Pré-Publicações do Departamento de Matemática
Universidade de Coimbra
Preprint Number 21–35

FREENESS OF SCHÜTZENBERGER GROUPS OF PRIMITIVE SUBSTITUTIONS

HERMAN GOULET-OUELLET

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.
Math. Subject Classification (2010): 20E18, 37B10, 20E05, 20M05.

1. Introduction

In [4], 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 [11].

In the study of Schützenberger groups corresponding to minimal shift spaces, the freeness question has been a recurring theme [4, 5, 6, 12]. These groups are known to be free for the family of dendric shift spaces, also known as tree sets [6, Theorem 6.5]. Notably, these include Arnoux-Rauzy shift spaces [8, Example 3.2], as well as shift spaces defined by regular interval exchange [9, Theorem 4.3]. On the other hand, failure of freeness was also observed,

Received September 23, 2021.
This work was conducted with the support of the Centre for Mathematics of the University of Coimbra (UIDB/00324/2021, 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 acknowledges the financial support of the Portuguese Government through a PhD grant (PD/BD/150350/2019).

for instance in the shift space defined by the Thue–Morse substitution [5, 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 [4, 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 [4, 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 [5]) 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 succesfully 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 [4, 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 [7] 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, [21, 26]; on profinite semigroups and Schützenberger groups of primitive substitutions, [3, 4, 5]; on return sets and return substitutions, [14, 16].

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 [21]. 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 *relations*. 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 [7, 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 $\widehat{A^*}$ [7, Positon 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 $\widehat{A^*}$ [7, 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 [7, 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 [7, Exercise 5.20], so from now on we focus on the aperiodic case.

Two-sided return substitutions, introduced in [16], play an important role in the study of Schützenberger groups of primitive substitutions [5]. It is based on the notion of return words, 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 [10, 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* [16, Lemma 17]. A further property worth mentionning 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 [14, Proposition 2.8] and [10, Proposition 4.4]).

By a *connection*[*] 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 $\mathcal{R}_{u,v}$ [16, 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 [7, Proposition 5.5.10].

Following the convention used in [14], we relabel return substitutions using the natural ordering of return words induced by leftmost occurrences. This ordering

[*]The term *connection* was coined by Almeida in [4], where it was used under the condition $|u| = |v| = 1$.

[6] J. Almeida and A. Costa. A geometric interpretation of the Schützenberger group of a minimal subshift. *Ark. Mat.*, 54(2):243–275, 2016.
[7] J. Almeida, A. Costa, R. Kyriakoglou, and D. Perrin. *Profinite Semigroups and Symbolic Dynamics*. Springer International Publishing, 2020.
[8] 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.
[9] 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.
[10] 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.
[11] A. Costa. Conjugacy invariants of subshifts: An approach from profinite semigroup theory. *Int. J. Algebra Comput.*, 16(4):629–655, 2006.
[12] A. Costa and B. Steinberg. Profinite groups associated to sofic shifts are free. *Proc. London Math. Soc.*, 102(3):341–369, 2011.
[13] 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.
[14] F. Durand. A characterization of substitutive sequences using return words. *Discrete Math.*, 179(1-3):89–101, 1998.
[15] 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.
[16] F. Durand, B. Host, and C. Skau. Substitutional dynamical systems, Bratteli diagrams and dimension groups. *Ergodic Theory Dynam. Systems*, 19(4):953–993, 1999.
[17] N. P. Fogg. *Substitutions in Dynamics, Arithmetics and Combinatorics*. Springer Berlin Heidelberg, 2002.
[18] C. Holton and L. Q. Zamboni. Geometric realizations of substitutions. *Bull. Soc. Math. Fr.*, 126(2):149–179, 1998.
[19] R. P. Hunter. Some remarks on subgroups defined by the Bohr compactification. *Semigr. Forum*, 26(1):125–137, 1983.
[20] I. Kapovich and A. Myasnikov. Stallings foldings and subgroups of free groups. *J. Algebra*, 248(2):608–668, 2002.
[21] A. Lubotzky. Pro-finite presentations. *J. Algebra*, 242(2):672–690, 2001.
[22] 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.
[23] B. H. Neumann and H. Neumann. Embedding theorems for groups. *J. London Math. Soc.*, s1-34(4):465–479, 1959.
[24] H. Neumann. *Varieties of Groups*. Springer Berlin Heidelberg, 1967.
[25] 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.
[26] L. Ribes and P. Zalesskii. *Profinite Groups*. Springer Berlin Heidelberg, second edition, 2010.
[27] B. Steinberg. On the endomorphism monoid of a profinite semigroup. *Port. Math.*, 68:177–183, 2010.

Herman Goulet-Ouellet
University of Coimbra, CMUC, Department of Mathematics, Apartado 3008, EC Santa Cruz, 3001-501 Coimbra, Portugal
E-mail address: hgouletouellet@student.uc.pt

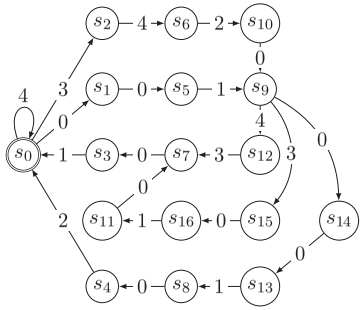

FIGURE 3. An automaton over the alphabet A_5. The distinguished state is identified by a double circle.

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 Figure 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 $F(A_5)$.

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.

References

[1] J. Almeida. Dynamics of implicit operations and tameness of pseudovarieties of groups. *Trans. Amer. Math. Soc.*, 354(1):387–411, 2001.

[2] J. Almeida. Dynamics of finite semigroups. In *Semigroups, Algorithms, Automata and Languages (Coimbra, 2001)*, pages 269–292. World Scientific, 2002.

[3] J. Almeida. Profinite semigroups and applications. In V. Kudryavtsev and I. G. Rosenberg, editors, *Structural Theory of Automata, Semigroups, and Universal Algebra*, volume 207 of *NATO Science Series II: Mathematics, Physics and Chemistry*, pages 1–45, Dordrecht, 2005. Springer.

[4] J. Almeida. Profinite groups associated with weakly primitive substitutions. *J. Math. Sci.*, 144(2):3881–3903, 2007. Translated from Fundam. Prikl. Mat., Vol. 11, No. 3, pp. 13–48, 2005.

[5] J. Almeida and A. Costa. Presentations of Schützenberger groups of minimal subshifts. *Israel J. Math.*, 196(1):1–31, 2013.

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 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 [7, Section 3.12])[†]. 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 [7, Section 3.7]. We now give the eponymous definition of this section.

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

[†]For historical context, Hunter proved in [19] 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 [3] and generalized by Steinberg [27].

is sometimes used for ω-presentations, using relations instead of relators, for instance in [5]:

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

The next lemma gives a different way to interpret ω-presentations. We use essentially the same argument as [21, 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 $\ker(\psi^{\omega})$.

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 ([5, 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 $G(\varphi)$.

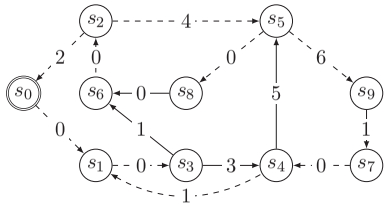

FIGURE 2. An automaton over the alphabet A_7. The distinguished state is identified by a double circle and a spanning tree is highlighted with dashed edges.

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 $r_1(\xi_{1,0})$.

$X = X_T$, so X is a basis of $\mathrm{Im}(\xi_{1,0})$ by [20, Lemma 6.1]. The restriction $r_1(\xi_{1,0})$, written in the basis X ordered as above, is (see Table 2 for details):

$$\begin{aligned} r_1(\xi_{1,0}):\ 0 &\mapsto 00100102 \\ 1 &\mapsto 0014301 \\ 2 &\mapsto 342000102 \\ 3 &\mapsto 3420301001 \\ 4 &\mapsto 4. \end{aligned}$$

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

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

$\theta_{1,0}^{-1}(r)$	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 $\xi_{1,0}$.

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 $H_{\mathscr{A}}$ [20, 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

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

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 Figure 2, where a spanning tree T is highlighted. A direct verification reveals that $\mathscr{A}$ is folded and that

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 $\varphi^n(b) \in a_1 A^* \cup A^* a_2$ for all $b \in A$. Then $G(\varphi)$ has the more straightforward ω-presentation $G(\varphi) \cong \langle A \mid \widehat{\varphi}^\omega(a)a^{-1} : a \in A\rangle$ [5, 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 [16, 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

$$\tau\colon \begin{array}{rcl} 0 & \mapsto & 01 \\ 1 & \mapsto & 10. \end{array}$$

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 $A_4 = \{0, 1, 2, 3\}$:

$$\tau_{0,1}\colon \begin{array}{rcl} 0 & \mapsto & 0123 \\ 1 & \mapsto & 013 \\ 2 & \mapsto & 02123 \\ 3 & \mapsto & 0213 \end{array} \qquad \tau_{0,10}\colon \begin{array}{rcl} 0 & \mapsto & 01 \\ 1 & \mapsto & 023132 \\ 2 & \mapsto & 0232 \\ 3 & \mapsto & 0131. \end{array}$$

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 [5], 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 [7, Theorem 4.6.7]. Moreover, from the equality $\phi \circ \eta = \eta \circ r_n(\phi)$, we deduce that the following diagram is commutative:

$$\begin{array}{ccc} \widehat{F}(B) & \xrightarrow{\widehat{\eta}} & \widehat{F}(A) \\ \downarrow{\scriptstyle \widehat{r_n(\phi)}} & & \downarrow{\scriptstyle \widehat{\phi}} \\ \widehat{F}(B) & \xrightarrow{\widehat{\eta}} & \widehat{F}(A). \end{array}$$

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

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

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 [24, 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

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 ← v;
    repeat
        w ← φ^k(w);
    until uv occurs twice in uw;
    let θ_{u,v}(0) = leftmost return word in uw;
    i ← 1 ;                          // least undefined letter of θ_{u,v}
    j ← 0 ;                          // least undefined letter of φ_{u,v}
    while j<i do
        foreach return word r in uφ^k(θ_{u,v}(j))v do
            if r is not in Im(θ_{u,v}) then
                let θ_{u,v}(i) = r;
                i ← i + 1;
            end if
        end foreach
        let φ_{u,v}(j) = θ^{-1}_{u,v}(φ^k(r));
        j ← j + 1;
    end while
end
```

ALGORITHM 1. Durand's algorithm for computing return substitutions.

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 [20].

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 $\mathscr{A}$ [20, Lemma 3.2].

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 which is not an automorphism and whose incidence matrix has a non-zero determinant. 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 7 generators.

Step 2. We compute the restriction $r_1(\xi_{1,0})$. This defines an ω-presentation of $G(\xi)$ with 5 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 [15, 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):

$\theta_{1,0}\colon$	0	$\mapsto$	001	$\xi_{1,0}\colon$	$0 \mapsto 00102$
	1	$\mapsto$	02001		$1 \mapsto 00310102$
	2	$\mapsto$	02001301		$2 \mapsto 003101040002$
	3	$\mapsto$	02320001		$3 \mapsto 003561010102$
	4	$\mapsto$	02001301320301		$4 \mapsto 00310104000461050002$
	5	$\mapsto$	02320301		$5 \mapsto 003561050002$
	6	$\mapsto$	001320001		$6 \mapsto 0010461010102.$

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 7 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

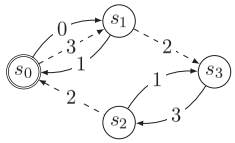

FIGURE 1. Stallings automaton of the image of the return substitution $\tau_{0,10}$ viewed as an endomorphism of $F(A_4)$. The distinguished state is identified by a double circle and the dashed edges form a spanning tree.

and the ω-presentations defined by $r_m(\phi)$ and $r_n(\phi)$ have the same number of generators. ∎

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 [20, Lemma 6.1]) by the spanning tree of the Stallings automaton of $\mathrm{Im}(\tau_{0,10})$ given in Figure 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

$\{3^{-1}2,\ 20^{-1},\ 2^{-1}302^{-1}1\}$ of $\mathrm{Im}(\tau_{0,1})$:

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

Another ω-presentation of $G(\tau)$ with 3 generators was obtained, by other means, in [5], where it is also shown that $d(G(\tau)) = 3$ [5, 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

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 $\mathbf{H}$ [26, 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 [4, 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 $A_4 = \{0, 1, 2, 3\}$:

$$\xi\colon\ \begin{aligned} 0 &\mapsto 001\\ 1 &\mapsto 02\\ 2 &\mapsto 301\\ 3 &\mapsto 320. \end{aligned}$$

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

$$\xi^{-1}\colon\ \begin{aligned} 0 &\mapsto 1^{-1}02^{-1}3\\ 1 &\mapsto (3^{-1}20^{-1}1)^20\\ 2 &\mapsto 3^{-1}20^{-1}11\\ 3 &\mapsto 20^{-1}1^{-1}02^{-1}3. \end{aligned}$$

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

Proof: First, note that the only unimodular substitution on a one-letter alphabet is the identity, which is not primitive. Thus, we may assume that φ is defined on an alphabet with at least two letters. By a result of Holton and Zamboni, it suffices to show that the invertible matrix $M(\varphi)$ has an eigenvalue of modulus less than 1 [18, Corollary 2.7]. We argue by contradiction. Suppose that all eigenvalues of $M(\varphi)$ have modulus at least 1 and let ρ be the spectral radius of $M(\varphi)$. Since $M(\varphi)$ is a primitive matrix, it follows from the Perron–Frobenius theorem that ρ is a simple eigenvalue of $M(\varphi)$ with strictly maximal modulus [17, Theorem 1.2.6]. Since φ is defined on at least two letters, $M(\varphi)$ has one eigenvalue λ distinct from ρ, and therefore $1 \leq |\lambda| < \rho$. But $\det(M(\varphi))$ is the product of the eigenvalues of $M(\varphi)$, all of which have modulus at least 1, hence $|\det(M(\varphi))| \geq \rho > 1$. This 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:

$$\begin{aligned} \varphi\colon\ 0 &\mapsto 02 \\ 1 &\mapsto 21 \\ 2 &\mapsto 10. \end{aligned}$$

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.

continuous surjective homomorphism between two free profinite groups of the same rank is an isomorphism [26, 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 [26, Lemma 3.2.3], it follows that $\widehat{\phi}$ is also an automorphism, and by [7, 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 [7, Proposition 3.7.4], $\widehat{\phi}$ is an automorphism and by [7, Proposition 4.6.8], so is ϕ. ∎

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 [5] which is recalled in the next proposition. Given $\psi \in \mathrm{End}(\widehat{F}(A))$ 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 [5, 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 ([5, 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 $\widehat{\phi}_H^n(t) = t$.

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 $a \in A$,

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

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

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

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. ∎

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

Proof: Let $L \in \mathbf{H}$ be generated by non-identity elements $x_1, \ldots, x_d$ of respective order $n_1, \ldots, n_d$. The main construction of [23] implies that for all integers m, n such that $m \geq 4d$ and $\mathrm{lcm}(n_1, \ldots, n_d) \mid n$, 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 $n = \mathrm{lcm}(n_1, \ldots, n_d)$. 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 $i = 1, \ldots, d$, 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 $m = p^k$ fulfills 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 [2, 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 [2, 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. This is mostly thanks to a result of Holton and Zamboni from [18], as we now proceed to show.

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

equivalent to showing that the pro-$\mathbf{H}$ topology of $\mathrm{Cl}_{\mathbf{H}}(K)$ coincides with the subspace topology induced by the pro-$\mathbf{H}$ topology of $F(A)$. This last statement holds by the last part of [22, 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:

$$\begin{array}{ccc} \widehat{F}(A_{u,v}) & \xrightarrow{\widetilde{\theta_{u,v}}} & \widehat{F}_{\mathbf{H}}(A) \\ \downarrow{\scriptstyle \widehat{\varphi_{u,v}}^{\omega}} & & \downarrow{\scriptstyle \widehat{\varphi}^{\omega}_{\mathbf{H}}} \\ \widehat{F}(A_{u,v}) & \xrightarrow{\widetilde{\theta_{u,v}}} & \widehat{F}_{\mathbf{H}}(A). \end{array}.$$

Since φ is $\mathbf{H}$-invertible, $\widehat{\varphi}^{\omega}_{\mathbf{H}}$ 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 [16, 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 [23].

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.*

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. ∎

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 [4, Example 7.2].

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

$$\begin{aligned} \alpha\colon\ 0 &\mapsto 01 \\ 1 &\mapsto 0001. \end{aligned}$$

This substitution is aperiodic (using for instance [7, 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:

$$\begin{aligned} \varrho\colon\ 0 &\mapsto 01 \\ 1 &\mapsto 00. \end{aligned}$$

It is a primitive substitution which is also aperiodic (using again [7, Exercise 5.15]). It admits $(1, 0)$ as a connection of order 2. The return substitution $\varrho_{1,0}$ is given by

$$\begin{aligned} \varrho_{1,0}\colon\ 0 &\mapsto 010 \\ 1 &\mapsto 01110. \end{aligned}$$

The incidence matrix of $\varrho_{1,0}$ has determinant 4. By Theorem 3.3, $\varrho_{1,0}$ defines an ω-presentation of $G(\varrho)$, hence we may apply Corollary 4.7 to conclude that $G(\varrho)$ 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 $\mathbf{G}_{\text{nil}}$ of finite nilpotent groups;
- the pseudovariety $\mathbf{G}_{\text{sol}}$ 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 $\mathbf{G}_{\text{sol}}$ are extension-closed, while $\mathbf{G}_{\text{nil}}$ 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-$\mathbf{H}$ groups can be found in [26, Section 3]. We call groups of the form $\widehat{F}_{\mathbf{H}}(A)$, where $\mathbf{H}$ 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 [5, 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 $\mathbf{H}$ 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 $\mathbf{H}$-*invertible* if $\widehat{\varphi}_{\mathbf{H}}$ is an automorphism, or equivalently if $\widehat{\varphi}^{\omega}_{\mathbf{H}}$ is the identity [7, Proposition 3.7.4]. Note that $\mathbf{G}$-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 $\widehat{F}(A)$ [7, Proposition 4.6.8].

Primitive substitutions also determine pseudovarieties of their own, which have been introduced in [5]: 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 $\mathbf{H}$ be a non-trivial extension-closed pseudovariety and φ be a primitive, aperiodic and $\mathbf{H}$-invertible substitution. Then, $\mathbf{H}$ 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 $\mathbf{H}$ is a non-trivial extension-closed pseudovariety, then free groups are residually $\mathbf{H}$ [26, 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-$\mathbf{H}$ 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 $\text{Cl}_{\mathbf{H}}(X)$ the closure of X in the pro-$\mathbf{H}$ 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 [22, 25, 26], but let us mention that results from [13] could be used as well. Alternatively, one could adapt the proof of [7, Proposition 4.6.5], which can be partly traced back to [1, Lemma 4.2].

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

Proof: By [25, Proposition 3.4], $\text{Cl}_{\mathbf{H}}(K)$ is a subgroup of $F(A)$ of rank at most that of K, so we may write $\text{Cl}_{\mathbf{H}}(K) = F(B)$, where $\text{Card}(B) \leq \text{Card}(A)$. Let $\iota\colon F(B) \hookrightarrow F(A)$ be the inclusion, and denote by $\widehat{\iota}_{\mathbf{H}}$ its extension to a continuous homormophism between the respective pro-$\mathbf{H}$ completions. By [26, Proposition 3.3.6], the pro-$\mathbf{H}$ 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

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

where the leftmost equality follows from [26, Lemma 3.2.4]. Therefore, it suffices to show that the pro-$\mathbf{H}$ extension $\widehat{\iota}_{\mathbf{H}}$ is injective. By [26, Lemma 3.2.6], this is