involve

a journal of mathematics

Whitehead graphs and separability in rank two

Matt Clay, John Conant and Nivetha Ramasubramanian

msp

2014 vol. 7, no. 4

INVOLVE 7:4 (2014)
dx.doi.org/10.2140/involve.2014.7.431

Whitehead graphs and separability in rank two

Matt Clay, John Conant and Nivetha Ramasubramanian

(Communicated by Gaven Martin)

By applying an algorithm of Stallings regarding separability of elements in a free group, we give an alternative approach to that of Osborne and Zieschang in describing all primitive elements in the free group of rank 2. As a result, we give a proof of a classical result of Nielsen, used by Osborne and Zieschang in their work, that the only automorphisms of F_2 that act trivially on the abelianization are those defined by conjugation. Finally, we compute the probability that a Whitehead graph in rank 2 contains a cut vertex. We show that this probability is approximately $1/l^2$, where l is the number of edges in the graph.

1. Introduction

The free group of rank n, F_n, is the set of reduced words in a fixed alphabet $\{x_1, x_1^{-1}, \dots, x_n, x_n^{-1}\}$ with group operation concatenation followed by free reduction. A word is *reduced* if it does not contain any of the two letter subwords $x_i x_i^{-1}$, $x_i^{-1} x_i$ for $i = 1, \dots, n$. *Free reduction* is the process of repeatedly removing such two-letter subwords. When the rank is small, we usually denote $x_1 = a$, $x_2 = b$, et cetera. Free groups form an important class of groups due to their connections with low-dimensional topology and geometry and also as every group is the quotient of two free groups (though possibly of infinite rank).

A subset of F_n with n elements that generates F_n is called a *basis*. In other words, given a basis $\{a_1, \dots, a_n\} \subset F_n$, we can uniquely express any element $g \in F_n$ as a (reduced) word in the alphabet $\{a_1, a_1^{-1}, \dots, a_n, a_n^{-1}\}$. We call such an expression the word representing g in the given basis.

Of particular interest are the elements that are part of some basis. Such elements are called *primitive*. Whitehead [1936] described an algorithm to determine whether or not a word in a given basis represents a primitive element.

MSC2010: primary 20E05; secondary 20F65.
Keywords: free groups, primitive elements.
This work is partially supported by NSF grant DMS-1006898 and by the Richard J. Cook and Teresa M. Lahti Student-Faculty Research Endowment.

Osborne and Zieschang [1981] gave a complete construction of primitive elements in rank 2. First they define a collection of primitive elements, indexed by an ordered pair of relatively prime integers. The relatively prime pair is the abelianization of the given element. Next, they quote a result of Nielsen [1917] (see also [Lyndon and Schupp 2001]) that up to conjugacy, primitive elements in F_2 are uniquely determined by their abelianization and that their abelianization is a relatively prime pair of integers. Thus, the list of primitive elements described by Osborne and Zieschang contains exactly one representative from each conjugacy class of a primitive element.

There is an alternative viewpoint due to Cohen, Metzler and Zimmermann [Cohen et al. 1981]. Their idea is to use Whitehead's algorithm to give a narrow condition that the exponents of primitive elements in F_2 need to satisfy. They do not give a complete characterization in the sense that there exist elements in F_2 that are not primitive but that satisfy their condition.

Several other results about the form of primitive elements in rank 2 are known. See for instance [Kassel and Reutenauer 2007; Piggott 2006].

One purpose of this article is to show that Whitehead graphs can be used to recover Osborne and Zieschang's construction and in turn give an alternative proof of the above-quoted result of Nielsen used by Osborne and Zieschang. In fact, we consider a slightly more general notion than primitivity, called *separable* (definitions appear in Section 2). Stallings [1999] proved a version of Whitehead's algorithm for determining when a given word in a basis represents a separable element. We review this algorithm in Section 3 and include proofs of two propositions in [Stallings 1999] that are left as exercises for the reader. In Section 4, we show how to use this algorithm to determine all the primitive elements in rank 2.

The other purpose is to explore the nongenericity of the separable property for an element of F_2. Borovik, Myasnikov and Shpilrain [Borovik et al. 2002] prove that the likelihood that a word in F_n of length k is separable decays to 0 exponentially in k. Actually, their proof as stated is about primitive elements, but an examination of their proof shows that it applies to separable elements as well. We consider a property of Whitehead graphs that is shared by all separable elements and indeed is the backbone of Stallings' algorithm. This property is the existence of a cut vertex. We show in Section 5 that the likelihood that a Whitehead graph of an element in F_2 with l edges has a cut vertex decays to 0 as $1/l^2$.

2. Preliminaries

Separability.

Definition 2.1. An element $g \in F_n$ is *separable* if there is a basis $\{a_1, a_2, \ldots, a_n\}$ for F_n such that the word representing g in this basis omits one of the a_i.

In [Stallings 1999], the notion of separability is defined for sets of elements in F_n. Our work in Section 4 can easily be adapted to this more general setting.

It is clear that the notion of separability is a conjugacy invariant. We recall that conjugacy classes of F_n can be identified with *reduced cyclic words*. These are reduced words considered as written on a circle and therefore there is no start or end to the word.

Example 2.2. Consider F_2 with basis $\{a, b\}$. Clearly, the words a, b, a^2, a^{-1} and b^{-1} are separable. It is not obvious to recognize, but these words are separable: ab, ba and $b^{-1}a$. Indeed, using Whitehead automorphisms (Example 2.5) one can see that $\{ab, b\}$, $\{ba, b\}$ and $\{b^{-1}a, b\}$ are all bases for F_2. With respect to these respective bases, the elements are clearly separable.

To show that an element is not separable, we must show that no basis as in Definition 2.1 exists. As there are infinitely many bases for F_n, we must have an effective algorithm that can tell us when to stop looking for such a basis. This is what Stallings' algorithm (Section 3) does for us. Using this, we will show that $ab^{-3}ab^{-1}$ and $aba^{-1}b^{-1}$ are not separable. See Example 3.3.

Remark 2.3. In rank 2, there is a connection between separable elements and primitive elements. An element $g \in F_n$ is *primitive* if there exists a basis $\{a_1, a_2, \dots, a_n\}$ such that the word representing g in this basis is one of the a_i or its inverse. In rank 2, an element is separable if and only if it is a nontrivial power of a primitive element.

Whitehead automorphisms. Like for vector spaces in linear algebra, changing from one basis of F_n to another involves applying an automorphism of F_n. The *Whitehead automorphisms* are analogous to elementary matrices in linear algebra in the sense that every automorphism of F_n can be expressed as a product of Whitehead automorphisms [Whitehead 1936].

Given a basis $\mathcal{A} = \{a_1, \dots, a_n\}$, by $\overline{\mathcal{A}}$ we denote the set $\{a_1^{-1}, \dots, a_n^{-1}\}$.

Definition 2.4. Let $\mathcal{A}$ be a basis for F_n and decompose $\mathcal{A} \cup \overline{\mathcal{A}} = Y \cup Z$ such that there is a $v \in Y$ with $v^{-1} \in Z$. The *Whitehead automorphism* $\phi = \phi_{(Y,Z,v)}$ is defined on $x \in \mathcal{A} \cup \overline{\mathcal{A}}$:

(i) If $x, x^{-1} \in Y$, then $\phi(x) = x$.

(ii) If $x, x^{-1} \in Z$, then $\phi(x) = vxv^{-1}$.

(iii) If $x = v$ or $x = v^{-1}$, then $\phi(x) = x$.

(iv) If $x \in Y$ and $x^{-1} \in Z$, then $\phi(x) = vx$.

(v) If $x^{-1} \in Y$ and $x \in Z$, then $\phi(x) = xv^{-1}$.

The map ϕ is extended as a homomorphism to the rest of F_n.

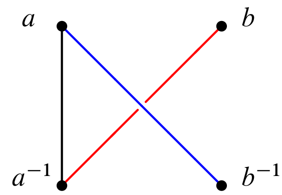


Figure 1. The Whitehead graph for $aba \in F_2$.

Example 2.5. Consider the Whitehead automorphism $\phi_{(Y,Z,v)}$ defined using the basis $\{a,b\}$ of F_2 where $Y = \{a^{-1}, b^{-1}\}$, $Z = \{a,b\}$ and $v = b^{-1}$. This automorphism sends the basis $\{a,b\}$ to $\{ab,b\}$.

Remark 2.6. Let $\{a_1,\dots,a_n\}$ be a basis for F_n. Suppose ϕ is an automorphism of F_n and $g \in F_n$ is such that the word representing $\phi(g)$ omits one of the a_i, i.e., $\phi(g)$ is separable. Then by considering the basis $\{\phi^{-1}(a_1),\dots,\phi^{-1}(a_n)\}$ we can witness that g is separable as well. In other words, if we can find some automorphism that removes all the occurrences of one of the basis elements from g, then g is separable. See Example 3.2.

Whitehead graphs. The key tool for detecting separability is the *Whitehead graph*.

Definition 2.7. Let $\mathcal{A}$ be a basis for the free group F_n. Given an element $g \in F_n$ whose conjugacy class is represented by the cyclic word w in the basis $\mathcal{A}$, we define the *Whitehead graph* of g, denoted $\mathrm{Wh}_{\mathcal{A}}(g)$, by

(vertices) $\mathcal{A} \cup \overline{\mathcal{A}}$,

(edges) between $u, v \in \mathcal{A} \cup \overline{\mathcal{A}}$ for each instance of uv^{-1} as a subword of w.

Example 2.8. Consider the word $aba \in F_2$. The vertices for $\mathrm{Wh}_{\{a,b\}}(aba)$ are denoted a, a^{-1}, b, b^{-1}. The edges are determined as follows:

First edge: the subword ab gives an edge from a to b^{-1}.

Second edge: the subword ba gives an edge from b to a^{-1}.

Third edge: the subword aa gives an edge from a to a^{-1}.

This Whitehead graph is shown in Figure 1.

Remark 2.9. An important property of Whitehead graphs to note is that the valence of a vertex v is the same as the valence of the vertex v^{-1}. This observation plays a key role in Sections 4 and 5.

Example 2.10. The Whitehead graph $\mathrm{Wh}_{\{a,b\}}(ab^{-3}ab^{-1})$ is shown in Figure 2.

The following definitions, applied to Whitehead graphs, will be used in Section 3 to determine whether a word is separable.

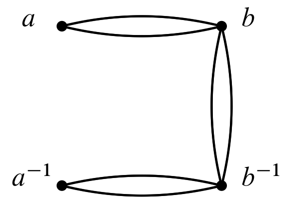


Figure 2. The Whitehead graph for $ab^{-3}ab^{-1} \in F_2$.

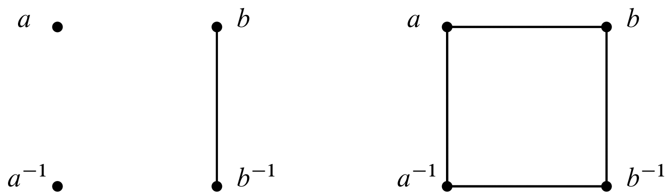


Figure 3. Left: the Whitehead graph of b is disconnected. Right: the Whitehead graph of $ab^{-1}a^{-1}b$ is connected and does not have a cut vertex.

Definition 2.11. A graph is connected if there is an edge path from any vertex to any other vertex in the graph.

The *trivial graph* is the graph with a single vertex and no edges.

Definition 2.12. A cut vertex v of a graph Γ is a vertex such that the graph decomposes into two nontrivial graphs Γ_1 and Γ_2 which intersect only at v. In other words, any edge path from a vertex of Γ_1 to a vertex in Γ_2 must go through v.

We remark that a disconnected Whitehead graph always has a cut vertex.

Figures 1 and 2 show Whitehead graphs that are connected and have a cut vertex. Figure 3 shows examples of Whitehead graphs that are respectively disconnected and connected without a cut vertex.

Remark 2.13. In terms of the Whitehead graph, an element $g \in F_n$ is separable if there is a basis $\mathscr{A}$ such that $\mathrm{Wh}_{\mathscr{A}}(g)$ has an isolated vertex. The isolated vertex exactly corresponds to the omitted basis element.

3. Stallings' algorithm

There is an algorithm due to Stallings [1999] that determines whether or not a word is separable. A flowchart for the algorithm is depicted in Figure 5. We will describe the algorithm in more detail, work out a couple of examples and provide proofs to a couple of the steps that are omitted in [Stallings 1999].

The important theorem needed to use the algorithm is the following.

Theorem 3.1 [Stallings 1999, Theorem 2.4]. *If $g \in F_n$ is separable, then the Whitehead graph of g in any basis contains a cut vertex.*

Using the contrapositive of this theorem, we can see that $ab^{-1}a^{-1}b$ is not a separable element of F_2, as its Whitehead graph in Figure 3, right, does not have a cut vertex. In general, an element that is not separable may have a Whitehead graph with respect to some basis that does have a cut vertex. To determine that the element is not separable, we need to find a basis in which its Whitehead graph does not have cut a vertex.

Stallings' algorithm. To determine whether a reduced cyclic word w in some basis $\mathcal{A}$ is separable or not, we start by constructing the Whitehead graph of w and determine if the graph is connected. If the graph is not connected, then Proposition 3.5 shows that after possibly applying a single Whitehead automorphism, the new Whitehead graph has an isolated vertex and hence w is separable (Remark 2.13).

If the graph is connected, then we determine if the graph has a cut vertex. If not, then by Theorem 3.1, w is not separable. If it does have a cut vertex, then by Proposition 3.6 there is a Whitehead automorphism ϕ such that the complexity of

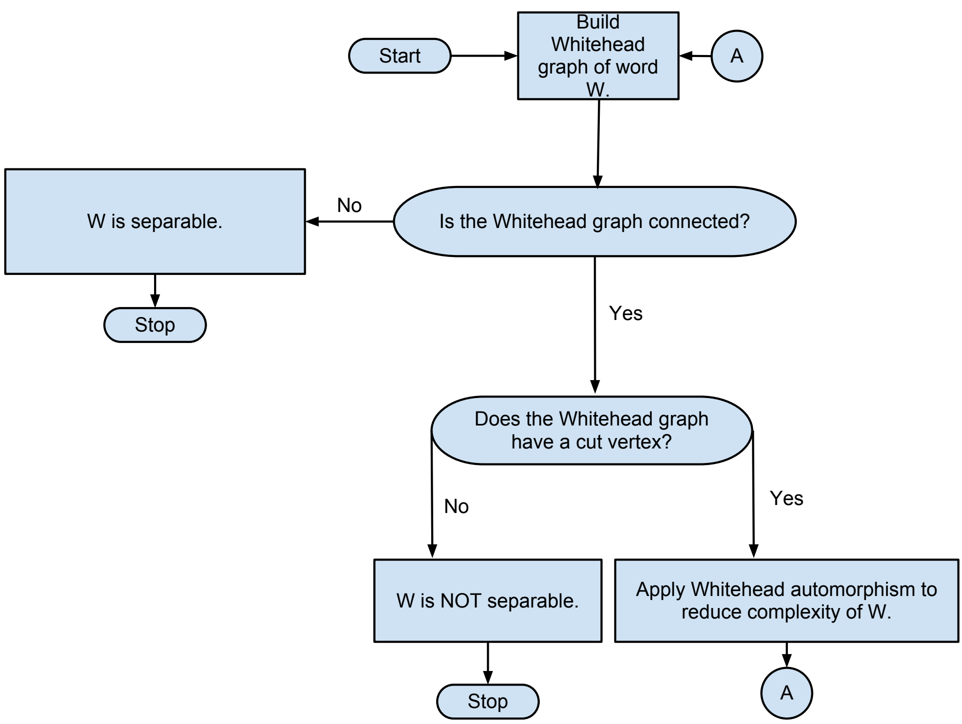


Figure 5. Flowchart for Stallings' algorithm.

$\phi(w)$ (that is, the length of the cyclic word representing it) is strictly less than the complexity of w. We now repeat the algorithm using the word w'.

Now in order for the algorithm to work, we need to know that it will terminate. That is precisely what Proposition 3.6 assures us. Since the complexity will be reduced, we know that eventually either the Whitehead graph will either be disconnected, or it will be connected without a cut vertex.

We now present an example of both a separable word and nonseparable word.

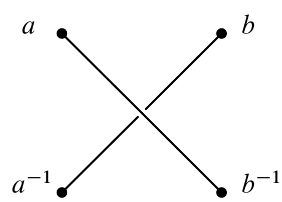
Example 3.2. The Whitehead graph of aba is shown in Figure 1. This graph has a cut vertex at a^{-1}. (The vertex a is also a cut vertex.) According to Proposition 3.6, we should apply the Whitehead automorphism with $Y = \{a^{-1}, b\}$, $Z = \{a, b^{-1}\}$, $v = a$ to reduce the complexity. The automorphism is given by

$$a \mapsto a, \quad b \mapsto a^{-1}b. \tag{1}$$

Applying the automorphism to aba, we get

$$aba \mapsto a(a^{-1}b)a = ba.$$

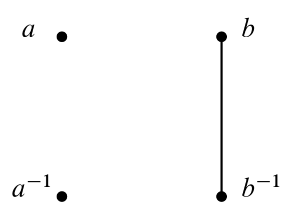
The graph of this new word ba is



This graph is disconnected, and thus by Proposition 3.5 we know that ba and hence aba is separable. We can apply the Whitehead automorphism using $Y = \{a, b^{-1}\}$, $Z = \{a^{-1}, b\}$, $v = a$ to see this explicitly. This is the automorphism:

$$a \mapsto a, \quad b \mapsto ba^{-1}. \tag{2}$$

Applying this automorphism, we have $ba \mapsto (ba^{-1})a = b$. The Whitehead graph of b looks like



So aba is separable, as there is an isolated vertex in this graph. By working backwards, applying the inverse automorphism of (2) and then the inverse automorphism of (1) to $\{a, b\}$, we can find a basis in which aba omits an element. The inverse to (2) is

$$a \mapsto a, \quad b \mapsto ba. \tag{3}$$

Applying this automorphism followed by the inverse to (1), given by

$$a \mapsto a, \quad b \mapsto ab, \tag{4}$$

we get $a \mapsto a \mapsto a$ and $b \mapsto ba \mapsto aba$. It is clear, in terms of the basis $\{a, aba\}$, that aba is separable.

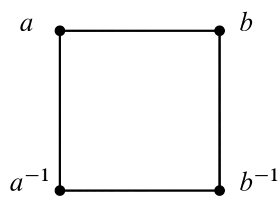
Example 3.3. Applying the algorithm to $ab^{-3}ab^{-1}$, we can show that this word is not separable. The Whitehead graph for this word is shown in Figure 2. Both b and b^{-1} are cut vertices; we choose b^{-1} to define our Whitehead automorphism. According to Proposition 3.6, we use the automorphism defined by the data $Y = \{a^{-1}, b^{-1}\}$, $Z = \{a, b\}$, $v = b^{-1}$. This is the automorphism:

$$a \mapsto ab, \quad b \mapsto b. \tag{5}$$

Applying this automorphism, we get

$$ab^{-3}ab^{-1} \mapsto (ab)b^{-3}(ab)b^{-1} = ab^{-2}a.$$

The Whitehead graph of $ab^{-2}a$ is this:



This graph does not have a cut vertex, so $ab^{-3}ab^{-1}$ is not separable.

Stallings provides examples to convince the reader of the validity of the steps:

(i) disconnected $\Longrightarrow$ separable [Stallings 1999, Proposition 2.2];

(ii) cut vertex $\Longrightarrow$ reduce complexity [Stallings 1999, Proposition 2.3].

However, he does not provide proofs. We will give proofs of these steps here. First, we prove a lemma that makes the arguments easier. The lemma shows that when the Whitehead graph has cut vertex v, subwords without $v^{\pm 1}$ behave like single elements.

Lemma 3.4. *Suppose $\mathcal{A}$ is a basis for F_n, let Y, Z be subsets of $\mathcal{A} \cup \overline{\mathcal{A}}$ and let $v \in \mathcal{A} \cup \overline{\mathcal{A}}$ define a Whitehead automorphism $\phi = \phi_{(Y,Z,v)}$. Suppose $w = w_1 w_2 \cdots w_k$ is a word over the basis $\mathcal{A}$ such that $w_i \neq v^{\pm 1}$ for all $i = 1, \dots, k$. Further suppose that either $w_i, w_{i+1}^{-1} \in Y$ or $w_i, w_{i+1}^{-1} \in Z$ for each $i = 1, \dots, k-1$.*

(i) *If* $w_1^{-1}, w_k \in Y$, *then* $\phi(w) = w$.

(ii) *If* $w_1^{-1}, w_k \in Z$, *then* $\phi(w) = vwv^{-1}$.

(iii) *If* $w_k \in Y$ *and* $w_1^{-1} \in Z$, *then* $\phi(w) = vw$.

(iv) *If* $w_1^{-1} \in Y$, $w_k \in Z$, *then* $\phi(w) = wv^{-1}$.

Proof. We will prove this by induction on k. If $k = 1$, this is just the definition of the Whitehead automorphism $\phi_{(Y,Z,v)}$ applied to $w = w_1$.

Now given $w = w_1 \cdots w_{k-1} w_k$, we have $\phi(w_1 \cdots w_{k-1}) = v^{\epsilon_1} w_1 \cdots w_{k-1} v^{-\epsilon_2}$ by induction, where ϵ_1, ϵ_2 are either 0 or 1 depending if w_1^{-1} and w_{k-1} are in Y or Z, respectively. Since w_k^{-1} is in Z if and only if w_{k-1} is in Z, we have $\phi(w_k) = v^{\epsilon_2} w_k v^{-\epsilon_3}$ for some ϵ_3 equal to either 0 or 1 depending if w_k is in Y or Z. Hence

$$\begin{aligned}\phi(w) &= \phi(w_1 \cdots w_{k-1})\phi(w_k) \\ &= v^{\epsilon_1} w_1 \cdots w_{k-1} v^{-\epsilon_2} \cdot v^{\epsilon_2} w_k v^{-\epsilon_3} \\ &= v^{\epsilon_1} w v^{-\epsilon_3}.\end{aligned}$$

This proves the lemma. □

Proposition 3.5 [Stallings 1999, Proposition 2.2]. *Suppose $\mathcal{A}$ is a basis for F_n and w is a word in this basis such that the Whitehead graph* $\mathrm{Wh}_{\mathcal{A}}(w)$ *does not have an isolated vertex and is not connected. Then w is separable. Specifically, separate the vertices of* $\mathrm{Wh}_{\mathcal{A}}(w)$ *into two subsets Y and Z such that there is no edge from a vertex in Y to a vertex in Z. Then there is a vertex $v \in Y$ such that $v^{-1} \in Z$ and the Whitehead graph of $\phi_{(Y,Z,v)}(w)$ has v an isolated vertex.*

Proof. If for all $v \in \mathcal{A}$ there is an edge between v and v^{-1} in $\mathrm{Wh}_{\mathcal{A}}(w)$, then we claim that the graph is connected. Indeed, let Γ be the graph obtained by collapsing all the edges between v and v^{-1} for each $v \in \mathcal{A}$, and denote the image vertices by the element of the basis. Then Γ has the same number of connected components as $\mathrm{Wh}_{\mathcal{A}}(w)$. But now reading off the elements of the basis $\mathcal{A}$ in the order in which they appear in w traces out a path in Γ. As there are no isolated vertices, every element in the basis appears along the path. Thus Γ and hence $\mathrm{Wh}_{\mathcal{A}}(w)$ is connected.

Hence, we have some vertex v as in the statement. By conjugating w, we can write $w = w_1 v^{\epsilon_1} w_2 v^{\epsilon_2} \cdots w_k v^{\epsilon_k}$, where $\epsilon_i \in \{-1, 1\}$ and v and v^{-1} do not appear in any of the w_i's. Indeed, as there is no edge between v and v^{-1}, v can only appear in w to the power 1 or -1. Notice, the w_i's satisfy the hypotheses of Lemma 3.4 using $\phi = \phi_{(Y,Z,v)}$.

Let X represent either Y or Z. We will write $w_i \in X$ to mean that when writing $w_i = u_1 u_2 \cdots u_k$ as a word in the basis $\mathcal{A}$, we have $u_k \in X$. Similarly, $w_i^{-1} \in X$ means that $u_1^{-1} \in X$. By Lemma 3.4, this is sufficient to specify the image of w_i under ϕ.

Suppose $i = 1, \dots, k-1$. If $\epsilon_i = 1$, then $w_i \in Z$ and $w_{i+1}^{-1} \in Y$, hence

$$\phi(w_i v w_{i+1}) = (v^{\kappa_1} w_i v^{-1}) v (w_{i+1} v^{-\kappa_2}) = v^{\kappa_1} w_i w_{i+1} v^{-\kappa_2},$$

where $\kappa_1, \kappa_2 \in \{0, 1\}$. Likewise, if $\epsilon_i = -1$, then $w_i \in Y$ and $w_{i+1}^{-1} \in Z$, hence

$$\phi(w_i v^{-1} w_{i+1}) = (v^{\kappa_1} w_i) v^{-1} (v w_{i+1} v^{-\kappa_2}) = v^{\kappa_1} w_i w_{i+1} v^{-\kappa_2},$$

where again $\kappa_1, \kappa_2 \in \{0, 1\}$.

These equations hold true for $i = k$ interpreting w_{k+1} as w_1. Therefore, the cyclic word representing $\phi(w)$ is $w_1 \cdots w_k$. □

Proposition 3.6 [Stallings 1999, Proposition 2.3]. *Suppose $\mathcal{A}$ is a basis for F_n and w is a word in this basis such that the Whitehead graph $\mathrm{Wh}_{\mathcal{A}}(w)$ is connected and that v is a cut vertex decomposing $\mathrm{Wh}_{\mathcal{A}}(w)$ into two nontrivial subgraphs Γ_1 and Γ_2, which only intersect at v. Suppose that Γ_2 contains the vertex v^{-1}. Let Y be the set of vertices of Γ_1, and Z the set of vertices of Γ_2 with the vertex v removed. Then the complexity of $\phi_{(Y,Z,v)}(w)$ is strictly less than the complexity of w.*

Proof. We can conjugate w to have form $w = w_1 v^{n_1} \cdots w_k v^{n_k}$, where $n_i \neq 0$ for all i and $v^{\pm 1}$ does not appear in any of the w_i's. As in Proposition 3.5, the w_i's satisfy the hypotheses of Lemma 3.4 using $\phi = \phi_{(Y,Z,v)}$. We continue to use the convention $w_i \in Y$, et cetera, from the proof of Proposition 3.5.

Suppose $i = 1, \dots, k-1$. If $n_i > 0$, then $w_i \in Z$. If $w_{i+1}^{-1} \in Y$, then

$$\phi(w_i v^{n_i} w_{i+1}) = (v^{\kappa_1} w_i v^{-1}) v^{n_i} (w_{i+1} v^{-\kappa_2}) = v^{\kappa_1} w_i v^{n_i - 1} w_{i+1} v^{-\kappa_2},$$

where $\kappa_1, \kappa_2 \in \{0, 1\}$. Otherwise, $w_{i+1}^{-1} \in Z$ and then

$$\phi(w_i v^{n_i} w_{i+1}) = (v^{\kappa_1} w_i v^{-1}) v^{n_i} (v w_{i+1} v^{-\kappa_2}) = v^{\kappa_1} w_i v^{n_i} w_{i+1} v^{-\kappa_2},$$

where $\kappa_1, \kappa_2 \in \{0, 1\}$.

Likewise, if $n_i < 0$, then $w_{i+1}^{-1} \in Z$. If $w_i \in Y$, then

$$\phi(w_i v^{n_i} w_{i+1}) = (v^{\kappa_1} w_i) v^{n_i} (v w_{i+1} v^{-\kappa_2}) = v^{\kappa_1} w_i v^{n_i + 1} w_{i+1} v^{-\kappa_2},$$

where $\kappa_1, \kappa_2 \in \{0, 1\}$. Otherwise, $w_i \in Z$ and then

$$\phi(w_i v^{n_i} w_{i+1}) = (v^{\kappa_1} w_i v^{-1}) v^{n_i} (v w_{i+1} v^{-\kappa_2}) = v^{\kappa_1} w_i v^{n_i} w_{i+1} v^{-\kappa_2},$$

where again $\kappa_1, \kappa_2 \in \{0, 1\}$.

Like in Proposition 3.5, for $i = k$ these equations hold interpreting $w_{k+1} = w_1$. Thus, we see that the length of the cyclic word representing $\phi(w)$ is reduced every time either $w_i \in Y$ or $w_{i+1}^{-1} \in Y$. This is the number of edges adjacent to v that are in Γ_1. □

Using Stallings' algorithm, we can compute the length of the shortest word in any basis that is not separable.

Theorem 3.7. *Let $g \in F_n$ be an element that is not separable. Then with respect to any basis of F_n, the length of the word representing g is at least $2n$. Furthermore, there is a word of length $2n$ that represents an element that is not separable.*

Proof. Let w be a word in some basis of F_n with length at most $2n-2$. Let Γ be the Whitehead graph of w. Then Γ will have $2n$ vertices. Before we add any edges to Γ, we can count each vertex as a connected component. So the initial number of connected components is $2n$, and as long as the number of components is greater than 1, we know that Γ is disconnected. Each edge added to Γ will be adjacent with two vertices which are either previously connected or disconnected. If the former occurs, then the number of components does not change. If the latter occurs, then the number of components is reduced by 1. Since w has at most $2n-2$ edges, the fewest number of components of Γ is $2n-(2n-2)=2$. So we know that the Whitehead graph is disconnected for all words of length at most $2n-2$, and hence by Proposition 3.5, every word of length at most $2n-2$ represents a separable element.

Now suppose the length of w is $2n-1$. After adding $2n-2$ edges, the Whitehead graph Γ will be disconnected. Then when we add the last edge, Γ will either become connected or remain disconnected. If Γ becomes connected, we know that at least one of the vertices adjacent to the last edge added will be a cut vertex. Then by Proposition 3.6 we can reduce the complexity of w. Since all shorter words will have a disconnected Whitehead graph by the above paragraph, we know that w represents a separable element.

This proves the first statement of the theorem. Now we will construct a word of length $2n$ that represents an element that is not separable.

Fix a basis $\mathcal{A}=\{a_1,\dots,a_n\}$ and define a word w in this basis by

$$w = a_1^{-1}a_2\cdots a_n^{(-1)^n}a_n^{(-1)^n}\cdots a_2a_1^{-1}.$$

We claim that the Whitehead graph is a circuit that contains every vertex. Let $1 \le i < n$. Then w will contain either $a_ia_{i+1}^{-1}$ and $a_{i+1}^{-1}a_i$ or $a_i^{-1}a_{i+1}$ and $a_{i+1}a_i^{-1}$ depending on if i is even or odd. In both cases the Whitehead graph will have edges between a_i and a_{i+1} and between a_i^{-1} and a_{i+1}^{-1}. Then since a_1^{-1} is on either side of w we will have an edge from a_1 to a_1^{-1}. Additionally, the $a_n^{\pm 2}$ in the center will add an edge from a_n to a_n^{-1}. This creates a circular graph which is connected without any cut vertices. So by Theorem 3.1, w represents an element that is not separable. □

In contrast with the fact that the likelihood of a element being separable decays to 0 as the word length increases [Borovik et al. 2002], the likelihood that a word of length $2n$ in F_n is *not* separable decays to 0 as $n \to \infty$. Let $\Sigma(l,n)$ denote the words of F_n of length l and $N(l,n)$ the subset that represent elements that are not separable.

Theorem 3.8. $$\lim_{n\to\infty} \frac{\#|N(2n,n)|}{\#|\Sigma(2n,n)|} = 0.$$

Proof. As we saw in the proof of Theorem 3.7, if a word w of length $2n$ is not separable, then its Whitehead graph is a circuit that contains every vertex. Hence for each element a_i of the basis, two elements (possibly the same) from $\{a_i, a_i^{-1}\}$ appear in w. This gives 2^{2n} choices. Multiplying this by the number of ways to order the $2n$ elements, we see that

$$\#|N(2n,n)| \le 2^{2n}(2n)!.$$

It is well known that the number of words of length l in rank n is

$$\#|\Sigma(l,n)| = 2n(2n-1)^{l-1}.$$

Therefore

$$\frac{\#|N(2n,n)|}{\#|\Sigma(2n,n)|} \le \frac{2^{2n}(2n)!}{2n(2n-1)^{2n-1}} \le \frac{2^{2n}(2n)!}{(2n-1)^{2n}}.$$

We will prove the theorem by showing this last ratio converges to 0.

Let us consider the series

$$\sum \frac{2^{2n}(2n)!}{(2n-1)^{2n}}.$$

We now show that this series converges. By applying the ratio test, we get

$$\begin{aligned}
\lim_{n\to\infty} \frac{\frac{2^{2n+2}(2n+2)!}{(2n+1)^{2n+2}}}{\frac{2^{2n}(2n)!}{(2n-1)^{2n}}} &= \lim_{n\to\infty} \frac{2^{2n+2}(2n+2)!}{(2n+1)^{2n+2}} \frac{(2n-1)^{2n}}{2^{2n}(2n)!} \\
&= \lim_{n\to\infty} \frac{2^2(2n+2)(2n+1)}{(2n+1)(2n+1)} \frac{(2n-1)^{2n}}{(2n+1)^{2n}} \\
&= 4 \lim_{n\to\infty} \frac{(2n-1)^{2n}}{(2n+1)^{2n}}.
\end{aligned}$$

Upon substitution of $x = 2n$, this becomes

$$4 \lim_{x\to\infty} \frac{(x-1)^x}{(x+1)^x} = 4 \lim_{x\to\infty} \exp\left(\ln\Big(\frac{x-1}{x+1}\Big)^x\right) = 4e^{\lim_{x\to\infty} x(\ln(x-1)-\ln(x+1))}.$$

Now we apply l'Hospital's rule to the exponent:

$$\lim_{x\to\infty} x\bigl(\ln(x-1)-\ln(x+1)\bigr) = \lim_{x\to\infty} \frac{\frac{1}{x-1}-\frac{1}{x+1}}{\frac{-1}{x^2}} = \lim_{x\to\infty} \frac{-2x^2}{x^2-1} = -2.$$

Hence the limit of the ratio of successive terms is $4e^{-2} < 1$. So by the ratio test, the series $\sum 2^{2n}(2n)!/(2n-1)^{2n}$ converges. $\square$

4. Separability in F_2

By Theorem 3.1, if an element is separable, then with respect to any basis its Whitehead graph has a cut vertex. In rank 2, this means that the Whitehead graph has one of the eight forms depicted in Figures 6 and 7. The labels α, β represent the multiplicity of an edge. Notice that we used that in a Whitehead graph the vertices v and v^{-1} have the same valence. This rules out, for instance, the $\sqcup$-shaped graph with edges only between a and a^{-1}, a^{-1} and b^{-1}, and b and b^{-1}. The labels on the graphs also reflect this observation.

We make the following simple observations. These observations appear in [Cohen et al. 1981] as well.

Lemma 4.1. *Suppose $g \in F_2$ is separable. Let w be the cyclic word representing the conjugacy class of g.*

(i) *If a^k appears as a subword of w, where $|k| > 1$, then for every nontrivial subword of the form b^m, we have $m = \pm 1$. Similarly, if b^m appears as a subword of w, where $|m| > 1$, then for every nontrivial subword of the form a^k, we have $k = \pm 1$.*

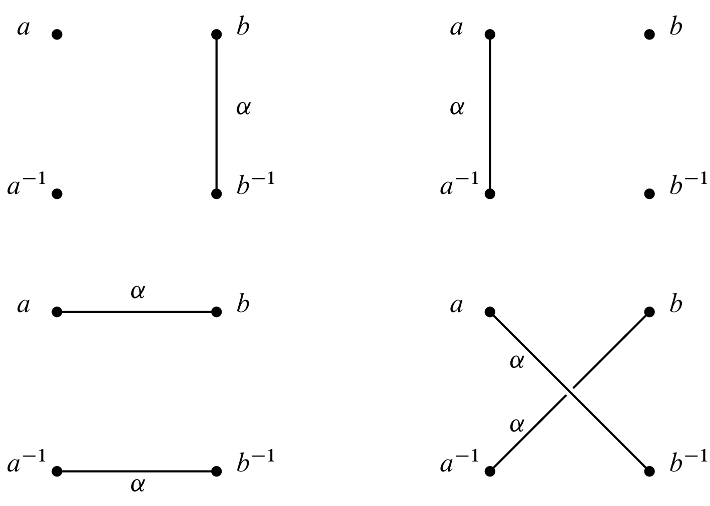


Figure 6. Disconnected Whitehead graphs in rank 2.

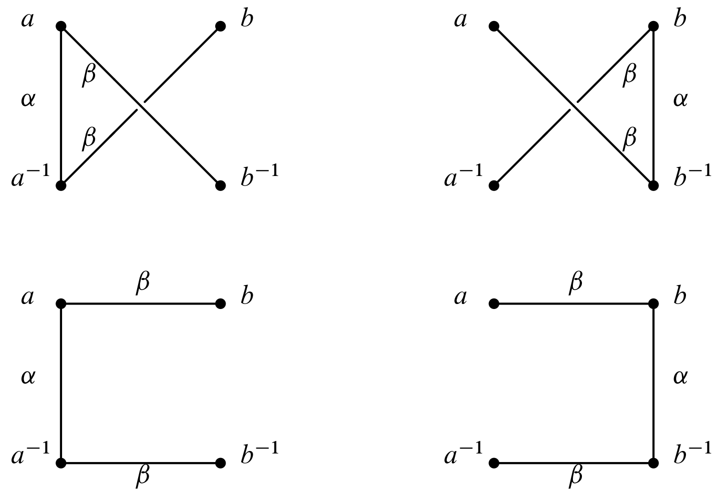


Figure 7. Connected Whitehead graphs with a cut vertex in rank 2.

(ii) *If a^{k_1} and a^{k_2} are nontrivial subwords of w, then $k_1k_2 > 0$. Similarly, if b^{m_1} and b^{m_2} are nontrivial subwords of w, then $m_1m_2 > 0$.*

Proof. Item (i) is clear, as in all the Whitehead graphs in Figures 6 and 7 there never appear edges both between a and a^{-1} and between b an b^{-1}. Thus either a or b can appear to a power other than ± 1, but not both.

Item (ii) is also clear if the Whitehead graph for g is as in Figure 6, since in this case w is either $a^{\pm\alpha}$, $b^{\pm\alpha}$, $(ab^{-1})^{\pm\alpha}$ or $(ab)^{\pm\alpha}$.

Suppose the Whitehead graph for g is the one depicted in the top left corner of Figure 7. Suppose both b and b^{-1} appeared as subwords of w. Then we have a subword of the form ba^kb^{-1}, where $k \neq 0$. The shape of the Whitehead graph applied to the initial ba^k forces $k > 0$, whereas applied to the latter a^kb^{-1} forces $k < 0$. This is a contradiction. A similar argument works if there is a subword of the form $ab^{\pm 1}a^{-1}$.

The other three Whitehead graphs are dealt with similarly by permuting $a \leftrightarrow b$ and/or $a \leftrightarrow a^{-1}$. □

Let $S^{+,+}(l, \alpha, \beta)$ be the set of cyclic words of length l that are separable, where any power of a or b that appears is positive and where α and β are the amount of a's and b's, respectively. We allow for the possibility that α or β is negative, in which case $S^{+,+}(l, \alpha, \beta) = \varnothing$. Notice that $l = \alpha + \beta$.

Likewise define $S^{-,+}(l, \alpha, \beta)$ as the set of cyclic words of length l that are separable and only use a^{-1} and b. Define $S^{+,-}(l, \alpha, \beta)$ and $S^{-,-}(l, \alpha, \beta)$ in a similar fashion. By Lemma 4.1, we have that every cyclic word that is separable is contained in one of these four sets. By S we denote one of $S^{+,+}$, $S^{-,+}$, $S^{+,-}$ or $S^{-,-}$.

Our goal is to show that there is exactly one element in $S(l,\alpha,\beta)$ (Theorem 4.3). We will use an inductive argument based on the following proposition.

Proposition 4.2. *Suppose* $\alpha, \beta \geq 0$. *Then*

$$\#|S(l,\alpha,\beta)| = \max\bigl\{\#|S(l-\alpha,\alpha,\beta-\alpha)|, \#|S(l-\beta,\alpha-\beta,\beta)|\bigr\}.$$

Proof. To simplify the argument, assume $S = S^{+,+}$. The other three cases are similar. Since $\#|S(l,\alpha,\beta)| = \#|S(l,\beta,\alpha)|$, without loss of generality we can assume $\alpha \geq \beta$.

If $\beta = 0$, then $S(l,\alpha,\beta) = S(l-\beta,\alpha-\beta,\beta)$ and $S(l-\alpha,\alpha,\beta-\alpha) = \varnothing$ and so the proposition holds. Notice that $S(l,l,0) = \{a^l\}$.

Now we assume that $\alpha = \beta > 0$. The Whitehead graph of any $x \in S(l,\alpha,\beta)$ is the bottom right graph of Figure 6 (recall we are assuming that $S = S^{+,+}$). Thus we must have that x can be represented by the cyclic word $(ab)^\alpha$, and hence $\#|S(l,\alpha,\beta)| = 1$. As

$$S(l-\alpha,\alpha,\beta-\alpha) = S(\alpha,\alpha,0) \quad \text{and} \quad S(l-\beta,\alpha-\beta,\beta) = S(\beta,0,\beta),$$

the proposition holds.

We are left with the case that $\alpha > \beta > 0$. Therefore, by Lemma 4.1, each $x \in S(l,\alpha,\beta)$ is represented by a cyclic word of the form

$$a^{\alpha_1} b a^{\alpha_2} b \cdots a^{\alpha_\beta} b,$$

where $\alpha_1 + \alpha_2 + \cdots + \alpha_\beta = \alpha$ and each $\alpha_i > 0$. We apply Proposition 3.6 in this case using $Y = \{a^{-1}, b\}$, $Z = \{a, b^{-1}\}$ and $v = a^{-1}$. This gives the Whitehead automorphism ϕ of F_2 defined by $\phi(a) = a$ and $\phi(b) = a^{-1}b$. When we apply ϕ to a word we will reduce its length and number of a's by β. So for each $x \in S(l,\alpha,\beta)$, we have $\phi(x) \in S(l-\beta,\alpha-\beta,\beta)$. Therefore

$$\#|S(l,\alpha,\beta)| \leq \#|S(l-\beta,\alpha-\beta,\beta)|.$$

To see the opposite inequality, we consider the automorphism ϕ^{-1}. This is the map $\phi^{-1}(a) = a$ and $\phi^{-1}(b) = ab$. Then applying ϕ^{-1} to an element

$$x \in S(l-\beta,\alpha-\beta,\beta)$$

will increase the number of a's and the length of x by β (recall we are assume that $S = S^{+,+}$). So for each $x \in S(l-\beta,\alpha-\beta,\beta)$, we have $\phi^{-1}(x) \in S(l,\alpha,\beta)$. Thus

$$\#|S(l-\beta,\alpha-\beta,\beta)| \leq \#|S(l,\alpha,\beta)|,$$

and therefore

$$\#|S(l-\beta,\alpha-\beta,\beta)| = \#|S(l,\alpha,\beta)|.$$

Notice that $\#|S(l-\alpha, \alpha, \beta-\alpha)| = 0$ as $\beta - \alpha < 0$. Thus

$$\#|S(l, \alpha, \beta)| = \max\bigl\{\#|S(l-\alpha, \alpha, \beta-\alpha)|, \#|S(l-\beta, \alpha-\beta, \beta)|\bigr\}. \qquad \square$$

Theorem 4.3. *Suppose* $\alpha, \beta \geq 0$. *Then*

$$\#|S(l, \alpha, \beta)| = 1.$$

Proof. As in Proposition 4.2, we assume that $S = S^{+,+}$.

Recall from the proof of Proposition 4.2 that

$$S(\alpha, \alpha, 0) = \{a^\alpha\} \quad \text{and} \quad S(\alpha, 0, \alpha) = \{b^\alpha\},$$

for all $\alpha > 0$. Hence, the Theorem holds for these special cases.

If $\alpha \geq \beta > 0$, then by Proposition 4.2,

$$\#|S(l, \alpha, \beta)| = \#|S(l-\beta, \alpha-\beta, \beta)|.$$

Likewise, if $\beta \geq \alpha > 0$, then by Proposition 4.2,

$$\#|S(l, \alpha, \beta)| = \#|S(l-\alpha, \alpha, \beta-\alpha)|.$$

Applying these repeatedly and using the Euclidean algorithm, we see

$$\#|S(l, \alpha, \beta)| = \#|S(d, d, 0)| = 1,$$

where $d = \gcd(\alpha, \beta)$. $\square$

Theorem 4.3 allows us to give an alternative proof to a classical result of Nielsen [1917]. First, we offer a corollary from which we will deduce Nielsen's result. Let $A\colon F_2 \to \mathbb{Z}^2$ denote the abelianization map. Given a word w in the basis $\{a, b\}$, this is the map

$$A(w) = \begin{bmatrix} \exp_a(w) \\ \exp_b(w) \end{bmatrix},$$

where $\exp_a(w)$ is the exponent sum of a in w, i.e., the number of a's that appear minus the number of a^{-1}'s. The function $\exp_b(w)$ is defined similarly.

Corollary 4.4. *Let* $g, h \in F_2$ *be separable. Then* $A(g) = A(h)$ *if and only if* g *and* h *are conjugate. Moreover, every nonzero element in* $\mathbb{Z}^2$ *is the image of some separable element and a separable element* $g \in F_2$ *is primitive if and only if the greatest common divisor of the components of* $A(g)$ *is* 1.

Proof. If g and h are separable, then the cyclic words representing their conjugacy classes belong to $S_1(l_1, \alpha_1, \beta_1)$ and $S_2(l_2, \alpha_2, \beta_2)$, respectively, where S_1 and S_2 denote one of $S^{+,+}$, $S^{-,+}$, $S^{+,-}$ or $S^{-,-}$. As the abelianization of an element in $S^{\pm,\pm}(l, \alpha, \beta)$ is $\left[\begin{smallmatrix} \pm\alpha \\ \pm\beta \end{smallmatrix}\right]$, if $A(g) = A(h)$, then $S_1(l_1, \alpha_1, \beta_1) = S_2(l_2, \alpha_2, \beta_2)$. By Theorem 4.3, this implies that g and h are conjugate.

The second part of the corollary can be seen by running the Euclidean algorithm that arises in Theorem 4.3 in reverse. We will explicitly show this in Theorem 4.6. □

As the subgroup of commutators $[F_2, F_2]$ is characteristic, an automorphism of F_2 defines an automorphism of $\mathbb{Z}^2$. This defines a homomorphism

$$\rho\colon \mathrm{Aut}(F_2) \to \mathrm{Aut}(\mathbb{Z}^2) = \mathrm{GL}(2, \mathbb{Z}).$$

This homomorphism satisfies $A \circ \phi = \rho(\phi) \circ A$. In terms of matrices, this map is defined by

$$\rho(\phi) = \begin{bmatrix} \exp_a(\phi(a)) & \exp_a(\phi(b)) \\ \exp_b(\phi(a)) & \exp_b(\phi(b)) \end{bmatrix}.$$

Corollary 4.5 [Nielsen 1917]. *Let $\phi \in \mathrm{Aut}(F_2)$. If $\rho(\phi) = \mathrm{Id}$, then there is a $g \in F_2$ such that $\phi(x) = gxg^{-1}$.*

Proof. If $\rho(\phi) = \mathrm{Id}$, then as $\phi(a)$ is primitive and $A\phi(a) = \rho(\phi)A(a) = A(a)$, we have that $\phi(a)$ is conjugate to a by Corollary 4.4. Say $\phi(a) = g_1 a g_1^{-1}$. Likewise, we have that $\phi(b) = g_2 b g_2^{-1}$. Define $\psi \in \mathrm{Aut}(F_2)$ by $\psi(x) = g_1^{-1} x g_1$. Thus $\psi\phi(a) = a$ and $\psi\phi(b) = g_3 b g_3^{-1}$, where $g_3 = g_1^{-1} g_2$. As $\psi\phi$ is an automorphism of F_2, the set $\{a, g_3 b g_3^{-1}\}$ is a basis for F_2; in particular, this set generates F_2. Using a method such as Stallings' foldings [Stallings 1983], it is clear that this is only possible if $g_3 = a^k$ for some k. Thus $\phi(x) = g_1 a^k x a^{-k} g_1^{-1}$. □

We will now give an explicit description of the cyclic word in $S(l, \alpha, \beta)$ when $\gcd(\alpha, \beta) = 1$. When the $\gcd(\alpha, \beta) = d \neq 1$, the cyclic word is obtained by taking the d-th power of the cyclic word in $S(l/d, \alpha/d, \beta/d)$. Our description matches that of Osborne and Zieschang [1981].

For simplicity, we assume $S = S^{+,+}$. Let $\left[\begin{smallmatrix} \alpha \\ \beta \end{smallmatrix}\right] \in \mathbb{Z}^2$ be such that $\alpha, \beta \geq 1$ and $\gcd(\alpha, \beta) = 1$. Let $L_{\alpha,\beta}$ denote the line segment in $\mathbb{R}^2$ from $(0, 0)$ to (α, β). Define $v_{\alpha,\beta}$ as the word in $\{a, b\}$ where an a appears for each integer vertical line $L_{\alpha,\beta}$ crosses and a b appears for each integer horizontal line $L_{\alpha,\beta}$ crosses. The letters appear in the order of the lines $L_{\alpha,\beta}$ crosses. As $\gcd(\alpha, \beta) = 1$, the interior of $L_{\alpha,\beta}$ does not simultaneously cross both an integer horizontal line and a integer vertical line. See Figure 8.

Now define $w_{\alpha,\beta} = a v_{\alpha,\beta} b$. Also define $w_{1,0} = a$ and $w_{0,1} = b$. In the case that α or β are negative, the words $v_{\alpha,\beta}$ and $w_{\alpha,\beta}$ are defined analogously.

Theorem 4.6. *Suppose $\alpha, \beta \geq 0$ and that $\gcd(\alpha, \beta) = 1$. The unique cyclic word in $S^{+,+}(l, \alpha, \beta)$ is determined by $w_{\alpha,\beta}$.*

Proof. For simplicity we denote $S = S^{+,+}$. If $\alpha = 0$ or $\beta = 0$ then the theorem is clear. Likewise if $\alpha = \beta = 1$. In this case, $v_{1,1}$ is the empty word and therefore

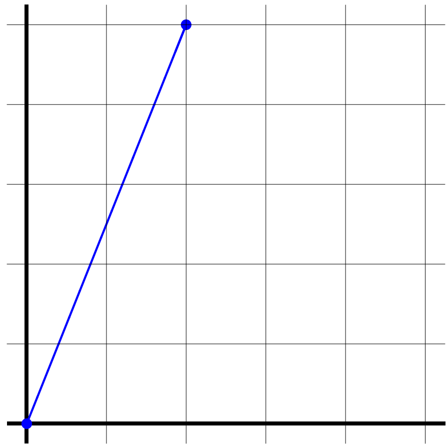


Figure 8. The line segment $L_{2,5}$ and the word $v_{2,5} = bbabb$.

$w_{1,1} = ab$. The cyclic word determined by $w_{1,1}$ is the unique separable word in $S(2, 1, 1)$.

Assume that $\alpha > \beta > 0$. We show that $w_{\alpha-\beta,\beta} = \phi(w_{\alpha,\beta})$, where ϕ is the Whitehead automorphism from the proof of Proposition 4.2, namely $\phi(a) = a$ and $\phi(b) = a^{-1}b$. Since $\alpha > \beta$, each of the b's in $w_{\alpha,\beta}$ is isolated, as crossing two adjacent horizontal lines without crossing a vertical line implies the slope of $L_{\alpha,\beta}$ is greater than 1, i.e., $\beta/\alpha > 1$.

Thus it is clear that both $w_{\alpha-\beta,\beta}$ and $\phi(w_{\alpha,\beta})$ contain the same number of a's and b's, namely $\alpha-\beta$ and β, respectively. The difference between $w_{\alpha,\beta}$ and $\phi(w_{\alpha,\beta})$ is one fewer a between adjacent b's.

Notice that for $i = 0, \dots, \beta - 1$, the number of a's between the i-th and $(i+1)$-st b of $v_{\alpha,\beta}$ is $\langle((i+1)\alpha)/\beta\rangle - \langle i\alpha/\beta\rangle$, where $\langle x\rangle$ is the largest integer *strictly less*[1] *than* x. The 0-th b is interpreted as the beginning of $v_{\alpha,\beta}$ and the β-th b is interpreted as the end of $v_{\alpha,\beta}$. Indeed, $x = \langle i\alpha/\beta\rangle$ is the vertical line crossed by $L_{\alpha,\beta}$ immediately preceding crossing the horizontal line $y = i$. Hence, we observe that the number of a's between the i-th and $(i+1)$-st b of $v_{\alpha-\beta,\beta}$ is

$$\begin{aligned}\left\langle\frac{(i+1)(\alpha-\beta)}{\beta}\right\rangle - \left\langle\frac{i(\alpha-\beta)}{\beta}\right\rangle &= \left(\left\langle\frac{(i+1)\alpha}{\beta}\right\rangle - (i+1)\right) - \left(\left\langle\frac{i(\alpha-\beta)}{\beta}\right\rangle - i\right)\\ &= \left\langle\frac{(i+1)\alpha}{\beta}\right\rangle - \left\langle\frac{i\alpha}{\beta}\right\rangle - 1.\end{aligned}$$

This shows that $\phi(w_{\alpha,\beta}) = w_{\alpha-\beta,\beta}$.

If $\beta > \alpha > 0$, we have $w_{\alpha,\beta-\alpha} = \psi(w_{\alpha,\beta})$ as above, where $\psi(a) = ab^{-1}$ and $\psi(b) = b$.

[1] We use this variant of the floor function to avoid having to subtract 1 in the case $i = \beta - 1$.

By induction, this shows that $w_{\alpha,\beta}$ is separable. By construction, the length of $w_{\alpha,.\beta}$ is $l = \alpha + \beta$ and this word contains α a's and β b's. Hence, the cyclic word determined by $w_{\alpha,\beta}$ is the unique word in $S(l, \alpha, \beta)$. □

We end this section by showing that the above analysis allows for an exact count of the number of separable cyclic words of a given length. Let $S^{+,+}(l)$ be the set of all positive conjugacy classes of length l that are separable. Then $S^{+,+}(l)$ is the disjoint union

$$S^{+,+}(l) = S^{+,+}(l,0,l) \cup S^{+,+}(l,1,l-1) \cup \cdots \cup S^{+,+}(l,l-1,1) \cup S^{+,+}(l,l,0).$$

So

$$\#|S^{+,+}(l)| = \sum_{\alpha=0}^{l} \#|S^{+,+}(l,\alpha,l-\alpha)| = l+1.$$

Likewise, we can define $S^{-,+}(l)$, $S^{+,-}(l)$ and $S^{-,-}(l)$. The cardinality of each of these sets is also $l+1$. Notice that $S^{+,+}(l) \cap S^{+,-}(l) = \{a^l\}$. There are three similar equations regarding the other intersections.

Theorem 4.7. *The number of cyclic words of length l in F_2 that are separable is* $4l$.

5. Whitehead graphs in F_2

In this final section we will explore to what extent the decay in the likelihood of an element being separable is a property of Whitehead graphs in rank 2.

Let $\mathrm{WhG}(l)$ denote the set of Whitehead graphs in ranks 2 with l edges. Let $\mathrm{Dis}(l)$ denote the subset that are disconnected and let $\mathrm{Cut}(l)$ denote the subset that are connected with a cut vertex.

By counting the number for each l we arrive at:

Theorem 5.1. $$\#|\mathrm{Dis}(l)| + \#|\mathrm{Cut}(l)| = 2l.$$

Proof. First, separate the equation into two parts: $\#|\mathrm{Cut}(l)|$ and $\#|\mathrm{Dis}(l)|$; we compute each separately.

To compute $\#|\mathrm{Dis}(l)|$, we refer to Figure 6. When l is even, each of the 4 forms can appear ($\alpha = l$ in the top two and $\alpha = l/2$ in the bottom two), and when l is odd, only the top two forms appear ($\alpha = l$). Hence

$$\#|\mathrm{Dis}(l)| = \begin{cases} 4 & \text{if } l \text{ is even,} \\ 2 & \text{if } l \text{ is odd.} \end{cases} \tag{6}$$

To compute $\#|\mathrm{Cut}(l)|$, we again consider two cases depending on if l is even or odd. Referring to Figure 7, we must have $l = \alpha + 2\beta$.

When l is odd, as $l = \alpha + 2\beta$, l is odd too. The least odd number that α can be is 1, in this case $\beta = (l-1)/2$. Therefore, the range of β when l is odd is

$$1 \leq \beta \leq \frac{l-1}{2}.$$

Each value of β results in four distinct graphs in $\mathrm{Cut}(l)$.

When l is even, we have the same equation as above, $l = \alpha + 2\beta$, but the least even number that α can be is 2, in this case $\beta = (l-2)/2$. So the range of β when l is even is

$$1 \leq \beta \leq \frac{l-2}{2}.$$

Again, each value of β corresponds to four distinct graphs in $\mathrm{Cut}(l)$. Combining these calculations, we have

$$\#|\mathrm{Cut}(l)| = \begin{cases} 2l-4 & \text{if } l \text{ is even,} \\ 2l-2 & \text{if } l \text{ is odd.} \end{cases} \tag{7}$$

Combining (6) and (7) we get $\#|\mathrm{Dis}(l)| + \#|\mathrm{Cut}(l)| = 2l$. □

Remark 5.2. Comparing Theorems 4.7 and 5.1, we see that for each Whitehead graph in $\mathrm{Dis}(l) \cup \mathrm{Cut}(l)$ there are exactly two separable conjugacy classes associated to that graph. These two conjugacy classes are related by inversion.

Next we count the total number of Whitehead graphs in rank 2 by taking combinations of the graphs in Figure 6. Again, we are using the observation that in a Whitehead graph the valence of the vertex v is the same as the valence of the vertex v^{-1}.

Theorem 5.3. $\#|\mathrm{WhG}(l)| = \begin{cases} \frac{1}{24}(l^3 + 9l^2 + 26l + 24) & \textit{if } l \textit{ is even,} \\ \frac{1}{24}(l^3 + 9l^2 + 23l + 15) & \textit{if } l \textit{ is odd.} \end{cases}$

Proof. We begin by constructing a generating function $f(x)$ for $\#|\mathrm{WhG}(l)|$ [Brualdi 2010, Section 7.4]. A Whitehead graph with l edges is formed by combining graphs in Figure 6 with $\alpha = 1$. Each graph from the top row contributes one edge and each graph from the bottom row contributes two edges. Hence

$$f(x) = (1+x+x^2+\cdots)(1+x+x^2+\cdots)(1+x^2+x^4+\cdots)(1+x^2+x^4+\cdots).$$

Then $\#|\mathrm{WhG}(l)|$ is the coefficient of x^l in $f(x)$. In order to compute this coefficient, we will compute the Taylor series for f centered at 0. To compute $f^{(l)}$, we rewrite f and take the partial fraction decomposition:

$$\begin{aligned} f(x) &= \frac{1}{(1-x)^2(1-x^2)^2} \\ &= \frac{1}{8}\left(\frac{1}{1+x} + \frac{1}{1-x}\right) + \frac{1}{16}\left(\frac{1}{(1+x)^2} + \frac{3}{(1-x)^2}\right) + \frac{1}{4}\left(\frac{1}{(1-x)^3} + \frac{1}{(1-x)^4}\right). \end{aligned}$$

The l-th derivative of f at 0 is

$$f^{(l)}(0)=\frac{1}{8}l!\big((-1)^l+1\big)+\frac{1}{16}(l+1)!\big((-1)^n+3\big)+\frac{1}{4}\Big(\frac{(l+2)!}{2}+\frac{(l+3)!}{6}\Big).$$

After dividing by $l!$, the equation simplifies to

$$\frac{f^{(l)}(0)}{l!}=\frac{1}{8}\big((-1)^l+1\big)+\frac{1}{16}(l+1)\big((-1)^l+3\big)\\ +\frac{1}{4}\Big(\frac{(l+1)(l+2)}{2}+\frac{(l+1)(l+2)(l+3)}{6}\Big).$$

We will have two cases, looking at the equation above, for $(-1)^{\text{even}}=1$ and $(-1)^{\text{odd}}=-1$. Thus

$$\frac{f^{(l)}(0)}{l!}=\begin{cases}\frac{1}{24}(l^3+9l^2+26l+24) & \text{if } l \text{ is even,}\\ \frac{1}{24}(l^3+9l^2+23l+15) & \text{if } l \text{ is odd.}\end{cases}$$

As $\#|\mathrm{WhG}(l)|=f^{(l)}(0)/l!$, the proof is complete. □

Notice that although the likelihood of a cyclically reduced word being separable decays to 0 exponentially in the length of the word [Borovik et al. 2002], the likelihood of a Whitehead graph containing a cut vertex approaches 0 like $1/l^2$, where l is the number of edges of the graph.

Acknowledgement

This research was conducted as a Student/Faculty Summer Research project at Allegheny College. The authors thank Allegheny College for its support.

References

[Borovik et al. 2002] A. V. Borovik, A. G. Myasnikov, and V. Shpilrain, "Measuring sets in infinite groups", pp. 21–42 in *Computational and statistical group theory* (Las Vegas, NV/Hoboken, NJ, 2001), edited by R. Gilman et al., Contemp. Math. **298**, Amer. Math. Soc., Providence, RI, 2002. MR 2003m:20024 Zbl 1022.20010

[Brualdi 2010] R. A. Brualdi, *Introductory combinatorics*, 5th ed., Pearson Prentice Hall, Upper Saddle River, NJ, 2010. MR 2012a:05001 Zbl 0915.05001

[Cohen et al. 1981] M. Cohen, W. Metzler, and A. Zimmermann, "What does a basis of $F(a,b)$ look like?", *Math. Ann.* **257**:4 (1981), 435–445. MR 82m:20028 Zbl 0458.20028

[Kassel and Reutenauer 2007] C. Kassel and C. Reutenauer, "Sturmian morphisms, the braid group B_4, Christoffel words and bases of F_2", *Ann. Mat. Pura Appl.* (4) **186**:2 (2007), 317–339. MR 2007j:20029 Zbl 1150.05042

[Lyndon and Schupp 2001] R. C. Lyndon and P. E. Schupp, *Combinatorial group theory*, Springer, Berlin, 2001. MR 2001i:20064 Zbl 0997.20037

[Nielsen 1917] J. Nielsen, "Die Isomorphismen der allgemeinen, unendlichen Gruppe mit zwei Erzeugenden", *Math. Ann.* **78**:1 (1917), 385–397. MR 1511907

[Osborne and Zieschang 1981] R. P. Osborne and H. Zieschang, “Primitives in the free group on two generators”, *Invent. Math.* **63**:1 (1981), 17–24. MR 82i:20042 Zbl 0438.20017

[Piggott 2006] A. Piggott, “Palindromic primitives and palindromic bases in the free group of rank two”, *J. Algebra* **304**:1 (2006), 359–366. MR 2007g:20026 Zbl 1111.20028

[Stallings 1983] J. R. Stallings, “Topology of finite graphs”, *Invent. Math.* **71**:3 (1983), 551–565. MR 85m:05037a Zbl 0521.20013

[Stallings 1999] J. R. Stallings, “Whitehead graphs on handlebodies”, pp. 317–330 in *Geometric group theory down under: proceedings of a special year in geometric group theory* (Canberra, 1996), edited by J. Cossey et al., de Gruyter, Berlin, 1999. MR 2000e:20002 Zbl 1127.57300

[Whitehead 1936] J. H. C. Whitehead, “On equivalent sets of elements in a free group”, *Ann. of Math.* (2) **37**:4 (1936), 782–800. MR 1503309 Zbl 0015.24804

Received: 2012-03-14 Accepted: 2012-12-27

mattclay@uark.edu *Department of Mathematical Sciences, University of Arkansas, SCEN 301, Fayetteville, AR 72701, United States*

jconan01@rams.shepherd.edu *Department of Education, Shepherd University, Shepherdstown, WV 25443, United States*

nivetharamas@gmail.com *Clinton Township, MI 48036, United States*

involve

msp.org/involve

See inside back cover or msp.org/involve for submission instructions. The subscription price for 2014 is US $120/year for the electronic version, and $165/year (+$35, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues from the last three years and changes of subscribers address should be sent to MSP.

Involve (ISSN 1944-4184 electronic, 1944-4176 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840, is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

Involve peer review and production are managed by EditFLOW® from Mathematical Sciences Publishers.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

involve

2014 vol. 7 no. 4

Whitehead graphs and separability in rank two 431
MATT CLAY, JOHN CONANT AND NIVETHA RAMASUBRAMANIAN

Perimeter-minimizing pentagonal tilings 453
PING NGAI CHUNG, MIGUEL A. FERNANDEZ, NIRALEE SHAH, LUIS SORDO VIEIRA AND ELENA WIKNER

Discrete time optimal control applied to pest control problems 479
WANDI DING, RAYMOND HENDON, BRANDON CATHEY, EVAN LANCASTER AND ROBERT GERMICK

Distribution of genome rearrangement distance under double cut and join 491
JACKIE CHRISTY, JOSH MCHUGH, MANDA RIEHL AND NOAH WILLIAMS

Mathematical modeling of integrin dynamics in initial formation of focal adhesions 509
AURORA BLUCHER, MICHELLE SALAS, NICHOLAS WILLIAMS AND HANNAH L. CALLENDER

Investigating root multiplicities in the indefinite Kac–Moody algebra E_{10} 529
VICKY KLIMA, TIMOTHY SHATLEY, KYLE THOMAS AND ANDREW WILSON

On a state model for the SO$(2n)$ Kauffman polynomial 547
CARMEN CAPRAU, DAVID HEYWOOD AND DIONNE IBARRA

Invariant measures for hybrid stochastic systems 565
XAVIER GARCIA, JENNIFER KUNZE, THOMAS RUDELIUS, ANTHONY SANCHEZ, SIJING SHAO, EMILY SPERANZA AND CHAD VIDDEN

1944-4176(2014)7:4;1-5