Linear involutions, bifix codes and free groups

Valérie Berthé*, Vincent Delecroix†, Francesco Dolce‡, Dominique Perrin ‡, Christophe Reutenauer§, Giuseppina Rindone‡

Abstract

We investigate the natural codings of linear involutions. We show that they have essentially the same combinatorial and algebraic properties as that of interval exchange transformations. One has to modify the definition of return words and to replace the basis of a subgroup by its symmetric version containing the inverses of its elements, called a monoidal basis. With these modifications, the set of first return words to a given word is a monoidal basis of the free group on the underlying alphabet A. Next, the set of first return words to a subgroup of finite index G of the free group on A is a monoidal basis of G. We give two different proofs of these results. The first one uses combinatorial arguments on labeled graphs. The second one is based on the geometric representation of linear involutions as Poincaré maps of measured foliations.

1 Introduction

A linear involution is an injective piecewise isometry of the interval. It allows to work with nonorientable foliations on nonorientable surfaces. Linear involutions were introduced by Danthony and Nogueira in [11, 12] as a natural generalization of interval exchange transformations. The study of linear involutions was later developed by Boissy and Lanneau in [8].

We initiate here the study of natural codings of linear involutions, in the spirit of our previous results on Sturmian sets [2] and on their generalizations as tree sets, introduced in [6]. A tree set is a language defined by the condition that the extension graph of each word is a tree. This graph describes the possible extensions of a word in the language on the left and on the right. We have proved in [6] that in a uniformly recurrent tree set, the sets of first return words are bases of the free group on the alphabet. Furthermore, we prove in [4] that if S is a uniformly recurrent tree set, then a finite bifix code is S-maximal with degree d if and only if it is a basis of a subgroup of index d. In particular, regular interval exchange sets are tree sets.

The natural codings of a linear involution are infinite words on an alphabet A whose letters and their inverses index the intervals exchanged by the involution. These infinite words encode the sequence of subintervals met by the orbits of the transformation.

We extend to natural codings of linear involutions most of the properties proved for uniformly recurrent tree sets [4, 5, 6]. One has to modify the definition of return words and to replace the basis of a subgroup by its symmetric version containing the inverses of its elements, called a monoidal basis. These definitions are motivated by the geometric representation of involutions as Poincaré maps of measured foliations.

We prove that if S is the natural coding of a linear involution without connection on the alphabet A, the following holds.

*Corresponding author, CNRS, Université Paris 7, funded by ANR Dyna3S
†CNRS, Université de Bordeaux
‡Université Paris Est, funded by ANR Eqinocs
§Université du Québec à Montréal

1. The set of first return words to a given word $u \in S$ is a monoidal basis of the free group on A (Theorem 5 or First Return Theorem).

2. A finite symmetric bifix code X is S-maximal if and only if it is a monoidal basis of a subgroup of finite index of the free group (Theorem 9 or Finite Index Basis Theorem).

The results that are given here combine concepts and tools issued from symbolic dynamical systems, the theory of codes, the study of subgroups of free groups and the geometry of measured foliations on surfaces. Indeed Theorem 5 and 10 can be proved with algebraic and combinatorial tools, but also geometrically, with the main actors being measured foliations of surfaces introduced by W. P. Thurston. They are defined on a compact surface X in which a finite number of points $\Sigma \subset X$ are removed. The free group is geometrically seen as the fundamental group $\pi_1(X \backslash \Sigma)$. Poincaré sections of these measured foliations are linear involutions. The return words to a given word can be seen as different ways of choosing a section that captures the geometry of the surface.

2 Linear involutions

Let A be an alphabet with k elements and let $A^{-1} = \{a^{-1} \mid a \in A\}$ be a copy of A. The map $a \mapsto a^{-1}$ is extended to an involution on $A \cup A^{-1}$ by defining $(a^{-1})^{-1} = a$. The notation a^{-1} is interpreted as an inverse in the free group on A.

We consider two copies $I \times \{0\}$ and $I \times \{1\}$ of an open interval I of the real line and denote $\hat{I} = I \times \{0, 1\}$. We call the sets $I \times \{0\}$ and $I \times \{1\}$ the two *components* of $\hat{I}$. We consider each component as an open interval.

A *generalized permutation* on A of type (ℓ, m), with $\ell + m = 2k$, is a bijection $\pi : \{1, 2, \ldots, 2k\} \to A \cup A^{-1}$. We represent it by a two line array

$$\pi = \begin{pmatrix} \pi(1)\ \pi(2)\ \ldots \pi(\ell) \\ \pi(\ell+1)\ \ldots \pi(\ell+m) \end{pmatrix}$$

A *length data* associated with (ℓ, m, π) is a positive vector $\lambda \in \mathbb{R}_+^{A \cup A^{-1}} = \mathbb{R}_+^{2k}$ such that

$$\lambda_{\pi(1)} + \ldots + \lambda_{\pi(\ell)} = \lambda_{\pi(\ell+1)} + \ldots + \lambda_{\pi(2k)} \text{ and } \lambda_a = \lambda_{a^{-1}} \text{ for all } a \in A.$$

We consider a partition of $I \times \{0\}$ (minus $\ell - 1$ points) in ℓ open intervals $I_{\pi(1)}, \ldots, I_{\pi(\ell)}$ of lengths $\lambda_{\pi(1)}, \ldots, \lambda_{\pi(\ell)}$ and a partition of $I \times \{1\}$ (minus $m - 1$ points) in m open intervals $I_{\pi(\ell+1)}, \ldots, I_{\pi(\ell+m)}$ of lengths $\lambda_{\pi(\ell+1)}, \ldots, \lambda_{\pi(\ell+m)}$. Let Σ be the set of $2k - 2$ *division points* separating the intervals I_a for $a \in A \cup A^{-1}$.

The *linear involution* on I relative to these data is the map $T = \sigma_2 \circ \sigma_1$ defined on the set $\hat{I} \setminus \Sigma$, formed of $\hat{I}$ minus $2k - 2$ points, and which is the composition of two involutions defined as follows.

(i) The first involution σ_1 is defined on $\hat{I} \setminus \Sigma$. It is such that for each $a \in A \cup A^{-1}$, its restriction to I_a is either a translation or a symmetry from I_a onto $I_{a^{-1}}$. Thus, there are real numbers α_a such that for any $(x, \delta) \in I_a$, one has $\sigma_1(x, \delta) = (x + \alpha_a, \gamma)$ in the first case and $\sigma_1(x, \delta) = (-x + \alpha_a, \gamma)$ in the second case (with $\gamma \in \{0, 1\}$).

(ii) The second involution exchanges the two components of $\hat{I}$. It is defined for $(x, \delta) \in \hat{I}$ by $\sigma_2(x, \delta) = (x, 1 - \delta)$. The image of z by σ_2 is called the *mirror image* of z.

Example 1 Let $A = \{a, b, c, d\}$ and

$$\pi = \begin{pmatrix} a & b & a^{-1} & c \\ c^{-1} & d^{-1} & b^{-1} & d \end{pmatrix}$$

Let T be the 4-linear involution corresponding to the length data represented in Figure 1 (we represent $I \times \{0\}$ above $I \times \{1\}$) with the assumption that the restriction of σ_1 to I_a and I_d is a symmetry while its restriction to I_b, I_c is a translation. We indicate on the figure the effect of

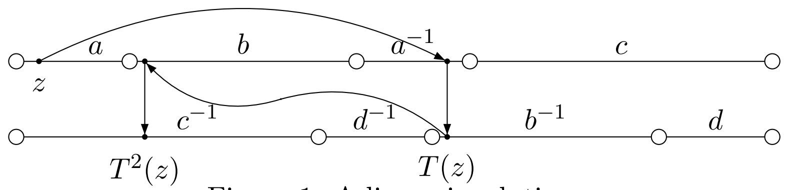

Figure 1: A linear involution.

the transformation T on a point z located in the left part of the interval I_a. The point $\sigma_1(z)$ is located in the right part of $I_{a^{-1}}$ and the point $T(z) = \sigma_2\sigma_1(z)$ is just below on the left of $I_{b^{-1}}$. Next, the point $\sigma_1 T(z)$ is located on the left part of I_b and the point $T^2(z)$ just below.

Thus the notion of linear involution is an extension of the notion of interval exchange transformation in the following sense. Assume that $\ell = k$, that $A = \{\pi(1), \ldots, \pi(k)\}$ and that the restriction of σ_1 to each subinterval is a translation. Then the restriction of T to $I \times \{0\}$ is an interval exchange (and so is its restriction to $I \times \{1\}$ which is the inverse of the first one). Thus in this case T is a pair of mutually inverse interval exchange transformations.

Two particular cases of linear involutions deserve attention. A linear involution T on the alphabet A relative to a generalized permutation π of type (ℓ, m) is said to be *nonorientable* if there are indices $i, j \le \ell$ such that $\pi(i) = \pi(j)^{-1}$ (and thus indices $i, j \ge \ell + 1$ such that $\pi(i) = \pi(j)^{-1}$). Otherwise T is said to be *orientable*. Linear involutions which are orientable correspond to interval exchange transformations. They also correspond to orientable laminations.

A linear involution $T = \sigma_2 \circ \sigma_1$ on I relative to the alphabet A is said to be *coherent* if for each $a \in A \cup A^{-1}$, the restriction of σ_1 to I_a is a translation if and only if I_a and $I_{a^{-1}}$ belong to distinct components of $\hat{I}$. Coherent linear involutions correspond to orientable surfaces. Thus coherent nonorientable involutions correspond to nonorientable laminations on orientable surfaces. The linear involution of Example 1 is coherent.

Let $O = \bigcup_{n \ge 0} T^{-n}(\Sigma)$ and $\hat{O} = O \cup \sigma_2(O)$ be respectively the negative orbit of the singular points and its closure under mirror image.

A *connection* of a linear involution T is a triple (x, y, n) where x is a singularity of T^{-1}, y is a singularity of T and $T^n x = y$. We call n the length of the connection.

We say that a transformation T defined on a topological space X is *minimal* if the nonnegative orbit $P(z) = \cup_{n \ge 0} T^n(z)$ of any point $z \in X$ is dense in X. In particular, a linear involution T on I without connection is minimal if for any point $z \in \hat{I} \setminus \hat{O}$ the nonnegative orbit of z is dense in $\hat{I}$. It is shown in [12] that noncoherent linear involutions are almost surely not minimal.

Let $X \subset I \times \{0, 1\}$. The *return time* ρ_X to X is the function from $I \times \{0, 1\}$ to $\mathbb{N} \cup \{\infty\}$ defined by

$$\rho_X(x) = \inf\{n \ge 1; T^n(x) \in X\}.$$

Let T be a linear involution without connection on I. If T is nonorientable, it is minimal. Otherwise, its restriction to each component of $\hat{I}$ is minimal. Moreover, for each interval of positive length included in $\hat{I}$, the return time to this interval takes a finite number of values. This is proved in [8] (Proposition 4.2) for the class of coherent involutions. The proof uses Keane's theorem proving that an interval exchange transformation without connection is minimal [13]. The proof of Keane's theorem also implies that for each interval of positive length, the return time to this interval is bounded.

3 Natural coding

3.1 Words and free groups

We denote by F_A the free group on A. We recall that, by *Scheier's Formula*, any basis of a subgroup of index d of a free group on k symbols has $d(k-1)+1$ elements.

A set of reduced words is said to be *symmetric* if it contains the inverses of its elements.

If X is a basis of a subgroup H of F_A, the set $X \cup X^{-1}$ is called a *monoidal basis* of H. In particular, $A \cup A^{-1}$ is a monoidal basis of F_A. Note that a monoidal basis is not a basis of H but that any $w \in H$ can be written uniquely $w = x_1 x_2 \cdots x_n$ with $x_i \in X \cup X^{-1}$ and $x_i x_{i+1}$ not equivalent to 1 for $1 \leq i \leq n-1$. In this sense, X generates uniquely the subgroup H without using inverses, justifying the term of 'monoidal basis'. If Y is a monoidal basis of a subgroup of index d in a free group on k symbols, then $\mathrm{Card}(Y) = 2d(k-1)+2$ by Schreier's Formula.

A set of words is said to be *factorial* if it contains the factors of its elements. Let S be a factorial set on an alphabet B (we have in mind the case $B = A \cup A^{-1}$). For $w \in S$, we denote

$$L(w) = \{a \in B \mid aw \in S\},\ R(w) = \{a \in B \mid wa \in S\},\ E(w) = \{(a,b) \in B \times B \mid awb \in S\}$$

and further

$$\ell(w) = \mathrm{Card}(L(w)), \quad r(w) = \mathrm{Card}(R(w)), \quad e(w) = \mathrm{Card}(E(w)).$$

For $w \in S$, we denote

$$m(w) = e(w) - \ell(w) - r(w) + 1.$$

According to [9] and [7, Chap. 4], the word w is called *weak* if $m(w) < 0$, *neutral* if $m(w) = 0$ and *strong* if $m(w) > 0$.

A symmetric factorial set of reduced words on the alphabet $A \cup A^{-1}$ is called a *laminary set* on A (following [10] and [14]). Following again the terminology of [10], we say that a laminary set S is *orientable* if there exist two factorial sets S_+, S_- such that $S = S_+ \cup S_-$ with $S_+ \cap S_- = \{\varepsilon\}$ and for any $x \in S$, one has $x \in S_-$ if and only if $x^{-1} \in S_+$.

3.2 Natural coding of linear involutions

Let T be linear involution on I. Given $z \in \hat{I} \setminus \hat{O}$, the *infinite natural coding* of T relative to z is the infinite word $\Sigma_T(z) = a_0 a_1 \ldots$ on the alphabet $A \cup A^{-1}$ defined by

$$a_n = a \quad \text{if} \quad T^n(z) \in I_a.$$

We denote by $L(T)$ the set of factors of the infinite natural codings of T. We say that $L(T)$ is the *natural coding* of T.

We first observe that the infinite word $\Sigma_T(z)$ is reduced. Indeed, assume that $a_n = a$ and $a_{n+1} = a^{-1}$ with $a \in A \cup A^{-1}$. Set $x = T^n(z)$ and $y = T(x) = T^{n+1}(z)$. Then $x \in I_a$ and $y \in I_{a^{-1}}$. But $y = \sigma_2(u)$ with $u = \sigma_1(x)$. Since $x \in I_a$, we have $u \in I_{a^{-1}}$. This implies that $y = \sigma_2(u)$ and u belong to the same component of $\hat{I}$, a contradiction.

The *factor complexity* of a factorial set S of words on an alphabet B is the sequence $p_n = \mathrm{Card}(S \cap B^n)$.

Proposition 2 *The factor complexity of the natural coding of a k-linear involution without connection is $p_n = 2n(k-1)+2$ for $n \geq 1$. Let T be a linear involution and let $S = L(T)$. If T is orientable, then S is orientable. The converse is true if T has no connection.*

3.3 Extension graphs

Let S be a biextendable set of words. For $w \in S$, we consider the set $E(w)$ as an undirected graph on the set of vertices which is the disjoint union of $L(w)$ and $R(w)$ with edges the pairs $(a,b) \in E(w)$. This graph is called the *extension graph* of w.

We say that a biextendable set of words S is *acyclic* if for every word $w \in S$, the graph $E(w)$ is acyclic. We say that S is a *tree set* if $E(w)$ is a tree for all $w \in S$. For more on tree sets, see [6].

Note that a word w such that $E(w)$ is acyclic is weak and that it is neutral if $E(w)$ is a tree.

One checks that the natural coding of any regular interval exchange set is a tree set. We will prove the following extension to linear involutions. It relies on the simple fact that for a linear involution T and for any word w of length n, the map T^n is a translation or symmetry from I_w to $T^n(I_w)$, where, for a nonempty word $w = a_0a_1 \cdots a_{m-1}$ on $A \cup A^{-1}$, we define $I_w = I_{a_0} \cap T^{-1}(I_{a_1}) \cap \ldots \cap T^{-m+1}(I_{a_{m-1}})$.

Theorem 3 *The natural coding S of a linear involution without connection is acyclic. Moreover, $E(\varepsilon)$ is a union of two disjoint isomorphic trees and for every nonempty word $w \in S$, the graph $E(w)$ is a tree.*

3.4 The First Return Theorem

Let S be a laminary set. For $w \in S$, a *complete return word* to w in S is a word that contains w or w^{-1} as a proper prefix and w or w^{-1} as a proper suffix. A complete return word to w is *simple* if its only occurrences of w, w^{-1} are as a prefix or a suffix.

The following result is the counterpart for linear involutions of Theorem 3.6 in [6] where a similar result is proved for uniformly recurrent tree sets (see also [1]).

Theorem 4 *Let S be the natural coding of a linear involution without connection on the alphabet A. For any $w \in S$, the set of simple complete return words to w has $2\,\mathrm{Card}(A)$ elements.*

To a complete return word u to w, we associate a word $N(u)$ obtained as follows. If u has w as prefix, we erase it and if u has a suffix w^{-1}, we also erase it. Note that these two operations can be made in any order since w and w^{-1} cannot overlap. The *first return words to w* are the words $N(u)$ associated with simple complete return words u to w.

The following result, which is the counterpart for linear involutions of Theorem 5.6 in [6] which states that the set of first return words to a given word in a uniformly recurrent tree set on the alphabet A is a basis of the free group on A. The proof relies on the fact that for $n \geq 2$, the Rauzy graph $\mathcal{G}_{n-1}$ is obtained from $\mathcal{G}_n$ by Stalling foldings corresponding to left special words.

Theorem 5 (The First Return Theorem) *Let S be the natural coding of a linear involution without connection on the alphabet A. For any $w \in S$, the set of first return words to w is a monoidal basis of F_A.*

4 Bifix codes

A prefix code is a set of nonempty words which does not contain any proper prefix of its elements. A suffix code is defined symmetrically. A *bifix code* is a set which is both a prefix code and a suffix code. For more on codes, see [3].

Let S be a set of words. A prefix (resp. bifix) code $X \subset S$ is S-maximal if it is not properly contained in any prefix (resp. bifix) code $Y \subset S$. A set of words S is *recurrent* if it is factorial and for any $u, w \in S$, there is a $v \in S$ such that $uvw \in S$. If S is recurrent, a finite S-maximal bifix code is also an S-maximal prefix code (see [2], Theorem 2.2).

A *parse* of a word w with respect to a bifix code X is a triple (v, x, u) such that $w = vxu$ where v has no suffix in X, u has no prefix in X and x belongs the submonoid X^* generated by X. By definition, the S-*degree* of X, denoted $d_X(S)$ is the maximal number of parses of a word in S. Thus, denoting $d_X(w)$ the number of parses of w, we have $d_X(S) = \max\{d_X(w) \mid w \in S\}$. Note that the degree of a word w is also equal to the number of suffixes of w which are not prefixes of X.

Let S be a recurrent set of words and let $X \subset S$ be a finite bifix code. By Theorem 4.2.8 in [2], X is S-maximal if and only if its S-degree d is finite.

We consider symmetric bifix codes. One checks that for any symmetric recurrent set of words S, an S-maximal bifix code X is symmetric if and only if $X \cup X^{-1}$ is a bifix code.

Example 6 Let S be a laminary set and let $X = S \cap (A \cup A^{-1})^n$ be the bifix code formed of the words of S of length n. It is an S-maximal bifix code of degree n.

The following result is a generalization of Theorem 3.6 in [4]. We will use it for natural codings of linear involutions. We state it for an alphabet B with intention to use it with $B = A \cup A^{-1}$ (as we did with Theorem 4).

Theorem 7 (Cardinality Theorem) *Let S be a recurrent set containing the alphabet B such that any nonempty word is neutral. For any finite S-maximal bifix code X with $d = d_X(S)$, one has* $\mathrm{Card}(X) + m(\varepsilon) - 1 = d(\mathrm{Card}(B) + m(\varepsilon) - 1)$.

Applying with $B = A \cup A^{-1}$ and $m(\varepsilon) = -1$ by Theorem 3, we have the following corollary.

Corollary 8 *Let S be the natural coding of a linear involution without connection on the alphabet A. For any finite S-maximal bifix code, one has* $\mathrm{Card}(X) - 2 = 2d_X(S)(\mathrm{Card}(A) - 1)$.

The following result is the counterpart for linear involutions of the finite index basis property holding for interval exchange transformations and, more generally, for uniformly recurrent tree sets (see [4]).

Theorem 9 (Finite index basis property) *Let S be the natural coding of a linear involution without connection and let $X \subset S$ be a finite symmetric bifix code. Then X is an S-maximal bifix code if and only if it is a monoidal basis of a subgroup of index $d_X(S)$.*

Let G be a subgroup of the free group F_A and let S be a laminary set on A. The set of *first return words* to G in S is the set of nonempty words in $G \cap S$ without a proper nonempty prefix in $G \cap S$. The set of first return words to G in S is a symmetric S-maximal bifix code. The following consequence of Theorem 9 is the counterpart for linear involutions of [5, Theorem 5.6].

Theorem 10 *Let T be a linear involution on A without connection and let $S = L(T)$. For any subgroup G of finite index of the free group F_A, the set of first return words to G in S is a monoidal basis of G.*

References

[1] L. Balková, E. Pelantová, and W. Steiner, *Sequences with constant number of return words*, Monatsh. Math., 155(3-4):251–263, 2008.

[2] J. Berstel, C. De Felice, D. Perrin, C. Reutenauer, and G. Rindone, *Bifix codes and Sturmian words*, J. Algebra, 369:146–202, 2012.

[3] J. Berstel, D. Perrin, and C. Reutenauer, *Codes and Automata*. Cambridge University Press, 2009.

[4] V. Berthé, C. De Felice, F. Dolce, J. Leroy, D. Perrin, C. Reutenauer, and G. Rindone, *The finite index basis property*, 2013. `http://arxiv.org/abs/1305.0127`.

[5] V. Berthé, C. De Felice, F. Dolce, J. Leroy, D. Perrin, C. Reutenauer, and G. Rindone, *Maximal bifix decoding*, 2013. `http://arxiv.org/abs/1308.5396`.

[6] V. Berthé, C. De Felice, F. Dolce, D. Perrin, J. Leroy, C. Reutenauer, and G. Rindone, *Acyclic, connected and tree sets*, 2013. `http://arxiv.org/abs/1308.4260`.

[7] V. Berthé and M. Rigo, *Combinatorics, automata and number theory*, volume 135 of *Encyclopedia Math. Appl.* Cambridge Univ. Press, Cambridge, 2010.

[8] C. Boissy and E. Lanneau, *Dynamics and geometry of the Rauzy-Veech induction for quadratic differentials*, Ergodic Theory Dynam. Systems, 29(3):767–816, 2009.

[9] J. Cassaigne, *Complexité et facteurs spéciaux*, Bull. Belg. Math. Soc. Simon Stevin, 4(1):67–88, 1997.

[10] T. Coulbois, A. Hilion, and M. Lustig, *$\mathbb{R}$-trees and laminations for free groups. I. Algebraic laminations*, J. Lond. Math. Soc. (2), 78(3):723–736, 2008.

[11] C. Danthony and A. Nogueira, *Involutions linéaires et feuilletages mesurés*, C. R. Acad. Sci. Paris Sér. I Math., 307(8):409–412, 1988.

[12] C. Danthony and A. Nogueira, *Measured foliations on nonorientable surfaces*, Ann. Sci. École Norm. Sup. (4), 23(3):469–494, 1990.

[13] M. Keane, *Interval exchange transformations*, Math. Z., 141:25–31, 1975.

[14] L.-M. Lopez and P. Narbel, *Lamination languages*, Ergodic Theory Dynam. Systems, 33(6):1813–1863, 2013.