Annali di Matematica (2007) 186(2):317–339
DOI 10.1007/s10231-006-0008-z

Christian Kassel · Christophe Reutenauer

Sturmian morphisms, the braid group B_4, Christoffel words and bases of F_2

Received: 11 June 2004 / Published online: 6 May 2006

Abstract We give a presentation by generators and relations of a certain monoid generating a subgroup of index two in the group $\mathrm{Aut}(F_2)$ of automorphisms of the rank two free group F_2 and show that it can be realized as a monoid in the group B_4 of braids on four strings. In the second part we use Christoffel words to construct an explicit basis of F_2 lifting any given basis of the free abelian group $\mathbf{Z}^2$. We further give an algorithm allowing to decide whether two elements of F_2 form a basis or not. We also show that, under suitable conditions, a basis has a unique conjugate consisting of two palindromes.

Keywords Free group · Sturmian morphism · Braid group · Symbolic dynamics · Christoffel word

Mathematics Subject Classification (2000) 05E99, 20E05, 20F28, 20F36, 20M05, 37B10, 68R15

1 Introduction

Let F_2 be the free group on two generators a and b. An automorphism of F_2 is said to be *positive* if it sends a and b onto words involving only positive powers of a and b. It follows from the results of Mignosi and Séébold [25] and Wen and Wen [30] that the positive automorphisms of F_2 preserve an important class of infinite words in a and b, called the Sturmian sequences. (Sturmian sequences occur

C. Kassel (✉)
Institut de Recherche Mathématique Avancée, CNRS – Université Louis Pasteur,
7 rue René Descartes, 67084 Strasbourg, Cedex, France
E-mail: kassel@math.u-strasbg.fr

C. Reutenauer
Mathématiques, Université du Québec à Montréal, Montréal, CP 8888,
succ. Centre Ville, Canada H3C 3P8
E-mail: reutenauer.christophe@uqam.ca

in various fields such as number theory, ergodic theory, dynamical systems, computer science, crystallography.) For this reason positive automorphisms are also called *Sturmian morphisms* in the literature. Following [22], Sect. 2.3, we denote St the submonoid of positive automorphisms in the group $\mathrm{Aut}(F_2)$ of automorphisms of F_2; the monoid St generates $\mathrm{Aut}(F_2)$ as a group.

In this article, we are interested in the submonoid St_0 of St consisting of the positive automorphisms acting by linear transformations of determinant one on the free abelian group $\mathbf{Z}^2$, which is obtained by abelianizing F_2. We call St_0 the *special Sturmian monoid* by analogy with the special linear group. The monoid St_0 is generated by four elements $G, \widetilde{G}, D, \widetilde{D}$ whose actions on $\mathbf{Z}^2$ coincide with the linear transformations $A, A, B, B \in \mathrm{Aut}(\mathbf{Z}^2) = GL_2(\mathbf{Z})$, respectively, where A and B are represented by the matrices

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \tag{1.1}$$

in the canonical basis of $\mathbf{Z}^2$. As is well known, the pair (A, B) satisfies the relation

$$AB^{-1}A = B^{-1}AB^{-1}. \tag{1.2}$$

The starting point of this paper was the observation that the pairs (G, D), $(G, \widetilde{D})$, $(\widetilde{G}, D)$, $(\widetilde{G}, \widetilde{D})$ satisfy Relation (1.2) in $\mathrm{Aut}(F_2)$, together with the commutation relations $G\widetilde{G} = \widetilde{G}G$ and $D\widetilde{D} = \widetilde{D}D$. This observation led us to an action of the braid group B_4 (whose elements are representable by braids with four strings) on the free group F_2, fitting into a commutative diagram of exact sequences of the form

$$\begin{array}{ccccccccc} 1 & \to & Z_4 & \to & B_4 & \to & \mathrm{Aut}(F_2) & \to & \mathbf{Z}/2 & \to 1 \\ & & \downarrow & & \downarrow & & \downarrow & & =\downarrow & \\ 1 & \to & 2Z_3 & \to & B_3 & \to & GL_2(\mathbf{Z}) & \to & \mathbf{Z}/2 & \to 1 \end{array} \tag{1.3}$$

where Z_4 (resp. Z_3) is the center of B_4 (resp. of the group B_3 of braids on three strings). Actually, we obtain a more precise expression of $\mathrm{Aut}(F_2)$ as a semi-direct product of $\mathbf{Z}/2$ with the quotient group B_4/Z_4.

The special Sturmian monoid St_0 mentioned above embeds in the kernel of $\mathrm{Aut}(F_2) \to \mathbf{Z}/2$, which by (1.3) is isomorphic to B_4/Z_4. We give a presentation of St_0 and show that it can be realized as a submonoid of B_4. This submonoid is generated in B_4 by four braids $\sigma_1, \sigma_2^{-1}, \sigma_3, \sigma_4^{-1}$, where $\sigma_1, \sigma_2, \sigma_3$ are the standard generators of B_4, and σ_4 is a braid interchanging the first and fourth strings behind the second and third ones.

A basis of F_2 is a pair (u, v) of elements of F_2 generating F_2 freely. A basis determines uniquely an automorphism of F_2, and *vice versa*. In 1917, Nielsen [26][1] proved that the group of outer automorphisms of F_2 is isomorphic to $GL_2(\mathbf{Z})$. In other words, two bases of F_2 are conjugate if and only if their images in the abelian quotient group $\mathbf{Z}^2$ coincide. Using Christoffel words, which are finite words related to Sturmian sequences, we construct in a simple way an explicit basis of F_2 lifting any given basis of $\mathbf{Z}^2$. Our construction is a geometric variant of Cohn's

[1] The title page of this paper carries the indication *Von J. Nielsen im Felde* and the last page the words *Konstantinopel im Oktober 1917*. According to Fenchel [15], Nielsen served as a military adviser to the Ottoman government during the First World War.

construction of primitive elements [10] and of Osborne and Zieschang's construction of bases (see [27] with corrections in [17]).

It is also shown in [26] that (u, v) is a basis of F_2 if and only if $uvu^{-1}v^{-1}$ is conjugate to $aba^{-1}b^{-1}$ or to $(aba^{-1}b^{-1})^{-1}$. In this paper we provide another criterion for (u, v) to be a basis; this criterion is based on chains of mutually conjugate couples of elements of F_2. Using these chains, we show that, if (u, v) is a basis of F_2 whose elements u and v are of odd length, then there is exactly one basis conjugate to (u, v) consisting of two palindromes.

The paper is organized as follows. In Sect. 2 we construct a group homomorphism $f : B_4 \to \mathrm{Aut}(F_2)$ and use it to express $\mathrm{Aut}(F_2)$ as a semi-direct product of $\mathbf{Z}/2$ by the quotient group B_4/Z_4. (Incidentally, we recover the well-known fact that B_4 and F_2 have isomorphic automorphism groups [21].) We also derive a quick proof of the freeness of the kernel of the standard epimorphism $B_4 \to B_3$. Section 3 is devoted to the special Sturmian monoid St_0: we give a presentation of St_0 by generators and relations and show that this monoid can be embedded into B_4. In Sect. 4 we use Christoffel words to associate to any basis of $\mathbf{Z}^2$ an explicit basis of F_2. Our characterization of bases and the existence of palindromic bases are presented in Sect. 5.

2 An action of the braid group B_4 on the free group F_2

In Ref. [13] Dyer et al. constructed a group homomorphism $h : B_4 \to \mathrm{Aut}(F_2)$ inducing an isomorphism of the quotient group B_4/Z_4 onto a subgroup of index two in $\mathrm{Aut}(F_2)$; their construction relies on the fact that the kernel of the standard epimorphism $B_4 \to B_3$ is a free group of rank two. In this section we proceed the other way round: we construct an action of B_4 on F_2 by observing *braid relations* between certain generators of the monoid of positive automorphisms of F_2. From this we derive that $\mathrm{Aut}(F_2)$ is isomorphic to a semi-direct product of $\mathbf{Z}/2$ by the quotient group B_4/Z_4, and we easily recover the freeness of the kernel of $B_4 \to B_3$.

Following the notation of [22], Sect. 2.2.2, we define positive automorphisms $D, \widetilde{D}, G, \widetilde{G}, E$ of F_2 of the free group F_2 on a and b by

$$\begin{array}{llll} D(a) = ba, & D(b) = b, & \widetilde{D}(a) = ab, & \widetilde{D}(b) = b, \\ G(a) = a, & G(b) = ab, & \widetilde{G}(a) = a, & \widetilde{G}(b) = ba, \\ & E(a) = b, & E(b) = a. & \end{array} \tag{2.1}$$

The sets $\{E, D, \widetilde{D}\}$ and $\{E, G, \widetilde{G}\}$ are generating sets of the monoid St (see Ref. [30] or [22], Sect. 2.3). The automorphisms G and $\widetilde{G}$ map to the automorphism $A \in \mathrm{Aut}(\mathbf{Z}^2)$ under the abelianization map $\mathrm{Aut}(F_2) \to \mathrm{Aut}(\mathbf{Z}^2)$, whereas D and $\widetilde{D}$ map to $B \in \mathrm{Aut}(\mathbf{Z}^2)$, where A and B are defined by (1.1).

The following lemma will be our main tool for the construction of an action of B_4 on F_2.

Lemma 2.1 *The automorphisms $D, \widetilde{D}, G, \widetilde{G}, E$ satisfy the relations*

$$GD^{-1}G = D^{-1}GD^{-1}, \quad D^{-1}\widetilde{G}D^{-1} = \widetilde{G}D^{-1}\widetilde{G}, \quad G\widetilde{G} = \widetilde{G}G,$$

$$\widetilde{G}\widetilde{D}^{-1}\widetilde{G} = \widetilde{D}^{-1}\widetilde{G}\widetilde{D}^{-1}, \quad \widetilde{D}^{-1}G\widetilde{D}^{-1} = G\widetilde{D}^{-1}G, \quad D\widetilde{D} = \widetilde{D}D,$$

$$GD\widetilde{G} = \widetilde{G}\widetilde{D}G, \quad DG\widetilde{D} = \widetilde{D}\widetilde{G}D,$$
$$E^2 = \mathrm{id}, \quad D = EGE, \quad \widetilde{D} = E\widetilde{G}E.$$

Proof These relations are easily checked on the generators a and b after observing that $D^{-1}(a) = b^{-1}a$ and $D^{-1}(b) = b$, and that $\widetilde{D}^{-1}(a) = ab^{-1}$ and $\widetilde{D}^{-1}(b) = b$. □

In the previous lemma the first three relations involving G, D^{-1}, and $\widetilde{G}$ are defining relations for the braid group B_4. (Actually, the first six relations are the defining relations for the generalized braid group associated to the affine Coxeter group of type $\widetilde{A}_3$ in the nomenclature of [8], but we won't make use of this fact.)

Recall that the braid group B_n ($n \geq 2$) is the group generated by $\sigma_1, \ldots, \sigma_{n-1}$ and the relations

$$\sigma_i \sigma_j = \sigma_j \sigma_i \tag{2.2}$$

for all $i, j \in \{1, \ldots, n-1\}$ such that $|i-j| \geq 2$, and

$$\sigma_i \sigma_{i+1} \sigma_i = \sigma_{i+1} \sigma_i \sigma_{i+1} \tag{2.3}$$

for all $i \in \{1, \ldots, n-2\}$.

Set $\delta = \sigma_1 \cdots \sigma_{n-1}$. It is well known see [5] that the center Z_n of B_n is the infinite cyclic group generated by δ^n, and that

$$\delta \sigma_i \delta^{-1} = \sigma_{i+1} \tag{2.4}$$

for all $i = 1, \ldots, n-2$. We define a new element $\sigma_n \in B_n$ by

$$\sigma_n = \delta \sigma_{n-1} \delta^{-1} = \delta^{n-1} \sigma_1 \delta^{-(n-1)}. \tag{2.5}$$

The group B_n can also be viewed as the fundamental group of the configuration space of n (unordered) points in the complex line $\mathbf{C}$. The standard generators $\sigma_1, \ldots, \sigma_{n-1}$ appear naturally when one makes the standard choice of base point for the configuration space, namely the point $\{1, 2, \ldots, n\}$. When one chooses the set of n-th roots of unity in $\mathbf{C}$ as a base point, then the braid σ_n comes up as well. When one disposes n strings vertically on a cylinder, then the element δ can be represented as the braid obtained by applying a rotation of angle $2\pi/n$ to the bottom ends of the strings, and σ_n is the braid intertwining the n-th and the first strings (see Fig. 1 for the case $n = 4$).

Introducing σ_n yields *cyclic braid relations* as shown in the following lemma.

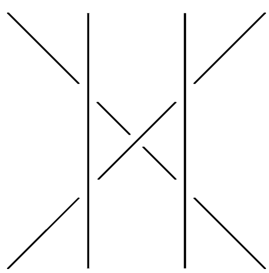

Fig. 1 The braid σ_4 in B_4

Lemma 2.2 *We have the following relations in B_n:*
(a) $\delta\sigma_n\delta^{-1} = \sigma_1$,
(b) *for all* $i = 1, 2, \ldots, n$,

$$\delta = \sigma_i\sigma_{i+1}\cdot\cdots\cdot\sigma_{i-2},$$

where indices are taken modulo n,
(c) $\sigma_i\sigma_n = \sigma_n\sigma_i$ *for all* $i = 2, \ldots, n-2$, *and*

$$\sigma_{n-1}\sigma_n\sigma_{n-1} = \sigma_n\sigma_{n-1}\sigma_n \quad \textit{and} \quad \sigma_n\sigma_1\sigma_n = \sigma_1\sigma_n\sigma_1.$$

Proof (a) Since δ^n is central, we have $\delta\sigma_n\delta^{-1} = \delta^n\sigma_1\delta^{-n} = \sigma_1$.
(b) We have

$$\sigma_i\sigma_{i+1}\cdot\cdots\cdot\sigma_{i-2} = \delta^{i-1}(\sigma_1\cdots\sigma_{n-1})\delta^{-(i-1)} = \delta^{i-1}\delta\delta^{-(i-1)} = \delta.$$

(c) If $i = 2, \ldots, n-2$, Relation (2.2) implies

$$\sigma_i\sigma_n = \delta(\sigma_{i-1}\sigma_{n-1})\delta^{-1} = \delta(\sigma_{n-1}\sigma_{i-1})\delta^{-1} = \sigma_n\sigma_i.$$

Relation (2.3) implies

$$\sigma_{n-1}\sigma_n\sigma_{n-1} = \delta(\sigma_{n-2}\sigma_{n-1}\sigma_{n-2})\delta^{-1} = \delta(\sigma_{n-1}\sigma_{n-2}\sigma_{n-1})\delta^{-1} = \sigma_n\sigma_{n-1}\sigma_n$$

and

$$\sigma_n\sigma_1\sigma_n = \delta^{-1}(\sigma_1\sigma_2\sigma_1)\delta = \delta^{-1}(\sigma_2\sigma_1\sigma_2)\delta = \sigma_1\sigma_n\sigma_1. \qquad \square$$

In the sequel we are interested only in the case when $n = 4$. The group B_4 has a presentation with generators $\sigma_1, \sigma_2, \sigma_3$, and relations

$$\sigma_1\sigma_2\sigma_1 = \sigma_2\sigma_1\sigma_2, \quad \sigma_2\sigma_3\sigma_2 = \sigma_3\sigma_2\sigma_3, \quad \sigma_1\sigma_3 = \sigma_3\sigma_1. \tag{2.6}$$

The element δ defined above now is $\delta = \sigma_1\sigma_2\sigma_3$. Its fourth power δ^4 generates the center Z_4 of B_4. The element $\sigma_4 = \delta\sigma_3\delta^{-1} \in B_4$ satisfies the following relations, which are special instances of the relations in Lemma 2.2:

$$\begin{gathered}\sigma_1\sigma_2\sigma_3 = \sigma_2\sigma_3\sigma_4 = \sigma_3\sigma_4\sigma_1 = \sigma_4\sigma_1\sigma_2 = \delta,\\ \sigma_2\sigma_4 = \sigma_4\sigma_2, \quad \sigma_3\sigma_4\sigma_3 = \sigma_4\sigma_3\sigma_4, \quad \sigma_4\sigma_1\sigma_4 = \sigma_1\sigma_4\sigma_1.\end{gathered} \tag{2.7}$$

As a consequence, σ_4 has the following expressions:

$$\sigma_4 = \sigma_3^{-1}\sigma_2^{-1}\sigma_1\sigma_2\sigma_3 = \sigma_3^{-1}\sigma_1\,\sigma_2\,\sigma_3\sigma_1^{-1} = \sigma_1\sigma_2\sigma_3\sigma_2^{-1}\sigma_1^{-1} \tag{2.8}$$

(see Fig. 1 for a geometric representation of σ_4).
Using σ_4, we define an involution ω on B_4 as follows.

Lemma 2.3 *There is an involutive automorphism ω of B_4 defined by*

$$\omega(\sigma_1) = \sigma_2^{-1}, \quad \omega(\sigma_2) = \sigma_1^{-1}, \quad \omega(\sigma_3) = \sigma_4^{-1}.$$

Moreover, $\omega(\delta) = \delta^{-1}$.

Proof (a) The existence of ω follows from (2.6) and (2.7). To complete the proof that ω is an involution, it remains to check that $\omega(\sigma_4) = \sigma_3^{-1}$. This follows from (2.7) and (2.8). Indeed,

$$\begin{aligned}\omega(\sigma_4) &= \omega(\sigma_1\sigma_2\sigma_3\sigma_2^{-1}\sigma_1^{-1}) = \sigma_2^{-1}\sigma_1^{-1}\sigma_4^{-1}\sigma_1\sigma_2 \\ &= (\sigma_4\sigma_1\sigma_2)^{-1}\sigma_1\sigma_2 = (\sigma_1\sigma_2\sigma_3)^{-1}\sigma_1\sigma_2 \\ &= \sigma_3^{-1}\sigma_2^{-1}\sigma_1^{-1}\sigma_1\sigma_2 = \sigma_3^{-1}.\end{aligned}$$

(b) By (2.7),

$$\omega(\delta) = \omega(\sigma_1\sigma_2\sigma_3) = \sigma_2^{-1}\sigma_1^{-1}\sigma_4^{-1} = (\sigma_4\sigma_1\sigma_2)^{-1} = \delta^{-1}. \qquad \square$$

Remark 2.4 Karrass et al. [21], Theorem 3 showed that the group $\mathrm{Out}(B_4)$ of outer automorphisms of B_4 is generated by an involution α, which they define using a presentation of B_4 that is different from the one above. A quick computation shows that our ω coincides with their α. In Dyer et al. [14] it is proved that $\mathrm{Out}(B_4)$ is also generated by the involution θ sending each generator $\sigma_1, \sigma_2, \sigma_3$ of B_4 to its inverse. It is easy to check that ω and θ are related by

$$\omega = \mathrm{Ad}(\sigma_1\sigma_2\sigma_1) \circ \theta,$$

where $\mathrm{Ad}(\sigma_1\sigma_2\sigma_1)$ is the inner automorphism of B_4 defined for all $\beta \in B_4$ by $\mathrm{Ad}(\sigma_1\sigma_2\sigma_1)(\beta) = (\sigma_1\sigma_2\sigma_1)\beta(\sigma_1\sigma_2\sigma_1)^{-1}$.

Let $\widetilde{B}_4 = B_4 \rtimes \mathbf{Z}/2$ be the semi-direct product of $\mathbf{Z}/2$ by B_4, where $\mathbf{Z}/2$ acts on B_4 *via* ω. The group $\widetilde{B}_4$ has a presentation with generators $\sigma_1, \sigma_2, \sigma_3, \omega$, subject to Relations (2.6) and to the relations

$$\omega^2 = 1, \quad \omega\sigma_1 = \sigma_2^{-1}\omega, \quad \omega\sigma_2 = \sigma_1^{-1}\omega, \quad \omega\sigma_3 = \sigma_4^{-1}\omega, \tag{2.9}$$

where σ_4 is given by (2.8). By Lemma 2.3 we have

$$\omega\delta = \omega(\delta)\omega = \delta^{-1}\omega \in \widetilde{B}_4. \tag{2.10}$$

Since the involution ω preserves the center Z_4, it induces an involution on the quotient group B_4/Z_4 and we may consider the semi-direct product $\widetilde{B}_4/Z_4 = B_4/Z_4 \rtimes \mathbf{Z}/2$ of $\mathbf{Z}/2$ by B_4/Z_4.

Remark 2.5 It follows from [21], Theorem 3 and from Remark 2.4 that $\widetilde{B}_4/Z_4$ is isomorphic to the group $\mathrm{Aut}(B_4)$ of automorphisms of B_4:

$$\mathrm{Aut}(B_4) \cong \widetilde{B}_4/Z_4 = B_4/Z_4 \rtimes \mathbf{Z}/2.$$

Therefore, $\mathrm{Aut}(B_4)$ has $\widetilde{B}_4$ as an extension with abelian kernel $Z_4 \cong \mathbf{Z}$:

$$1 \to Z_4 \to \widetilde{B}_4 \to \mathrm{Aut}(B_4) \to 1.$$

The group $\mathrm{Aut}(B_4)$ acts by conjugation on the kernel Z_4 as follows: the generators $\sigma_1, \sigma_2, \sigma_3$ act trivially (since Z_4 is the center of B_4) and, as a consequence of (2.10), ω acts on the generator δ^4 of Z_4 by sending it to its inverse.

We now relate B_4 and $\mathrm{Aut}(F_2)$.

Lemma 2.6 *There is a group homomorphism $f : B_4 \to \mathrm{Aut}(F_2)$ defined by*

$$f(\sigma_1) = G, \quad f(\sigma_2) = D^{-1}, \quad f(\sigma_3) = \widetilde{G}.$$

Moreover,

$$f(\sigma_4) = \widetilde{D}^{-1}, \quad f(\delta^4) = \mathrm{id}, \quad Ef(\sigma_i) = f(\omega(\sigma_i))E$$

for $i = 1, 2, 3$.

The homomorphism $h : B_4 \to \mathrm{Aut}(F_2)$ of ([13], p. 406) is related to the above-defined homomorphism f by $f(\beta) = V \circ h(\beta) \circ V^{-1}$ for all $\beta \in B_4$, where V is the automorphism of F_2 fixing a and sending b onto ab^{-1}.

One can also check that our homomorphism f is a special case of a homomorphism $B_{2g+2} \to \mathrm{Aut}(F_{2g})$ defined for all $g \geq 1$ and obtained from considering an orientable genus g surface with two punctures as a double covering of $\mathbf{R}^2$ branched over $2g + 2$ points under the hyperelliptic involution (see [4, 6]).

Proof of Lemma 2.6 (a) The existence of f is a consequence of the first three relations in Lemma 2.1 and Relations (2.6).
(b) By (2.8) and Lemma 2.1 (third and seventh relations) we obtain

$$\begin{aligned} f(\sigma_4) &= f(\sigma_3^{-1}\sigma_1\,\sigma_2\,\sigma_3\sigma_1^{-1}) \\ &= \widetilde{G}^{-1}GD^{-1}\widetilde{G}G^{-1} = G\widetilde{G}^{-1}D^{-1}G^{-1}\widetilde{G} \\ &= G(GD\widetilde{G})^{-1}\widetilde{G} = G(\widetilde{G}\widetilde{D}G)^{-1}\widetilde{G} \\ &= GG^{-1}\widetilde{D}^{-1}\widetilde{G}^{-1}\widetilde{G} = \widetilde{D}^{-1}. \end{aligned}$$

We have $f(\delta) = GD^{-1}\widetilde{G}$. A quick computation yields $f(\delta)(a) = b^{-1}$ and $f(\delta)(b) = a$, from which $f(\delta^4) = \mathrm{id}$ follows immediately. The relations $Ef(\sigma_i) = f(\omega(\sigma_i))E$ for $i = 1, 2, 3$ are respectively equivalent to $EG = DE$, $ED^{-1} = G^{-1}E$, $E\widetilde{G} = \widetilde{D}E$, which follow from the relations in Lemma 2.1 involving E. □

The following is an immediate consequence of Lemma 2.6.

Corollary 2.7 *The homomorphism $f : B_4 \to \mathrm{Aut}(F_2)$ extends to a group homomorphism $\widetilde{f} : \widetilde{B}_4 \to \mathrm{Aut}(F_2)$ such that $\widetilde{f}(\omega) = E$ and $\widetilde{f}(Z_4) = \{\mathrm{id}\}$.*

The next theorem is the main result of this section.

Theorem 2.8 *The group homomorphism $\widetilde{B}_4/Z_4 \to \mathrm{Aut}(F_2)$ induced by $\widetilde{f}$: $\widetilde{B}_4 \to \mathrm{Aut}(F_2)$ is an isomorphism*

$$\widetilde{B}_4/Z_4 = B_4/Z_4 \rtimes \mathbf{Z}/2 \cong \mathrm{Aut}(F_2).$$

Proof The group $\mathrm{Aut}(F_2)$ has a presentation with generators E, $\widetilde{D}$, O, where the latter is defined by $O(a) = a^{-1}$ and $O(b) = b$; and relations

$$\begin{aligned} E^2 = O^2 = (EOE\widetilde{D})^2 = 1, \\ (O\widetilde{D})^2 = (\widetilde{D}O)^2, \\ (EO)^4 = (\widetilde{D}OE)^3 = 1 \end{aligned} \tag{2.11}$$

(see [11], pp. 89–90). Set

$$g(E) = \omega, \quad g(\widetilde{D}) = \sigma_4^{-1}, \quad g(O) = \omega\sigma_1\sigma_2\sigma_3.$$

Let us use the above presentation to prove that these formulas define a group homomorphism

$$g : \mathrm{Aut}(F_2) \to \widetilde{B_4}/Z_4.$$

We have to check that the elements $g(E)$, $g(O)$, $g(\widetilde{D})$ satisfy Relations (2.11) in $\widetilde{B_4}/Z_4$ (actually, the first four relations are satisfied in $\widetilde{B_4}$). In the computations below we shall use Relations (2.7) and (2.9) repeatedly.

Relation $E^2 = 1$: The identity $g(E)^2 = 1$ follows from $\omega^2 = 1$.

Relation $O^2 = 1$: We obtain

$$\begin{aligned} g(O)^2 &= \omega\sigma_1\sigma_2\sigma_3\omega\sigma_1\sigma_2\sigma_3 \\ &= \sigma_2^{-1}\sigma_1^{-1}\sigma_4^{-1}\omega^2\sigma_1\sigma_2\sigma_3 \\ &= (\sigma_4\sigma_1\sigma_2)^{-1}(\sigma_1\sigma_2\sigma_3) = 1. \end{aligned}$$

Relation $(EOE\widetilde{D})^2 = 1$: We obtain

$$\begin{aligned} (g(E)g(O)g(E)g(\widetilde{D}))^2 &= (\sigma_1\sigma_2\sigma_3\omega\sigma_4^{-1})^2 \\ &= \sigma_1\sigma_2\sigma_3\omega\sigma_4^{-1}\,\underbrace{\sigma_1\sigma_2\sigma_3}\,\omega\sigma_4^{-1} \\ &= \sigma_1\sigma_2\sigma_3\,\underbrace{\omega\,\overbrace{\sigma_4^{-1}\sigma_4}\,\sigma_1\sigma_2}\,\omega\sigma_4^{-1} \\ &= \sigma_1\sigma_2\sigma_3\,\underbrace{\sigma_2^{-1}\sigma_1^{-1}\sigma_4^{-1}} \\ &= \sigma_1\sigma_2\sigma_3(\sigma_4\sigma_1\sigma_2)^{-1} = 1. \end{aligned}$$

Relation $(O\widetilde{D})^2 = (\widetilde{D}O)^2$: We have

$$\begin{aligned} (g(O)g(\widetilde{D}))^2 &= (\omega\,\underbrace{\sigma_1\sigma_2\sigma_3}\,\sigma_4^{-1})^2 \\ &= (\omega\sigma_2\sigma_3\,\underbrace{\sigma_4\sigma_4^{-1}})^2 \\ &= \underbrace{\omega\sigma_2\sigma_3}\,\omega\sigma_2\sigma_3 \\ &= \sigma_1^{-1}\sigma_4^{-1}\sigma_2\sigma_3. \end{aligned}$$

On the other hand,

$$
\begin{aligned}
(g(\widetilde{D})g(O))^2 &= \left(\sigma_4^{-1}\omega\sigma_1\sigma_2\sigma_3\right)^2 \\
&= \sigma_4^{-1}\omega \underbrace{\sigma_1\sigma_2\sigma_3}\sigma_4^{-1}\omega\sigma_1\sigma_2\sigma_3 \\
&= \sigma_4^{-1}\omega\sigma_2\sigma_3 \underbrace{\sigma_4\sigma_4^{-1}}\omega\sigma_1\sigma_2\sigma_3 \\
&= \sigma_4^{-1} \underbrace{\omega\sigma_2\sigma_3}\omega\sigma_1\sigma_2\sigma_3 \\
&= \underbrace{\sigma_4^{-1}\sigma_1^{-1}\sigma_4^{-1}}\sigma_1\sigma_2\sigma_3 \\
&= \sigma_1^{-1}\sigma_4^{-1} \underbrace{\sigma_1^{-1}\sigma_1}\sigma_2\sigma_3 \\
&= \sigma_1^{-1}\sigma_4^{-1}\sigma_2\sigma_3.
\end{aligned}
$$

Therefore, $(g(O)g(\widetilde{D}))^2 = (g(\widetilde{D})g(O))^2$.

Relation $(EO)^4 = 1$: We have

$$
(g(E)g(O))^4 = (\omega^2\sigma_1\sigma_2\sigma_3)^4 = (\sigma_1\sigma_2\sigma_3)^4 = \delta^4 = 1 \in \widetilde{B_4}/Z_4.
$$

Relation $(\widetilde{D}OE)^3 = 1$: We obtain

$$
\begin{aligned}
(g(\widetilde{D})g(O)g(E))^3 &= \left(\sigma_4^{-1}\underbrace{\omega\sigma_1\sigma_2\sigma_3}\omega\right)^3 = \left(\sigma_4^{-1}\sigma_2^{-1}\sigma_1^{-1}\sigma_4^{-1}\right)^3 \\
&= \left(\underbrace{\sigma_4\sigma_1\sigma_2}\sigma_4\right)^{-3} = (\sigma_1\sigma_2\sigma_3\sigma_4)^{-3} \\
&= \left(\underbrace{\sigma_1\sigma_2\sigma_3}\underbrace{\sigma_4\sigma_1\sigma_2}\underbrace{\sigma_3\sigma_4\sigma_1}\underbrace{\sigma_2\sigma_3\sigma_4}\right)^{-1} \\
&= (\sigma_1\sigma_2\sigma_3)^{-4} = \delta^{-4} = 1 \in \widetilde{B_4}/Z_4.
\end{aligned}
$$

We claim that $\widetilde{f} \circ g = \mathrm{id}$, which implies that g is injective. To prove the claim, it suffices to check that $\widetilde{f} \circ g$ fixes the generators E, $\widetilde{D}$, O of $\mathrm{Aut}(F_2)$. Indeed, by Lemma 2.6 and Corollary 2.7 we have

$$
(\widetilde{f} \circ g)(E) = \widetilde{f}(\omega) = E \quad \text{and} \quad (\widetilde{f} \circ g)(\widetilde{D}) = \widetilde{f}\left(\sigma_4^{-1}\right) = \widetilde{D}.
$$

Moreover, $(\widetilde{f} \circ g)(O) = \widetilde{f}(\omega\sigma_1\sigma_2\sigma_3) = EGD^{-1}\widetilde{G}$. Now a simple check shows that the automorphism $EGD^{-1}\widetilde{G}$ sends a to a^{-1} and fixes b, hence is the same as the automorphism O.

To complete the proof of the theorem, it now suffices to establish that g is surjective or, equivalently, that the generators $\sigma_1, \sigma_2, \sigma_3, \omega$ are in the image of g. This is clear for ω and σ_3 since $\omega = g(E)$ and $\sigma_3 = \omega\sigma_4^{-1}\omega = g(E\widetilde{D}E)$. For σ_2 we have $\sigma_2 = \omega\sigma_1^{-1}\omega = g(E)\sigma_1^{-1}g(E)$. It thus suffices to verify that σ_1

belongs to the image of g. We claim $\sigma_1 = g(OEO\widetilde{D}OEO)$. Indeed, by (2.4), (2.9), (2.10),

$$\begin{aligned} g(OEO\widetilde{D}OEO) &= \omega\sigma_1\sigma_2\sigma_3\omega^2\sigma_1\sigma_2\sigma_3 \underbrace{\sigma_4^{-1}\omega}\, \sigma_1\sigma_2\sigma_3\omega^2\sigma_1\sigma_2\sigma_3 \\ &= \omega(\sigma_1\sigma_2\sigma_3)^2\omega\sigma_3(\sigma_1\sigma_2\sigma_3)^2 = \omega\delta^2\omega\sigma_3\delta^2 \\ &= \delta^{-2}\omega^2\sigma_3\delta^2 = \delta^{-2}\sigma_3\delta^2 = \sigma_1. \end{aligned}$$ □

Corollary 2.9 *The subgroup of* Aut(F_2) *generated by* $D, \widetilde{D}, G, \widetilde{G}$ *is isomorphic to* B_4/Z_4.

Remark 2.10 As a consequence of Theorem 2.8 and of Remark 2.5, we recover the isomorphism

$$\mathrm{Aut}(B_4) \cong \mathrm{Aut}(F_2)$$

proved by Karrass et al. (see [21], Theorem 5).

We next determine the braids $\beta \in B_4$ for which the automorphim $f(\beta)$ of F_2 is inner. It is well known (see [11], Sects. 6.1 and 7.2) that the modular group $SL_2(\mathbf{Z}) = \{g \in GL_2(\mathbf{Z}) \mid \det(g) = 1\}$ is generated by the matrices

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad B^{-1} = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix},$$

and that all relations in this group can be deduced from the relations

$$AB^{-1}A = B^{-1}AB^{-1} \quad \text{and} \quad (AB^{-1}A)^4 = 1. \tag{2.12}$$

It follows that there is a group homomorphism $\bar{\pi} : B_3 \to GL_2(\mathbf{Z})$ defined by $\bar{\pi}(\sigma_1) = A$ and $\bar{\pi}(\sigma_2) = B^{-1}$.

Lemma 2.11 *The kernel of* $\bar{\pi} : B_3 \to GL_2(\mathbf{Z})$ *is the central subgroup of* B_3 *generated by* $(\sigma_1\sigma_2\sigma_1)^4 = (\sigma_1\sigma_2)^6$.

Proof It follows from the presentation of B_3 and from (2.12) that the kernel of $\bar{\pi} : B_3 \to GL_2(\mathbf{Z})$ is the normal subgroup generated by $(\sigma_1\sigma_2\sigma_1)^4$. We conclude by observing that the latter is the square of the element

$$(\sigma_1\sigma_2\sigma_1)^2 = (\sigma_1\sigma_2\sigma_1)(\sigma_2\sigma_1\sigma_2) = (\sigma_1\sigma_2)^3,$$

which generates the center Z_3 of B_3 □

Let N be the subgroup of B_4 generated by $\sigma_1\sigma_3^{-1}$, $\sigma_2\sigma_1\sigma_3^{-1}\sigma_2^{-1}$, and δ^4.

Proposition 2.12 *An automorphism* $f(\beta) \in$ Aut(F_2) $(\beta \in B_4)$ *is inner if and only if* β *belongs to* N.

Proof Let $\pi : B_4 \to GL_2(\mathbf{Z})$ be the group homomorphism obtained by composing $f : B_4 \to \mathrm{Aut}(F_2)$ with the abelianization map $\mathrm{Aut}(F_2) \to GL_2(\mathbf{Z})$. Since by [26] the kernel of the map $\mathrm{Aut}(F_2) \to GL_2(\mathbf{Z})$ is the subgroup of inner automorphisms of F_2, the automorphism $f(\beta)$ of F_2 is inner if and only if $\pi(\beta) \in GL_2(\mathbf{Z})$ is the identity matrix. An easy computation yields

$$\pi(\sigma_1) = \pi(\sigma_3) = A \quad \text{and} \quad \pi(\sigma_2) = B^{-1}, \tag{2.13}$$

where A and B^{-1} are the above-defined matrices. Let $F \subset B_4$ be the kernel of the group homomorphism $q : B_4 \to B_3$ sending both σ_1 and σ_3 onto $\sigma_1 \in B_3$, and σ_2 onto $\sigma_2 \in B_3$. The subgroup F is the normal subgroup of B_4 generated by $\sigma_1\sigma_3^{-1}$. It follows from (2.13) that $\pi = \bar{\pi} \circ q : B_4 \to GL_2(\mathbf{Z})$, where $\bar{\pi} : B_3 \to GL_2(\mathbf{Z})$ is the homomorphism defined above. Lemma 2.11 then implies that $f(\beta)$ is inner if and only if β belongs to the smallest normal subgroup of B_4 containing F and $(\sigma_1\sigma_2\sigma_1)^4$. We observe that $(\sigma_1\sigma_2\sigma_1)^4 \equiv (\sigma_1\sigma_2\sigma_3)^4 = \delta^4$ modulo F.

To conclude, it suffices to check that the normal subgroup of B_4 generated by $\sigma_1\sigma_3^{-1}$ and δ^4 is N. The element δ^4 being central, it is invariant under conjugation. Set $x = \sigma_1\sigma_3^{-1}$ and $y = \sigma_2\sigma_1\sigma_3^{-1}\sigma_2^{-1}$. The following relations are well known (see [16], Relations (7)) and easy to check:

$$\sigma_1 x \sigma_1^{-1} = x, \quad \sigma_2 x \sigma_2^{-1} = y, \quad \sigma_3 x \sigma_3^{-1} = x,$$
$$\sigma_1 y \sigma_1^{-1} = yx^{-1}, \quad \sigma_2 y \sigma_2^{-1} = yx^{-1}y, \quad \sigma_3 y \sigma_3^{-1} = x^{-1}y.$$

The conclusion follows immediately. □

As an application of Theorem 2.8, we give a quick proof of the following result, which was established by Gassner [16], Theorem 7 and by Gorin and Lin [18], Theorem 2.6 with different methods.

Proposition 2.13 *The kernel F of the group homomorphism $q : B_4 \to B_3$ is a free group of rank two.*

Proof Consider the diagram

$$\begin{array}{ccccccccccc}
1 & \longrightarrow & Z_4 & \longrightarrow & B_4 & \xrightarrow{f} & \mathrm{Aut}(F_2) & \longrightarrow & \mathbf{Z}/2 & \to & 1 \\
 & & \cong\downarrow & & q\downarrow & & \mathrm{ab}\downarrow & & \cong\downarrow & & \\
1 & \longrightarrow & 2Z_3 & \longrightarrow & B_3 & \xrightarrow{\bar{\pi}} & GL_2(\mathbf{Z}) & \to & \mathbf{Z}/2 & \to & 1
\end{array}$$

where $f : B_4 \to \mathrm{Aut}(F_2)$ was defined in Lemma 2.6, $q : B_4 \to B_3$ was defined in the proof of Proposition 2.12, $\mathrm{ab} : \mathrm{Aut}(F_2) \to GL_2(\mathbf{Z})$ is the homomorphism induced by abelianization, $\bar{\pi} : B_3 \to GL_2(\mathbf{Z})$ was defined in Lemma 2.11, and $2Z_3$ is the infinite cyclic group generated by $(\sigma_1\sigma_2)^6$, which is the square of the generator of the center Z_3 of B_3. Since $\mathrm{ab} \circ f = \pi = \bar{\pi} \circ q$, the diagram is commutative. The first row is exact as a consequence of Theorem 2.8. The second row is exact by Lemma 2.11. The homomorphisms q and ab are surjective, which implies that the rightmost vertical map is surjective, hence an isomorphism. The homomorphism q sends the generator $(\sigma_1\sigma_2\sigma_3)^4$ of the center Z_4 of B_4 to $(\sigma_1\sigma_2\sigma_1)^4 = (\sigma_1\sigma_2)^6$.

Therefore, $q : Z_4 \to 2Z_3$ is an isomorphism. It follows that f induces an isomorphism from $F = \mathrm{Ker}(q : B_4 \to B_3)$ to $\mathrm{Ker}(\mathrm{ab} : \mathrm{Aut}(F_2) \to GL_2(\mathbf{Z}))$; the latter is the group of inner automorphisms of F_2 by [26]. As F_2 has trivial center, the group of inner automorphisms is isomorphic to F_2. Therefore, F is isomorphic to F_2. □

Remark 2.14 (a) As was observed in the proof of Proposition 2.12, the group F of Proposition 2.13 is generated by $x = \sigma_1\sigma_3^{-1}$ and $y = \sigma_2\sigma_1\sigma_3^{-1}\sigma_2^{-1}$. It is easy to check that

$$f(x) = G\widetilde{G}^{-1} = \mathrm{Ad}(a) \quad \text{and} \quad f(y) = D^{-1}G\widetilde{G}^{-1}D = \mathrm{Ad}(b^{-1}a),$$

where for any element $w \in F_2$ the inner automorphism $\mathrm{Ad}(w)$ is defined by $\mathrm{Ad}(w)(u) = wuw^{-1}$ $(u \in F_2)$.

(b) The subgroup N of B_4 defined above is the direct product of the rank two free group F and the central rank one free group Z_4.

(c) Using the results of this section, one easily checks that the subgroup of $\mathrm{Aut}(F_2)$ generated by G and D is isomorphic to the braid group B_3 (compare to Corollary 2.9).

3 The special Sturmian monoid

The submonoid St of $\mathrm{Aut}(F_2)$ generated by the automorphisms $E, G, \widetilde{G}$ or, equivalently, by $E, D, \widetilde{D}$, all defined in (2.1), was called the *monoid of Sturm* by Berstel and Séébold [22], Sect. 2.3. These authors proved that all relations in St are consequences of the relations $E^2 = 1$ and

$$GEG^kE\widetilde{G} = \widetilde{G}E\widetilde{G}^kEG \tag{3.1}$$

for all $k \geq 0$. Observe that St is a generating set for the group $\mathrm{Aut}(F_2)$.

From the presentation of St we obtain a homomorphism of monoids $\varepsilon : \mathrm{St} \to \mathbf{Z}/2$ uniquely determined by $\varepsilon(E) = 1$ and $\varepsilon(G) = \varepsilon(\widetilde{G}) = 0$. We call its kernel $\mathrm{St}_0 = \{X \in \mathrm{St} \,|\, \varepsilon(X) = 0\}$ the *special Sturmian monoid*. The submonoid St_0 contains the elements $G, \widetilde{G}$, and also the elements $D, \widetilde{D}$ since $D = EGE$ and $\widetilde{D} = E\widetilde{G}E$. It is easy to check that St_0 consists of all positive automorphisms of F_2 acting on $\mathbf{Z}^2$ by linear transformations of determinant one.

We now give a presentation of St_0.

Proposition 3.1 *The monoid* St_0 *has a presentation with generators* $D, \widetilde{D}, G, \widetilde{G}$, *and relations*

$$GD^k\widetilde{G} = \widetilde{G}\widetilde{D}^kG \quad \text{and} \quad DG^k\widetilde{D} = \widetilde{D}\widetilde{G}^kD \tag{3.2}$$

for all $k \geq 0$.

Proof Let M_0 be the monoid generated by $D, \widetilde{D}, G, \widetilde{G}$, subject to Relations (3.2). There is an involutive monoid automorphism κ of M_0 exchanging D and G, $\widetilde{D}$ and $\widetilde{G}$. Let us consider the semi-direct product $M = M_0 \rtimes \mathbf{Z}/2$ with respect to this involution. As a set, $M = M_0 \times \mathbf{Z}/2$, the product being given by

$$(X, 0)(Y, n) = (XY, n) \quad \text{and} \quad (X, 1)(Y, n) = (X\kappa(Y), n + 1)$$

for all $X, Y \in M_0$ and $n \in \mathbf{Z}/2$. It it easy to check that the monoid M has a presentation with generators $E = (0, 1)$, D, $\widetilde{D}$, G, $\widetilde{G}$, and relations (3.2), $E^2 = 1$, $D = EGE$, and $\widetilde{D} = E\widetilde{G}E$. Using the last two relations, we can remove D and $\widetilde{D}$ from Relations (3.2). In this way we obtain a presentation that is clearly equivalent to the presentation (3.1) of St. Therefore, there is an isomorphism of monoids $M \cong \mathrm{St}$ fixing E. Such an isomorphism induces an isomorphism $M_0 \cong \mathrm{St}_0$. □

By Lemma 2.6 the monoid St_0 sits in the image of $f : B_4 \to \mathrm{Aut}(F_2)$, which is isomorphic to the quotient group B_4/Z_4. We now establish that St_0 can be lifted to the whole braid group B_4.

Theorem 3.2 *There is an injective homomorphism of monoids* $i : \mathrm{St}_0 \to B_4$ *defined by*

$$i(G) = \sigma_1, \quad i(\widetilde{G}) = \sigma_3, \quad i(D) = \sigma_2^{-1}, \quad i(\widetilde{D}) = \sigma_4^{-1}.$$

Proof Since $f \circ i$ is the identity on the generators $G, \widetilde{G}, D, \widetilde{D}$, it suffices to check that the images under i of the generators satisfy Relations (3.2) in B_4.

For $k = 0$ this means

$$\sigma_1\sigma_3 = \sigma_3\sigma_1 \quad \text{and} \quad \sigma_2^{-1}\sigma_4^{-1} = \sigma_4^{-1}\sigma_2^{-1}. \tag{3.3}$$

These relations hold in B_4 in view of (2.6) and (2.7).

For $k = 1$ we have to check

$$\sigma_1\sigma_2^{-1}\sigma_3 = \sigma_3\sigma_4^{-1}\sigma_1 \quad \text{and} \quad \sigma_2^{-1}\sigma_1\sigma_4^{-1} = \sigma_4^{-1}\sigma_3\sigma_2^{-1}. \tag{3.4}$$

Indeed, using $\sigma_4^{-1} = \sigma_3^{-1}\sigma_1\sigma_2^{-1}\sigma_3\sigma_1^{-1}$, we obtain

$$\sigma_3\sigma_4^{-1}\sigma_1 = \underbrace{\sigma_3\sigma_3^{-1}}\sigma_1\sigma_2^{-1}\sigma_3\underbrace{\sigma_1^{-1}\sigma_1} = \sigma_1\sigma_2^{-1}\sigma_3.$$

Similarly,

$$\begin{aligned}
\sigma_4^{-1}\sigma_3\underbrace{\sigma_2^{-1}\sigma_4} &= \underbrace{\sigma_4^{-1}\sigma_3\sigma_4}\sigma_2^{-1} \\
&= \sigma_3\sigma_4\sigma_3^{-1}\sigma_2^{-1} \\
&= \underbrace{\sigma_3\sigma_3^{-1}}\sigma_1\sigma_2\sigma_1^{-1}\underbrace{\sigma_3\sigma_3^{-1}}\sigma_2^{-1} \\
&= \underbrace{\sigma_1\sigma_2\sigma_1^{-1}}\sigma_2^{-1} \\
&= \sigma_2^{-1}\sigma_1\underbrace{\sigma_2\sigma_2^{-1}} = \sigma_2^{-1}\sigma_1.
\end{aligned}$$

For $k \geq 2$ we use the following observation whose proof is left to the reader: in a group the relations $ac = xz$ and $abc = xyz$ imply $ab^kc = xy^kz$ for all $k \geq 0$. We apply this observation successively to $a = \sigma_1$, $b = \sigma_2^{-1}$, $c = \sigma_3$, $x = \sigma_3$, $y = \sigma_4^{-1}$, $z = \sigma_1$, and to $a = \sigma_2^{-1}$, $b = \sigma_1$, $c = \sigma_4^{-1}$, $x = \sigma_4^{-1}$, $y = \sigma_3$, $z = \sigma_2^{-1}$. □

Corollary 3.3 *The submonoid of B_4 generated by $\sigma_1, \sigma_2^{-1}, \sigma_3, \sigma_4^{-1}$ has a presentation with generators $\sigma_1, \sigma_2^{-1}, \sigma_3, \sigma_4^{-1}$, and relations*

$$\sigma_1\sigma_2^{-k}\sigma_3 = \sigma_3\sigma_4^{-k}\sigma_1 \quad \textit{and} \quad \sigma_2^{-1}\sigma_1^k\sigma_4^{-1} = \sigma_4^{-1}\sigma_3^k\sigma_2^{-1}$$

for all $k \geq 0$.

Remark 3.4 (a) This corollary should be compared to the fact that the submonoid of B_3 generated by σ_1 and σ_2^{-1} is free. Indeed, its image under $\bar{\pi} : B_3 \to SL_2(\mathbf{Z})$ is the monoid generated by the matrices A and B given by (1.1). It is well known (and easy to check) that the monoid generated by these matrices, whose entries are nonnegative, is free.

(b) As follows from the proof of Theorem 3.2, the special Sturmian monoid St_0 can be lifted to the group generated by $\sigma_1, \sigma_2, \sigma_3, \sigma_4$ and Relations (3.3) and (3.4). This group maps surjectively onto B_4.

(c) In the proof of Proposition 3.1 we showed that the monoid St is a semidirect product of $\mathbf{Z}/2$ by St_0. As a consequence of this and of Theorem 3.2, there is an injective homomorphism of monoids $\mathrm{St} \to \widetilde{B}_4 = B_4 \rtimes \mathbf{Z}/2$ extending $i : \mathrm{St}_0 \to B_4$ and mapping the automorphism E onto the generator ω of $\mathbf{Z}/2$ in $\widetilde{B}_4$.

4 A geometric construction of bases out of Christoffel words

A *basis* of F_2 is an element $(u, v) \in F_2 \times F_2$ such that $\{u, v\}$ is a generating set of the group F_2. If (u, v) is a basis, then so are (u^{-1}, v), (u, v^{-1}), (u^{-1}, v^{-1}), as well as (v, u), (uv, v), (u, uv). An element $u \in F_2$ is *primitive* if there is $v \in F_2$ such that (u, v) is a basis of F_2. The elements u, v of a basis are sometimes called *associate primitives* in the literature (*"zusammengehörige, primitive Elemente"* in [26]). Two bases (u, v) and (u', v') (resp. two primitive elements u and u') of F_2 are *conjugate* if there is $w \in F_2$ such that $u' = wuw^{-1}$ and $v' = wvw^{-1}$ (resp. such that $u' = wuw^{-1}$).

Bases are related to automorphisms of F_2 as follows. If $\varphi \in \mathrm{Aut}(F_2)$, then $(\varphi(a), \varphi(b))$ is a basis of F_2. Conversely, if (u, v) is a basis of F_2, then there is a unique $\varphi \in \mathrm{Aut}(F_2)$ such that $\varphi(a) = u$ and $\varphi(b) = v$. We say that φ is the automorphism determined by the basis (u, v), and that (u, v) is the basis associated to φ. If φ (resp. φ') is the automorphism determined by a basis (u, v) (resp. by (u', v')), and (u, v) and (u', v') are conjugate by $w \in F_2$, then $\varphi' = \mathrm{Ad}(w) \circ \varphi$, where $\mathrm{Ad}(w)$ is the inner automorphism defined by $\mathrm{Ad}(w)(x) = wxw^{-1}$ ($x \in F_2$). Conversely, two automorphisms differing by an inner automorphism have conjugate associated bases.

In [26], Nielsen showed that two automorphisms differ by an inner automorphism if and only if their images in $\mathrm{Aut}(\mathbf{Z}^2) = GL_2(\mathbf{Z})$ are the same. Equivalently, two bases of F_2 are conjugate if and only if their images in $\mathbf{Z}^2$ coincide. Hence the conjugacy classes of bases of F_2 are in one-to-one correspondence with the bases of $\mathbf{Z}^2$. There have been several constructions of explicit bases of F_2, one in each conjugacy class, in the literature, see [10, 17, 27]. Our aim in this section is to give a variant of such constructions using the very simple geometric language of Christoffel words.

We first define Christoffel words (our definition is a slight modification of the definition given in [7]). Such words have a long history (see e.g., [1, 2, 9[2], 24, 32]), and they are related to Farey sequences and continued fractions ([19], Chapter III). For a nice recent account, see [7].

Let $\bar{u} = (p, q) \in \mathbf{Z}^2$ be such that p and q are coprime, i.e., $p\mathbf{Z} + q\mathbf{Z} = \mathbf{Z}$. We now construct an explicit lifting $u = u(p, q) \in F_2$ of $\bar{u} \in \mathbf{Z}^2$. Such an element u will be called the *Christoffel word* associated to $\bar{u}$.

Let $\Lambda = (\mathbf{R} \times \mathbf{Z}) \cup (\mathbf{Z} \times \mathbf{R})$ be the set of horizontal and vertical lines in $\mathbf{R}^2$. Suppose first that p and q are nonnegative. There is a unique oriented path $\Gamma_{p,q}$ contained in Λ, starting from $O = (0, 0)$ and ending at $P = (p, q)$, satisfying the following properties:

(i) $\Gamma_{p,q}$ lies under the segment OP, that is, each point $(x, y) \in \Gamma_{p,q}$ satisfies $px \geq qy$,

(ii) the coordinates (x, y) of a point on $\Gamma_{p,q}$ never decrease when one runs along the path from O to P,

(iii) there is no point of $\mathbf{Z}^2$ in the interior of the polygonal surface enclosed by $\Gamma_{p,q}$ and the segment OP.

When one runs along $\Gamma_{p,q}$ from O to P, one obtains a word $u(p, q) \in F_2$ by writing a for each horizontal segment encountered along the path and b for each vertical segment. For instance,

$$u(1, 0) = a, \quad u(0, 1) = b, \quad u(5, 2) = a^3ba^2b.$$

All words $u(p, q)$ start with the letter a, except $u(0, 1)$, and end with b, except $u(1, 0)$.

Conversely, one can recover the path $\Gamma_{p,q}$ from the word $u(p, q)$ by the following rule: reading the word $u(p, q)$ from left to right, start from the point O and move to the right (resp. upwards) by one unit segment in Λ each time one encounters the letter a (resp. the letter b). Figure 2 shows the path $\Gamma_{5,2}$ (in thick lines) and the corresponding word $u(5, 2)$.

The construction of the Christoffel word $u(p, q)$ lends itself to the following factorization formula, which is a rephrasing of [7], Proposition 1 (see also [3], Sect. 4, [10], Sect. 8, [17, 27]). We give a proof for the sake of completeness.

Lemma 4.1 *If p, q, r, s are nonnegative integers such that $ps - qr = 1$, then*

$$u(p, q)u(r, s) = u(p + r, q + s).$$

Proof Set $\bar{u} = (p, q)$ and $\bar{v} = (r, s) \in \mathbf{Z}^2$. Since $\det(\bar{u}, \bar{v}) = ps - qr = 1$, there are no points of $\mathbf{Z}^2$ in the interior of the parallelogram with vertices $0, \bar{u}, \bar{v}, \bar{u} + \bar{v}$ ([19], Theorem 32). It then follows from the very definition of Christoffel words that the Christoffel word associated to $\bar{u} + \bar{v}$ is the word uv, where u is the Christoffel word associated to $\bar{u}$ and v is the Christoffel word associated to $\bar{v}$ (see Fig. 3 for an illustration of this proof when $\bar{u} = (3, 1)$ and $\bar{v} = (2, 1)$). □

[2] Quite amazingly for the end of the 19th century, Christoffel wrote [9] in Latin, but he also published papers in the *Annali* in German, French, and Italian! The author's name appears as follows on the first page of [9]: *auctore E. B. Christoffel, prof. Argentinensi*. The last word is derived from the Latin name given by the Romans to the city of Strasbourg. Christoffel was the founder with Reye of the *Mathematisches Institut der Universität Straßburg* in 1872 (for details, see [31]).

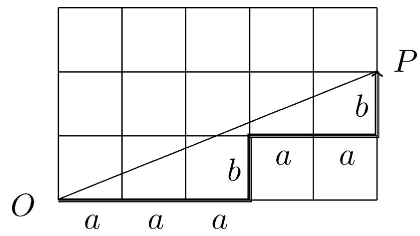

Fig. 2 The path $\Gamma_{5,2}$

In order to define the Christoffel words $u(p,q)$ when p or q is negative, we use the automorphism T defined by $T(a) = a$ and $T(b) = b^{-1}$. (In terms of the automorphisms D, E, G, $\widetilde{G}$ introduced in Sect. 2, we have $T = GD^{-1}\widetilde{G}E$.) If $p \geq 0$ and $q \geq 0$, we set

$$u(p,-q) = Tu(p,q), \quad u(-p,q) = Tu(p,q)^{-1}, \quad u(-p,-q) = u(p,q)^{-1}. \tag{4.1}$$

For instance,

$$u(5,-2) = a^3b^{-1}a^2b^{-1}, \quad u(-5,2) = ba^{-2}ba^{-3},$$
$$u(-5,-2) = b^{-1}a^{-2}b^{-1}a^{-3}.$$

A geometric representation of the Christoffel words $u(p,-q)$, $u(-p,q)$, $u(-p,-q)$ $(p,q \geq 0)$ will be given in Remark 4.4 (a) below.

Theorem 4.2 *If $(\bar{u}, \bar{v})$ is a basis of $\mathbf{Z}^2$ and u (resp. v) is the Christoffel word associated to $\bar{u}$ (resp. to $\bar{v}$), then (u, v) is a basis of F_2.*

We call such a basis a *Christoffel basis*.

Proof Before we start the proof, we observe that, if $(\bar{u}, \bar{v})$ is a basis of $\mathbf{Z}^2$, then $\bar{u}$ and $\bar{v}$ are either in the same quadrant or in opposite quadrants.

(1) Assume first that both $\bar{u} = (p,q)$ and $\bar{v} = (r,s)$ have nonnegative coordinates and that $\det(\bar{u}, \bar{v}) = ps - qr = 1$. We shall prove the assertion of the theorem in this case by induction on $|\bar{u}| + |\bar{v}| = p + q + r + s$. If $|\bar{u}| + |\bar{v}| = 2$, then $\bar{u} = (1,0)$ and $\bar{v} = (0,1)$; the corresponding Christoffel words are $u = a$ and $v = b$, which form a basis of F_2.
Now consider the case when $|\bar{u}| + |\bar{v}| > 2$. The equalities

$$\det(\bar{u}, \bar{v}) = \det(\bar{u}, \bar{v} - \bar{u}) = \det(\bar{u} - \bar{v}, \bar{v}) = 1$$

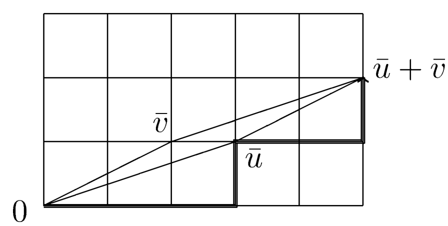

Fig. 3 The factorization $u(3,1)u(2,1) = u(5,2)$

show that $(\bar{u}, \bar{v} - \bar{u})$ and $(\bar{u} - \bar{v}, \bar{v})$ are bases of $\mathbf{Z}^2$. Since $\bar{u}$ and $\bar{v}$ are in the first quadrant, it follows from the observation above that either $\bar{v}-\bar{u}$ or $\bar{u}-\bar{v}$ is in the first quadrant. In the first case, namely when $r \geq p$ and $s \geq q$, we have $|\bar{u}| + |\bar{v} - \bar{u}| = |\bar{u}| < |\bar{u}| + |\bar{v}|$. Then by induction $(u(p, q), u(r - p, s - q))$ is a basis of F_2. We are now in a situation where we can apply Lemma 4.1. We obtain $u(p, q)u(r-p, s-q) = u(r, s)$, from which it follows that $u = u(p, q)$ and $v = u(r, s)$ form a basis of F_2. In the second case, namely when $r \leq p$ and $s \leq q$, we have $|\bar{u} - \bar{v}| + |\bar{v}| = |\bar{v}| < |\bar{u}| + |\bar{v}|$. Then by induction $(u(p-r, q-s), u(r, s))$ is a basis of F_2. We again apply Lemma 4.1, obtaining $u(p - r, q - s)u(r, s) = u(p, q)$, from which it also follows that $u = u(p, q)$ and $v = u(r, s)$ form a basis of F_2.

(2) If $\bar{u}$, $\bar{v}$ are in the first quadrant and $\det(\bar{u}, \bar{v}) = -1$, we exchange the roles of u and v, and conclude that (v, u), hence (u, v), is a basis of F_2.

(3) We now deal with a basis $(\bar{u}, \bar{v})$ of $\mathbf{Z}^2$ with arbitrary coordinates. Then by the observation above $\bar{u}$ and $\bar{v}$ are either in the same quadrant, or in opposite quadrants. If they are in the same quadrant, then we obtain the Christoffel words u and v from Christoffel words whose ends are in the first quadrant by a simultaneous application of one of the transformations appearing in (4.1), namely the inversion, T, or their composition. These transformations being invertible, (u, v) is a basis by the previous case. If $\bar{u} = (p, q)$ and $\bar{v} = (r, s)$ are in opposite quadrants, then $\bar{u}$ and $-\bar{v} = (-r, -s)$ are in the same quadrant. Therefore, by (4.1) and by the previous case, $(u, u(-r, -s)) = (u, v^{-1})$ is a basis of F_2. It follows that (u, v) is a basis as well. □

We have the following consequences of Theorem 4.2 and of Nielsen's result quoted at the beginning of this section.

Corollary 4.3 *(a) Any basis of F_2 is conjugate to a unique Christoffel basis.*

(b) The primitive elements of F_2 are exactly the conjugates of Christoffel words.

Remark 4.4 (a) For coprime nonnegative integers p, q, the words $u(p, -q)$, $u(-p, q)$, $u(-p, -q)$ defined by (4.1) can be obtained graphically in a similar way as $u(p, q)$ above. Let $\Gamma_{p,-q}$ (resp. $\Gamma_{-p,q}$, resp. $\Gamma_{-p,-q}$) be the oriented path contained in Λ, starting from $O = (0, 0)$ and ending at $P' = (p, -q)$ (resp. at $P'' = (-p, q)$, resp. at $P''' = (-p, -q)$), obtained by the following rule: reading the word $u(p, -q)$ (resp. $u(-p, q)$, resp. $u(-p, -q)$) from left to right, move to the right (resp. to the left) by one unit segment in Λ when encountering the letter a (resp. a^{-1}) and move upwards (resp. downwards) by one unit segment in Λ when encountering the letter b (resp. b^{-1}). Figure 4 depicts the paths $\Gamma_{5,-2}$, $\Gamma_{-5,2}$, $\Gamma_{-5,-2}$ in thick lines, and the corresponding words $u(5, -2)$, $u(-5, 2)$, $u(-5, -2)$ (we have denoted a^{-1} by $\bar{a}$ and b^{-1} by $\bar{b}$ in the figure).

The oriented path $\Gamma_{p,-q}$ (resp. $\Gamma_{-p,q}$) is the image of $\Gamma_{p,q}$ (resp. of $\Gamma_{-p,-q}$) under the reflection in the line $\mathbf{R} \times \{0\}$. The path $\Gamma_{-p,-q}$ is obtained from $\Gamma_{p,q}$ by applying the translation $(x \mapsto x - p, y \mapsto y - q)$ and reversing the orientation. These geometric considerations allow to characterize the paths $\Gamma_{p,-q}$, $\Gamma_{-p,q}$, $\Gamma_{-p,-q}$ by conditions similar to Conditions (i–iii) above (we leave such a characterization to the reader).

(b) In the definition of $\Gamma_{p,q}$ $(p, q \geq 0)$ above we may replace Condition (i) by the following condition (i'): each point $(x, y) \in \Gamma_{p,q}$ satisfies $px \leq qy$. Under

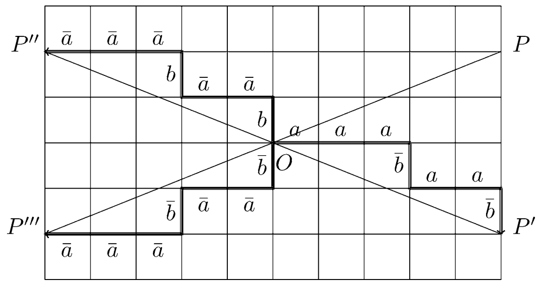

Fig. 4 Representing general Christoffel words graphically

this new condition we obtain an oriented path $\Gamma'_{p,q}$ contained in Λ, starting from $O = (0,0)$ and ending at $P = (p,q)$, and a word $u'(p,q)$, which we call the *upper Christoffel word* associated to $\bar{u} = (p,q) \in \mathbf{Z}^2$. It follows from the definition that $\Gamma'_{p,q}$ is the image of the oriented path $\Gamma_{-p,q}$ (resp. of $\Gamma_{-p,-q}$) defined in Remark (a) under the reflection in the line $\{0\} \times \mathbf{R}$ (resp. under the reflection in the point O). Consequently, the upper Christoffel word $u'(p,q)$ is obtained from the lower Christoffel word $u(p,q)$ by first inverting it, then applying the automorphism $TO : a \mapsto a^{-1}, b \mapsto b^{-1}$. In other words,

$$u'(p,q) = \widetilde{u(p,q)}, \tag{4.2}$$

where for any $w \in F_2$ we denote $\widetilde{w}$ the image of w under the anti-automorphism of F_2 extending the identity of $\{a,b\}$. The word $\widetilde{w}$ is called the *reverse* of w.

It follows from Theorem 4.2 and (4.2) that $u'(p,q)$ is a primitive element of F_2, mapping to $\bar{u} \in \mathbf{Z}^2$. Therefore, by Corollary 4.3 (b), $u'(p,q)$ is a conjugate of $u(p,q)$, a result that can already be found in [10], Lemma 6.1 (see also [22, 28]).

(c) The Christoffel bases constructed above can be related to the bases constructed in [27]. Let $\bar{u} = (p,q)$ be an element of $\mathbf{Z}^2$ whose coordinates p, q are positive and coprime. The Christoffel word u we associated above to $\bar{u}$ is then of the form $u = avb$ for some element v in the monoid generated by a and b. It is easy to check that the primitive element $w \in F_2$ constructed in [27] as a lift of $\bar{u}$ is given by $w = abv$ for the same element v. (Beware that the definition of the primitive element in Osborne and Zieschang [27] is not correct in the cases p or $q < 0$; see [17] for a correct definition.)

5 Chains of conjugate bases. Application to palindromicity

In Ref. ([26] p. 389), Nielsen gave an algorithm for deciding when a couple (u, v) of cyclically reduced elements of F_2 forms a basis. In order to describe this algorithm, we may assume that the respective lengths $|u|$ and $|v|$ of u and v with respect to the generating set $\{a, a^{-1}, b, b^{-1}\}$ are such that $1 \leq |u| \leq |v| \neq 1$. If neither u, nor u^{-1} is a prefix or a suffix of v, then (u, v) is not a basis. Otherwise, there is $w \in F_2$ such that $v = uw$, or wu, or $u^{-1}w$, or wu^{-1}, in which case we replace v by the shorter element w, and we start the whole procedure again with the couple (u, w). Nielsen gave also the following criterion, which he attribues to Dehn: (u, v) is a basis of F_2 if and only if $uvu^{-1}v^{-1}$ is conjugate to $aba^{-1}b^{-1}$ or to $(aba^{-1}b^{-1})^{-1}$ (see [26], p. 393).

In this section we provide another characterization for bases. Our criterion is based on chains of mutually conjugate couples of elements of F_2. Using these chains, we obtain an additional result, which states that under suitable hypotheses a basis has a unique conjugate consisting of two palindromes.

We start with positive words, i.e., with elements of the submonoid $\{a, b\}^*$ of F_2 generated by a and b. We define a rewriting system on $\{a, b\}^* \times \{a, b\}^*$ as follows: $(u, v) \to (u', v')$ if u and v start with the same letter $c \in \{a, b\}$, and $u' = u''c$ and $v' = v''c$, where $u'', v'' \in \{a, b\}^*$, $u = cu''$ and $v = cv''$. Any couple $(u, v) \in \{a, b\}^* \times \{a, b\}^*$ is contained in a unique maximal chain of arrows. The length of this maximal chain, which is the number of arrows in the chain, may be finite or infinite. For instance, if u and v are (positive) powers of a same word, then the maximal chain containing (u, v) is infinite. If the chain is finite of length $r \geq 1$, we order its constituents as follows:

$$(u_0, v_0) \to (u_1, v_1) \to (u_2, v_2) \to \cdots \to (u_r, v_r).$$

If the chain contains only one couple, we say that it is of length 0.

The following algorithm allows to decide in an efficient way when $u, v \in \{a, b\}^*$ form a basis of F_2.

Theorem 5.1 *Let $u, v \in \{a, b\}^*$ of respective lengths $|u|$ and $|v|$.*

(a) *The couple (u, v) is a basis of F_2 if and only if the maximal chain containing (u, v) is of length $|u| + |v| - 2$.*
(b) *If the maximal chain containing (u, v) is of length $> |u| + |v| - 2$, then it is infinite and u, v are positive powers of a same word.*

Proof (i) Suppose that the maximal chain containing (u, v) is of finite length equal to $|u| + |v| - 2$. We may assume that (u, v) is the left end of the chain. Then the infinite words $u^\infty = uuu\cdots$ and $v^\infty = vvv\cdots$ have a common prefix w of length $|u| + |v| - 2$. The word w has $|u|$ and $|v|$ as periods. If $\gcd(|u|, |v|) \geq 2$, then w is of length $\geq |u| + |v| - \gcd(|u|, |v|)$; then by Fine and Wilf's theorem (see [22], Proposition 1.2.1), u and v are powers of the same word, which implies that the chain is infinite, yielding a contradiction.

Therefore, $\gcd(|u|, |v|) = 1$ and w is a central word in the sense of ([22], p. 68). A *central* word is a word having two coprime periods p, q and a length equal to $p + q - 2$. It follows from the general theory of Sturmian sequences (see [22], especially Sect. 2.2.1) that the prefixes of length p and q of such a word form what is called a *standard pair*; moreover, the tree construction of standard pairs shows that each such pair is a basis of F_2. Hence we conclude that u, v form a basis of F_2, since they are the prefixes of length $|u|$ and $|v|$ of w.

Conversely, if (u, v) is a basis of F_2, then $a \mapsto u, b \mapsto v$ is a positive automorphism of F_2, hence a Sturmian morphism. We apply Séébold's theory of conjugate morphisms, see [22], Sect. 2.3.4 or [29]: given two (endo)morphisms f, g of the free monoid $\{a, b\}^*$, we say that g is a *right conjugate* of f if there is $w \in \{a, b\}^*$ such that $f(x)w = wg(x)$ for all $x \in \{a, b\}$. This is clearly equivalent to the following property: there is a chain for the above-defined binary relation $\to$ from the couple $(f(a), f(b))$ to the couple $(g(a), g(b))$. By [22], Proposition 2.3.18, for each Sturmian morphism g there is a standard morphism f such that g is a right conjugate of f. Moreover, a standard morphism is not the right conjugate of any morphism since the words $f(a)$, $f(b)$ have no common suffix, and by [22], Proposition 2.3.21, there are exactly $|f(a)| + |f(b)| - 1$ right conjugates of a standard morphism.

(ii) If the maximal chain starting from (u, v) is of length $> |u| + |v| - 2$, then u^∞ and v^∞ have a common prefix w of length $|u| + |v| - 1$. Fine and Wilf's theorem then implies that u and v are powers of the same word. Therefore, the chain is infinite. □

We now deal with arbitrary couples of elements of F_2. In the sequel elements of F_2 are reduced, but not necessarily cyclically reduced.

Corollary 5.2 *An element $(u, v) \in F_2 \times F_2$ is a basis of F_2 if and only if the following algorithm terminates.*

(i) *If (u, v) is not cyclically reduced, find some letter $c \in \{a, b, a^{-1}, b^{-1}\}$ that is a common prefix, or suffix, of u, v; then conjugate both u and v by c. Continue until (u, v) is cyclically reduced.*
(ii) *Check if the images of u and v in $\mathbf{Z}^2$ are in the same quadrant; if not, verify that the images of u and v^{-1} are in the same quadrant and replace (u, v) by (u, v^{-1}).*
(iii) *Check if the images of u and v in $\mathbf{Z}^2$ are both in the first quadrant; if not, apply simultaneously to u and v the transformations appearing in (4.1), namely the inversion, T, or their composition, so that the transformed elements have their images in the first quadrant.*
(iv) *Verify that $u, v \in \{a, b\}^*$.*
(v) *Verify that the maximal chain containing (u, v) is of length $|u| + |v| - 2$.*

Proof (i) It follows from ([26], p. 393, Item 2) that, if (u, v) is a basis that is not cyclically reduced, then a letter c as above exists (one can also make use of the Dehn criterion cited above). Conjugating by c will reduce $|u| + |v|$ by 4 if both u and v are not cyclically reduced, and by 2 if only one of them is not cyclically reduced.

(ii) We have observed in the proof of Theorem 4.2 that, if u and v form a basis, then their images in $\mathbf{Z}^2$ are either in the same quadrant, or in opposite quadrants. If the images are in opposite quadrants, then the images of u and v^{-1} are in the same quadrant. Note that, if v is cyclically reduced, then so is v^{-1}.

(iii) The transformations (4.1) preserve the property of being cyclically reduced and of being a basis.

(iv) By Corollary 4.3 (a) a basis (u, v) whose image in $\mathbf{Z}^2$ is in the first quadrant is conjugate to a Christoffel basis (u', v') with $u', v' \in \{a, b\}^*$ (u' and v' are cyclically reduced by construction). If (u, v) is cyclically reduced, then Lemma 5.3 below implies that (u, v) belongs to the maximal chain containing (u', v'). Therefore, u and v belong to $\{a, b\}^*$.

(v) This follows from Theorem 5.1 (a). □

In the previous proof we have made use of the following result.

Lemma 5.3 *Let $u', v' \in \{a, b\}^*$. Then a couple (u, v) of cyclically reduced elements of F_2 is a conjugate of (u', v') if and only if it belongs to the maximal chain containing (u', v').*

Proof If (u, v) belongs to the maximal chain containing (u', v'), then (u, v) is a conjugate of (u', v').

Conversely, suppose that $u = wu'w^{-1}$ and $v = wv'w^{-1}$ for some $w \in F_2$. We proceed by induction on the length $|w|$ of w. Since $u = wu'w^{-1}$ is cyclically reduced, there must be some reduction in one of the products wu' or $u'w^{-1}$ (not in both). To fix notation let us assume that $u' = u''c$ and $w^{-1} = c^{-1}t^{-1}$ for some $c \in \{a, b\}$, $u'' \in \{a, b\}^*$, and $t \in F_2$ with $|t| < |w|$. Then $u = tcu''t^{-1}$ and $v = wv'w^{-1} = tcv'c^{-1}t^{-1}$. Since the latter is cyclically reduced and v' cannot start with c^{-1} as it is an element of $\{a, b\}^*$, the word v' must end with c. Writing $v' = v''c$ where $v'' \in \{a, b\}^*$, we have $v = tcv''t^{-1}$. We may now conclude by induction since cu'', cv'' belong to $\{a, b\}^*$ and $|t| < |w|$. □

As a consequence of the previous considerations, we obtain the following.

Corollary 5.4 *For any cyclically reduced basis (u, v) of F_2 there are exactly $|u| + |v| - 1$ cyclically reduced bases conjugate to (u, v).*

We now deal with palindromes. Recall from Remark 4.4 (b) that the reverse $\widetilde{w}$ of an element $w \in F_2$ is the image of w under the anti-automorphism extending the identity on $\{a, b\}$. In other words, $\widetilde{w}$ is the element obtained by reading the letters of a (not necessarily reduced) expression of w from right to left. A *palindrome* is an element $w \in F_2$ such that $\widetilde{w} = w$. Note that a reduced palindrome is necessarily cyclically reduced. We say that a cyclically reduced basis (u, v) of F_2 is *palindromic* if both u and v are palindromes.

Theorem 5.5 *Let (u, v) be a cyclically reduced basis of F_2 such that $|u|$ and $|v|$ are odd. Then there is exactly one palindromic cyclically reduced basis conjugate to (u, v).*

Proof Using the transformations appearing in (4.1) and observing that palindromicity is preserved by these transformations, we may reduce to the case when u and v belong to $\{a, b\}^*$. Then by Theorem 5.1 (a) the basis (u, v) is contained in a maximal chain

$$(u_0, v_0) \to (u_1, v_1) \to \cdots \to (u_r, v_r)$$

of length $r = |u| + |v| - 2$. By [22], Lemma 2.2.8 and Proposition 2.3.21, the couple (u_0, v_0) is a standard pair, and there are palindromes p and q such that $u_0 = pab$ and $v_0 = qba$, or $u_0 = pba$ and $v_0 = qab$. Let us assume that we are in the first case (the second case can be treated in a similar manner). Then the words $u_i v_i$ $(i = 0, 1, \ldots, r)$ are clearly the successive factors of length $|u| + |v|$ of the word $u_0 v_0 u_0 q$. In particular, $u_r = bap$ and $v_r = abq$. Hence,

$$\widetilde{u_r} = \widetilde{p}ab = pab = u_0 \quad \text{and} \quad \widetilde{v_r} = \widetilde{q}ba = qba = v_0$$

in view of the palindromicity of p and q. More generally, we check easily that

$$\widetilde{u_i} = u_{r-i} \quad \text{and} \quad \widetilde{v_i} = v_{r-i} \tag{5.1}$$

for all $i = 0, 1, \ldots, r$. Consequently, u_k and v_k are palindromes when

$$k = \frac{r}{2} = \frac{|u| + |v|}{2} - 1$$

(which is an integer since $|u|$ and $|v|$ are both assumed to be odd integers). This proves the existence of a palindromic conjugate of (u, v).

The uniqueness of the palindromic conjugate is a consequence of the following observation: if a word w is not a power of another word and if the circular word associated to w has a central symmetry, then it has no other central symmetry (otherwise the circular word would be invariant under some nontrivial rotation and w would be a nontrivial power). □

Let us illustrate Theorems 5.1 and 5.5 on the couple (u, v), where $u = aba^2b$ and $v = aba$. The maximal chain containing (u, v) is

$$\begin{array}{ccccccc} (aba^2b, aba) & \longrightarrow & (ba^2ba, ba^2) & \longrightarrow & (a^2bab, a^2b) & & \\ & & & & & \searrow & \\ & & & & & & (ababa, aba) \\ & & & & & \swarrow & \\ (ba^2ba, aba) & \longleftarrow & (aba^2b, a^2b) & \longleftarrow & (baba^2, ba^2) & & \end{array}$$

It is of length $6 = |u| + |v| - 2$. Therefore, (u, v) is a basis. The maximal chain displays all seven cyclically reduced bases conjugate to (u, v). The middle element of the chain, namely $(ababa, aba)$, is the palindromic basis conjugate to (u, v). The symmetry encoded in the equalities (5.1) can be observed on the chain: each basis in the top row is the reverse of the basis immediately under it in the bottom row.

Remark 5.6 (a) It can be shown that a primitive element of F_2 of even length cannot be conjugate to a palindrome.

(b) The existence statement in Theorem 5.5 is equivalent to a result due to Droubay and Pirillo (see [12], Proposition 16); our proof is different from theirs.

(c) The main theorem of [20] states that u, v, and $vabu$ are palindromes ($u, v \in F_2$) if and only if $a \mapsto uba$, $b \mapsto vab$ defines an automorphism of F_2 fixing $b^{-1}a^{-1}ba$. This generalizes a result of de Luca and Mignosi [23], see also [22], Theorem 2.2.4. (The automorphims of F_2 fixing $b^{-1}a^{-1}ba$ are the ones belonging to the subgroup generated by G and D, see [10], Sect. 3, [20].)

Acknowledgements We wish to express our thanks to Jean-Pierre Borel, John Crisp, Gilbert Levitt, and Vladimir Turaev for helpful comments; also to Etienne Ghys who suggested that our action of B_4 on F_2 may be derived from considering a punctured torus as a double covering of $\mathbf{R}^2$ branched over four points.

References

1. Allouche, J.-P., Shallit, J.: Automatic Sequences. Theory, Applications, Generalizations. Cambridge University Press, Cambridge (2003)
2. Bernoulli, J.: Sur une nouvelle espèce de calcul. In: Recueil pour les astronomes, t. 1. pp. 255–284. Springer, Berlin Heidelberg New York (1772)

3. Berstel, J., de Luca, A.: Sturmian words, Lyndon words and trees. Theoret. Comput. Sci. **178**, 171–203 (1997)
4. Birman, J.S.: Automorphisms of the fundamental group of a closed, orientable 2-manifold. Proc. Amer. Math. Soc. **21**, 351–354 (1969)
5. Birman, J.S.: Braids, links and mapping class groups. Annals of Math. Studies, No. 82, Princeton University Press, Princeton (1975)
6. Birman, J.S., Hilden, H.M.: On the mapping class groups of closed surfaces as covering spaces. In: Advances in the Theory of Riemann Surfaces, Ann. of Math. Studies, vol. 66, pp. 81–115. Princeton University Press, Princeton (1971)
7. Borel, J.-P., Laubie, F.: Quelques mots sur la droite projective réelle. J. Théorie des Nombres de Bordeaux **5**, 23–51 (1993)
8. Bourbaki, N.: Groupes et algèbres de Lie, chapter IV–VI. Hermann, Paris (1968)
9. Christoffel, E.B.: Observatio arithmetica. Ann. Mat. Pura Appl. **6**, 148–152 (1875)
10. Cohn, H.: Markoff forms and primitive words. Math. Ann. **196**, 8–22 (1972)
11. Coxeter, H.S.M., Moser, W.O.J.: Generators and relations for discrete groups. Ergebnisse der Mathematik und ihrer Grenzgebiete 14, 4th edn. Springer, Berlin Heidelberg New York (1980)
12. Droubay, X., Pirillo, G.: Palindromes and Sturmian words. Theoret. Comput. Sci. **223**, 73–85 (1999)
13. Dyer, J.L., Formanek, E., Grossman, E.K.: On the linearity of automorphism groups of free groups. Arch. Math. **38**, 404–409 (1982)
14. Dyer, J.L., Grossman, E.K.: The automorphism groups of the braid groups. Amer. J. Math. **103**, 1151–1169 (1981)
15. Fenchel, W.: Jakob Nielsen in memoriam. Acta Math. **103**, VII–XIX (1960)
16. Gassner, B.J.: On braid groups. Abh. Math. Sem. Univ. Hamburg **25**, 10–22 (1962)
17. González-Acuña, F., Ramírez, A.: A composition formula in the rank two free group. Proc. Am. Math. Soc. **127**, 2779–2782 (1999)
18. Gorin, E.A., Lin, V.Ya.: Algebraic equations with continuous coefficients and some problems of the algebraic theory of braids. Mat. Sbornik **78**(120), 579–610 (1969) (English translation: Math. USSR-Sbornik **7**, 569–596 (1969))
19. Hardy, G.H., Wright, E.M.: An Introduction to the Theory of Numbers. Oxford University Press, Oxford (1979)
20. Helling, H.: A note on the automorphism group of the rank two free group. J. Algebra **223**, 610–614 (2000)
21. Karrass, A., Pietrowski, A., Solitar, D.: Some remarks on braid groups. In: Contributions to braid groups, Contemp. Math. **33**, 341–352. Providence: Amer. Math. Soc. (1984)
22. Lothaire, M.: Algebraic Combinatorics on Words, pp. 45–110. Cambridge University Press, Cambridge (2002)
23. de Luca, A., Mignosi, F.: On some combinatorial properties of Sturmian words. Theoret. Comput. Sci. **136**, 361–385 (1994)
24. Markoff, A.: Sur une question de Jean Bernouilli. Math. Ann. **19**, 27–36 (1882)
25. Mignosi, F., Séébold, P., Morphismes sturmiens et règles de Rauzy. J. Théorie des Nombres de Bordeaux **5**, 221–233 (1993)
26. Nielsen, J.: Die Isomorphismen der allgemeinen, unendlichen Gruppe mit zwei Erzeugenden. Math. Ann. **78**, 385–397 (1918)
27. Osborne, R.P., Zieschang, H.: Primitives in the free group on two generators. Invent. Math. **63**, 17–24 (1981)
28. Pirillo, G.: A new characteristic property of the palindrome prefixes of a standard Sturmian word. Sém. Lothar. Combin., art. B43f, 4pp. (2000) (electronic)
29. Séébold, P.: On the conjugation of standard morphisms. Theoret. Comput. Sci. **195**, 91–109 (1998)
30. Wen, Z.-X., Wen, Z.-Y.: Local isomorphisms of invertible substitutions. C.R. Acad. Sci., Paris **318**(série I), 299–304 (1994)
31. Wollmershäuser, F.R.: Das Mathematische Seminar der Universität Strassburg. In: Butzer, P.L., Fehér, F., (eds.). E.B. Christoffel, The Influence of His Work on Mathematics and the Physical Sciences, pp. 52–70. Birkhäuser Verlag, Basel, Boston, Stuttgart(1981)
32. Wynn, P.: The work of E.B. Christoffel on the theory of continued fractions. In: Butzer, P.L., Fehér, F., (eds.). E.B. Christoffel, The Influence of his Work on Mathematics and the Physical Sciences, pp. 190–202. Birkhäuser Verlag, Basel, Boston, Stuttgart (1981)