\mathbf{G}_{\mathrm{nil},\pi}$. Accordingly, a pronilpotent group is a quotient of $G(\varphi)$ if and only if it is cyclic and its 3-Sylow subgroup is trivial.

Next is a substitution for which the weak freeness test of Proposition 4.10 is conclusive.

Example 4.16. Consider the binary substitution

$$\varphi\colon 0 \mapsto 1001,\ 1 \mapsto 000.$$

It satisfies $\chi^*_\varphi(x) = -6x^2 - 2x + 1$, so its Schützenberger group is not relatively free (apply Proposition 4.10 with $p_1 = 2$, $p_2 = 3$). The connection $(0,0)$ of φ, which has order 2, gives the return substitution

$$\varphi_{0,0}\colon 0 \mapsto 0012100,\ 1 \mapsto 0012101221012100,\ 2 \mapsto 0012101222221012100.$$

We give below its reciprocal characteristic polynomial, the polynomials ξ_1, ξ_2 and the integer m_φ.

$$\chi^*_{\varphi_{0,0}}(x) = -(x-1)(36x^2 - 16x + 1), \quad \xi_1(x) = x - 1, \quad \xi_2(x) = 1, \quad m_\varphi = 1.$$

If π is the set of all primes distinct from 2 and 3, then Theorem 3.6 yields

$$Q_{\mathrm{nil}}(G(\varphi)) \cong \mathbb{Z}_2 \times \widehat{F}_3(2) \times \widehat{F}_{\mathrm{nil},\pi}(3).$$

Consequently, a pronilpotent group is a quotient of $G(\varphi)$ if and only if its 2-Sylow subgroup is cyclic, its 3-Sylow subgroup is 2-generated, and all other Sylow subgroups are 3-generated.

We gave, in Section 4.2, an example of a substitution on a quaternary alphabet whose return substitutions are very large. Let us revisit this example.

Example 4.17. Recall the substitution φ of Example 4.4,

$$\varphi\colon 0 \mapsto 12,\ 1 \mapsto 22,\ 2 \mapsto 33,\ 3 \mapsto 00.$$

Because it has constant length, its Schützenberger group is not absolutely free (Theorem 4.12). We find that its reciprocal characteristic polynomial is $-(2x-1)(4x^3 + 4x^2 + 2x + 1)$. Its return substitutions are too big to be represented here, but for the purpose of understanding the pronilpotent quotients of $G(\varphi)$, we only need the reciprocal characteristic polynomial of any return substitution. For instance, for the connection $(2,3)$ of φ, according to our computations,

$$\chi^*_{\varphi_{2,3}}(x) = (x-1)^6(2^{12}x - 1)(2^{26}x^3 - (2^{16}\cdot 11)x^2 - (2^8 \cdot 5)x - 1),$$

so we have

$$\xi_1(x) = (x-1)^6, \quad \xi_2(x) = 1, \quad m_\varphi = 6.$$

Applying Corollary 3.10 with $p = 2$, we conclude that $G(\varphi)$ is not relatively free. Moreover, we can apply Theorem 3.6 to deduce the following, where π is the set of all odd primes:

$$Q_{\mathrm{nil}}(G(\varphi)) \cong \widehat{F}_2(6) \times \widehat{F}_{\mathrm{nil},\pi}(10).$$

A pronilpotent group is a quotient of $G(\varphi)$ if and only if its 2-Sylow component is 6-generated and all the other components are 10-generated.

Recall, from Remark 4.9, that the polynomials ξ_1, ξ_2 of Proposition 4.6 do not vary between connections sharing the same middle letters. Our next example shows that this is not true between arbitrary connections.

Example 4.18. Consider the ternary substitution

$$\varphi\colon 0 \mapsto 010,\ 1 \mapsto 21,\ 2 \mapsto 102.$$

It is unimodular, so its Schützenberger group has a free maximal pronilpotent quotient. Its reciprocal characteristic polynomial is $-(x-1)(x^2-3x+1)$. Consider the connections $(1,0)$ and $(0,1)$: they have respective order 1 and 2, and the corresponding return substitutions are

$$\varphi_{1,0}\colon 0 \mapsto 01,\ 1 \mapsto 002,\ 2 \mapsto 0012,$$
$$\varphi_{0,1}\colon 0 \mapsto 011202312,\ 1 \mapsto 0112312,\ 2 \mapsto 012,\ 3 \mapsto 0112311202312.$$

With the connection $(1,0)$, we obtain the following values for the reciprocal characteristic polynomial, and the polynomials ξ_1, ξ_2:

$$\chi^*_{\varphi_{1,0}}(x) = (x+1)(x^2-3x+1), \quad \xi_1(x) = x+1, \quad \xi_2(x) = x-1,$$

while, with the connection $(0,1)$, we get instead

$$\chi^*_{\varphi_{0,1}}(x) = -(x-1)(x^2-7x+1), \quad \xi_1(x) = 1 = \xi_2(x).$$

In accordance with Corollary 4.8, both connections give the value $m_\varphi = 0$. The return substitutions have pseudodeterminant ± 1, hence the maximal pronilpotent quotient of $G(\varphi)$ is a free pronilpotent group of rank 3 by Proposition 3.9.

We finish with an infinite family of examples determined by two parameters k and l. One member of this family (the case $k=1$, $l=3$) was previously studied in early work of Almeida about maximal subgroups of free profinite monoids. To the best of our knowledge, it stands as the first published example of a non-free maximal subgroup of a free profinite monoid [8, Example 7.2].

Example 4.19. Fix $k,l \geq 0$ and let φ be the binary substitution

$$\varphi\colon 0 \mapsto 0^k1,\ 1 \mapsto 0^l1.$$

Provided $l \geq 1$, it is primitive. We claim that it is aperiodic if and only if $k \neq l$. Indeed, suppose that φ is periodic, and assume first that $k \geq l$. Let w be a period of $L(\varphi)$, by which we mean that every word $x \in L(\varphi)$ is a factor of some power w^n, and w is minimal for this property. By [19, Exercise 5.15], we may in fact assume that w is is a prefix of 0^k1, and clearly it cannot be a proper prefix; hence, we have $w = 0^k1$. But $L(\varphi)$ also contains 10^l1, and this can only be the case if $l=k$. The case $l \geq k$ is analogous. From now on, we assume $l \geq 1$ and $k \neq l$.

Next, we observe that φ is proper, hence it defines an ω-presentation of its own Schützenberger group (see Remark 4.3). The reciprocal characteristic polynomial of φ is given by: $\chi^*_\varphi(x) = (k-l)x^2-(k+1)x+1$. By Proposition 3.9, the maximal pronilpotent quotient of $G(\varphi)$ is free pronilpotent of rank 2 whenever $|k-l| = 1$. (In fact, in that case, it is not hard to see that φ induces an automorphism of the free group of rank 2. Such substitutions are well known to be Sturmian [40, Corollary 9.2.7], and the Schützenberger group of every Sturmian substitution must be a free profinite group of rank 2 [8, Corollary 6.1].)

On the other hand, when $|k-l|>1$, Corollary 3.11 implies that $G(\varphi)$ is not absolutely free. Moreover, when there is a prime that divides $k-l$ but not $k+1$, we conclude from Corollary 3.10 that the Schützenberger group is not relatively free. Let π_1 be the set of all primes that do not divide $k-l$ and π_2 be the (finite) set of all primes that divide $k-l$ but not $k+1$. We deduce from Theorem 3.6 that

$$Q_{\mathrm{nil}}(G(\varphi)) \cong \left(\prod_{p\in\pi_2}\mathbb{Z}_p\right)\times\widehat{F}_{\mathrm{nil},\pi_1}(2).$$

In particular, a pronilpotent group is a quotient of $G(\varphi)$ if and only if for every prime p, its p-Sylow component is: 2-generated if $p\in\pi_1$; cyclic if $p\in\pi_2$; trivial if p divides $\gcd(k-l,k+1)$.

Using other means, the group $G(\varphi)$ above was shown not to be relatively free in the case $k=1$ and $l=3$ [11, Theorem 7.2], but this case is not covered by Corollary 3.10. In fact, in light of our results, the pronilpotent quotients alone do not contain enough information about $G(\varphi)$ to reach this conclusion. Indeed, in that case, $\chi^*_\varphi(x)=-2x^2-2x+1$ and Theorem 3.6 implies $Q_{\mathrm{nil}}(G(\varphi))\cong\widehat{F}_{\mathrm{nil},\pi}(2)$, where π is the set of all odd primes.

Acknowledgements

This work was partially supported by the Centre for Mathematics of the University of Coimbra (UIDB/00324/2020, funded by the Portuguese Government through FCT/MCTES) and the Centre for Mathematics of the University of Porto (UIDB/00144/2020, funded by the Portuguese Government through FCT/MCTES). The author also benefited from a scholarship (PD/BD/150350/2019, funded by the Portuguese Government through FCT/MCTES).

My heartfelt thanks to Alfredo Costa, whose guidance and advice were invaluable throughout the long process of preparing this paper. Many thanks also to Jorge Almeida for his very helpful comments.

Paper 3

Suffix-connected languages

Theoretical Computer Science, 923 (2022) 126–143.

doi:10.1016/j.tcs.2022.05.001

Suffix-connected languages

Herman Goulet-Ouellet

Received 24 March 2022
Accepted 3 May 2022
Communicated by D. Perrin

Abstract. Inspired by a series of papers initiated in 2015 by Berthé et al., we introduce a new condition called suffix-connectedness. We show that the groups generated by the return sets of a uniformly recurrent suffix-connected language lie in a single conjugacy class of subgroups of the free group. Moreover, the rank of the subgroups in this conjugacy class only depends on the number of connected components in the extension graph of the empty word. We also show how to explicitly compute a representative of this conjugacy class using the first order Rauzy graph. Finally, we provide an example of suffix-connected, uniformly recurrent language that contains infinitely many disconnected words.

Keywords. Tree sets, Extension graphs, Return words, Rauzy graphs, Stallings algorithm, Free groups

Mathematics subject classification 2010. 68Q45, 68R15

1 Introduction

In [22], Berthé et al. introduced the notion of extension graph and used it to study the subgroups generated by the return sets in uniformly recurrent languages. One result achieved in that paper, dubbed the *Return Theorem*, states that if L is a uniformly recurrent language on the alphabet A such that all the extension graphs of L are trees, then the return sets of L are all bases of the free group on A [22, Theorem 4.5]. Moreover, they also show that part of this result holds under weaker assumptions: if we merely assume that the extension graphs of L are connected, then the return sets of L all generate the free group on A [22, Theorem 4.7]. The aim of this paper is to give a weaker condition under which a similar conclusion still holds. To do this, we introduce *suffix extension graphs*, a notion generalizing the extension graphs of [22]. This allows us to define a new condition called *suffix-connectedness*. Our main result is the following:

Theorem 1.1. *Let L be a suffix-connected uniformly recurrent language on an alphabet A. Then the subgroups generated by the return sets of L all lie in the same conjugacy class and their rank is $n-c+1$, where $n=\mathrm{Card}(A)$ and c is the number of connected components of the extension graph of the empty word.*

Our proof is constructive, in the sense that we can also deduce a way to explicitly compute a representative for this conjugacy class. Moreover, the proof of Theorem 1.1 has two notable consequences that we wish to highlight now. The first one is a characterization of suffix-connected, uniformly recurrent languages whose return sets generate the full free group.

Corollary 1.2. *Let L be a suffix-connected and uniformly recurrent language on the alphabet A. Then the following statements are equivalent:*

(1) All the return sets of L generate the free group on A.
(2) Some return set of L generates a group of rank $\mathrm{Card}(A)$.
(3) The extension graph of the empty word is connected.

The next corollary is a special case of our main result. It involves *neutrality*, which is a combinatorial condition also introduced in [22] (we will recall the definition in Section 8). A *connected set* is a language in which the extension graphs of non-empty words are connected, while a *tree set* is a language in which the extension graph of the empty word is a forest, and all other extension graphs are trees. These conventions differ slightly from [22], but are in line with other papers such as [25, 33]. The term *dendric* has also been used to refer to tree sets, for instance in [34]. A subset of the free group is called *free* if it forms a basis of the subgroup it generates.

Corollary 1.3. *Let L be a uniformly recurrent language on the alphabet A. If L is connected and neutral, then the following conditions are equivalent:*

(1) Some return set of L is a free subset of the free group on A.
(2) All return sets of L are free subsets of the free group on A.
(3) L is a tree set.

Since connectedness implies suffix-connectedness, the assumptions of the Return Theorem place us in the scope of both Corollary 1.2 and 1.3. It follows that the Return Theorem is a direct consequence of the above corollaries.

In order to further motivate this new *suffix-connectedness* condition, we give an example of a uniformly recurrent language which is suffix-connected but contains infinitely many disconnected elements. This language is defined by a primitive substitution. More precisely, we will show the following:

Theorem 1.4. *The language of the primitive substitution*

$$\varphi\colon 0 \mapsto 0001,\ 1 \mapsto 02,\ 2 \mapsto 001.$$

is suffix-connected and contains infinitely many disconnected words.

We will also see that, in the language of this substitution, the extension graph $\mathbf{E}(\varepsilon)$ is connected. Therefore, as a result of Corollary 1.2, all the return sets in this language generate the full free group of rank 3. However, further computations reveal that the language of φ has return sets of cardinality 3 and 4, which means that some but not all of them are free subsets of the free group.

This paper is structured as follows. In Section 2, we introduce suffix extension graphs and suffix-connectedness, while also recalling some relevant definitions in more details. Section 3 reviews some basic material about the groups generated by labelled digraphs. Section 4 is devoted to Rauzy graphs.

Section 5 presents a technical result that makes up the core of the proof of our main result. In Section 6, we examine the relationship between Rauzy graphs and return sets. In Section 7, we put everything together and give the proof of Theorem 1.1. Section 8 discusses the proof of the two corollaries above. Finally, Section 9 is devoted to our suffix-connected example.

2 Suffix-connectedness

In this paper, L denotes a language on a finite alphabet A of cardinality n, and $F(A)$ denotes the free group on A. We will always suppose that L is recurrent and that $A \subseteq L$. We recall that a language L is *recurrent* if it is closed under taking factors, and if for every two words $u, v \in L$, there exists a non-empty word w such that $uwv \in L$. A recurrent language L is called *uniformly recurrent* if for every word $u \in L$, there is a positive integer n such that u is a factor of every $v \in L$ with $|v| \geq n$. The *left extensions* and *right extensions* of order k of $w \in L$, are:

$$\mathbf{L}_k(w) = \{u \in L \cap A^k : uw \in L\}, \qquad \mathbf{R}_k(w) = \{v \in L \cap A^k : wv \in L\}.$$

The *extension graph of order* (k,l) of $w \in L$ is a bipartite graph over the disjoint union of $\mathbf{L}_k(w)$ and $\mathbf{R}_l(w)$ (the union of disjoint copies of $\mathbf{L}_k(w)$ and $\mathbf{R}_l(w)$). In this graph, there is an edge between $u \in \mathbf{L}_k(w)$ and $v \in \mathbf{R}_l(w)$ if $uwv \in L$. We denote this graph by $\mathbf{E}_{k,l}(w)$. Note that all extension graphs are simple and undirected. We abbreviate $\mathbf{R}_1$, $\mathbf{L}_1$ and $\mathbf{E}_{1,1}$ respectively by $\mathbf{R}$, $\mathbf{L}$ and $\mathbf{E}$. In the absence of further clarifications, the term *extension graph of w* refers to $\mathbf{E}(w)$. A word is *connected* if its extension graph is connected, and it is called *disconnected* otherwise. A language is *connected* if all its non-empty words are connected, and it is *disconnected* otherwise.

A word $w \in L$ is called *left special* if $\mathrm{Card}(\mathbf{L}(w)) > 1$. Similarly, w is called *right special* if $\mathrm{Card}(\mathbf{R}(w)) > 1$. By a *bispecial word*, we mean a word which is both left and right special.

Remark 2.1. If w is not bispecial, then $\mathbf{E}(w)$ is a star graph, and in particular a tree. Indeed, if w is not left special, then $\mathbf{L}(w)$ consists of only one element, which must be incident to every edge of $\mathbf{E}(w)$; and a similar situation occurs if w is not right special. Hence, only bispecial factors can be disconnected.

Given a word $w \in A^*$ and $0 \leq i < |w|$, we denote by $w(i)$ the i-th letter of w. In particular, the first letter of w is $w(0)$. Given $0 \leq i \leq j \leq |w|$, we denote $w[i:j]$ the factor of w defined by:

$$w[i:j] = w(i)w(i+1)\dots w(j-1)$$

Note that $|w[i:j]| = j-i$, $w[i:i]$ is the empty word and $w[0:|w|] = w$. Let $u \in A^*$ with $|u| = k$. We say that an index j is an *occurrence* of u in w if $w[j:j+k] = u$. We also define the *tail* and the *init* of a non-empty word w by putting:

$$\mathrm{tail}(w) = w[1:|w|], \quad \mathrm{init}(w) = w[0:|w|-1].$$

We view tail and init as maps $A^+ \to A^*$. With this, we are now ready to introduce suffix extension graphs.

Definition 2.2. For $w \in L$ and $1 \leq d \leq |w|+1$, the *depth d suffix extension graph* of w is the extension graph $\mathbf{E}_{d,d}(\mathrm{tail}^{d-1}(w))$.

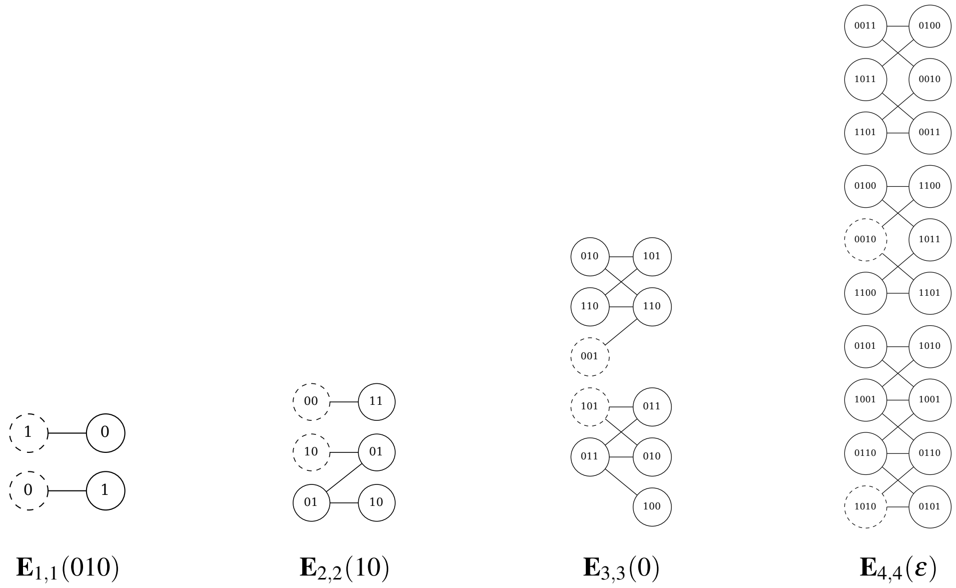


Fig. 1 Suffix extension graphs of the word 010 in the language of the Thue–Morse substitution. The dashed vertices represent the natural embeddings of $\mathbf{L}(010)$.

The set $\mathbf{L}(w)$ naturally embeds in the suffix extension graphs of w. Indeed, let u be the prefix of length $d-1$ of w, which means that u satisfies $w = u\,\mathrm{tail}^{d-1}(w)$. Then $a \mapsto au$ is an injective map $\mathbf{L}(w) \to \mathbf{L}_d(\mathrm{tail}^{d-1}(w))$, with the latter set being viewed as a subset of $\mathbf{E}_{d,d}(\mathrm{tail}^{d-1}(w))$. We call this the *natural embedding* of $\mathbf{L}(w)$ in the depth d suffix extension graph.

Definition 2.3. A word w is called *suffix-connected* if the natural embedding of $\mathbf{L}(w)$ in $\mathbf{E}_{d,d}(\mathrm{tail}^{d-1}(w))$ lies in one connected component, for some $1 \le d \le |w|+1$. A language is called suffix-connected if all its non-empty words are suffix-connected.

We note that this definition is sensitive to both increases and decreases in the depth parameter. That is, for a given word w, it may happen that some of the natural embeddings $\mathbf{L}(w)$ lie in a single connected component, while others do not. The next example is a good illustration of this behaviour. It features a language defined by a primitive substitution, and such languages are well known to be uniformly recurrent (see for instance [40, Proposition 1.2.3]).

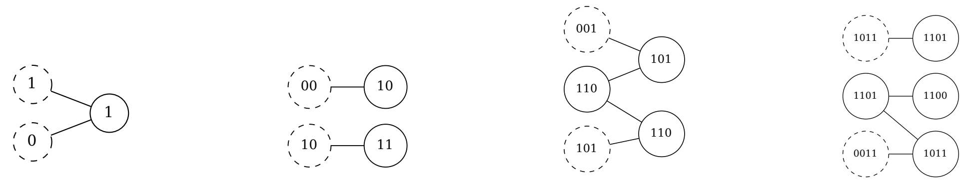
Example 2.4. Let us consider the following binary substitution, known as the *Thue–Morse* substitution:

$$\mu\colon 0 \mapsto 01,\ 1 \mapsto 10.$$

Let L be the language defined by μ. That is, L is the set of factors of all words of the form $\mu^n(a)$ for $n \in \mathbb{N}$ and $a \in \{0,1\}$. Fig. 1 gives all the suffix extension graphs of the word $010 \in L$, which show that L is not suffix-connected.

On the other hand, Fig. 2, gives some extension graphs of $01100 \in L$. These graphs show that the natural embeddings of a given word can alternate between being connected and disconnected as the depth increases.

Replacing tail by init and $\mathbf{L}$ by $\mathbf{R}$ yields the dual notions of *prefix extension graphs* and *prefix-connectedness*. Note that the depth 1 suffix and prefix extension graphs of w both coincide with $\mathbf{E}(w)$, so a connected word or language is both prefix and suffix-connected.



$\mathbf{E}_{1,1}(01100)$ $\mathbf{E}_{2,2}(1100)$ $\mathbf{E}_{3,3}(100)$ $\mathbf{E}_{4,4}(00)$

Fig. 2 First four suffix extension graphs of the word 01100 in the language of the Thue–Morse substitution. The dashed vertices represent the natural embeddings of $\mathbf{L}(01100)$.

3 Stallings equivalence

Let us start this section by clarifying some basic terminology. A *labelled digraph* over the alphabet A (or, more simply, a *digraph*) is a diagram of sets G of the following form:

$$\begin{tikzcd} & \mathcal{E}(G) \arrow[dl, "\lambda"'] \arrow[dr, shift left, "\alpha"] \arrow[dr, shift right, "\omega"'] & \\ A & & \mathcal{V}(G) \end{tikzcd}$$

One can think of $\mathcal{V}$ as the set of *vertices*, $\mathcal{E}$ as the set of *edges*, and A, the alphabet, as the set of *labels*. The maps α, ω and λ give us respectively the origin, terminus and label of a given edge. For our purposes, we may assume that there are no redundant edges, meaning that (α,λ,ω) are jointly injective. This means in effect that $\mathcal{E}$ may be considered a subset of $\mathcal{V}\times A\times\mathcal{V}$ whenever convenient.

Given an edge $e=(x,a,y)$, we consider its formal inverse $e^{-1}=(y,a^{-1},x)$. From now on, we use the term *edge* both for elements of $\mathcal{E}(G)$ and for their formal inverses. Two edges are said to be *consecutive* if the last component of the first is equal to the first component of the second. A *path* is a sequence of consecutive edges. We can naturally extend the maps α,ω to paths, and talk about *consecutive paths*. Two consecutive paths can be composed, and any path can be inverted; we write respectively pq and p^{-1}. A self-consecutive path is called a *loop*. As expected, if p,q are consecutive, then so are q^{-1},p^{-1} and the relation $(pq)^{-1}=q^{-1}p^{-1}$ holds.

The labelling map λ also naturally extends, mapping the set of all paths to the free group $F(A)$. This map satisfies $\lambda(pq)=\lambda(p)\lambda(q)$ and $\lambda(p^{-1})=\lambda(p)^{-1}$. We write $p\colon x\xrightarrow{u}y$ as a shorthand for $\alpha(p)=x$, $\omega(p)=y$, $\lambda(p)=u$. The set of all labels of loops over a given vertex x forms a subgroup of $F(A)$, which we call the *group of G at x*. Note that under the assumption that G is connected (any two vertices can be joined by a path), all the groups of G lie in the same conjugacy class of subgroups of $F(A)$.

Let $\equiv$ be an equivalence relation on the vertices of a digraph G. Then $\equiv$ can also be seen as an equivalence relation on $\mathcal{E}(G)$,

$$(x,a,y)\equiv(x',b,y') \iff x\equiv x',\ a=b,\ y\equiv y'.$$

The *quotient digraph* $G/{\equiv}$ is then defined by:

$$\mathcal{V}(G/{\equiv})=\mathcal{V}(G)/{\equiv},\quad \mathcal{E}(G/{\equiv})=\mathcal{E}(G)/{\equiv},$$

together with the following adjacency and labelling maps:

$$\alpha(x/{\equiv}) = \alpha(x)/{\equiv}, \quad \omega(x/{\equiv}) = \omega(x)/{\equiv}, \quad \lambda(x/{\equiv}) = \lambda(x).$$

The definition of $G/{\equiv}$ can be summarized by the following commutative diagrams:

$$\begin{tikzcd} A & \mathcal{E}(G) \arrow[l, "\lambda"'] \arrow[d, "\equiv"'] \\ & \mathcal{E}(G/{\equiv}) \arrow[ul, "\lambda"] \end{tikzcd} \qquad \begin{tikzcd} \mathcal{E}(G) \arrow[r, "\alpha"] \arrow[d, "\equiv"'] & \mathcal{V}(G) \arrow[d, "\equiv"'] \\ \mathcal{E}(G/{\equiv}) \arrow[r, "\alpha"] & \mathcal{V}(G/{\equiv}) \end{tikzcd} \qquad \begin{tikzcd} \mathcal{E}(G) \arrow[r, "\omega"] \arrow[d, "\equiv"'] & \mathcal{V}(G) \arrow[d, "\equiv"'] \\ \mathcal{E}(G/{\equiv}) \arrow[r, "\omega"] & \mathcal{V}(G/{\equiv}) \end{tikzcd}$$

The natural projection $G \to G/{\equiv}$ is a *digraph morphism*, meaning that it preserves the maps α, ω, λ. If, conversely, $\phi\colon G \to H$ is a digraph morphism, then the quotient $G/\ker(\phi)$ is isomorphic to $\mathrm{Im}(\phi)$, where $\ker(\phi) = \{(x,y) : \phi(x) = \phi(y)\}$. Note that for a digraph morphism $\phi\colon G \to G'$ to be onto, it needs to be onto on both $\mathcal{V}(G')$ and $\mathcal{E}(G')$. The latter condition can be written as follows:

$$\forall (x,a,y) \in \mathcal{E}(G'), \exists (x',a,y') \in \mathcal{E}(G),\ \phi(x') = x \wedge \phi(y') = y.$$

We say that an equivalence relation $\equiv$ on $\mathcal{V}(G)$ is *group-preserving* if the group of G at x is equal to the group of $G/{\equiv}$ at $x/{\equiv}$, for all $x \in \mathcal{V}(G)$. We also call *group-preserving* a digraph morphism whose kernel is a group-preserving relation. Note that the group of G at x is always a subgroup of the group of $G/{\equiv}$ at $x/{\equiv}$. Therefore, to prove that $\equiv$ is group-preserving, one only needs to prove the reverse inclusion. Moreover, in the case of a connected digraph, this inclusion needs only to be checked on a single vertex.

The family of group-preserving equivalence relations of a digraph G also has the property of being closed under taking subrelations. Indeed, let us suppose that $\equiv_1$ is group-preserving and consider $\equiv_2 \subseteq \equiv_1$. Then, the canonical surjection of $\equiv_1$ factors through that of $\equiv_2$, giving us the following commutative diagram:

$$\begin{tikzcd} G \arrow[r, "\equiv_1"] \arrow[d, "\equiv_2"'] & G/{\equiv_1} \\ G/{\equiv_2} \arrow[ur, dashed] & \end{tikzcd}$$

Let us fix $x \in \mathcal{V}(G)$ and let H, H_1, H_2 be respectively the group of G at x; the group of $G/{\equiv_1}$ at $x/{\equiv_1}$; and the group of $G/{\equiv_2}$ at $x/{\equiv_2}$. Then the diagram above implies $H \leq H_2 \leq H_1$, while the fact that $\equiv_1$ is group-preserving implies $H = H_1$. Thus, $H_2 = H$ and $\equiv_2$ is also group-preserving.

A well-known algorithm due to Stallings implies that a digraph always has a greatest group-preserving equivalence relation. We now proceed to give a description of this equivalence relation, starting with the following definition.

Definition 3.1. The *Stallings equivalence* of G is the least equivalence relation on $\mathcal{V}(G)$ closed under the two following rules:

(F) If x, y are related, and (x,a,x'), (y,a,y') are edges in G, then x' and y' are also related.
(F') If x, y are related, and (x',b,x), (y',b,y) are edges in G, then x' and y' are also related.

We denote the Stallings equivalence by $\equiv_S$.

Fig. 3 The rules defining Stallings equivalence. The arrows represent edges, the thick lines represent existing relations, and the dashed lines represent the relations deduced from each rule.

An illustration of the rules (F) and (F') may be found in Fig. 3. Note that if two equivalence relations are closed under either rule (F) or (F'), then so is their intersection (this follows immediately from the definitions). Moreover, the total relation $\mathcal{V}(G) \times \mathcal{V}(G)$ is trivially closed under the two rules. Hence, the relation $\equiv_S$ is simply the intersection of all equivalence relations on $\mathcal{V}(G)$ that are closed under (F) and (F').

By a *trivially-labelled path*, we mean a path whose label is the identity element of $F(A)$. The next result relates Stallings equivalence with trivially-labelled paths, and can be seen as a reformulation of Stallings algorithm.

Proposition 3.2. *Let G be a connected digraph. The equivalence $\equiv_S$ is, simultaneously,*

(1) the equivalence relation induced by trivially-labelled paths;
(2) the greatest group-preserving equivalence of G.

For the proof of this result, the following definition will be useful: given an equivalence relation $\equiv$ on $\mathcal{V}(G)$, an *$\equiv$-path* in G is a sequence of edges $p = (e_1, \dots, e_k)$ satisfying $\alpha(e_{i+1}) \equiv \omega(e_i)$. The notions of *label* and *length* extend in a straightforward way to $\equiv$-paths. We also use the notation $p\colon x \xrightarrow{u} y$ for $\equiv$-paths, to mean $\alpha(p) \equiv x$, $\omega(p) \equiv y$ and $\lambda(p) = u$. Finally, we adopt the convention that an $\equiv$-path of length 0 is a pair $x \equiv y$.

Proof of Proposition 3.2. (1). Let us denote by $\sim$ the relation induced by trivially-labelled paths and by $\approx$ the relation induced by trivially-labelled $\equiv_S$-paths. Clearly $\sim$ is contained in $\approx$. Let us show that $\approx$ is contained in $\equiv_S$.

We proceed by induction on the length of the trivially-labelled $\equiv_S$-path. Note that by definition, an $\equiv_S$-path of length 0 is nothing but a pair $x \equiv_S y$, so the basis of the induction is trivial. Let us suppose that there is a trivially-labelled $\equiv_S$-path $p\colon x \to y$ of length $k \geq 1$. Write $p = (e_1, \dots, e_k)$. Since p is trivially-labelled, k is even and there must exist i such that $\lambda(e_i) = a^{-1}$ and $\lambda(e_{i+1}) = a$, where a is either a letter, or the inverse of a letter. Write $e_i = (u', a^{-1}, u)$ and $e_{i+1} = (v, a, v')$, where $u \equiv_S v$. If $a \in A$, then we may use rule (F) to conclude $u' \equiv_S v'$. Otherwise, one uses rule (F') to obtain the same conclusion. It follows that $p' = (e_1, \dots, e_{i-1}, e_{i+2}, \dots, e_k)$ is also a trivially-labelled $\equiv_S$-path between x and y. Since p' has length $k-2 < k$, we conclude by induction that $x \equiv_S y$.

We finish the proof of (1) by showing that $\equiv_S$ is contained in $\sim$. By definition of $\equiv_S$, it suffices to show that $\sim$ is closed under the rules (F) and (F'). Suppose that $x \sim y$ and that there are two edges $e = (x, a, x')$ and $f = (y, a, y')$. Consider a trivially-labelled path $p\colon x \to y$. Then, the composition $e^{-1}pf$ is a trivially-labelled path in G between x' and y'. Thus, $x' \sim y'$, which proves $\sim$ is closed under (F). The proof for (F') is similar.

(2). We first show that $\equiv_S$ is a group-preserving equivalence relation, and then we show it is the greatest. Let us fix any path $p\colon x/{\equiv_S} \to y/{\equiv_S}$ in the quotient $G/{\equiv_S}$. We say that an $\equiv_S$-path q in G *lifts* p if $q\colon x' \to y'$ with $x \equiv_S x'$, $y \equiv_S y'$ and $\lambda(p) = \lambda(q)$. Note that any path in the quotient $G/{\equiv_S}$ admits such a lift in G. If $q = (e_0, \dots, e_k)$ lifts p, we put $D(q) = \{0 \le i < k : \omega(e_i) \ne \alpha(e_{i+1})\}$. Clearly, q is a path if and only if $D(q)$ is empty. Assume $j = \max(D(q))$, and consider a trivially-labelled path $r\colon \omega(e_j) \to \alpha(e_{j+1})$ in G, which we know exists by Part (1). Let $q = q_1q_2$ be the factorization of q where $|q_1| = j+1$. Then, $q' = q_1rq_2$ is an $\equiv_S$-path between x' and y' satisfying $\lambda(q') = \lambda(q)$ and $D(q') = D(q) \setminus \{j\}$. Thus, we may assume that q is a path. Composing on both ends with trivially-labelled paths $x \to x'$ and $y' \to y$, we get a lift of p which is a path between x and y in G. This result applied to loops shows that $\equiv_S$ is group-preserving.

Finally, let us suppose that $\equiv$ is another group-preserving congruence, and let $x \equiv y$. Choose any path $p\colon x \to y$. Then $p/{\equiv}$ is a loop over $y/{\equiv}$ in $G/{\equiv}$. Since $\equiv$ is group-preserving, there is a loop q over y with $\lambda(q) = \lambda(p/{\equiv}) = \lambda(p)$. It follows that pq^{-1} is a trivially-labelled path between x and y, so $x \equiv_S y$. $\square$

From now on, we will use the three equivalent descriptions of $\equiv_S$ interchangeably.

4 Rauzy graphs

Recall that we defined the two maps init and tail by $\mathrm{init}(x) = x[0 : |x|-1]$ and $\mathrm{tail}(x) = x[1 : |x|]$. For $k \in \mathbb{N}$, let us also define the map eval_k by $\mathrm{eval}_k(x) = x(k)$. Note that init and tail are defined on A^+, while eval_k is defined on $A^{>k}$.

Definition 4.1. Let L be a recurrent language on A and $m,k \in \mathbb{N}$ with $k \le m$. The *k-labelled Rauzy graph* of level m of L is the digraph $G_{m,k}$ defined by the diagram:

$$\begin{tikzcd} & L \cap A^{m+1} \arrow[dl, "\mathrm{eval}_k"'] \arrow[dr, shift left, "\mathrm{init}"] \arrow[dr, shift right, "\mathrm{tail}"'] & \\ A & & L \cap A^m \end{tikzcd}$$

Special cases of these labelled Rauzy graphs have appeared in the literature, including in [22] with $k = m$, and in [12] with $m = 2k$.

The maps init, tail and eval_k used to define the Rauzy graphs are jointly injective, and moreover the following diagrams commute:

$$\begin{tikzcd} A^{\ge 2} \arrow[r, "\mathrm{init}"] \arrow[d, "\mathrm{tail}"] & A^+ \arrow[d, "\mathrm{tail}"] \\ A^+ \arrow[r, "\mathrm{init}"] & A^* \end{tikzcd} \qquad \begin{tikzcd} A^{>k+1} \arrow[r, "\mathrm{init}"] \arrow[dr, "\mathrm{eval}_k"'] & A^{>k} \arrow[d, "\mathrm{eval}_k"] \\ & A \end{tikzcd} \qquad \begin{tikzcd} A^{>k+1} \arrow[r, "\mathrm{tail}"] \arrow[dr, "\mathrm{eval}_{k+1}"'] & A^{>k} \arrow[d, "\mathrm{eval}_k"] \\ & A \end{tikzcd}$$

Therefore, init and tail also define onto digraph morphisms for $m \ge 1$:

$$\begin{aligned} \mathrm{init}\colon G_{m,k} &\to G_{m-1,k} && (0 \le k \le m-1), \\ \mathrm{tail}\colon G_{m,k} &\to G_{m-1,k-1} && (1 \le k \le m). \end{aligned}$$

These morphisms will allow us to relate the groups defined the Rauzy graphs. In the next definition, we introduce a convenient notation for these groups.

Definition 4.2. Let (u,v) be such that $uv \in L$, $|u| = k$ and $|u|+|v| = m$. We denote by $H_{u,v}$ the group of $G_{m,k}$ at uv. We call $H_{u,v}$ a *Rauzy group* of L.

The fact that tail and init define digraph morphisms immediately implies that:

$$H_{u,v} \leq H_{\mathrm{tail}(u),v}, \quad H_{u,v} \leq H_{u,\mathrm{init}(v)}.$$

We further note that $H_{ua,v} = a^{-1}H_{u,av}a$. Since we are assuming that L is recurrent, the Rauzy graphs are connected: for $x,y \in L \cap A^m$, a word w such that $xwy \in L$ yields a path $x \to y$ in the Rauzy graph $G_{m,k}$, for every $m,k \in \mathbb{N}$ with $k \leq m$. Moreover, letting H, H' be the group of $G_{m,k}$ at x, y respectively, one finds that $H = gH'g^{-1}$ whenever g is the label of a path $x \to y$ in $G_{m,k}$. Hence, $H_{u,v}$ and $H_{u',v'}$ lie in the same conjugacy class whenever $|uv| = |u'v'|$.

5 Paths in suffix extension graphs

For this section, it is useful to introduce a local version of suffix-connectedness. We do this in the next definition.

Definition 5.1. Let $m,e \in \mathbb{N}$ with $1 \leq e \leq m+1$. We say that L is (m,e)*-suffix-connected* if for every $w \in L \cap A^m$, there exists $1 \leq d \leq e$ such that the natural embedding of $\mathbf{L}(w)$ in $\mathbf{E}_{d,d}(\mathrm{tail}^{d-1}(w))$ lies in a single connected component.

Remark 5.2. This local version of suffix-connectedness has the following feature: suppose that $1 \leq e \leq e' \leq m+1$ and that L is (m,e)-suffix-connected; then L is also (m,e')-suffix-connected. In particular, if we suppose that L is suffix-connected, then it must be $(m,m+1)$-suffix-connected for all $m \geq 1$.

The main result of this section is the following proposition, which is the main ingredient in the proof of Theorem 1.1:

Proposition 5.3. *Assume that L is recurrent and* $(m-1,e)$*-suffix-connected, where* $m \geq 1$ *and* $1 \leq e \leq m$. *Then,* $\ker(\mathrm{tail})$ *is a group-preserving equivalence relation of* $G_{m,k}$ *whenever* $e \leq k \leq m$.

The proof relies on the following lemma:

Lemma 5.4. *Let L be a recurrent language on A,* $m \in \mathbb{N}$, $0 \leq k \leq m$, $d \geq 1$ *and* $x \in L \cap A^{m+d}$. *Then there exists a path* p_x *in* $G_{m,k}$ *such that:*

$$p_x\colon \mathrm{init}^d(x) \xrightarrow{x[k:k+d]} \mathrm{tail}^d(x).$$

Proof. We proceed by induction on d. If $d = 1$, then x itself is an edge in $G_{m,k}$ providing the required path.

For the induction step, we assume that $d > 1$. Let $x' = \mathrm{init}(x)$ and $x'' = \mathrm{tail}^{d-1}(x)$. Note that $|x''| = |x| - d + 1 = m+1$, so x'' is an edge in $G_{m,k}$, which we see as a path of length 1. Moreover, the induction hypothesis gives us a path p' such that

$$p'\colon \mathrm{init}^{d-1}(x') \xrightarrow{x'[k:k+d-1]} \mathrm{tail}^{d-1}(x').$$

Recalling that init and tail commute, we find that:

$$\mathrm{tail}^{d-1}(x') = \mathrm{tail}^{d-1} \circ \mathrm{init}(x) = \mathrm{init} \circ \mathrm{tail}^{d-1}(x) = \mathrm{init}(x'').$$

Hence, p' and x'' are consecutive, and we may form the composition $p = p'x''$. Note that p is a path between $\mathrm{init}^d(x)$ and $\mathrm{tail}^d(x)$, as required. Moreover, the label of this path is given by:

$$x'[k : k+d-1]x''(k) = x[k : k+d-1]x(k+d-1) = x[k : k+d],$$

and this concludes the proof. □

We are now ready to prove the proposition above.

Proof of Proposition 5.3. Let us fix a pair of vertices identified by the digraph morphism $\mathrm{tail}\colon G_{m,k} \to G_{m-1,k-1}$, that is to say two words $ax, bx \in L \cap A^m$ where $x \in L \cap A^{m-1}$ and $a, b \in A$. We want to show $ax \equiv_S bx$, which amounts to find a trivially-labelled path in $G_{m,k}$ between ax and bx.

By assumption, there exists $d \leq e$ such that the natural embedding of $\mathbf{L}(x)$ in $\mathbf{E}_{d,d}(\mathrm{tail}^{d-1}(x))$ lies in one connected component. Let us write $y = \mathrm{tail}^{d-1}(x)$, and let u, v be the natural embeddings of $a, b \in \mathbf{L}(x)$ inside $\mathbf{E}_{d,d}(y)$. In other words, u and v satisfy $ax = uy$ and $bx = vy$. Let us consider a path in $\mathbf{E}_{d,d}(y)$ joining u and v. Since $\mathbf{E}_{d,d}(y)$ is bipartite, this path must have the following form:

$$u = s_0,\ t_0,\ s_1,\ t_1,\ \ldots,\ t_{j-1},\ s_j = v,$$

where $s_i \in \mathbf{L}_d(y)$, $t_i \in \mathbf{R}_d(y)$. The fact that this forms a path in $\mathbf{E}_{d,d}(y)$ means that, for each $0 \leq i < j$, we have:

$$s_i y t_i,\ s_{i+1} y t_i \in L.$$

Let us put $w_i = s_i y t_i$ and $z_i = s_{i+1} y t_i$. By Lemma 5.4, there exist paths:

$$p_i\colon \mathrm{init}^d(w_i) \xrightarrow{w_i[k:k+d]} \mathrm{tail}^d(w_i), \qquad q_i\colon \mathrm{init}^d(z_i) \xrightarrow{z_i[k:k+d]} \mathrm{tail}^d(z_i).$$

We notice that $\mathrm{init}^d(w_i) = s_i y$, $\mathrm{tail}^d(w_i) = y t_i = \mathrm{tail}^d(z_i)$, $\mathrm{init}^d(z_i) = s_{i+1} y$. Therefore, p_i, q_i^{-1} are consecutive and their composition is a path $s_i y \to s_{i+1} y$. Moreover, since $k \geq e \geq d$, it follows that

$$w_i[k : k+d] = (y t_i)[k-d : k] = z_i[k : k+d].$$

Therefore, $p_i q_i^{-1}$ is trivially-labelled. Composing these paths for $i = 0, \ldots, j-1$ gives us a trivially-labelled path between $ax = uy = s_0 y$ and $s_j y = vy = bx$. □

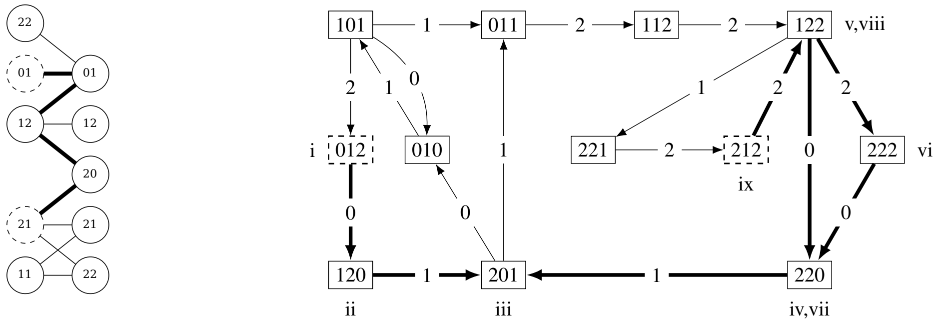
We give in Fig. 4 a concrete example of a trivially-labelled path in a Rauzy graph which is induced by a path in a suffix extension graph.

Combining Proposition 5.3 with Remark 5.2, we deduce that for each $m \geq 1$, the map tail defines a group-preserving morphism:

$$\mathrm{tail}\colon G_{m,m} \to G_{m-1,m-1}.$$

But clearly, the class of all group-preserving morphisms is closed under composition. Therefore, in a suffix-connected language, the following is a group-preserving morphism for all $m \geq 1$:

$$\mathrm{tail}^{m-1}\colon G_{m,m} \to G_{1,1}.$$



$\mathbf{E}_{2,2}(\mathrm{tail}(12))$ $G_{3,3}$

Fig. 4 A trivially-labelled path between a pair of words in $\ker(\mathrm{tail})$ induced by a path in a depth 2 suffix extension graph. The Roman numerals indicate the order in which the vertices are visited in the Rauzy graph. This takes place in the language defined by the primitive substitution $0 \mapsto 12, 1 \mapsto 2, 2 \mapsto 01$.

We immediately deduce the following:

Corollary 5.5. *Let L be a suffix-connected recurrent language and $u \in L$ with $u \neq \varepsilon$. Then $H_{u,\varepsilon} = H_{b,\varepsilon}$, where b is the last letter of u.*

Let us highlight another particular case of this result. The condition of being $(m,1)$-suffix-connected is equivalent to being m-connected, meaning that $\mathbf{E}(w)$ is connected for all $w \in L \cap A^m$, which in turn is equivalent to the dual condition of being $(m,1)$-prefix-connected. Combining Proposition 5.3 with its dual for the special case $e = 1$, we obtain the following result, which is reminiscent of [22, Proposition 4.2]:

Corollary 5.6. *If L is a $(m-1)$-connected recurrent language, where $m \geq 1$, then:*

(1) For $0 \leq k \leq m-1$, $\ker(\mathrm{init})$ is a group-preserving equivalence relation of $G_{m,k}$.
(2) For $1 \leq k \leq m$, $\ker(\mathrm{tail})$ is a group-preserving equivalence relation of $G_{m,k}$.

6 Return sets

Let us recall that the *return set to (u,v) in L* is the set of all words $r \in L$ such that $urv \in L$, urv starts and ends with uv, and contains exactly two occurrences of uv. We denote this set by $\mathcal{R}_{u,v}$. For basic properties of return sets, see [35].

Definition 6.1. Let (u,v) be such that $uv \in L$. The subgroup of $F(A)$ generated by $\mathcal{R}_{u,v}$ is denoted by $K_{u,v}$. We call this a *return group* of L.

Our main result for this section relates the return groups with the Rauzy groups.

Proposition 6.2. *Let L be a recurrent language and let u,v be such that $uv \in L$.*

(1) $K_{u,v} \leq H_{u,v}$.
(2) If $\mathcal{R}_{u,v}$ is finite and s is one of its longest elements, then $H_{u,sv} \leq K_{u,v}$.

The following lemma recalls several properties of Rauzy graphs that will be relevant. By a *positive path*, we mean a path which consists only of edges in $\mathcal{E}(G)$ or, equivalently, which contains no formal inverses. We say that two words are *suffix-comparable* if one is a suffix of the other, and dually that they are *prefix-comparable* if one is a prefix of the other.

Lemma 6.3. *Let L be a recurrent language and let u,v be such that $uv \in L$, $|u| = k$ and $|u| + |v| = m$.*

(1) Any element $w \in L$ is the label of a positive path in $G_{m,k}$.
(2) Any label w of a positive path in $G_{m,k}$ of length at most $m+1$ is in L.
(3) If $p\colon x \to uv$ is a positive path in $G_{m,k}$, then $\lambda(p)$ is suffix-comparable with u. Moreover, there is at least one such path satisfying $\lambda(p) = u$.
(4) If $q\colon uv \to y$ is a positive path in $G_{m,k}$, then $\lambda(q)$ is prefix-comparable with v. Moreover, there is at least one such path satisfying $\lambda(q) = v$.

All of these properties follow from the definition of $G_{m,k}$ in a straightforward manner. Parts (1) and (2) are standard and can be found for instance in [22, Section 4.1]. Parts (3) and (4) are analogous to [12, Lemma 4.5].

We are now ready to prove the proposition. Let us mention that Part (2) of the proposition is inspired by the proof of [22, Theorem 4.7], which relied partly on the fact that return sets of the form $\mathcal{R}_{u,\varepsilon}$ are prefix codes. However, this property no longer holds for general return sets and we had to find a way to avoid it. This is essentially what is accomplished by the very last paragraph of the proof.

Proof of Proposition 6.2. (1). Let $k = |u|$, $m = |u| + |v|$, and fix $r \in \mathcal{R}_{u,v}$. Then $urv \in L$ is the label of a positive path p in $G_{m,k}$ by Part (1) of Lemma 6.3. Consider the factorization $p = q_1 p' q_2$, where $\lambda(q_1) = u$, $\lambda(p') = r$ and $\lambda(q_2) = v$. Write $\alpha(p') = x_1$ and $\omega(p') = x_2$. Consider the factorization $x_1 = u_1 v_1$, where $|u_1| = k$. Since $\omega(q_1) = x_1$, it follows from Part (3) of Lemma 6.3 that u_1 is suffix-comparable with $\lambda(q_1) = u$. As $|u| = k = |u_1|$, we conclude that $u_1 = u$. Similarly, $\alpha(p'q_2) = x_1$, so Part (4) implies that v_1 is prefix-comparable with $\lambda(p'q_2) = rv$. Since $r \in \mathcal{R}_{u,v}$, the word rv starts with v, and since $|v| = m - k = |v_1|$, we conclude that $v_1 = v$. Thus, $x_1 = uv$. A similar argument yields $x_2 = uv$, so p' is a loop over uv, and $\mathcal{R}_{u,v} \subseteq H_{u,v}$. This proves (1).

(2). Let $m' = |u| + |s| + |v|$, and consider a positive path in $G_{m',k}$ of the form $p\colon uvx \to uvy$. We start by proving the following claim: $w = \lambda(p)$ is a concatenation of elements of $\mathcal{R}_{u,v}$.

To prove this claim, let us first consider two positive paths $q_1\colon x_1 \xrightarrow{u} uvx$ and $q_2\colon uvy \xrightarrow{v} x_2$, whose existence is a consequence of Part (3) and (4) of Lemma 6.3. Since $\alpha(pq_2) = uvx$, Part (4) of Lemma 6.3 implies that $\lambda(pq_2)$ is prefix-comparable with vx; thus, it starts with v. Similarly, since $\omega(q_1 p) = uvy$, Part (3) of Lemma 6.3 implies that $\lambda(q_1 p)$ is suffix-comparable with u; thus, it ends with u. In particular, this implies

$$uwv = \lambda(q_1)\lambda(pq_2) = \lambda(q_1 p)\lambda(q_2) \in uvA^* \cap A^*uv.$$

We now prove the claim by induction on $|w| = |p|$. If $|w| \leq |s|$, then uwv is the label of the positive path $q_1 p q_2$ in $G_{m',k}$, which has length at most m'. Hence, Part (2) of Lemma 6.3 implies that $uwv \in L$. This, taken together with the fact that uwv belongs to $uvA^* \cap A^*uv$, implies that w is a concatenation of elements of $\mathcal{R}_{u,v}$. This establishes the basis of the induction.

For the inductive step, let us suppose that $|w| > |s|$. Let p' be the prefix of length m' of $q_1 p q_2$, and let $z = \lambda(p')$. By Part (2) of Lemma 6.3, $z \in L$. Moreover, $z \in uvA^*$, so it is prefix-comparable with some element of $u\mathcal{R}_{u,v}v$. But by assumption, $|z|$ is the maximal length of an element of $u\mathcal{R}_{u,v}v$. Therefore, it follows that z has at least two occurrences of uv. Since z is a proper prefix of uwv, we deduce that uwv has an occurrence of uv at position $0 < j < |s|$ (meaning that $uwv[j : j + |uv|] = uv$). Consider the factorization $p = p_1p_2$ where $|p_1| = j$, and let $x' = \omega(p_1) = \alpha(p_2)$. Since j is an occurrence of uv in $uwv = \lambda(q_1pq_2)$ and $|q_1p_1| = |u| + j$, it follows that $\lambda(q_1p_1)$ ends with u. Consider the factorization $x' = u'x''$, where $|u'| = |u|$. By Part (3) of Lemma 6.3, u' is suffix-comparable with $\lambda(q_1p_1)$, and since $|u'| = |u|$, it follows that $u' = u$. Similarly, the fact that j is an occurrence of uv in uwv, with $uwv = \lambda(q_1p_1p_2q_2)$ and $|q_1p_1| = |u| + j$, implies that $\lambda(p_2q_2)$ starts with v. By Part (4) of Lemma 6.3, it follows that x'' is prefix-comparable with $\lambda(p_2q_2)$, and hence with v. However, recall that $x' \in L \cap A^{m'}$ where $m' = |u| + |s| + |v|$:

$$|x''| = |x'| - |u| = |s| + |v| \geq |v|.$$

Therefore, v is a prefix of x'', and $x'' = vt$ for some word t. Hence, we conclude that p_1, p_2 satisfy:

$$p_1 \colon uvx \to uvt, \quad p_2 \colon uvt \to uvy.$$

Since $0 < j < |s| < |w|$, we have $|p_1| < |p|$ and $|p_2| < |p|$. Thus, by the induction hypothesis, both $\lambda(p_1)$ and $\lambda(p_2)$ are product of words in $\mathcal{R}_{u,v}$. And, therefore, so is w. This finishes the proof of the claim.

We finish the proof of Part (2) of the proposition by showing that it follows from that claim. First, recall that $G_{m',k}$ is *strongly connected*, in the sense that any two vertices can be joined by a positive path. Moreover, the groups of a strongly connected digraph are generated by the labels of positive loops [70, Corollary 4.5]. Since the claim above shows in particular that the labels of positive loops over usv in $G_{m',k}$ lie in $K_{u,v}$, the result follows. □

7 Proof of the main result

Let us first recall the statement of our main result, Theorem 1.1: if L is a suffix-connected uniformly recurrent language on A, then all the return groups of L lie in the same conjugacy class and their rank is $n - c + 1$, where $n = \mathrm{Card}(A)$ and c is the number of connected components of $\mathbf{E}(\varepsilon)$.

The proof is split in two lemmas. In the first one, we apply the results obtained in the previous sections to show that (under the assumptions of Theorem 1.1) all the return groups of L belong to the same conjugacy class. The second lemma finishes the proof by showing that the groups in this conjugacy class have rank $n - c + 1$.

Lemma 7.1. *Let L be a uniformly recurrent suffix-connected language. Then, the return groups of L lie in the conjugacy class of subgroups of $F(A)$ generated by the groups of the Rauzy graph $G_{1,1}$.*

Proof. Consider a pair (u, v) such that $uv \in L$ and $uv \neq \varepsilon$. By Corollary 5.5, $H_{uv,\varepsilon} = H_{b,\varepsilon}$, where b is the last letter of uv. Using the conjugacy relation between Rauzy groups, we then have:

$$H_{u,v} = vH_{uv,\varepsilon}v^{-1} = vH_{b,\varepsilon}v^{-1},$$

and this equality holds for any such pair (u, v).

Since L is uniformly recurrent, the set $\mathcal{R}_{u,v}$ must be finite and we may choose an element $s \in \mathcal{R}_{u,v}$ of maximum length. By Proposition 6.2, we obtain:

$$H_{u,sv} \leq K_{u,v} \leq H_{u,v}.$$

(F) (F')

Fig. 5 The rules (F) and (F') as they appear in the proof of Lemma 7.2 when showing that $\equiv_S \subseteq \sim$.

Applying the conclusion of the previous paragraph to the pair u, sv while noting that $s \in K_{u,v} \leq H_{u,v}$, we get:

$$H_{u,sv} = svH_{b,\varepsilon}v^{-1}s^{-1} = sH_{u,v}s^{-1} = H_{u,v}.$$

Hence, $K_{u,v} = H_{u,v} = vH_{b,\varepsilon}v^{-1}$. $\square$

The next lemma concludes the proof of Theorem 1.1. It also gives an effective way of computing the Stallings equivalence of $G_{1,1}$ and, in turn, the Stallings equivalence can be used to find a basis for any of the groups defined by $G_{1,1}$.

Lemma 7.2. *Let L be a recurrent language. Then, the groups of the Rauzy graph $G_{1,1}$ have rank $n-c+1$, where $n = \mathrm{Card}(A)$ and c is the number of connected components of $\mathbf{E}(\varepsilon)$.*

Proof. A well-known consequence of Stallings algorithm is that the rank of any group generated by a connected digraph G is

$$\mathrm{Card}(\mathcal{E}(G/{\equiv_S})) - \mathrm{Card}(\mathcal{V}(G/{\equiv_S})) + 1$$

(see [48, Lemma 8.2]). Thus, we need only to show that the quotient $G_{1,1}/{\equiv_S}$ has c vertices and n edges.

Let us start by showing that $G_{1,1}/{\equiv_S}$ has c vertices. By definition, we have $\mathcal{V}(G_{1,1}) = A = \mathbf{L}(\varepsilon)$. Let $\sim$ be the relation defined as follow: for $a, b \in A$, we have $a \sim b$ exactly when, viewed as elements of $\mathbf{L}(\varepsilon)$, a and b lie in the same connected component of $\mathbf{E}(\varepsilon)$. Note that the relation $\sim$ has precisely c classes because every connected component of $\mathbf{E}(\varepsilon)$ contains at least one vertex in $\mathbf{L}(\varepsilon)$. Therefore, it suffices to show that $\sim \, = \, \equiv_S$.

We now prove the inclusion $\sim \, \subseteq \, \equiv_S$. Since $\mathbf{E}(\varepsilon)$ is bipartite, any path in $\mathbf{E}(\varepsilon)$ between elements of $\mathbf{L}(\varepsilon)$ has even length, and thus it suffices to argue for elements related by paths of length 2. Let us assume that $a, b \in \mathbf{L}(\varepsilon) = A$ are related by a path of length 2 inside $\mathbf{E}(\varepsilon)$. By definition of $\mathbf{E}(\varepsilon)$, the existence of such a path means that there is some $d \in A$ such that $ad, bd \in L$. But recall that $\mathcal{E}(G_{1,1}) = L \cap A^2$, so we may view $e = ad$ and $f = bd$ as edges in $G_{1,1}$, both of which have label d. The path (e, f^{-1}) is then a trivially-labelled path between a and b, so $a \equiv_S b$ as required.

Let us prove the inclusion $\equiv_S \, \subseteq \, \sim$. By definition of $\equiv_S$, we only need to show that $\sim$ is closed under the two rules (F) and (F'). We argue for each separately, as illustrated in Fig. 5. Let us fix $a, b, a', b' \in A$ with $a \sim b$.

(F) We assume that there are edges $e \colon a \to a'$, $f \colon b \to b'$ such that $\lambda(e) = \lambda(f)$. Note that the maps tail and eval_1 agree on A^2, so by definition $\omega = \lambda$ in the Rauzy graph $G_{1,1}$. Thus, $a' = b'$ and $a' \sim b'$ trivially.

(F') We assume that there are edges $e \colon a' \to a$, $f \colon b' \to b$ such that $\lambda(e) = \lambda(f)$. Since $\omega = \lambda$ in $G_{1,1}$, we deduce that $a = b$. By definition, $\mathcal{E}(G_{1,1}) = L \cap A^2$, $e = a'a \in L$ and $f = b'b = b'a \in L$.

In particular, there is an edge in $\mathbf{E}(\varepsilon)$ joining a' and a, and another one joining b' and a; by definition, $a' \sim b'$.

It only remains to show that $G_{1,1}/{\equiv_S}$ has n edges. We do this by showing that the labelling map $\lambda\colon G_{1,1}/{\equiv_S} \to A$ is a bijection. Fix a letter $a \in A$. Since L is recurrent, there exists $b \in A$ with $ba \in L$. Hence, there is at least one edge labelled a in $G_{1,1}$, and therefore also in $G_{1,1}/{\equiv_S}$. Hence, $\lambda\colon G_{1,1}/{\equiv_S} \to A$ is surjective. Now suppose that $G_{1,1}$ has two edges e, f labelled a. As noted before, $\lambda = \omega$ in $G_{1,1}$, so $\omega(e) = a = \omega(f)$. Applying rule (F'), we conclude that $\alpha(e) \equiv_S \alpha(f)$. In particular, $e/{\equiv_S} = f/{\equiv_S}$, which proves that the labelling map $\lambda\colon G_{1,1}/{\equiv_S} \to A$ is injective. $\square$

8 Proof of the corollaries

Let us start this section by recalling the statement of Corollary 1.2: if L is suffix-connected and uniformly recurrent, then the following statements are equivalent:

(1) All the return sets of L generate the full free group $F(A)$.
(2) Some return set of L generates a group of rank $\mathrm{Card}(A)$.
(3) The extension graph of the empty word is connected.

Proof of Corollary 1.2. (1) implies (2). Trivial.

(2) implies (3). By Theorem 1.1, all return groups of L have rank $n-c+1$ where c is the number of connected components of $\mathbf{E}(\varepsilon)$ and $n = \mathrm{Card}(A)$. Under the assumption (2), we therefore have $n = n-c+1$ and $c = 1$.

(3) implies (1). If $\mathbf{E}(\varepsilon)$ is connected, then by Corollary 5.6, there is a group-preserving morphism $G_{1,1} \to G_{0,0}$. But note that $G_{0,0}$ has a single vertex with loops labelled by the letters of A. Thus, the group generated by $G_{0,0}$ is equal to the full free group $F(A)$, and so are all the groups of the level 1 Rauzy graph $G_{1,1}$. But recall that, for a suffix-connected language, all the return groups lie in the conjugacy class generated by the level 1 Rauzy groups (see Lemma 7.1), and so the result follows. $\square$

Before proving Corollary 1.3, we need some preliminary material. A word $w \in L$ is called *neutral* if:

$$1 - \chi(\mathbf{E}(w)) = 0,$$

where $\chi(\mathbf{E}(w))$, the characteristic of $\mathbf{E}(w)$, is the difference between the number of vertices and edges in $\mathbf{E}(w)$. A *neutral language* is a language in which all non-empty words are neutral. The next result, quoted from [33, Corollary 5.4], will be useful to prove Corollary 1.3.

Lemma 8.1. *If L is recurrent and neutral, then for all u, v with $uv \in L$,*

$$\mathrm{Card}(\mathcal{R}_{u,v}) = \mathrm{Card}(A) - \chi(\mathbf{E}(\varepsilon)) + 1.$$

With this lemma in mind, let us recall the statement of Corollary 1.3: if L is uniformly recurrent, connected and neutral, then the following statements are equivalent:

(1) Some return set of L is a free subset of the free group $F(A)$.
(2) All return sets of L are free subsets of the free group $F(A)$.
(3) L is a tree set.

Proof of Corollary 1.3. We first recall the following fact, which is a straightforward consequence of the well-known Hopfian property of $F(A)$: a finite subset of $F(A)$ is free if and only if its cardinality agrees with the rank of the subgroup it generates. Moreover, note that under our assumptions, the return sets of L all have the same cardinality (by Lemma 8.1), as well as the same rank (by Theorem 1.1). Therefore if *some* return set is free, then *all* return sets are free, that is to say (1) and (2) are equivalent.

To prove the equivalence of (2) and (3), we use the following fact about graphs: a simple graph G is a forest if and only if it has exactly $\chi(G)$ connected components [27, Exercise 2.1.7 (b)]. On the one hand, this implies that in a connected neutral language, the extension graph of any non-empty word must be a tree (since neutrality implies $\chi(\mathbf{E}(w)) = 1$). Thus, a neutral connected language is a tree set if and only if $\mathbf{E}(\varepsilon)$ is a forest, if and only if $\chi(\mathbf{E}(\varepsilon)) = c$, where c denotes the number of connected components of $\mathbf{E}(\varepsilon)$. This is also equivalent to the following equality:

$$\mathrm{Card}(A) - \chi(\mathbf{E}(\varepsilon)) + 1 = \mathrm{Card}(A) - c + 1.$$

Let us fix u, v with $uv \in L$. Lemma 8.1 implies that $\mathrm{Card}(\mathcal{R}_{u,v})$ is equal to the left-hand side of the previous equation, while Theorem 1.1 implies that $\mathrm{rank}(K_{u,v})$ is equal to the right hand side. Since (2) holds exactly when $\mathrm{Card}(\mathcal{R}_{u,v}) = \mathrm{rank}(K_{u,v})$ for all such u, v, the result follows. □

9 Suffix-connected example

This section is devoted to the proof of Theorem 1.4. We consider the following substitution on the alphabet $A = \{0, 1, 2\}$:

$$\varphi\colon 0 \mapsto 0001,\ 1 \mapsto 02,\ 2 \mapsto 001.$$

Note that φ is primitive (since for every $a, b \in A$, a occurs in $\varphi^3(b)$), and that $\varphi(A)$ is a *prefix code* (no word in $\varphi(A)$ is a proper prefix of another). In particular, this implies that φ is injective, a fact that will be used several times. We recall that the *language* defined by φ is the subset of all words $w \in A^+$ such that w is a factor of $\varphi^n(a)$ for some $a \in A$ and $n \in \mathbb{N}$. For the current section, L denotes the language of φ. As we already mentioned, it is well known that the language of a primitive substitution is uniformly recurrent. We will show that L is suffix-connected, and deduce that all the return sets of L generate the full free group $F(A)$.

The proof, being a bit lengthy, is organized in 5 steps. Let us give a quick outline of each step:

(1) We show that every right special factor x of length at least 2 either ends with 00 and satisfies $\mathbf{R}(x) = \{0, 1\}$; or ends with 10 and satisfies $\mathbf{R}(x) = \{0, 2\}$. Similarly, we show that every left special factor x of length at least 3 either starts with 000 and satisfies $\mathbf{L}(x) = \{1, 2\}$; or starts with 001 and satisfies $\mathbf{L}(x) = \{0, 1\}$.

(2) We show that L contains only four bispecial factors starting with 001 and we compute them.

(3) We show that if x is a bispecial factor that starts with 000, then

$$\mathbf{E}(x) \cong \begin{cases} \mathbf{E}(\varphi(x)0) & \text{if } x \text{ ends with } 00, \\ \mathbf{E}(\varphi(x)00) & \text{if } x \text{ ends with } 10. \end{cases}$$

(4) We define inductively a sequence of words $(w_k)_{k\in\mathbb{N}}$ of increasing lengths, and we show that the disconnected elements of L are precisely the members of that sequence.
(5) We define a sequence of integers $(d_k)_{k\in\mathbb{N}}$ such that $\mathbf{L}(w_k)$ embeds in one connected component of $\mathbf{E}_{d_k,d_k}(\mathrm{tail}^{d_k-1}(w_k))$.

Some of these steps involve the computation of the sets $L\cap A^k$ for several values of k, some of them quite large. We will omit the details of these computations and provide only the results. These computations can be checked either by hand (e.g. with the algorithm described in [20, Section 3.2]), or perhaps more appropriately using SageMath [68]. At the time of writing, a SageMath web interface can be accessed at the address https://sagecell.sagemath.org. To compute the set $L\cap A^k$, simply evaluate the following line of code in the web interface:

```
WordMorphism({0:[0,0,0,1],1:[0,2],2:[0,0,1]}).language(k).
```

Step 1

We prove the following claim.

Claim. Let x be a right special factor of L of length at least 2. Then one of the two following alternatives hold:

(1) x ends with 00 and $\mathbf{R}(x)=\{0,1\}$.
(2) x ends with 10 and $\mathbf{R}(x)=\{0,2\}$.

Dually, let y be a left special factor of L of length at least 3. Then one of the two following alternatives hold:

(1) y starts with 000 and $\mathbf{L}(y)=\{1,2\}$.
(2) y starts with 001 and $\mathbf{L}(y)=\{0,1\}$.

Proof of the claim. Direct computations reveal that:

$$L\cap A^3=\{000,001,010,020,100,102,200\}.$$

Hence, the only two right special factors in $L\cap A^2$ are 00 and 10, and they satisfy respectively:

$$\mathbf{R}(00)=\{0,1\},\qquad \mathbf{R}(10)=\{0,2\}.$$

Since the sets $\mathbf{R}(x)$ are weakly increasing under taking suffixes, the first part follows.

Similarly, we find:

$$L\cap A^4=\{0001,0010,0100,0102,0200,1000,1001,1020,2000\}.$$

Therefore $L\cap A^3$ contains only two left special factors, 000 and 001, satisfying respectively:

$$\mathbf{L}(000)=\{1,2\},\qquad \mathbf{L}(001)=\{0,1\}.$$

Since the sets $\mathbf{L}(x)$ are weakly increasing under taking prefixes, the second part follows as well. $\square$

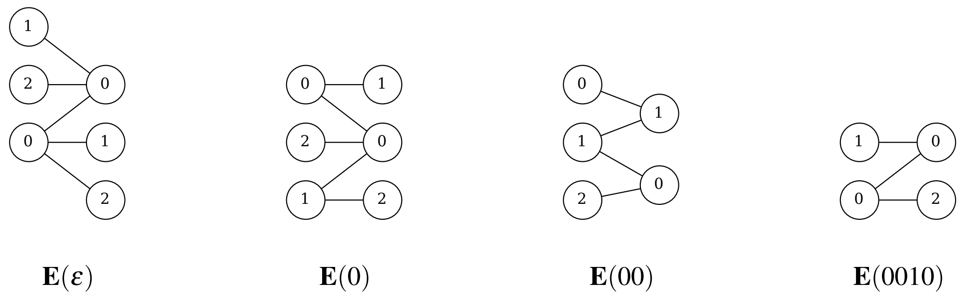


Fig. 6 Extension graphs of all the bispecial words of length at most 4 in L.

Step 2

We now know that all long enough bispecial factors must start with either 000 or 001, and end with either 00 or 10. We restrict the possibilities even further by proving the following claim:

Claim. The only four bispecial factors of L starting with 001 are:

$$0010, \quad 00100, \quad 00100010, \quad 001000100010.$$

The proof of this claim makes use of the concept of *cutting points*, by which we mean the following: in a word of the form $\varphi(z)$, a cutting point is an index $0 \leq j \leq |\varphi(z)| - 1$ such that $j = |\varphi(z_1)|$, for some prefix z_1 of z. We observe that in the specific case of φ, the cutting points are located exactly after the occurrences of the letters 1 and 2. The following elementary lemma will be useful.

Lemma 9.1. *Let $\varphi(z) = u_1 \dots u_n$ be a factorization such that $|u_1 \dots u_k|$ is a cutting point for all $1 \leq k < n$. Then there is a factorization $z = z_1 \dots z_n$ such that $\varphi(z_i) = u_i$ for all $1 \leq i \leq n$.*

Proof. By assumption, $u_1 \dots u_{j-1}, u_1 \dots u_j \in \varphi(A^*)$ for all $1 \leq j \leq n$. Since $\varphi(A)$ is a prefix code, we have $u_j \in \varphi(A^*)$ and we may write $u_j = \varphi(z_j)$ for some z_j. Then $\varphi(z) = \varphi(z_1 \dots z_n)$ and as φ is injective, $z = z_1 \dots z_n$ as required. □

Proof of the claim. Let us start by noting that the only bispecial factors of L with length at most 4 are:

$$\varepsilon, \quad 0, \quad 00, \quad 0010.$$

This can be proven simply by inspecting the sets $L \cap A^k$ for $2 \leq k \leq 6$. The extension graphs of these four words can be found in Fig. 6. From now on, we work only with bispecial factors of length at least 5.

Let us suppose that u is bispecial, $|u| \geq 5$ and 001 is a prefix of u. We distinguish two cases: $u = 001x10$ and $u = 001x00$.

We start by the case $u = 001x10$. Let $x' = x1$. By Step 1, we know that $0u, 1u \in L$. Thus, there exist $z_1, z_2 \in L$ such that, for some words s_1, t_1, s_2, t_2,

$$\varphi(z_1) = s_1 0001x'0t_1, \qquad \varphi(z_2) = s_2 1001x'0t_2.$$

Since $0000 \notin L$, it follows that s_1 ends with either 1 or 2. Therefore $|s_1|$ is a cutting point in $\varphi(z_1)$. Similarly, there is a cutting point in $\varphi(z_1)$ at the end of x'. It follows from Lemma 9.1 that z_1 has a

$\mathbf{E}(0010)$ $\quad$ $\mathbf{E}(00100)$ $\quad$ $\mathbf{E}(00100010)$ $\quad$ $\mathbf{E}(001000100010)$

Fig. 7 Extension graphs of all bispecial factors of L starting with 001.

factor of the form $0y_1$ such that $\varphi(y_1) = x'$. With similar arguments, we conclude that z_2 has a factor of the form $2y_2$ such that $\varphi(y_2) = x'$. Since φ is injective, we find $y_1 = y_2 = y$, and $\mathbf{L}(y) \supseteq \{0,2\}$. By Step 1, it follows that $|y| < 3$, which means y must be one of the nine words in $L \cap A^{\leq 2}$. Further accounting for the fact that $2 \in \mathbf{L}(y)$ and $\varphi(y) \neq \varepsilon$, we narrow it down to only two possibilities, namely $y = 0$ and $y = 00$. Trying out both values, we obtain either:

$$u = 001\varphi(0)0 = 00100010; \text{ or}$$
$$u = 001\varphi(00)0 = 001000100010.$$

A direct computation shows that both of those words are bispecial.

Finally, we treat the case $u = 001x00$. By Step 1, $u0 = 001x000 \in L$. Since $0000 \notin L$, it follows that x cannot end with 0. Moreover, we also have $0u, 1u, u1 \in L$, so there exist $z_1, z_2, z_3 \in L$ such that:

$$\varphi(z_1) = s_1 0001x00t_1, \quad \varphi(z_2) = s_2 1001x00t_2, \quad \varphi(z_3) = s_3 001x001t_3,$$

for some words s_i, t_i ($i = 1,2,3$). Again, since $0000 \notin L$, s_1 cannot end with 0. Recalling that cutting points are located exactly after the occurrences of 1 or 2, we apply Lemma 9.1 to conclude that there exist: a factor of z_1 of the form $0y_1$ such that $\varphi(y_1) = x$; a factor of z_2 of the form $2y_2$ such that $\varphi(y_2) = x$; and a factor of z_3 of the form $y_3 2$ such that $\varphi(y_3) = x$. Since φ is injective, $y_1 = y_2 = y_3 = y$, and $\mathbf{L}(y) \supseteq \{0,2\}$, $2 \in \mathbf{R}(y)$. By Step 1, we conclude that $|y| < 3$, which again leaves us with nine possible values for y. Accounting for the fact that $2 \in \mathbf{R}(y)$ and $2 \in \mathbf{L}(y)$ narrows this to only two possibilities: $y = \varepsilon$ and $y = 0$. Testing both possibilities, we find that $y = 0$ does not yield a bispecial factor, leaving us with only one bispecial factor for that case:

$$u = 001\varphi(\varepsilon)00 = 00100.$$

All in all, we exhausted all cases and found four bispecial factors:

$$0010,\ 00100,\ 00100010,\ 001000100010.$$

This proves the claim. $\square$

We give the extension graphs of these four bispecial factors in Fig. 7. The longest among these, which has length 12, is the only one which is disconnected. We also saw that all the bispecial factors of L of length at most 4 are connected, and it is not hard from there to complete the picture and show that 001000100010 is both the *longest bispecial factor starting with 001* and the *smallest disconnected factor* of L. This can be done by explicit computations for the only three missing bispecial factors of length at most 12, which are 00010, 000100 and 000100010.

Step 3

Next, we give conditions ensuring stability of some extension graphs under $x \mapsto \varphi(x)0$ or $x \mapsto \varphi(x)00$.

Claim. Let x be a bispecial factor of L starting with 000. Then:

$$\mathbf{E}(x) \cong \begin{cases} \mathbf{E}(\varphi(x)0) & \text{if } x \in A^*00 \\ \mathbf{E}(\varphi(x)00) & \text{if } x \in A^*10. \end{cases}$$

Proof of the claim. Let us put:

$$y = \begin{cases} \varphi(x)0 & \text{if } x \in A^*00 \\ \varphi(x)00 & \text{if } x \in A^*10. \end{cases}$$

Let σ be the permutation of $A = \{0,1,2\}$ fixing 0 and exchanging 1, 2. We readily deduce from Step 1 that $\sigma(a)$ is a suffix of $\varphi(a)$, for all $a \in \mathbf{L}(x)$. Similarly, if $x \in A^*00$, then $0\sigma(b)$ is a prefix of $\varphi(b)$, for all $b \in \mathbf{R}(x)$; and if $x \in A^*10$, then $00\sigma(b)$ is a prefix of $\varphi(b)$, for all $b \in \mathbf{R}(x)$. In particular, $\sigma(a)y\sigma(b)$ is a factor of $\varphi(axb)$. Thus,

$$axb \in L \implies \varphi(axb) \in L \implies \sigma(a)y\sigma(b) \in L.$$

This shows that σ defines a graph morphism $\mathbf{E}(x) \to \mathbf{E}(y)$, which we also denote σ, and that y is bispecial. Moreover, it follows from Step 1 that σ is bijective on vertices. It remains only to show that σ is onto on edges.

Let us suppose that $\sigma(a)y\sigma(b) \in L$ for $a,b \in A$. We need to show that $axb \in L$. The fact that $\sigma(a)y\sigma(b) \in L$ implies that, for certain words s,t,

$$\exists z \in L,\ \varphi(z) = s\sigma(a)y\sigma(b)t.$$

Note that $y = \varphi(x)0$ or $\varphi(x)00$. In both cases, $\varphi(x)$ is a prefix of y ending with 1 or 2. Moreover, we have $\sigma(a) \in \{1,2\}$ by Step 1. Thus, in the factorization $s\sigma(a)y\sigma(b)t$ given above, there must be one cutting point at the start of y, and one at the end of $\varphi(x)$. By Lemma 9.1, this implies that z has a factor of the form $cx'd$, where $c,d \in A$ and:

(1) $\varphi(x') = \varphi(x)$;
(2) $\sigma(a)$ is a suffix of $\varphi(c)$;
(3) $\varphi(d)$ starts with $0\sigma(b)$ if $x \in A^*00$; or $00\sigma(b)$ if $x \in A^*10$.

Injectivity of φ implies $x = x'$, so $c \in \mathbf{L}(x)$ and $d \in \mathbf{R}(x)$. Using Step 1, we can then deduce from a case-by-case analysis that $a = c$ and $b = d$. This proves that σ is onto on edges, thus finishing the proof. □

Step 4

Recall that the longest bispecial factor of L that starts with 001 is also its smallest disconnected element. We will see that *all* disconnected elements of L arise from this word. Consider the sequence of words $\{w_k\}_{k\in\mathbb{N}}$ defined by:

$$w_0 = 001000100010, \qquad w_{k+1} = \begin{cases} \varphi(w_k)00 & \text{if } k \text{ is even;} \\ \varphi(w_k)0 & \text{if } k \text{ is odd.} \end{cases}$$

For the purpose of the proof below, it is useful to notice that w_k ends with 10 if k is even, and with 00 if k is odd. We now prove the following claim.

Claim. A word $w \in L$ is disconnected if and only if $w = w_k$ for some $k \in \mathbb{N}$.

Proof. We already saw that w_0 is disconnected, and one can check via explicit computations that so is w_1. Since w_k starts with 000 whenever $k \geq 1$, it follows from Step 3 that w_k is disconnected for all $k \in \mathbb{N}$.

For the converse, we proceed by induction on $|w|$. The smallest disconnected word, w_0, provides the basis for the induction. Let us consider a disconnected word $w \in L$ such that $|w| > |w_0| = 12$. Since w_0 is also the longest bispecial factor starting with 001 (see Step 2), we may assume that w starts with 000.

We start by treating the case $w \in A^*00$. By Step 1, we know that:

$$\mathbf{L}(w) = \{1,2\}, \quad \mathbf{R}(w) = \{0,1\}.$$

Let us write $w = w'00$. Since $w0 \in L$, it follows that w' cannot end with 0. Let us consider $z_1, z_2, z_3, z_4 \in L$ such that,

$$\varphi(z_1) = s_1 2 w t_1, \quad \varphi(z_2) = s_2 1 w t_2, \quad \varphi(z_3) = s_3 w 0 t_3, \quad \varphi(z_4) = s_4 w 1 t_4,$$

for certain words s_i, t_i ($i = 1,2,3,4$). By repeatedly applying Lemma 9.1, we deduce that:

- z_1 has a factor of the form $1x_1$ such that $\varphi(x_1) = w'$.
- z_2 has a factor of the form ax_2 such that $\varphi(x_2) = w'$ and $a \in \{0,2\}$.
- z_3 has a factor of the form $x_3 0$ such that $\varphi(x_3) = w'$.
- z_4 has a factor of the form $x_4 2$ such that $\varphi(x_4) = w'$.

Since φ is injective, we deduce $x_1 = x_2 = x_3 = x_4 = x$, and x is bispecial. Note that $|x| \leq 2$ would imply $|w| = |\varphi(x)| + 2 \leq 10$, which is a contradiction. Thus, we may assume $|x| \geq 3$. Since 2 is a right extension of x, we deduce by Step 1 that $x \in A^*10$. By Step 4, $\mathbf{E}(x) \cong \mathbf{E}(\varphi(x)00) = \mathbf{E}(w)$; thus, x is disconnected. By induction, $x = w_k$ for some $k \in \mathbb{N}$, and since x ends with 10, k is even. Therefore $w = \varphi(w_k)00 = w_{k+1}$.

The case $w \in A^*10$ is handled in a similar fashion. Let us go quickly over the argument. This time, we have

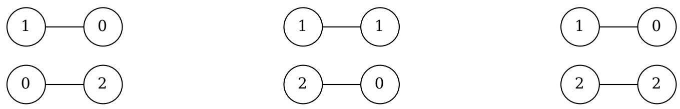
$$\mathbf{L}(w) = \{1,2\}, \quad \mathbf{R}(w) = \{0,2\}.$$

We write $w = w'0$. Take $z_1, z_2, z_3, z_4 \in L$ such that:

$$\varphi(z_1) = s_1 2 w t_1, \quad \varphi(z_2) = s_2 1 w t_2, \quad \varphi(z_3) = s_3 w 0 t_3, \quad \varphi(z_4) = s_4 w 2 t_4,$$

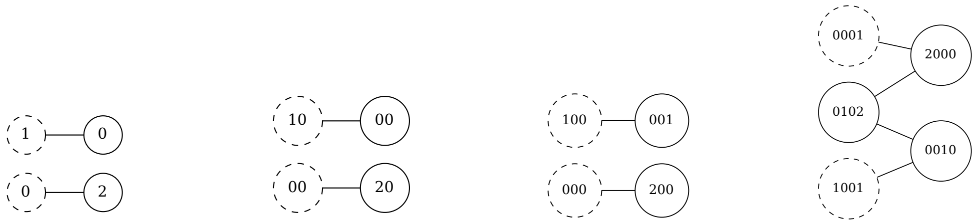
for certain words s_i, t_i ($i = 1,2,3,4$). Again, it follows from Lemma 9.1 that:

- z_1 has a factor of the form $1x_1$ such that $\varphi(x_1) = w'$.
- z_2 has a factor of the form ax_2 such that $\varphi(x_2) = w'$ and $a \in \{0,2\}$.
- z_3 has a factor of the form $x_3 b$ such that $\varphi(x_3) = w'$ and $b \in \{0,2\}$.
- z_4 has a factor of the form $x_4 1$ such that $\varphi(x_4) = w'$.



$\mathbf{E}(w_0)$ $\quad$ $\mathbf{E}(w_k), k \geq 1$ odd $\quad$ $\mathbf{E}(w_k), k \geq 1$ even

Fig. 8 Extension graphs of the disconnected words of L.



$\mathbf{E}_{1,1}(001000100010)$ $\quad$ $\mathbf{E}_{2,2}(01000100010)$ $\quad$ $\mathbf{E}_{3,3}(1000100010)$ $\quad$ $\mathbf{E}_{4,4}(000100010)$

Fig. 9 Suffix extension graphs of $w_0 = 001000100010$ at depth up to 4. The dashed vertices represent the natural embeddings of $\mathbf{L}(w_0)$.

By injectivity of φ, we have $x_1 = x_2 = x_3 = x_4 = x$ and x is bispecial. Moreover, $|x| \leq 2$ would imply $|w| = |\varphi(x)| + 1 \leq 9$, which contradicts our standing assumption that $|w| > 12$. Thus, we may assume $|x| \geq 3$. Since 1 is a right extension of x, it follows from Step 1 that x ends with 00, so by Step 3, $\mathbf{E}(x) \cong \mathbf{E}(\varphi(x)0) = \mathbf{E}(w)$. This implies that x is disconnected, so by induction $x = w_k$ for some $k \in \mathbb{N}$. As x ends with 00, k is odd and $w = \varphi(w_k)0 = w_{k+1}$. $\square$

This, combined with the graph isomorphism identified in Step 3, allows us to explicitly compute the extension graphs of all the disconnected words of L. These extension graphs are shown in Fig. 8.

Step 5

Now that we know exactly which are the disconnected words of L, it remains to show that these words are suffix-connected. For $k \in \mathbb{N}$, let us write $d_k = |\varphi^k(001)| + 1$ and $y_k = \mathrm{tail}^{d_k - 1}(w_k)$. This means that $w_k = \varphi^k(001)y_k$ and the depth d_k suffix extension graph of w_k is precisely $\mathbf{E}_{d_k,d_k}(y_k)$. For the case $k = 0$, we have $d_0 = 4$ and $y_0 = 000100010$. Notably, the depth 4 suffix extension graph of w_0, which is shown in Fig. 9, is connected, hence w_0 is suffix-connected at depth 4. We will show that w_k is suffix-connected at depth d_k for all $k \in \mathbb{N}$.

Let us first note that the natural embedding of $\mathbf{L}(w_k)$ in $\mathbf{E}_{d_k,d_k}(y_k)$ is given by right multiplication by $\varphi^k(001)$. Before concluding the proof of Theorem 1.4, we need to establish the following technical lemma, which gives some properties of the words $x_k = \mathrm{init}(\varphi^k(2))$.

Lemma 9.2. *For all $k \in \mathbb{N}$, the following hold:*

(1) $x_{k+1} = \begin{cases} \varphi(x_k)00 & \text{if } k \text{ is even;} \\ \varphi(x_k)0 & \text{if } k \text{ is odd.} \end{cases}$

(2) $x_k 0$ *is a prefix of* $\varphi^k(0)$.

Proof. (1). If k is even, then $\varphi^k(2) = x_k2$ and $\varphi^{k+1}(2) = x_{k+1}1$. It follows that

$$x_{k+1}1 = \varphi(x_k2) = \varphi(x_k)001.$$

Hence, the result follows. Similarly, if k is odd, $\varphi^k(2) = x_k1$, $\varphi^{k+1}(2) = x_{k+1}2$, and

$$x_{k+1}2 = \varphi(x_k1) = \varphi(x_k)02.$$

(2). We proceed by induction on k. The basis, $k = 0$, is obvious. Let us assume $\varphi^k(0) = x_k0t_k$, for some $t_k \in A^*$. Hence,

$$\varphi^{k+1}(0) = \varphi(x_k0t_k) = \varphi(x_k)0001\varphi(t_k) = \begin{cases} x_{k+1}01\varphi(t_k) & \text{if } k \text{ even;} \\ x_{k+1}001\varphi(t_k) & \text{if } k \text{ odd.} \end{cases} \qquad \square$$

By the recursive definition of w_k and a straightforward inductive argument involving Part (1) of the lemma, we have $\varphi^k(y_0)x_k = y_k$ for all $k \in \mathbb{N}$. Moreover, note that x_k is a prefix of both $\varphi^k(2000)$ and $\varphi^k(0010)$, the former by definition and the latter by Part (2) of the lemma. Given a prefix x of a word y, let us denote by $x^{-1}y$ the suffix of y of length $|y| - |x|$. Since 2000 and 0010 are right extensions of y_0 (see Fig. 9), it follows that $x_k^{-1}\varphi^k(2000)$ and $x_k^{-1}\varphi^k(0010)$ are right extensions of y_k. With these observations in mind, we are ready to conclude the proof of Theorem 1.4. We do this by establishing the following claim.

Claim. For $k \geq 1$, there is a path in $\mathbf{E}_{d_k,d_k}(y_k)$ between $1\varphi^k(001)$ and $2\varphi^k(001)$.

Proof of the claim. Consider the map $\sigma_k \colon \mathbf{E}_{d_0,d_0}(y_0) \to \mathbf{E}_{d_k,d_k}(y_k)$ defined as follows: an element $u \in \mathbf{L}_{d_0}(y_0) = \{0001, 0102, 1001\}$ is mapped to the suffix of length d_k of $\varphi^k(u)$, and an element $v \in \mathbf{R}_{d_0}(y_0) = \{2000, 0010\}$ is mapped to the prefix of length d_k of $x_k^{-1}\varphi^k(v)$. We first need to show that this map is well-defined. This amounts to show that $|\varphi^k(u)| \geq d_k$ for all $u \in \mathbf{L}(y_0)$, and $|\varphi^k(v)| - |x_k| \geq d_k$ for all $v \in \mathbf{R}(y_0)$. The former condition is obvious, and the latter boils down to a few computations:

$$\begin{aligned} |\varphi^k(0010)| - |x_k| &= |\varphi^k(001)| + |\varphi^k(0)| - |\varphi^k(2)| + 1 \\ &> |\varphi^k(001)| + 1 = d_k; \\ |\varphi^k(2000)| - |x_k| &= |\varphi^k(2000)| - |\varphi^k(2)| + 1 \\ &= |\varphi^k(000)| + 1 \\ &> |\varphi^k(001)| + 1 = d_k. \end{aligned}$$

Note that σ_k maps $\{0001, 1001\}$ onto the natural embedding of $\mathbf{L}(w_k)$. Since $\mathbf{E}_{d_0,d_0}(y_0)$ is connected, it suffices to show that σ_k defines a graph morphism. Take $u \in \mathbf{L}_{d_0}(y_0)$ and $v \in \mathbf{R}_{d_0}(y_0)$, and suppose that $uy_0v \in L$. Then, it follows that $\varphi^k(uy_0v) \in L$. Since $\sigma_k(u)$ is a suffix of u and $x_k\sigma_k(v)$ is a prefix of v, we conclude that $\sigma_k(u)y_k\sigma_k(v) = \sigma_k(u)\varphi^k(y_0)x_k\sigma_k(v)$ is a factor of $\varphi^k(uy_0v)$. Therefore, it must also be in L, and σ_k induces a graph morphism $\mathbf{E}_{d_0,d_0}(y_0) \to \mathbf{E}_{d_k,d_k}(y_k)$. $\square$

With some extra work, we were able to show that the map σ_k defined in the previous proof is in fact a graph isomorphism. To prove this, we made use of the following observation, which is a consequence of the Cayley-Hamilton theorem: for any word $x \in A^*$, the sequence $(|\varphi^k(x)|)_{k\in\mathbb{N}}$ follows the linear recurrence determined by the characteristic polynomial of φ. This is a general observation which holds for any substitution, and we believe it could be useful for establishing suffix-connectedness in harder cases.

10 Conclusion

Let us end this paper by suggesting a few ideas for future research.

Firstly, we feel that the proof presented in Section 9, on account of its ad-hoc and technical nature, is somewhat unsatisfactory. We hope it could be improved.

Question 10.1. Is there a more systematic approach to show that a given language is suffix-connected?

In particular, it could be interesting to study other examples of suffix-connected languages defined by primitive substitutions, and see how much of Section 9 can be recycled. According to our computations, the languages defined by the following primitive substitutions are likely to be suffix-connected while also having infinitely many disconnected elements:

$$0 \mapsto 12,\ 1 \mapsto 2,\ 2 \mapsto 01;$$
$$0 \mapsto 01,\ 1 \mapsto 2,\ 2 \mapsto 3,\ 3 \mapsto 02;$$
$$0 \mapsto 100,\ 1 \mapsto 032,\ 2 \mapsto 232,\ 3 \mapsto 03.$$

In [34], Dolce and Perrin introduced the notion of an *eventually dendric language*, which requires all but finitely many extension graphs to be trees. This suggests the analogous notion of an *eventually suffix-connected language*, in which all but finitely many words are suffix-connected.

Question 10.2. Can we find a generalization of Theorem 1.1 for eventually suffix-connected languages?

Finally, Dolce and Perrin also showed that the class of eventually dendric languages is closed under two operations, namely conjugacy and complete bifix decoding [34]. We wonder if analogous results hold for suffix-connected languages.

Question 10.3. Is the class of suffix-connected languages closed under complete bifix decoding or conjugacy?

Acknowledgements

The author is grateful for the financial support provided by the Centre for Mathematics of the University of Coimbra (UIDB/00324/2020, funded by the Portuguese Government through FCT/MCTES), the Centre for Mathematics of the University of Porto (UIDB/00144/2020, funded by the Portuguese Government through FCT/MCTES), as well as a PhD grant from FCT/MCTES (PD/BD/150350/2019).

Special thanks go to Jorge Almeida and Alfredo Costa for many helpful discussions and comments which greatly improved this paper.

Appendix A

Consequences of Paper 3

This appendix highlights some consequences of the results presented in Paper 3. We rely crucially on two key results of Almeida and Costa found in [12]. Section 1 of this appendix reviews some material from their paper, including the two results, which are stated below as Lemma 1.1 and Theorem 1.3. In Section 2, we use Lemma 1.1 to study the group projections of the maximal subgroups corresponding to suffix-connected minimal shift spaces, that is, minimal shift spaces whose languages are suffix-connected in the sense of Paper 3, Definition 2.3. We deduce that proper relative freeness of the Schützenberger group never occurs in this case. (By *proper relative freeness*, we simply mean relative freeness in the absence of absolute freeness.) We then proceed to state a freeness criterion for Schützenberger groups of suffix-connected minimal shift spaces based on Theorem 1.3, generalizing Almeida and Costa's proof that dendric minimal shift spaces have free Schützenberger groups [12, Theorem 6.5]. We conclude the appendix by giving a simple condition for invertibility of primitive aperiodic substitutions that define suffix-connected shift spaces.

1 Two results of Almeida and Costa

We start by recalling some relevant material from [12, Section 3]. Let A be a finite alphabet and $X \subseteq A^{\mathbb{Z}}$ be a minimal shift space. Let $L(X) \subseteq A^*$ be the language of X. We denote by $J(X)$ the $\mathcal{J}$-class corresponding to X, which is given by the formula

$$J(X) = \overline{L(X)} \setminus A^*,$$

where $\overline{L(X)}$ denotes the closure $L(X)$ in the free profinite monoid $\widehat{A^*}$.

As is customary, we refer to the elements of $\widehat{A^*}$ as *pseudowords*. Recall that infinite pseudowords $w \in \widehat{A^*} \setminus A^*$ have a well-defined right-infinite prefix and a well-defined left-infinite suffix, denoted by $\overrightarrow{w}$ and $\overleftarrow{w}$ respectively. Using this, we define a mapping $\widehat{A^*} \setminus A^* \to A^{\mathbb{Z}}$ by $w \mapsto \overleftarrow{w} \cdot \overrightarrow{w}$. Then, two elements of $J(X)$ are $\mathcal{H}$-equivalent if and only if they take the same value under this mapping. Moreover, an $\mathcal{H}$-class $H \subseteq J(X)$ is a maximal subgroup precisely when its elements map to an element of X. Hence, the following defines a bijection between X and the maximal subgroups of $J(X)$:

$$x \mapsto \{w \in J(X) : x = \overleftarrow{w} \cdot \overrightarrow{w}\}.$$

See [12, Lemma 3.2]. Let us denote by G_x the maximal subgroup of $J(X)$ corresponding to $x \in X$. The groups G_x all give, up to isomorphism, the same profinite group $G(X)$, called the *Schützenberger group* of X. Extending the convention used in Paper 3, for $i \leq j \in \mathbb{Z}$ and $x = (x_k)_{k\in\mathbb{Z}} \in A^{\mathbb{Z}}$, we let $x[i:j] = x_i \cdots x_{j-1}$. For $n \geq 1$ and $x \in X$, we let $\mathcal{R}_n(x)$ be the set of return words to $(x[-n:0], x[0:n])$ in $L(X)$. We denote by $\overline{\langle W \rangle}$ the closed subsemigroup of $\widehat{A^*}$ generated by a subset $W \subseteq \widehat{A^*}$. The first of Almeida and Costa's results gives a description of the maximal subgroups G_x.

Lemma 1.1 ([12, Lemma 5.3])**.** *Let X be a minimal aperiodic shift space. Then, for every $x \in X$, we have $G_x = \bigcap_{n\geq 1} \overline{\langle \mathcal{R}_n(x) \rangle}$.*

Let $\widehat{F}(A)$ be the free profinite group over A and let $p_{\mathbf{G}} : \widehat{A^*} \to \widehat{F}(A)$ be the continuous epimorphism extending the canonical mapping $A \to \widehat{F}(A)$. We call $p_{\mathbf{G}}$ the *group projection*.

Remark 1.2. Since $p_{\mathbf{G}}$ is a continuous homomorphism of compact (Hausdorff) semigroups, it maps the closed subsemigroup generated by a given set $B \subseteq \widehat{A^*}$ to the closed subsemigroup of $\widehat{F}(A)$ generated by $p_{\mathbf{G}}(B)$, which is in fact a closed subgroup (see [19, Corollary 3.7.5]). In particular, it follows from the previous lemma that $p_{\mathbf{G}}(G_x)$ is the intersection of the closed subgroups of $\widehat{F}(A)$ generated by the sets $\mathcal{R}_n(x)$ for $n \geq 1$.

The relationship between G_x and its group projection $p_{\mathbf{G}}(G_x)$ is not always straightforward. The second result of Almeida and Costa gives conditions ensuring that they are isomorphic.

Theorem 1.3 ([12, Theorem 6.1])**.** *Let $X \subseteq A^{\mathbb{Z}}$ be a minimal aperiodic shift space, and take $x \in X$. Suppose there is a subgroup K of the free group $F(A)$ and an infinite set P of positive integers such that, for every $n \in P$, the set $\mathcal{R}_n(x)$ is a basis of K. Then, the restriction to G_x of the group projection $p_{\mathbf{G}}$ is a continuous isomorphism from G_x onto $\overline{K}$.*

Note that in the above theorem, K is a free group of finite rank, hence $\overline{K}$ is a free profinite group of equal rank (see for instance [19, Theorem 4.6.7]). Therefore, this result provides a sufficient condition for freeness of the Schützenberger group.

2 Group projections and freeness under suffix-connectedness

Lemma 1.1 implies that in a minimal aperiodic shift space X, the group projections of the maximal subgroups G_x for $x \in X$ are related with the collective behaviour of the return groups (see Remark 1.2). The fact that the return groups are so tightly constrained in suffix-connected minimal shift spaces thus leads to equally strong conclusions about the group projections of the corresponding maximal subgroups, as we proceed to show.

Let $X \subseteq A^{\mathbb{Z}}$ be a minimal aperiodic shift space. For convenience, we recall the notation for return groups introduced in Paper 3: given (u, v) with $uv \in L(X)$, we let $K_{u,v}$ be the subgroup of $F(A)$ generated by $\mathcal{R}_{u,v}$, the set of return words to (u, v) in $L(X)$. By analogy, given $x \in X$ and $n \geq 1$, we let $K_n(x)$ be the subgroup of $F(A)$ generated by $\mathcal{R}_n(x)$. It follows from Remark 1.2 that $p_{\mathbf{G}}(G_x) = \bigcap_{n\geq 1} \overline{K_n(x)}$.

Proposition 2.1. *Let X be a suffix-connected aperiodic minimal shift space over n letters. Then, for every $x \in X$ and $m \geq 1$, the equality $K_1(x) = K_m(x)$ holds. In particular, $p_{\mathbf{G}}(G_x)$ equals $\overline{K_1(x)}$ and is a free profinite group of rank $n - c + 1$, where c is the number of connected components of $\mathbf{E}(\varepsilon)$.*

Proof. Let $x[-1:1] = ab$, so $\mathcal{R}_1(x) = \mathcal{R}_{a,b}$ and $K_1(x) = K_{a,b}$. Recall that in the proof of the main result of Paper 3 (more precisely, in the proof of Lemma 7.1), we established that for all (u,v) with $uv \in L(X)$, the following equality holds:

$$K_{u,v} = vH_{d,\varepsilon}v^{-1},$$

where d is the last letter of uv and $H_{d,\varepsilon}$ is the Rauzy group corresponding to (d,ε). In particular, we have $K_1(x) = bH_{b,\varepsilon}b^{-1}$. Let $m \geq 1$ be such that $x[m-2:m] = ab$; by uniform recurrence, this holds for infinitely many m. Letting $r = x[0:m-1]$, it follows that r is a concatenation of return words to (a,b), hence it belongs to $K_1(x)$. We deduce:

$$K_m(x) = rbH_{b,\varepsilon}b^{-1}r^{-1} = rK_1(x)r^{-1} = K_1(x).$$

Hence, $K_m(x) = K_1(x)$ for infinitely many $m \geq 1$. Since $(K_m(x))_{m\geq 1}$ is a descending chain of subgroups, it follows that $K_m(x) = K_1(x)$ for all $m \geq 1$.

Combining Lemma 1.1 with the first part of this proposition, we obtain $p_{\mathbf{G}}(G_x) = \overline{K_1(x)}$. By the main result of Paper 3, the subgroup $K_1(x)$ is a free group of rank $n-c+1$, hence $\overline{K_1(x)}$ is a free profinite group of equal rank (see [19, Theorem 4.6.7]). $\square$

A closer look at the case where $\mathbf{E}(\varepsilon)$ is connected leads to the next corollary.

Corollary 2.2. *Let X be a suffix-connected aperiodic minimal shift space over an alphabet A with n letters. The following statements are equivalent.*

(1) For every $x \in X$, the group projection maps G_x onto $\widehat{F}(A)$.
(2) For some $x \in X$, the group projection of G_x is a free profinite group of rank n.
(3) The extension graph of the empty word is connected.

Proof. *(1) implies (2).* Trivial.

(2) implies (3). Taking into account Proposition 2.1, whenever (2) holds, we must have $n-c+1 = n$ where c is the number of connected components of $\mathbf{E}(\varepsilon)$, hence $c = 1$ and $\mathbf{E}(\varepsilon)$ is connected.

(3) implies (1). When $\mathbf{E}(\varepsilon)$ is connected, all the return sets generate the free group $F(A)$ by Corollary 1.2 of Paper 3, hence $p_{\mathbf{G}}(G_x) = \overline{F(A)} = \widehat{F}(A)$ for every $x \in X$ by Proposition 2.1. $\square$

Similar to what we did in Section 5 of Paper 1, we can also use Proposition 2.1 to deduce that, if the Schützenberger group of a suffix-connected minimal shift space is relatively free, then it must be absolutely free. In fact, we have the following more general result.

Corollary 2.3. *Let X be a suffix-connected aperiodic minimal shift space. Then, the only pseudovariety of finite groups $\mathbf{H}$ for which the Schützenberger group $G(X)$ is pro-$\mathbf{H}$ is the pseudovariety $\mathbf{G}$ of all finite groups. In particular, $G(X)$ is relatively free if and only if it is absolutely free.*

Proof. First, observe that in an aperiodic minimal shift space over n letters, the extension graph of the empty word must have strictly less than n connected components. Indeed, $\mathbf{E}(\varepsilon)$ having n connected components implies that $\mathrm{Card}(L(X)\cap A) = \mathrm{Card}(L(X)\cap A^2) = n$, which in turn implies periodicity by the Morse–Hedlund theorem [55, Theorem 7.3]. It follows from Proposition 2.1 that the Schützenberger group $G(X)$ admits a free profinite group of rank at least 2 as a continuous homomorphic image, and in particular, every 2-generated finite group is a continuous homomorphic image of $G(X)$. If $\mathbf{H}$ is a pseudovariety of finite groups for which $G(X)$ is pro-$\mathbf{H}$, then by standard properties of pro-$\mathbf{H}$ groups, all finite continuous homomorphic images of $G(X)$ must belong to $\mathbf{H}$ (see e.g., [67, Theorem 2.1.3]). Therefore, $\mathbf{H}$ contains all 2-generated finite groups, whence we deduce that $\mathbf{H} = \mathbf{G}$, for instance[1] by Lemma 5.4 of Paper 1. □

Therefore, when it comes to relative freeness, suffix-connected minimal shift spaces behave like shift spaces defined by primitive invertible substitutions (recall that a substitution over an alphabet A is called *invertible* when it induces an automorphism of the free group over A). These two families of shift spaces are incomparable: there are non-substitutive dendric, ergo suffix-connected, minimal shift spaces (e.g., by the main result of [62]), and there are primitive invertible substitutions whose shift spaces are not suffix-connected (e.g., the substitution found in Section 6 of Paper 1). Note however that a primitive substitution which defines a minimal dendric shift space must be invertible [26, Theorem 9]. A more general sufficient condition for invertibility of suffix-connected aperiodic substitutions is given at the end of the appendix (Corollary 2.8).

Theorem 1.3 gives a criterion for freeness whose scope goes beyond substitutive shift spaces. However, it requires a very detailed understanding of the return groups. When [12] was published, the only cases where this could be achieved were the dendric minimal shift spaces, wherein all return sets are bases of the free group over the alphabet of the shift space (the *Return Theorem* of Berthé et al. [23]). In that case, Theorem 1.3 always implies that the Schützenberger group is free over the alphabet of the shift space [12, Theorem 6.5]. More generally, Theorem 1.3 yields the following sufficient condition for freeness of the Schützenberger group in suffix-connected minimal shift spaces.

Proposition 2.4. *Let X be a suffix-connected aperiodic minimal shift space over n letters, and let c be the number of connected components of* $\mathbf{E}(\varepsilon)$. *If there is an element $x \in X$ and an infinite set P of positive integers such that* $\operatorname{Card}(\mathcal{R}_m(x)) = n - c + 1$ *for every $m \in P$, then $G(X)$ is a free profinite group of rank $n - c + 1$.*

Proof. By Proposition 2.1, all $K_m(x)$ with $m \geq 1$ are equal to $K_1(x)$, which is a free group of rank $n-c+1$ by the main result of Paper 3. Since all the sets $\mathcal{R}_m(x)$ with $m \in P$ generate $K_1(x)$ and have cardinality $n-c+1$ by assumption, it follows that they are all bases of $K_1(x)$ (see [52, Proposition 2.7]). We may then apply Theorem 1.3 to conclude that $p_{\mathbf{G}}$ restricts to an isomorphism $G_x \cong \overline{K_1(x)}$. □

The previous proposition has an interesting variation, stated below, which was pointed out to the author by Costa. In this variation, the infinite set of integers P is replaced by a single integer $m \geq 1$, making the criterion easier to utilize in practice. This comes at the price of restricting the scope of the criterion to shift spaces defined by primitive substitutions.

Let φ be a primitive substitution and $X(\varphi)$ be the shift space defined by φ. We call φ *suffix-connected* if $X(\varphi)$ is a suffix-connected shift space. Moreover, we abbreviate $G(X(\varphi))$ by $G(\varphi)$ and $L(X(\varphi))$ by $L(\varphi)$. Consider the natural action of φ on $A^{\mathbb{Z}}$, defined on a two-sided infinite word $x = \cdots x_{-2}x_{-1} \cdot x_0x_1 \cdots$ by

$$\varphi(x) = \cdots \varphi(x_{-2})\varphi(x_{-1}) \cdot \varphi(x_0)\varphi(x_1) \cdots .$$

[1] Alternatively, one could use Cayley's representation theorem together with the well-known fact that the finite symmetric groups are 2-generated.

We say that $x \in A^{\mathbb{Z}}$ is a *periodic point* of φ if $x = \varphi^k(x)$ for some $k > 0$. If x belongs to $X(\varphi)$, then we say that the periodic point is *admissible*. We note that every primitive substitution has at least one admissible periodic point (this is a consequence of [19, Proposition 5.5.10]).

Proposition 2.5 (A. Costa)**.** *Let φ be a primitive aperiodic suffix-connected substitution over n letters, and let c be the number of connected components of* $\mathbf{E}(\varepsilon)$*. If there is an admissible periodic point x of φ and an integer $m \geq 1$ such that* $\mathrm{Card}(\mathcal{R}_m(x)) = n - c + 1$*, then $G(\varphi)$ is a free profinite group of rank $n - c + 1$.*

Proof. Let $\widehat{\varphi}$ be the continuous endomorphism of the free profinite monoid $\widehat{A^*}$ that extends φ. We claim that $G_x = \overline{\langle \widehat{\varphi}^{\omega}(\mathcal{R}_m(x)) \rangle}$. Firstly, we have $\widehat{\varphi}^{\omega}(G_x) = G_x$ by [11, Theorem 5.6] and $G_x \subseteq \overline{\langle \mathcal{R}_m(x) \rangle}$ by Lemma 1.1, thus

$$G_x \subseteq \widehat{\varphi}^{\omega}(\overline{\langle \mathcal{R}_m(x) \rangle}) = \overline{\langle \widehat{\varphi}^{\omega}(\mathcal{R}_m(x)) \rangle}.$$

To establish the remaining inclusion, it suffices to show that for every $r \in \mathcal{R}_m(x)$, the pseudoword $w = \widehat{\varphi}^{\omega}(r)$ belongs to G_x. Because $r \in L(\varphi)$ and $\varphi(L(\varphi)) \subseteq L(\varphi)$, it follows that $w \in \overline{L(\varphi)}$. Moreover, letting $ab = x[-1:1]$, we have $r \in bA^* \cap A^*a$, hence $w \in \varphi^{n!}(b)\widehat{A^*} \cap \widehat{A^*}\varphi^{n!}(a)$ for every sufficiently large $n \in \mathbb{N}$. On the other hand, the fact that x is a periodic point of φ implies that for $n \in \mathbb{N}$ large enough,

$$x[-|\varphi^{n!}(a)| : 0] = \varphi^{n!}(a), \quad x[0 : |\varphi^{n!}(b)|] = \varphi^{n!}(b).$$

Therefore, $\overleftarrow{w} \cdot \overrightarrow{w} = x$, and so $w \in G_x$. This completes the proof of the claim.

The rest of the proof is an application of the Hopfian property, similar to what is done in the proof of [12, Theorem 6.1]. Recall that $p_{\mathbf{G}}|_{G_x}$, the restriction of $p_{\mathbf{G}}$ to G_x, is a continuous epimorphism onto the free profinite group $\overline{K_1(x)}$ of rank $n - c + 1$ (Proposition 2.1). By the above claim, G_x is generated as a profinite group by $n - c + 1$ elements, hence there is a continuous group epimorphism $\psi \colon \overline{K_1(x)} \to G_x$. The composite $\psi p_{\mathbf{G}}|_{G_x}$ is a continuous surjective endomorphism of G_x, and as finitely generated profinite groups enjoy the Hopfian property (see [67, Proposition 2.5.2] for instance), it is in fact an isomorphism. In particular, $\psi p_{\mathbf{G}}|_{G_x}$ is injective and so is $p_{\mathbf{G}}|_{G_x}$. □

Let us mention that the substitution studied in Appendix B defines a suffix-connected shift space with a free Schützenberger group which fails the freeness criteria given by the two previous propositions. Let us give an example where Proposition 2.5 does apply.

Example 2.6. Recall the primitive aperiodic substitution found in Paper 3,

$$\varphi \colon 0 \mapsto 0001, \ 1 \mapsto 02, \ 2 \mapsto 001.$$

It is suffix-connected (Theorem 1.4 of Paper 3) and the extension graph $\mathbf{E}(\varepsilon)$ is connected (Fig. 6 of Paper 3). Moreover, $\varphi^2(1)$ ends with 1 and $\varphi^2(0)$ starts with 0, hence φ admits a periodic point of the form

$$x = \cdots 1 \cdot 0 \cdots.$$

It is easily verified that this periodic point is admissible and that $\mathcal{R}_1(x) = \{001, 0001, 020001\}$, hence $G(\varphi)$ is a free profinite group of rank 3 by Proposition 2.5.

Corollary 2.3 hints at a relationship between suffix-connected shift spaces and primitive invertible substitutions. We conclude this appendix by presenting a sufficient condition for invertibility of primitive aperiodic suffix-connected substitutions, which arose from discussions between the author and Costa. It is derived from the more general result presented in the next proposition. Once again, the example of Appendix B shows that it is not a necessary condition.

Mossé's notion of recognizability, introduced in [56], plays a key role in what follows. We recall it here for convenience. Let φ be a substitution with a periodic point x of order k. Consider the set of cutting points of φ^k in x,

$$C(\varphi^k,x) = \{|\varphi^k(x[0:i])| : i \geq 0\} \cup \{-|\varphi^k(x[i:0])| : i \leq 0\}.$$

We say that φ is *recognizable for x* if there exists an integer $L \geq 0$ such that for every $i \in C(\varphi^k,x)$, the following holds:

$$\forall j \in \mathbb{Z}, \quad x[i-L:i+L] = x[j-L:j+L] \implies j \in C(\varphi^k,x).$$

The least integer with that property is called the *constant of recognizability* of φ for x. According to a celebrated theorem of Mossé, every primitive aperiodic substitution is recognizable for all of its admissible periodic points [56] (see also [19, Theorem 5.5.22]).

Proposition 2.7. *Let φ be a primitive aperiodic substitution over an alphabet A. Fix an admissible periodic point x of φ and let L be the constant of recognizability of φ for x. Suppose that for some integers $i_1, i_2 \geq L$, the words $u = x[-i_1:0]$ and $v = x[0:i_2]$ are such that $\mathcal{R}_{u,v}$ generates $F(A)$. Then, φ is invertible.*

Proof. Let l be the order of x as a periodic point of φ. As Almeida and Costa observed in the proof of [11, Proposition 5.5.], the assumption that $i_1, i_2 \geq L$ implies that $\mathcal{R}_{u,v} \subseteq \mathrm{Im}(\varphi^l)$. To see why, first note that every return word $r \in \mathcal{R}_{u,v}$ satisfies $r = x[j:k]$ for some $j < k \in \mathbb{N}$ such that

$$x[j-i_1 : j+i_2] = x[k-i_1 : k+i_2] = uv.$$

Since $i_1, i_2 \geq L$, we have $x[j-L:j+L] = x[k-L:k+L] = x[-L:L]$ and applying recognizability, we find $j,k \in C_\sigma(\varphi^l,x)$. Therefore, there exist $m < n \in \mathbb{N}$ such that $j = |\varphi^l(x[0:m])|$ and $k = |\varphi^l(x[0:n])|$, and this implies $r = \varphi^l(x[m:n])$.

Finally, since $\mathcal{R}_{u,v}$ generates $F(A)$, we deduce that the endomorphism of $F(A)$ induced by φ^l is surjective. Since finitely generated free groups have the Hopfian property (see [61, Theorem 41.52]), it follows that φ^l is invertible, hence so is φ. $\square$

In light of Corollary 1.2 from Paper 3, the following is a special case of the above proposition (recall also that every primitive substitution has at least one admissible periodic point).

Corollary 2.8. *Let φ be a primitive aperiodic suffix-connected substitution. If the extension graph of the empty word in $L(\varphi)$ is connected, then φ is invertible.*

This explains invertibility of the suffix-connected example found in Paper 3, but not of the substitution ψ presented in Appendix B. The following is a return substitution of ψ, and we conjecture it to be a primitive aperiodic suffix-connected substitution which is not invertible:

$$0 \mapsto 01,\ 1 \mapsto 02,\ 2 \mapsto 013,\ 3 \mapsto 01443,\ 4 \mapsto 0143.$$

Appendix B

Another suffix-connected example

This appendix is devoted to the following primitive substitution over the alphabet $\{0,1,2,3\}$:

$$\psi\colon 0 \mapsto 100,\ 1 \mapsto 032,\ 2 \mapsto 232,\ 3 \mapsto 03.$$

Our main purpose is to establish that the language $L(\psi)$ is suffix-connected. Our motivation for this is twofold: first, this example helps to clarify the strength of some of the results presented in Appendix A (see Remark 2.8 at the end of the current appendix). Second, it is a good opportunity to explore some ideas which allow for easier proofs of suffix-connectedness. Establishing our first suffix-connected example in Paper 3 involved a lot of tedious work, starting with a detailed examination of the bispecial factors of the language. After the publication of Paper 3, the author of these lines became aware of a paper of Klouda [49] which gives a much better method for tackling the latter task. In the first section of this appendix, we propose a comprehensive account of Klouda's algorithm, illustrated using our main example ψ. Section 2, contains the proof that $L(\psi)$ is suffix-connected. We rely on a technical lemma which makes use of the notion of $f_{\mathcal{B}}$-images, one of the central concepts in Klouda's algorithm. We conclude the appendix by studying the Schützenberger group of ψ, a straightforward task thanks to the main result from [11].

For the most part, we carry the notation over from Paper 3. We also rely on explicit computations of some of the sets $L(\psi)\cap A^k$, $k \in \mathbb{N}$, of which we simply give the outcome without further justifications. Such computations can easily be checked using SageMath [68]: recall that a web interface can be accessed at the address https://sagecell.sagemath.org, wherein the set $L \cap A^k$ can be computed by evaluating:

```
WordMorphism({0:[1,0,0],1:[0,3,2],2:[2,3,2],3:[0,3]}).language(k).
```

1 Klouda's algorithm

The purpose of this section is to give a detailed account of the algorithm devised by Klouda in his 2012 paper [49]. This algorithm allows to obtain a description of the bispecial factors in certain languages, namely circular non-pushy D0L languages. Klouda's work is formulated in the setting of D0L-systems, but for the purpose of this appendix, we may restrict ourselves to languages defined by primitive substitutions.

We start by recalling a few basic notions. Let φ be a primitive substitution. An *interpretation* of $w \in L(\varphi)$ is a triplet (t_1, v, t_2) such that $\varphi(v) = t_1 w t_2$ and $v \in L(\varphi)$. A *synchronizing point* of w is a pair (w_1, w_2) such that $w = w_1 w_2$ and for all interpretations (t_1, v, t_2), there is a pair (v_1, v_2) such that $t_1 w_1 = \varphi(v_1)$ and $w_2 t_2 = \varphi(v_2)$. An *encoding* is a substitution which is injective. Following Klouda's terminology, we say that φ is *circular* if it is an encoding and if there exists an integer $D > 0$, called the *synchronizing delay* such that every word in $L(\varphi) \cap A^{\geq D}$ has a synchronizing point. This should not be confused with the notion of *circular codes* found elsewhere in the literature (e.g., [21, 38]). As Klouda himself remarked in [49], Mossé's seminal work on recognizability [57] implies that primitive aperiodic encodings are circular.

Example 1.1. The substitution ψ is an encoding, and in fact a suffix encoding, meaning that no $\psi(a)$ for $a \in \{0, 1, 2, 3\}$ is a suffix of another. One can verify that it is aperiodic, using for instance [19, Exercise 5.15]. Moreover, ψ has synchronizing delay 3. This can be established by checking that the following are synchronizing points for each of the twelve words of length 3 in $L(\psi)$:

$$(00,0),\ (00,1),\ (0,03),\ (0,10),\ (\varepsilon,032),\ (\varepsilon,100),$$
$$(2,03),\ (2,10),\ (\varepsilon,232),\ (32,0),\ (32,1),\ (3,23).$$

The synchronizing delay is not 2 because the word 00 admits the interpretations $(1, 0, \varepsilon)$ and $(10, 03, 3)$ which, taken together, imply that 00 has no synchronizing point.

To devise his algorithm, Klouda introduced two key notions: *L-forky sets* and *R-forky sets*. We now proceed to recall them. Two words are *prefix-comparable* (*suffix-comparable*) if one is a prefix (suffix) of the other. Furthermore, we say that two pairs of words (u_1, u_2) and (v_1, v_2) are *R-aligned* (*L-aligned*) if there is a permutation σ of $\{1, 2\}$ such that u_i is prefix-comparable (suffix-comparable) with $v_{\sigma(i)}$ for every $i \in \{1, 2\}$. We also say that a pair (u_1, u_2) is a prefix (suffix) of (v_1, v_2) if, for some permutation σ of $\{1, 2\}$, u_i is a prefix (suffix) of $v_{\sigma(i)}$ for every $i \in \{1, 2\}$. Given a substitution φ, we define a mapping $f_R \colon A^* \times A^* \to A^*$ by letting $f_R(u, v)$ be the longest common prefix of $\varphi(u)$ and $\varphi(v)$. Dually, we let $f_L(u, v)$ be the longest common suffix of $\varphi(u)$ and $\varphi(v)$.

Definition 1.2 ([49, Definition 20])**.** Let φ be a primitive substitution and let $\mathcal{B}_R$ be a finite set of pairs of non-empty words in $L(\varphi)$. We say that $\mathcal{B}_R$ is an *R-forky set* (for φ) if it satisfies the following conditions:

(1) The components of every pair in $\mathcal{B}_R$ have distinct first letters.
(2) No two distinct elements of $\mathcal{B}_R$ are R-aligned.
(3) Every pair of non-empty words of $L(\varphi)$ with distinct first letters is R-aligned with a pair in $\mathcal{B}_R$.
(4) For every $(u_1, u_2) \in \mathcal{B}_R$, there exists $(v_1, v_2) \in \mathcal{B}_R$ such that

$$(f_R(u_1, u_2)v_1, f_R(u_1, u_2)v_2) \text{ is a prefix of } (\varphi(u_1), \varphi(u_2)).$$

Dually, a finite set $\mathcal{B}_L$ of pairs of non-empty words of $L(\varphi)$ is called *L-forky* if it satisfies the conditions

(1') The components of every pair in $\mathcal{B}_L$ have distinct last letters.
(2') No two distinct elements of $\mathcal{B}_L$ are L-aligned.
(3') Every pair of non-empty words of $L(\varphi)$ with distinct last letters is L-aligned with a pair in $\mathcal{B}_L$.
(4') For every $(u_1, u_2) \in \mathcal{B}_L$, there exists $(v_1, v_2) \in \mathcal{B}_L$ such that

$$(v_1 f_L(u_1, u_2), v_2 f_L(u_1, u_2)) \text{ is a suffix of } (\varphi(u_1), \varphi(u_2)).$$

Fig. 1 Graphs of left and right prolongations of ψ.

Importantly, every primitive aperiodic encoding admits an L-forky set and an R-forky set [49, Theorem 22]. Moreover, we observe that two pairs that are prefixes of the same pair must be R-aligned. Thus, for every $(u_1,u_2) \in \mathcal{B}_R$, the pair (v_1,v_2) given by (4) is unique; we denote it by $g_R(u_1,u_2)$. We define $g_L(u_1,u_2)$ in a dual manner.

Definition 1.3 ([49, Definition 24])**.** Let φ be a primitive aperiodic encoding with an R-forky set $\mathcal{B}_R$. The *graph of right prolongations* $\mathrm{GR}_\varphi^{(\mathcal{B}_R)}$ is the labelled digraph defined as follows:

- the vertex set of $\mathrm{GR}_\varphi^{(\mathcal{B}_R)}$ is $\mathcal{B}_R$;
- every $(u_1,u_2) \in \mathcal{B}_R$ has a unique outgoing edge, with terminus $g_R(u_1,u_2)$ and label $f_R(u_1,u_2)$.

The *graph of left prolongations* $\mathrm{GL}_\varphi^{(\mathcal{B}_L)}$ is defined dually. When the forky sets are clear from context, we write GL_φ and GR_φ for short.

In his paper, Klouda sketches a step-by-step procedure which allows to compute forky sets for primitive aperiodic substitutions [49, Example 21]. The starting point of this procedure is the observation that, given a linearly ordered finite alphabet $(A,\leq)$, the set $\{(a,b) : a < b \in A\}$ always satisfies Conditions (1)–(3) and (1')–(3') from Definition 1.3. Roughly speaking, by taking right or left extensions in $L(\varphi)$, this set may be gradually turned into an R-forky or L-forky set.

Example 1.4. Let us compute forky sets for the substitution ψ. The fact that ψ is a suffix encoding implies that

$$\mathcal{B}_L = \{(0,1),\ (0,2),\ (0,3),\ (1,2),\ (1,3),\ (2,3)\}$$

is already an L-forky set for ψ. It is not however an R-forky set: since $\psi(3)$ is a prefix of $\psi(1)$, the pair $(1,3)$ fails Condition (4) from Definition 1.3. To fix this, we observe that in $L(\psi)$, we have $\mathbf{R}(3) = \{2\}$ and $\mathbf{R}(1) = \{0\}$. Thus, when we replace $(1,3)$ by $(10,32)$, the resulting set still satisfies Conditions (1)–(3), and it now also satisfies Condition (4) since

$$(f_R(10,32)10, f_R(10,32)32) = (03210,03232) \text{ is a prefix of } (\psi(10),\psi(32)) = (032100,03232).$$

Therefore, the following is an R-forky set for ψ:

$$\mathcal{B}_R = \{(0,1),\ (0,2),\ (0,3),\ (1,2),\ (10,32),\ (2,3)\}.$$

The graphs GL_ψ and GR_ψ corresponding to these forky sets are given in Fig. 1.

Let φ be a primitive aperiodic encoding and take a bispecial factor $w \in L(\varphi)$. Then, there exist pairs of distinct letters (a_1,a_2) and (b_1,b_2) such that a_1wb_1 and a_2wb_2 belong to $L(\varphi)$. Given a choice of forky sets $\mathcal{B}_R$ and $\mathcal{B}_L$, we may apply the conditions (3) and (3') from Definition 1.3 to obtain pairs $(u_1,u_2) \in \mathcal{B}_L$ and $(v_1,v_2) \in \mathcal{B}_R$ such that $u_1wv_1, u_2wv_2 \in L(\varphi)$ or $u_1wv_2, u_2wv_1 \in L(\varphi)$. This motivates the next definition.

Definition 1.5 ([49, Definition 27])**.** Let φ be a primitive aperiodic encoding and let $\mathcal{B}_L$ and $\mathcal{B}_R$ be a choice of forky sets for φ. A *bispecial triplet* is an element $\mathcal{T} = ((u_1,u_2),w,(v_1,v_2))$ of $\mathcal{B}_L \times L(\varphi) \times \mathcal{B}_R$ such that $u_1wv_1, u_2wv_2 \in L(\varphi)$ or $u_1wv_2, u_2wv_1 \in L(\varphi)$.

In particular, given a primitive aperiodic substitution and a choice of forky sets $\mathcal{B}_L$, $\mathcal{B}_R$, the observation preceding the above definition may be formulated as follows: every bispecial factor of $L(\varphi)$ is the central component of a bispecial triplet. Let $\mathcal{B} = (\mathcal{B}_L, \mathcal{B}_R)$. By (4) and (4') from Definition 1.3, it follows that for every bispecial triplet $((u_1,u_2),w,(v_1,v_2))$, the following is again a bispecial triplet:

$$f_{\mathcal{B}}((u_1,u_2),w,(v_1,v_2)) = (g_L(u_1,u_2), f_L(u_1,u_2)\varphi(w)f_R(v_1,v_2), g_R(v_1,v_2)).$$

This defines a transformation $f_{\mathcal{B}}$ on the set of bispecial triplets, called the *$f_{\mathcal{B}}$-image*.

Example 1.6. With respect to the forky sets computed in Example 1.4, ψ admits a total of fourteen bispecial triplets with empty central components. However, we also observe that if $\mathcal{T}$ is such a bispecial triplet, then $f_{\mathcal{B}}(\mathcal{T})$ also has empty central component, unless $\mathcal{T}$ has either first component $(1,2)$ or last component $(10,32)$. Only three bispecial triplets with empty central components fit this description; their $f_{\mathcal{B}}$-images are as follows:

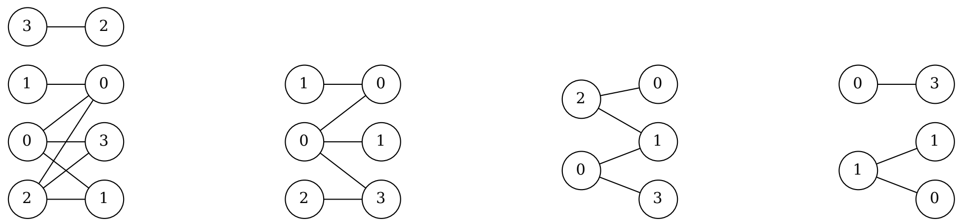
$$f_{\mathcal{B}}((1,2),\varepsilon,(0,1)) = f_{\mathcal{B}}((1,2),\varepsilon,(0,3)) = ((0,2),32,(0,1)),$$
$$f_{\mathcal{B}}((0,2),\varepsilon,(10,32)) = ((0,2),032,(10,32)).$$

In particular, for the purpose of understanding the non-empty bispecial factors of ψ, we may consider only two out of the fourteen bispecial triplets with empty central components.

The last ingredient in Klouda's algorithm is the observation that a bispecial triplet with a long enough central component is the $f_{\mathcal{B}}$-image of another bispecial triplet. To be more precise, Klouda notes, in the proof of [49, Theorem 36], that if φ is a primitive aperiodic encoding with synchronizing delay D, then a bispecial triplet whose central component satisfies $|w| \geq D$ is the $f_{\mathcal{B}}$-image of another bispecial triplet. In particular, there must exist a finite set ℓ of bispecial triplets such that every non-empty bispecial factor is the central component of $f_{\mathcal{B}}^n(\mathcal{T})$, for some $n \in \mathbb{N}$ and $\mathcal{T} \in \ell$. Once such a set ℓ has been chosen, we call its elements the *initial bispecial triplets*.

Example 1.7. Let us compute a set ℓ of initial bispecial triplets for ψ. In light of Example 1.1, it suffices to consider the bispecial triplets whose central components are the bispecial factors in $L(\psi)$ of length at most 2, of which there are four: ε, 0, 32 and 00. The extension graphs of these words are given in Fig. 2. By Example 1.6, the set ℓ needs to contain only two out of the fourteen bispecial triplets determined by ε, for instance $((1,2),\varepsilon,(0,1))$ and $((0,2),\varepsilon,(10,32))$. As for the words 0, 32 and 00, they define a total of ten bispecial triplets:

$$((0,1),0,(0,1)),\ ((0,1),0,(0,3)),\ ((1,2),0,(0,3)),\ ((0,2),0,(0,3)),\ ((0,2),0,(10,32)),$$
$$((0,2),32,(0,1)),\ ((0,2),32,(0,3)),\ ((0,2),32,(10,32)),$$
$$((0,1),00,(10,32)),\ ((0,1),00,(0,3)).$$



$\mathbf{E}(\varepsilon)$ $\mathbf{E}(0)$ $\mathbf{E}(32)$ $\mathbf{E}(00)$

Fig. 2 Extension graphs of the words ε, 0, 32 and 00 in $L(\psi)$.

i	$\mathcal{T}_i$	$f_{\mathcal{B}}(\mathcal{T}_i)$
1	$((1,2),\varepsilon,(0,1))$	$((0,2),32,(0,1))$
2	$((0,2),\varepsilon,(10,32))$	$((0,2),032,(10,32))$
3	$((0,1),0,(0,1))$	$((0,2),100,(0,1))$
4	$((1,2),0,(0,3))$	$((0,2),32100,(0,1))$
5	$((0,2),0,(10,32))$	$((0,2),100032,(10,32))$
6	$((0,1),00,(0,3))$	$((0,2),100100,(0,1))$
7	$((0,2),32,(10,32))$	$((0,2),03232032,(10,32))$
8	$((0,1),00,(10,32))$	$((0,2),100100032,(10,32))$

Table 1 Initial bispecial triplets of ψ and their $f_{\mathcal{B}}$-images.

However, for the purpose of computing non-empty bispecial factors, we may safely discard two of the triplets with central components 0, and two of those with central components 32, thanks to the following equalities:

$$f_{\mathcal{B}}((0,1),0,(0,1)) = f_{\mathcal{B}}((0,1),0,(0,3)) = f_{\mathcal{B}}((0,2),0,(0,1)),$$
$$f_{\mathcal{B}}((1,2),\varepsilon,(0,1)) = ((0,2),32,(0,1)) \quad \text{and} \quad f_{\mathcal{B}}((0,2),32,(0,1)) = f_{\mathcal{B}}((0,2),32,(0,3)).$$

Thus, we obtain the final set of eight initial bispecial triplets $\ell = \{\mathcal{T}_1,\dots,\mathcal{T}_8\}$ presented in Table 1. In particular, every bispecial factor of $L(\psi)$ appears as the central component of $f^n_{\mathcal{B}}(\mathcal{T}_i)$ for some $i \in \{1,\dots,8\}$ and $n \in \mathbb{N}$.

2 Suffix-connectedness and Schützenberger group of the main example

In this section, we take a closer look at our main example for this appendix, the substitution ψ. After proving our main result, which is stated in the next proposition, we proceed to study the Schützenberger group of ψ.

Proposition 2.1. *The language of the primitive substitution*

$$\psi\colon 0 \mapsto 100,\ 1 \mapsto 032,\ 2 \mapsto 232,\ 3 \mapsto 03$$

is suffix-connected.

The proof relies in large part on the classification of the bispecial factors of ψ obtained in the previous section. We also make use of a technical lemma, which is concerned with paths in suffix extension graphs of $f_{\mathcal{B}}$-images. Before stating the lemma, we introduce the following convenient notation: given a substitution φ, an integer $n \in \mathbb{N}$ and a pair of words (u,v), we let $f_R^{(n)}(u,v)$ be the longest common prefix of $\varphi^n(u)$ and $\varphi^n(v)$; we define $f_L^{(n)}(u,v)$ dually. Note that $f_L^{(1)}$ and $f_R^{(1)}$ are just f_L and f_R, and that $f_L^{(0)}(u,v) = \varepsilon$ (respectively $f_R^{(0)}(u,v) = \varepsilon$) whenever (u,v) belongs to an L-forky set (respectively an R-forky set).

Lemma 2.2. *Let φ be a primitive aperiodic encoding. Fix a choice of forky sets for φ and let $\mathcal{T} = ((u_1,u_2),w,(v_1,v_2))$ be a bispecial triplet. Suppose that there exists an integer $1 \leq d \leq |w|+1$ and a finite sequence of words*

$$\mathbf{s} = (s_0 = u_1 w[0:d-1],\ t_0,\ \ldots,\ s_k,\ t_k,\ s_{k+1} = u_2 w[0:d-1]),$$

satisfying the following properties for every $i \in \{0,\ldots,k\}$:

(1) t_i starts with v_1 or v_2;
(2) $s_i \operatorname{tail}^{d-1}(w) t_i,\ s_{i+1} \operatorname{tail}^{d-1}(w) t_i \in L(\varphi)$;
(3) $|\varphi^n(s_i)| > |f_L^{(n)}(u_1,u_2)| + |\varphi^n(w[0:d-1])|$, for all $n \in \mathbb{N}$;
(4) $|\varphi^n(t_i)| > |f_L^{(n)}(u_1,u_2)| + |\varphi^n(w[0:d-1])| + |f_R^{(n)}(v_1,v_2)|$, for all $n \in \mathbb{N}$.

Then, for every $n \in \mathbb{N}$, there is a path between the natural embeddings of the last letters of $g_L^n(u_1,u_2)$ in the depth d_n suffix extension graph of the central component of $f_{\mathcal{B}}^n(\mathcal{T})$, where $d_n = |f_L^{(n)}(u_1,u_2)| + |\varphi^n(w[0:d-1])| + 1$.

Proof. Fix $n \in \mathbb{N}$. By (3), we may consider for every $i \in \{0,\ldots,k+1\}$ the suffix $s_{n,i}$ of $\varphi^n(s_i)$ of length d_n. Moreover, it follows from (1) that $f_R^{(n)}(v_1,v_2)$ is a prefix of $\varphi^n(t_i)$, hence there is a factorization $\varphi^n(t_i) = f_R^{(n)}(v_1,v_2) t'_{n,i}$. By (4), we consider the prefix $t_{n,i}$ of $t'_{n,i}$ of length d_n. Let $x_n = \varphi^n(w[0:d-1])$ and w_n be the central component of $f_{\mathcal{B}}^n(\mathcal{T})$. It follows from [49, Lemma 31] that

$$w_n = f_L^{(n)}(u_1,u_2)\varphi^n(w) f_R^{(n)}(v_1,v_2).$$

In particular, $f_L^{(n)}(u_1,u_2)x_n$ is the prefix of length $d_n - 1$ of w_n, and thus

$$\operatorname{tail}^{d_n-1}(w_n) = \varphi^n(\operatorname{tail}^{d-1}(w)) f_R^{(n)}(v_1,v_2).$$

We claim that the following is a path between the natural embeddings of the last letters of $g_L^n(u_1,u_2)$ in the depth d_n suffix extension graph of w_n:

$$\mathbf{s}_n = (s_{n,0},\ t_{n,0},\ \ldots,\ s_{n,k},\ t_{n,k},\ s_{n,k+1}).$$

Indeed, we have for every $i \in \{0,\ldots,k+1\}$ that $s_{n,i} \operatorname{tail}^{d_n-1}(w_n) t_{n,i}$ is a prefix of $s_{n,i} \operatorname{tail}^{d_n-1}(w_n) t'_{n,i}$, and moreover,

$$s_{n,i} \operatorname{tail}^{d_n-1}(w_n) t'_{n,i} = s_{n,i}\varphi^n(\operatorname{tail}^{d-1}(w)) f_R^{(n)}(v_1,v_2) t'_{n,i} = s_{n,i}\varphi^n(\operatorname{tail}^{d-1}(w) t_i).$$

The latter term in the equation above is clearly a suffix of $\varphi^n(s_i \operatorname{tail}^{d-1}(w) t_i)$, thus $s_{n,i} \operatorname{tail}^{d_n-1}(w_n) t_{n,i}$ is a factor of $\varphi^n(s_i \operatorname{tail}^{d-1}(w) t_i)$. Combining (2) with the fact that $\varphi(L(\varphi)) \subseteq L(\varphi)$, we deduce that $\varphi^n(s_i \operatorname{tail}^{d-1}(w)t_i)$ belongs to $L(\varphi)$, hence so does $s_{n,i} \operatorname{tail}^{d_n-1}(w_n)t_{n,i}$ by factoriality of $L(\varphi)$. Similarly, $s_{n,i+1} \operatorname{tail}^{d_n-1}(w_n)t_{n,i}$ belongs to $L(\varphi)$. To conclude the proof, it remains only to show that $s_{n,0} = a_n f_L^{(n)}(u_1,u_2)x_n$ and $s_{n,k+1} = b_n f_L^{(n)}(u_1,u_2)x_n$, where a_n and b_n are the last letters in the pair $g_L^n(u_1,u_2)$.

Let $g_L^n(u_1,u_2) = (u_{n,1},u_{n,2})$. We argue by induction on $n \in \mathbb{N}$ that $(u_{n,1}f_L^{(n)}(u_1,u_2), u_{n,2}f_L^{(n)}(u_1,u_2))$ is a suffix of $(\varphi^n(u_1),\varphi^n(u_2))$. The case $n=0$ is trivial. For the induction step, let us assume that the statement holds for some $n \in \mathbb{N}$. By Condition (4') of Definition 1.3, we have that

$$(u_{n+1,1}f_L(u_{n,1},u_{n,2}), u_{n+1,2}f_L(u_{n,1}u_{n,2})) \text{ is a suffix of } (\varphi(u_{n,1}),\varphi(u_{n,2})).$$

Since, by the induction hypothesis, $(u_{n,1}f_L^{(n)}(u_1,u_2), u_{n,2}f_L^{(n)}(u_1,u_2))$ is a suffix of $(\varphi^n(u_1),\varphi^n(u_2))$, we further deduce that the following is a suffix of $(\varphi^{n+1}(u_1),\varphi^{n+1}(u_2))$:

$$(u_{n+1,1}f_L(u_{n,1},u_{n,2})\varphi(f_L^{(n)}(u_1,u_2)), u_{n+1,2}f_L(u_{n,1}u_{n,2})\varphi(f_L^{(n)}(u_1,u_2))).$$

But note that $u_{n+1,1}$ and $u_{n+1,2}$ have distinct last letters (Condition (1') of Definition 1.3), so we have $f_L(u_{n,1},u_{n,2})\varphi(f_L^{(n)}(u_1,u_2)) = f_L^{(n+1)}(u_1,u_2)$. This concludes the induction.

It follows from the previous paragraph that

$$(s_{n,0},s_{n,k+1}) \text{ and } (u_{n,1}f_L^{(n)}(u_1,u_2)x_n, u_{n,2}f_L^{(n)}(u_1,u_2)x_n) \text{ are suffixes of } (\varphi^n(u_1)x_n,\varphi^n(u_2)x_n),$$

hence they are L-aligned. Since $|s_{n,0}| = |s_{n,k+1}| = |f_L^{(n)}(u_1,u_2)| + |x_n| + 1$, we deduce that $f_L^{(n)}(u_1,u_2)x_n$ is a common suffix of $s_{n,0}$ and $s_{n,k+1}$, and that the first letters of $(s_{n,0},s_{n,k+1})$ are the last letters of $g_L^n(u_1,u_2) = (u_{n,1},u_{n,2})$, thereby finishing the proof of the lemma. □

For the sake of discussion, let us call $(\mathbf{s}_n)_{n\in\mathbb{N}}$ from the previous proof a *stream of paths*, and let us say that $\mathbf{s}$ is its *source sequence*. The integer d is called the *initial depth*. We call a word *left reduced* if it has at most two left extensions. We state for the record the following immediate consequence of the previous lemma.

Proposition 2.3. *Let φ be a primitive aperiodic encoding. Fix a choice of forky sets for φ and let $\mathcal{T}$ be a bispecial triplet. If $\mathcal{T}$ admits a source sequence, then the central components of $(f_{\mathcal{B}}^n(\mathcal{T}))_{n\in\mathbb{N}}$ that are left reduced must be suffix-connected.*

In order to check the last two conditions of Lemma 2.2 in concrete examples, we need to compare the lengths of words obtained by iterating a substitution. In the next lemma, we state an elementary observation serving that purpose. Let A be a finite alphabet and for $u \in A^*$, let $\mathrm{P}(u) = (|u|_a)_{a\in A}$ be the *Parikh vector* of u. Given two words $u,v \in A^*$, we say that u is a *proper Abelian factor* of v if $\mathrm{P}(u) < \mathrm{P}(v)$, in the sense that $|u|_a \le |v|_a$ for every $a \in A$ and at least one of these inequalities is strict.

Lemma 2.4. *Let φ be a substitution over A and let $u,v \in A^*$. If u is a proper Abelian factor of v, then $|\varphi^n(u)| < |\varphi^n(v)|$ for all $n \in \mathbb{N}$.*

Before giving the proof of Proposition 2.1, let us illustrate Lemma 2.2 with two concrete examples.

Example 2.5. Recall from Example 1.7 the bispecial triplet $\mathcal{T}_4 = ((1,2),0,(0,3))$ of ψ. Consider the sequence of words:

$$\mathbf{s} = (s_0 = 1,\ t_0 = 0,\ s_1 = 0,\ t_1 = 32,\ s_2 = 2).$$

We claim that $\mathbf{s}$ is a source sequence with initial depth $d = 1$. Condition (1) of Lemma 2.2 is plain and Condition (2) is easily verified with direct computations. As for the two remaining conditions, we first note that they are satisfied trivially for $n = 0$, as $f_L^{(0)}(1,2) = f_R^{(0)}(0,3) = \varepsilon$. For $n \geq 1$, we find $f_L^{(n)}(1,2) = \psi^{n-1}(32)$ and $f_R^{(n)}(0,3) = \varepsilon$, so we need to check the following inequalities:

$$|\psi^n(0)| > |\psi^{n-1}(32)|, \quad |\psi^n(1)| > |\psi^{n-1}(32)|, \quad |\psi^n(2)| > |\psi^{n-1}(32)|, \quad |\psi^n(32)| > |\psi^{n-1}(32)|.$$

The three rightmost inequalities are straightforward. As for the leftmost inequality, it clearly holds for $n = 1,2$, and moreover, we have that

$$\mathrm{P}(\psi^3(0)) = (13,5,4,4) > (4,1,4,4) = \mathrm{P}(\psi^2(32)),$$

hence $|\psi^n(0)| > |\psi^{n-1}(32)|$ for every $n \geq 3$ by Lemma 2.4.

Example 2.6. Consider the bispecial triplet $\mathcal{T}_8 = ((0,1),00,(10,32))$ and let

$$\mathbf{s} = (s_0 = 000,\ t_0 = 32100,\ s_1 = 2032,\ t_1 = 10010,\ s_2 = 100).$$

Let us check that $\mathbf{s}$ is a source sequence for $\mathcal{T}_8$ with initial depth $d = 3$. Again, the first condition from Lemma 2.2 is obvious and the second one only requires checking that a handful of words belong to $L(\psi)$. Since $f_L^{(n)}(0,1) = \varepsilon$ for all $n \in \mathbb{N}$, the last two conditions amount to the following inequalities:

$$|\psi^n(000)| > |\psi^n(00)|, \quad |\psi^n(100)| > |\psi^n(00)|, \quad |\psi^n(2032)| > |\psi^n(00)|,$$
$$|\psi^n(32100)| > |f_R^{(n)}(10,32)| + |\psi^n(00)|, \quad |\psi^n(10010)| > |f_R^{(n)}(10,32)| + |\psi^n(00)|.$$

The first two inequalities are trivial, as are the last two since, by definition, $f_R^{(n)}(10,32)$ is a common prefix of $\psi^n(10)$ and $\psi^n(32)$. For the remaining inequality, we note that $\psi^3(00)$ is a proper Abelian factor of $\psi^3(2032)$, as evidenced by

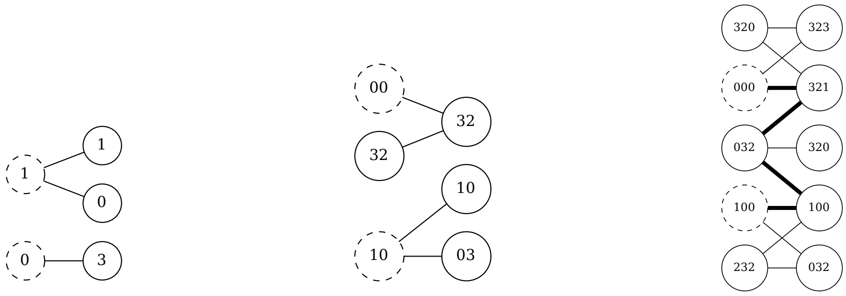
$$\mathrm{P}(\psi^3(2032)) = (31,10,21,20) > (26,10,8,8) = \mathrm{P}(\psi^3(00)).$$

Thus, the desired inequality holds for all $n \geq 3$. That it also holds for $n = 0,1,2$ is plain. This completes the proof that $\mathbf{s}$ is a source sequence. The first path in the corresponding stream is depicted in Fig. 3.

Hopefully, the two previous examples should give the reader a hint of what we have in mind for the proof that $L(\psi)$ is suffix-connected. Let us fill in the missing details.

Proof of Proposition 2.1. We start by observing that the left special words that belong to $L(\psi) \cap A^3$, namely 032, 100, 321, all satisfy the condition $\mathbf{L}(w) = \{0,2\}$. In particular, all bispecial factors of $L(\psi)$ of length at least 3 are left reduced. In fact, by checking the remaining cases, we find that the only bispecial factors which are not left reduced are ε and 0. Recall from Example 1.7 that every bispecial factor in $L(\psi)$ is the central component of an iterated $f_{\mathcal{B}}$-image of one of the bispecial triplets $\mathcal{T}_i$ found in Table 1. In Table 2, we give source sequences for the bispecial triplets $\mathcal{T}_i$ with $i \in \{1,\ldots,8\} \setminus \{6\}$, as well as for the $f_{\mathcal{B}}$-image of $\mathcal{T}_6$.[1] Details have already been given for $\mathcal{T}_4$ and $\mathcal{T}_8$ in Examples 2.5 and 2.6

[1]Note that $\mathcal{T}_6 = ((0,1),00,(0,3))$ admits no source sequence. Indeed, 00 is suffix-connected only at depth 3, and all paths between the natural embeddings of $\{0,1\} = \mathbf{L}(00)$ in the graph $\mathbf{E}_{3,3}(\varepsilon)$ must visit the vertex 100, which does not start with 0 or 3. See Fig. 3.



$\mathbf{E}_{1,1}(00)$ $\mathbf{E}_{2,2}(0)$ $\mathbf{E}_{3,3}(\varepsilon)$

Fig. 3 Connected components of the natural embeddings in the suffix extension graphs of 00 in $L(\psi)$. The natural embeddings are represented by dashed vertices. In the rightmost graph, the bold edges indicate the shortest path between the natural embeddings of the left extensions of 00.

$\mathcal{T}$	d	$\mathbf{s}$
$((1,2),\varepsilon,(0,1))$	1	(1, 0, 2)
$((0,2),\varepsilon,(10,32))$	1	(0, 10, 2)
$((0,1),0,(0,1))$	1	(0, 0, 1)
$((1,2),0,(0,3))$	1	(1, 0, 0, 32, 2)
$((0,2),0,(10,32))$	1	(0, 32, 2)
$((0,2),100100,(0,1))$	1	(0, 0, 2)
$((0,2),32,(10,32))$	1	(2, 10, 0)
$((0,1),00,(10,32))$	3	(000, 32100, 2032, 10010, 100)

Table 2 Source sequences $\mathbf{s}$ and initial depths d for some bispecial triplets $\mathcal{T}$ of ψ. The triplet appearing in the ith row is the bispecial triplet $\mathcal{T}_i$ from Table 1, except for the sixth row where $\mathcal{T} = f_{\mathcal{B}}(\mathcal{T}_6)$.

and the other cases are handled similarly. It follows from Proposition 2.3 that all left reduced bispecial words in $L(\psi)$ are suffix-connected (observe that $\mathcal{T}_6$ and $\mathcal{T}_8$ have the same central component). The only missing case is the word 0, which is connected (see Fig. 2). □

We conclude this appendix by studying the Schützenberger group of ψ. The reader may recall some useful definitions and notations from Paper 1, Section 2.

Proposition 2.7. *The Schützenberger group of ψ is a free profinite group of rank 4.*

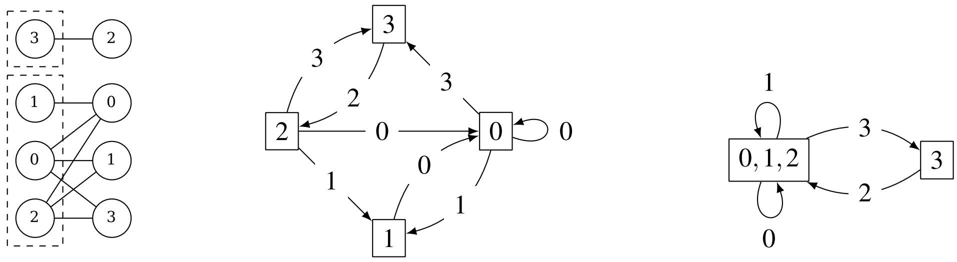
Proof. The pair $(03,2)$ is a connection of ψ of order 1. The corresponding return substitution, which we computed using Durand's algorithm (Algorithm 1 in Paper 1), is given by:

$$\psi_{03,2}\colon 0 \mapsto 01,\ 1 \mapsto 002,\ 2 \mapsto 0332,\ 3 \mapsto 032.$$

By the main result of [11], $\psi_{03,2}$ defines an ω-presentation of $G(\psi)$. Straightforward computations show that $\psi_{03,2}$ extends to the automorphism of the free group $F(\{0,1,2,3\})$ whose inverse is

$$\psi_{03,2}^{-1}\colon 0 \mapsto 13^{-1}23^{-1},\ 1 \mapsto 32^{-1}31^{-1}0,\ 2 \mapsto 32^{-1}31^{-1}32^{-1}3,\ 3 \mapsto 32^{-1}31^{-1}23^{-1}13^{-1}23^{-1}.$$

It follows that $G(\psi)$ is a free profinite group of rank 4 (see Theorem 4.1 in Paper 1). □



$\mathbf{E}(\varepsilon)$ $G_{1,1}$ $G_{1,1}/{\equiv_S}$

Fig. 4 Folding the Rauzy graph $G_{1,1}$ using the extension graph of the empty word.

Remark 2.8. In $L(\psi)$, the extension graph of the empty word has two connected components. Since it is suffix-connected, we may apply the main result of Paper 3 to conclude that the return groups in $L(\psi)$ are equal to one of two subgroups of $F(\{0,1,2,3\})$ of rank 3. We can obtain a description of these groups by folding the Rauzy graph $G_{1,1}$, as illustrated in Fig. 4. These two subgroups are the subgroup H with basis $\{0,1,32\}$ and its conjugate $3^{-1}H3$. On the other hand, by Proposition 2.7, the Schützenberger group $G(\psi)$ is a free profinite group of rank 4. In particular, $X(\psi)$, the shift space defined by ψ, must fail the freeness criteria given by Propositions 2.4 and 2.5 in Appendix A: otherwise, its Schützenberger group would be free of rank 3, contradicting the previous proposition. We also note that, despite being invertible, ψ fails the invertibility criterion provided by Corollary 2.8 of Appendix A.

Conclusion

The work presented in this thesis suggests a number of questions and problems which might present interesting avenues for future research. A few are already discussed in the three papers found in this thesis. Here, some are recalled and several more are ventured, organized loosely by theme.

Minimal ω-presentations

One of the main results of Paper 1 links absolute freeness with minimal ω-presentations. In fact, solving the following problem would mean that absolute freeness is decidable for Schützenberger groups of primitive substitutions.

Question 1. Is there an algorithm which, given a primitive aperiodic substitution φ, produces a minimal ω-presentation for the Schützenberger group of φ?

Since many ideas from Paper 1 apply more generally to ω-presented groups, the above question could also be asked within that broader setting.

Freeness and invertibility

As the counterexample presented in Paper 1 shows, the freeness question remains elusive even for Schützenberger groups of primitive invertible substitutions.

Question 2. When do Schützenberger groups of primitive invertible substitutions fail to be free?

A more precise version of this question was suggested to us by the referee of Paper 1. If a primitive invertible substitution is tame (in the sense of Berthé et al. [23]), then its shift space must be dendric and consequently, its Schützenberger group must be free [12]. On the other hand, the counterexample of Paper 1 is invertible but not tame.

Question 3. Do primitive tame substitutions always have free Schützenberger groups?

The counterexample presented in Paper 1 is defined on an alphabet with four letters, while on a binary alphabet, all primitive invertible substitutions are Sturmian, hence have free Schützenberger groups by a result from [12]. As for the ternary case, the situation remains unclear.

Question 4. Do primitive invertible ternary substitutions have free Schützenberger groups?

Finally, it would be interesting to find an infinite family of primitive invertible substitutions having non-free Schützenberger groups and defined on alphabets of all sizes larger than four.

Suffix-connected shift spaces

At time of writing, there are only two known examples of non-dendric suffix-connected shift spaces, both of which are defined by primitive substitutions (see Paper 3 and Appendix B).

Problem 5. Find non-dendric suffix-connected minimal shift spaces that are not substitutive.

The arguments used to establish suffix-connectedness in Paper 3 were highly specialized in nature and gave close to no insight into this phenomenon. This can be partially addressed using Klouda's work on bispecial factors [49], as we show in Appendix B. Klouda's approach provides a good starting point for establishing suffix-connectedness in substitutive shift spaces, but we are still short of a full algorithmic solution.

Question 6. Is suffix-connectedness a decidable property of substitutive minimal shift spaces?

We know that for Schützenberger groups of suffix-connected minimal shift spaces, relative freeness implies absolute freeness (see Appendix A). Moreover, the Schützenberger groups are absolutely free in all known suffix-connected cases, namely dendric shift spaces [12] plus the two non-dendric examples found in Paper 3 and Appendix B respectively.

Question 7. Do suffix-connected shift spaces always have free Schützenberger groups?

In 2020, Dolce and Perrin [34] proposed to extend the notion of dendricity by defining *eventually dendric* shift spaces. One can define in much the same way a notion of *eventual suffix-connectedness*.

Problem 8. Study return groups in eventually suffix-connected shift spaces.

The work of Dolce and Perrin [33, 34] shows that the class of eventually dendric shift spaces is stable under certain operations, such as maximal bifix decoding or conjugacy.

Problem 9. Investigate the stability, or lack thereof, of eventual suffix-connectedness under such operations as maximal bifix decoding, conjugacy, or flow equivalence.

Proper relative freeness

We would be remiss if we did not discuss the conspicuous lack of proper relative freeness among Schützenberger groups of minimal aperiodic shift spaces. In all known examples, the Schützenberger group is either absolutely free, or not relatively free. This is made even more intriguing by the fact that proper relative freeness is impossible for at least two classes of minimal shift spaces, namely shift spaces defined by primitive invertible substitutions (Paper 1) and suffix-connected minimal shift spaces (Appendix A).

Question 10. Is proper relative freeness possible for Schützenberger groups of minimal aperiodic shift spaces?

The class of shift spaces defined by primitive aperiodic substitutions of constant length might be a good starting point for investigating this question, since absolute freeness of the Schützenberger group never occurs in this case (see Paper 2).

Perfect and pro-p Schützenberger groups

In Paper 2, we showed that Schützenberger groups of primitive substitutions cannot be perfect nor pro-p. We are still unsure whether this is true of all minimal shift spaces.

Question 11. Can Schützenberger groups of minimal shift spaces be perfect or pro-p?

Ongoing work (joint with Almeida and Costa) points to a positive answer for the first part of the question: early results suggest that a minimal shift space with a perfect Schützenberger group could be constructed using S-adic representations. As for the existence of pro-p Schützenberger groups, it is in fact a restriction of Question 10: indeed, Schützenberger groups of minimal shift spaces are projective [65], and projective pro-p groups are free by a theorem of Tate (see [67]).

Prometabelian quotients

Since the pronilpotent quotients of ω-presented groups are now well understood, it seems that the following problem is next in line.

Problem 12. Study prometabelian quotients of ω-presented groups.

Recall that, for ω-presented groups, composition matrices contain all the information about maximal pronilpotent quotients. This is essentially because composition matrices realize the Abelianization functor. On the other hand, it is well-known that in the category of groups, the metabelianization functor is realized by the Fox Jacobian [52]. Hence, we conjecture that Fox's free calculus might play a key role in understanding prometabelian quotients of ω-presented groups.

The "good basis" phenomenon

When working on Paper 1, we noticed that some return substitutions, when expressed in the right basis, look very similar to the original substitution; a particularly careful reader might already have noticed this when looking at Example 3.5 in Paper 1. We dub this the *"good basis" phenomenon*. It is easier to understand through concrete examples.

Recall that the Thue–Morse substitution is the binary substitution τ defined by $\tau\colon 0 \mapsto 01,\ 1 \mapsto 10$. Consider the following subset of $F(\{0,1,2,3\})$, which the reader can check forms a basis:

$$\{20^{-1},\ 3^{-1}2,\ 02^{-1}12^{-1}3,\ 02^{-1}31^{-1}\}.$$

Here is τ^2 together with the return substitution $\tau_{0,1}$ expressed in that basis:

$$\tau^2\colon 0 \mapsto 0110,\ 1 \mapsto 1001,$$
$$\tau_{0,1}\colon 0 \mapsto 302110,\ 1 \mapsto 103021,\ 2 \mapsto 2,\ 3 \mapsto \varepsilon.$$

Evidently, τ^2 can be recovered from $\tau_{0,1}$ by erasing the letters 2 and 3, which are respectively a fixed point and a kernel element.

A similar situation occurs with the substitution $\xi\colon 0 \mapsto 001,\ 1 \mapsto 02,\ 2 \mapsto 301,\ 3 \mapsto 320$ studied in Section 6 of Paper 1. This time, we take the following basis of the free group over $\{0,1,2,3,4,5\}$:

$$\{0,\ 10^{-1},\ 1^{-1}2,\ 2^{-1}45^{-1}30^{-1},\ 01^{-1}54^{-1}2,\ 2^{-1}45^{-1}13^{-1}52^{-1}1,\ 63^{-1}54^{-1}20^{-1}\}.$$

Again, there is a clear resemblance between ξ^2 and the return substitution $\xi_{1,0}$ expressed in that basis:

$$\xi^2\colon 0 \mapsto 00100102,\ 1 \mapsto 001301,\ 2 \mapsto 32000102,\ 3 \mapsto 320301001,$$
$$\xi_{1,0}\colon 0 \mapsto 00100102,\ 1 \mapsto 0014301,\ 2 \mapsto 3452000102,\ 3 \mapsto 345260301001,\ 4 \mapsto 4,\ 5 \mapsto \varepsilon,\ 6 \mapsto \varepsilon.$$

In both cases, the “good basis” was found by trial and error. But it seems that not all return substitutions behave so nicely: going back to the Thue–Morse substitution, we were unable to find a “good basis” for the return substitution $\tau_{0,10}$, making this all the more intriguing.

Problem 13. Find an explanation for the “good basis” phenomenon.

References

[1] J. Almeida. Implicit operations on finite J-trivial semigroups and a conjecture of I. Simon. *J. Pure Appl. Algebra*, 69(3):205–218, 1991. doi:10.1016/0022-4049(91)90019-X. 15

[2] J. Almeida. *Finite Semigroups and Universal Algebra*. World Scientific, 1995. doi:10.1142/2481. 15

[3] J. Almeida. Dynamics of implicit operations and tameness of pseudovarieties of groups. *Trans. Amer. Math. Soc.*, 354(1):387–411, 2001. doi:10.1090/s0002-9947-01-02857-4. 15, 31

[4] J. Almeida. Dynamics of finite semigroups. In *Semigroups, Algorithms, Automata and Languages (Coimbra, 2001)*, pages 269–292. World Scientific, 2002. doi:10.1142/9789812776884_0009. 33

[5] J. Almeida. Profinite structures and dynamics. *CIM Bull.*, 14:8–18, 2003. 15, 41

[6] J. Almeida. Symbolic dynamics in free profinite semigroups. In *Algebraic Systems, Formal Languages and, Conventional and Unconventional Computation Theory*, volume 1366, pages 1–12. RIMS Kokyuroku, 2004. 15, 41

[7] J. Almeida. Profinite semigroups and applications. In V. Kudryavtsev and I. G. Rosenberg, editors, *Structural Theory of Automata, Semigroups, and Universal Algebra*, volume 207, pages 1–45. Springer, 2005. doi:10.1007/1-4020-3817-8_1. 15, 22, 24

[8] J. Almeida. Profinite groups associated with weakly primitive substitutions. *J. Math. Sci.*, 144(2):3881–3903, 2007. doi:10.1007/s10958-007-0242-y. Translated from Fundam. Prikl. Mat., 11(3):13–48, 2005. 15, 16, 21, 22, 23, 30, 34, 41, 52, 63, 64

[9] J. Almeida and A. Costa. Infinite-vertex free profinite semigroupoids and symbolic dynamics. *J. Pure Appl. Algebra*, 213(5):605–631, 2009. doi:10.1016/j.jpaa.2008.08.009. 15

[10] J. Almeida and A. Costa. On the transition semigroups of centrally labeled Rauzy graphs. *Int. J. Algebra Comput.*, 22(02):1250018–1–1250018–25, 2012. doi:10.1142/s021819671250018x.

[11] J. Almeida and A. Costa. Presentations of Schützenberger groups of minimal subshifts. *Isr. J. Math.*, 196 (1):1–31, 2013. doi:10.1007/s11856-012-0139-4. 16, 17, 21, 22, 23, 24, 25, 27, 29, 31, 41, 42, 46, 49, 51, 52, 53, 54, 59, 61, 64, 95, 96, 97, 105

[12] J. Almeida and A. Costa. A geometric interpretation of the Schützenberger group of a minimal subshift. *Ark. Mat.*, 54(2):243–275, 2016. doi:10.1007/s11512-016-0233-7. 15, 16, 18, 21, 37, 74, 78, 91, 92, 94, 95, 107, 108

[13] J. Almeida and M. V. Volkov. Profinite methods in finite semigroup theory. In S. Goncharov, editor, *Proceedings of the international conference "Logic and Applications" and of the International Conference on mathematical Logic*, pages 144–164, Novosibirsk, 2002. 15

[14] J. Almeida and M. V. Volkov. Subword complexity of profinite words and subgroups of free profinite semigroups. *Int. J. Algebra Comput.*, 16(02):221–258, 2006. doi:10.1142/s0218196706002883. 15, 16, 52, 53

[15] J. Almeida and P. Weil. Relatively free profinite monoids: An introduction and examples. In J. Fountain, editor, *Proceedings of the NATO Advanced Study Institute on Semigroups, Formal Languages, and Groups (University of York, 1993)*, volume 466, 1995. 15

[16] J. Almeida and P. Weil. Free profinite R-trivial monoids. *Int. J. Algebra Comput.*, 7(5):625–671, 1997. doi:10.1142/S0218196797000289. 15

[17] J. Almeida, A. Costa, J. C. Costa, and M. Zeitoun. The linear nature of pseudowords. *Publ. Mat.*, 63: 361–422, 2019. doi:10.5565/publmat6321901. 15

[18] J. Almeida, A. Costa, R. Kyriakoglou, and D. Perrin. On the group of a rational maximal bifix code. *Forum Math.*, 32(3):553–576, 2020. doi:10.1515/forum-2018-0270. 15

[19] J. Almeida, A. Costa, R. Kyriakoglou, and D. Perrin. *Profinite Semigroups and Symbolic Dynamics*. Springer International Publishing, 2020. doi:10.1007/978-3-030-55215-2. 15, 22, 23, 24, 26, 28, 30, 31, 47, 52, 53, 60, 63, 92, 93, 95, 96, 98

[20] S. Balchin and D. Rust. Computations for symbolic substitutions. *J. Integer Seq.*, 20, 2017. 83

[21] J. Berstel, D. Perrin, and C. Reutenauer. *Codes and Automata*. Cambridge University Press, 2009. doi:10.1017/cbo9781139195768. 98

[22] V. Berthé, C. De Felice, F. Dolce, J. Leroy, D. Perrin, C. Reutenauer, and G. Rindone. Acyclic, connected and tree sets. *Monatsh. Math.*, 176(4):521–550, 2015. doi:10.1007/s00605-014-0721-4. 16, 21, 67, 68, 74, 77, 78

[23] V. Berthé, C. De Felice, F. Dolce, J. Leroy, D. Perrin, C. Reutenauer, and G. Rindone. Maximal bifix decoding. *Discrete Math.*, 338(5):725–742, 2015. doi:10.1016/j.disc.2014.12.010. 16, 18, 23, 37, 94, 107

[24] V. Berthé, C. De Felice, F. Dolce, J. Leroy, D. Perrin, C. Reutenauer, and G. Rindone. Bifix codes and interval exchanges. *J. Pure Appl. Algebra*, 219(7):2781–2798, 2015. doi:10.1016/j.jpaa.2014.09.028. 16, 21

[25] V. Berthé, C. De Felice, V. Delecroix, F. Dolce, J. Leroy, D. Perrin, C. Reutenauer, and G. Rindone. Specular sets. *Theoret. Comput. Sci.*, 684:3–28, 2017. doi:10.1016/j.tcs.2017.03.001. 68

[26] V. Berthé, F. Dolce, F. Durand, J. Leroy, and D. Perrin. Rigidity and substitutive dendric words. *Int. J. Found. Comput.*, 29(05):705–720, 2018. doi:10.1142/S0129054118420017. 94

[27] J. A. Bondy and U. S. R. Murty. *Graph Theory with Applications*. Macmillan London, 1976. 82

[28] A. Costa. Conjugacy invariants of subshifts: An approach from profinite semigroup theory. *Int. J. Algebra Comput.*, 16(4):629–655, 2006. doi:10.1142/s0218196706003232. 15, 21, 41

[29] A. Costa and B. Steinberg. Profinite groups associated to sofic shifts are free. *Proc. Lond. Math. Soc.*, 102 (3):341–369, 2011. doi:10.1112/plms/pdq024. 15, 16, 21

[30] A. Costa and B. Steinberg. The Karoubi envelope of the mirage of a subshift. *Commun. Algebra*, 49: 4820–4856, 2021. doi:10.1080/00927872.2021.1931263. 15, 17, 41, 60

[31] J. C. Costa. Free profinite locally idempotent and locally commutative semigroups. *J. Pure Appl. Algebra*, 163(1):19–47, 2001. doi:10.1016/s0022-4049(00)00176-6. 15

[32] T. Coulbois, M. Sapir, and P. Weil. A note on the continuous extensions of injective morphisms between free groups to relatively free profinite groups. *Publ. Mat.*, 47(2):477–487, 2003. doi:10.5565/PUBLMAT_47203_10. 31

[33] F. Dolce and D. Perrin. Neutral and tree sets of arbitrary characteristic. *Theoret. Comput. Sci.*, 658: 159–174, 2017. doi:10.1016/j.tcs.2016.01.008. 18, 68, 81, 108

[34] F. Dolce and D. Perrin. Eventually dendric shift spaces. *Ergod. Theory Dyn. Syst.*, 41(7):2023–2048, 2020. doi:10.1017/etds.2020.35. 68, 90, 108

[35] F. Durand. A characterization of substitutive sequences using return words. *Discrete Math.*, 179(1-3): 89–101, 1998. doi:10.1016/S0012-365X(97)00029-0. 17, 22, 23, 56, 77

[36] F. Durand. A generalization of Cobham's theorem. *Theory Comput. Syst.*, 31(2):169–185, 1998. doi: 10.1007/s002240000084. 17, 54, 56, 59

[37] F. Durand. HD0L-ω-equivalence and periodicity problems in the primitive case (to the memory of G. Rauzy). *Unif. Distrib. Theory*, 7(1):199–215, 2012. 34, 54, 60

[38] F. Durand and D. Perrin. *Dimension Groups and Dynamical Systems: Substitutions, Bratteli Diagrams and Cantor Systems*. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2022. doi:10.1017/9781108976039. 53, 98

[39] F. Durand, B. Host, and C. Skau. Substitutional dynamical systems, Bratteli diagrams and dimension groups. *Ergod. Theory Dyn. Syst.*, 19(4):953–993, 1999. doi:10.1017/S0143385799133947. 22, 23, 25, 32, 53, 55

[40] N. P. Fogg. *Substitutions in Dynamics, Arithmetics and Combinatorics*. Springer Berlin Heidelberg, 2002. doi:10.1007/b13861. 64, 70

[41] M. D. Fried and M. Jarden. *Field Arithmetic*. Springer Berlin Heidelberg, 2008. doi:10.1007/978-3-540-77270-5. 15, 45, 46

[42] *GAP – Groups, Algorithms, and Programming, Version 4.11.0*. The GAP Group, 2020. 51

[43] H. Goulet-Ouellet. Suffix-connected languages. *Theoret. Comput. Sci.*, 923:126–143, 2022. doi:10.1016/j.tcs.2022.05.001. 15, 16

[44] H. Goulet-Ouellet. Pronilpotent quotients associated with primitive substitutions. *J. Algebra*, 606:341–370, 2022. doi:10.1016/j.jalgebra.2022.05.021. 16

[45] H. Goulet-Ouellet. Freeness of Schützenberger groups of primitive substitutions. *Int. J. Algebra Comput.*, 2022. doi:10.1142/S0218196722500473. In press. 15, 16, 42, 50, 60

[46] H. Hida. *Modular forms and Galois cohomology*. Cambridge Studies in Advanced Mathematics. Cambridge University Press, Cambridge, 2000. doi:10.1017/CBO9780511526046. 15

[47] R. P. Hunter. Some remarks on subgroups defined by the Bohr compactification. *Semigr. Forum*, 26(1):125–137, 1983. doi:10.1007/BF02572826. 24, 47

[48] I. Kapovich and A. Myasnikov. Stallings foldings and subgroups of free groups. *J. Algebra*, 248(2):608–668, 2002. doi:10.1006/jabr.2001.9033. 27, 35, 37, 80

[49] K. Klouda. Bispecial factors in circular non-pushy D0L languages. *Theoret. Comput. Sci.*, 445:63–74, 2012. doi:10.1016/j.tcs.2012.05.007. 97, 98, 99, 100, 102, 108

[50] S. Lang. *Algebra*. Springer New York, 2002. doi:10.1007/978-1-4613-0041-0. 58

[51] A. Lubotzky. Pro-finite presentations. *J. Algebra*, 242(2):672–690, 2001. doi:10.1006/jabr.2001.8805. 22, 24, 46

[52] R. C. Lyndon and P. E. Schupp. *Combinatorial Group Theory*. Springer Berlin Heidelberg, 2001. doi:10.1007/978-3-642-61896-3. 94, 109

[53] S. Mac Lane. *Categories for the Working Mathematician*. Springer New York, 1971. doi:10.1007/978-1-4612-9839-7. 43, 44

[54] S. Margolis, M. Sapir, and P. Weil. Closed subgroups in pro-V topologies and the extension problem for inverse automata. *Int. J. Algebra Comput.*, 11(04):405–445, 2001. doi:10.1142/s0218196701000498. 31

[55] M. Morse and G. A. Hedlund. Symbolic dynamics. *Am. J. Math.*, 60(4):815–866, 1938. doi:10.2307/2371264. 93

[56] B. Mossé. Puissance de mots et reconnaissabilité des points fixes d'une substitution. *Theoret. Comput. Sci.*, 99(2):327–334, 1992. doi:10.1016/0304-3975(92)90357-L. 96

[57] B. Mossé. Reconnaissabilité des substitutions et complexité des suites automatiques. *Bull. Soc. Math. Fr.*, 124(2):329–346, 1996. doi:10.24033/bsmf.2283. 98

[58] A. Moura. Representations of the free profinite object over DA. *Int. J. Algebra Comput.*, 21(05):675–701, 2011. doi:10.1142/S0218196711006467. 15

[59] A. Moura. The word problem for ω-terms over DA. *Theoret. Comput. Sci.*, 412(46):6556–6569, 2011. doi:10.1016/j.tcs.2011.08.003. 15

[60] B. H. Neumann and H. Neumann. Embedding theorems for groups. *J. Lond. Math. Soc.*, s1-34(4):465–479, 1959. doi:10.1112/jlms/s1-34.4.465. 32

[61] H. Neumann. *Varieties of Groups*. Springer Berlin Heidelberg, 1967. doi:10.1007/978-3-642-88599-0. 26, 96

[62] B. Parvaix. Substitution invariant sturmian bisequences. *J. Théor. Nr. Bordx.*, 11(1):201–210, 1999. doi:10.5802/jtnb.246. 94

[63] J.-E. Pin. Profinite methods in automata theory. In S. Albers and J.-Y. Marion, editors, *26^{th} International Symposium on Theoretical Aspects of Computer Science*, pages 31–50, Freiburg, Germany, 2009. doi:10.4230/LIPIcs.STACS.2009.1856. 15

[64] J. Rhodes and B. Steinberg. Closed subgroups of free profinite monoids are projective profinite groups. *Bull. Lond. Math. Soc.*, 40(3):375–383, 2008. doi:10.1112/blms/bdn017. 15, 16, 52

[65] J. Rhodes and B. Steinberg. *The q-theory of finite semigroups*. Springer US, 2009. doi:10.1007/b104443. 15, 109

[66] L. Ribes and P. A. Zaleskii. The pro-p topology of a free groups and algorithmic problems in semigroups. *Int. J. Algebra Comput.*, 04(03):359–374, 1994. doi:10.1142/s021819679400004x. 31

[67] L. Ribes and P. Zalesskii. *Profinite Groups*. Springer Berlin Heidelberg, second edition, 2010. doi:10.1007/978-3-642-01642-4. 15, 16, 22, 28, 31, 34, 42, 43, 44, 45, 47, 94, 95, 109

[68] *SageMath, the Sage Mathematics Software System, Version 9.2*. The Sage Developers, 2020. 51, 83, 97

[69] J.-P. Serre. *Galois Cohomology*. Springer Berlin Heidelberg, 1997. doi:10.1007/978-3-642-59141-9. 15

[70] B. Steinberg. Fundamental groups, inverse Schützenberger automata, and monoid presentations. *Commun. Algebra*, 28(11):5235–5253, 2000. doi:10.1080/00927870008827152. 79

[71] B. Steinberg. On the endomorphism monoid of a profinite semigroup. *Port. Math.*, 68:177–183, 2010. doi:10.4171/PM/1886. 24

[72] S. J. van Gool and B. Steinberg. Pro-aperiodic monoids via saturated models. *Isr. J. Math.*, 234(1):451–498, 2019. doi:10.1007/s11856-019-1947-6. 15

[73] P. Weil. Profinite methods in semigroup theory. *Int. J. Algebra Comput.*, 12(1-2):137–178, 2002. doi:10.1142/s0218196702000912. 15

[74] S. H. Weintraub. *Linear Algebra for the Young Mathematician*. American Mathematical Society, 2019. 48, 57

[75] J. S. Wilson. *Profinite Groups*. London Mathematical Society Monographs. Oxford University Press, 1999. 15

Index

Index of notations