Lifting Free Subgroups of $PSL(2,\mathbb{R})$ to Free Groups

Jane Gilman and Linda Keen

Dedicated to Clifford Earle on his 75th Birthday.

ABSTRACT. Let $F = \langle a, b \rangle$ be a rank two free group, let $G = \langle A, B \rangle$ be a two generator subgroup of $PSL(2,\mathbb{R})$ and let ρ be a faithful representation of F with $\rho(a) = A$ and $\rho(b) = B$. If G is discrete and free, many results about the primitive elements of G are proved using the geometry that G inherits from $PSL(2,\mathbb{R})$, the group of orientation preserving isometries of the hyperbolic plane. Some of these results can be lifted to F modulo the replacement of a and/or b by their inverse and the interchange of a and b. In this paper we lift these results and obtain results that are independent of any replacement by inverses or interchange of generators and independent of the given representation.

1. Introduction

Let $F = \langle a, b \rangle$ be a free group of rank two. An element of F is *primitive* if it, along with another group element, generates the group. Nielsen [**21**] proved that every primitive word was the result of a finite sequence of specific Nielsen transformations but didn't give explicit forms for them. Since free groups on two generators come up very often in different mathematical contexts, the question of what form primitive elements take, or equivalently, which words $w(a, b) \in F$ are primitive and which pairs of primitive elements generate the group comes up again and again and has been addressed by many authors. (See the bibliography and references cited there.)

Many results about primitive elements and/or pairs of elements that generate a free two generator subgroup of $PSL(2,\mathbb{R})$ are often stated *up to replacing one or both of the generators by their inverses and/or interchanging the generators.* Suppose ρ is a faithful non-elementary representation of $F = \langle a, b \rangle$ onto $G \subset PSL(2,\mathbb{R})$. Even if G is a free group isomorphic to F, these results often cannot be pulled back directly to statements about F. This is because the results depend on the geometric properties of elements of a subgroup of $PSL(2,\mathbb{R})$. For example, considered as isometries on the upper-half plane, the elements have orientations

---

1991 *Mathematics Subject Classification.* 20, 30F35, 30F40.

Key words and phrases. Free Groups, Discrete Groups, Hyperbolic Geometry.

Rutgers Research Council and the NSF..

PSC-CUNY research grant.

and translation lengths. In particular, in previous work, [**8, 10, 13**], we used the geometry to relate primitive elements and pairs of primitive elements that generate the free group G with rational numbers and continued fractions. In this paper we lift those results to F.

More specifically, in [**8**] we characterized the words in G corresponding to the primitive elements topologically, in terms of *winding*, and geometrically in terms of translation length. This winding, which we will explain later, is determined by a sequence of integers $\mathcal{F} = [\alpha_0, \dots, \alpha_k]$. We showed that this sequence is the continued fraction expansion of the rational p/q associated to the conjugacy class of the primitive.

In [**13**] an algorithm is given to decide, in finitely many steps, whether a given pair of hyperbolics $(A, B) \in PSL(2, \mathbb{R})$ with disjoint axes generate a discrete and free group. It was shown there that if the representation were discrete and free, then up to taking inverses as necessary, any pair of primitive words could be obtained from (A, B) by applying a specific sequence of Nielsen transformations to the generators. This sequence is described by an ordered set of integers, $[\beta_0, \dots \beta_k]$ and is used in computing the computational complexity of the algorithm [**5, 15**]. In [**8**] we showed that the sequence $[\beta_0, \dots \beta_k]$ corresponds to *unwinding*, a process dual to the winding. We also showed how the rationals associated to winding and unwinding are related.

The arguments in [**8, 13**] use the geometry of the hyperbolic plane. In particular, they make strong use of the ability to orient geodesics and hence to distinguish between a word in $G = \langle A, B \rangle$ and its inverse and between the pair (A, B) and the pair (B, A). Our aim in this paper is to lift these results for the generators of the representation groups to pairs of primitives that generate the free group. Therefore in lifting statements from $PSL(2, \mathbb{R})$ to F we need to carefully analyze the role of geometric orientation and the relative lengths of geodesics in the algorithm of [**13**].

In this paper we concentrate in detail on the case where under the representation the generators are hyperbolic and their axes are disjoint. In section 7 we discuss the other cases using our algorithmic approach. Some of the results proved here are not new, but are given with new proofs.

We state our main results leaving the definitions of terms such as the $\mathcal{F}$ sequence and notation such as $W_{[\alpha_0, \dots, \alpha_k]}$ for the introductory parts of later sections. Our main result is that the results in [**8**] hold for abstract free groups:

THEOREM 1.1. *Up to conjugacy, every primitive word of the free group on two generators, $F = \langle a, b \rangle$ can be written in the form $W(a, b)$ where $W(a, b) = W_{[\alpha_0, \dots, \alpha_k]}$ is formed by the sequence of Nielsen transformations determined by the $\mathcal{F}$-sequence $[\alpha_0, \dots, \alpha_k]$ and is, up to inverse, uniquely associated with the rational p/q whose continued fraction is the given $\mathcal{F}$-sequence.*

THEOREM 1.2. *A pair of primitives w, v generates F if and only if the corresponding rationals, $p/q, r/s$ satisfy $|ps - qr| = 1$.*

THEOREM 1.3. *Corresponding to any discrete faithful representation ρ of F there is a unique triple of primitive elements in F, $\{c, d, cd^{-1}\}$ such that any two of the three are a primitive pair and any other primitive pair can be derived from c and d using an $\mathcal{F}$-sequence.*

THEOREM 1.4. *The primitive exponents in the expanded form of the words $W(a, b) = W_{[\alpha_0, \dots, \alpha_k]} \in F$ satisfy the formulas in theorem 3.1.*

Our paper is organized as follows: Section 2 defines $\mathcal{F}$-sequences. Section 3 is concerned with the exponents in words and section 5 goes into detail about the exponents in a primitive word and in a pair of primitive words that generate the group. That section also states theorems from previous papers that apply to G along with their extensions to F. In section 4 the geometry of primitive pairs is developed giving definitions of coherently ordered pairs and winding and unwinding. In section 6 all results stated for G are lifted to F and proofs are given in the case of representations with disjoint axes. The final section 7 extends the results to representations with parabolic elements and cases with intersecting axes.

2. $\mathcal{F}$-sequences

The definitions in this section make sense for any two generator group whether or not it is free. To simplify things, therefore, we continue to use the notation F to denote an arbitrary two generator group.

Definition 1. *An $\mathcal{F}-$**sequence** is an ordered set of integers $[\alpha_0, \ldots \alpha_k]$ where all the α_i, $i = 0, \ldots, k$ have the same sign and all but α_0 are required to be non-zero. In addition, if $k > 1$, then $a_k > 1$. For completeness we also include the empty sequence, $[\emptyset]$.*

Given an $\mathcal{F}$-sequence we use it define a sequence of words and a sequence of ordered pairs of word in a free group $F = \langle a, b\rangle$. The sequence of words and pairs of words in the group so determined, of course, depends upon the fixed generators. The same word will have a different $\mathcal{F}$ sequence for a different choice of generators.

Definition 2. **$\mathcal{F}$-words.** *Let a and b generate the group F and let $\mathcal{F} = [\alpha_0, ..., \alpha_k]$ be an $\mathcal{F}-$sequence. We define the ordered pairs of words (a_t, b_t), $t = 0, \ldots, k$ inductively, replacing the pair (X, Y) given at step t by the pair $(Y^{-1}, X^{-1}Y^{a_t})$ as follows: If the $\mathcal{F}$-sequence is empty, we set*

$$(a_0, b_0) = (a, b)$$

and stop. Otherwise we set

$$(a_0, b_0) = (a, b)$$

and

$$(a_1, b_1) = (b^{-1}, a^{-1}b^{\alpha_0}).$$

Then for $t = 1, \ldots, k$, we set

$$(a_{t+1}, b_{t+1}) = (b_t^{-1}, a_t^{-1}b_t^{\alpha_t}).$$

Note that $a_{t+1} = b_t^{-1}$ and $b_{t+1} = b_{t-1}b_t^{\alpha_t}$. We call the words (a_t, b_t) the $\mathcal{F}$-words determined by the $\mathcal{F}$-sequence.

We use the notation $b_t = W_{[\alpha_0, \ldots \alpha_t]}(a, b)$. With this notation the first pair is

$$a_0 = W_{[\emptyset]}(a, b) \text{ and } b_0 = W_{[\alpha_0]}(a, b)$$

and the last pair is

$$a_{k+1} = (W_{[\alpha_0, \ldots \alpha_k]}(a, b))^{-1} \text{ and } b_{k+1} = W_{[\alpha_0, \ldots \alpha_{k+1}]}(a, b).$$

Recall the definition of a continued fraction expansion for a rational number p/q. For $p/q > 0$ we have

$$\frac{p}{q} = \alpha_0 + \cfrac{1}{\alpha_1 + \frac{1}{\alpha_2 + \frac{1}{\alpha_3 + \cdots + \frac{1}{a_k}}}} = [\alpha_0; \alpha_1, \ldots, \alpha_k]$$

where the α_i are integers with $\alpha_j > 0$, $j = 1 \dots k-1$, $a_k > 1$ for $k > 1$ and $a_0 \geq 0$.

Note that the condition $a_k > 1$ avoids the ambiguity coming from

$$[\alpha_0; \alpha_1, \dots, \alpha_{k-1}, 1] = [\alpha_0; \alpha_1, \dots, \alpha_{k-1} + 1].$$

For $p/q < 0$ we let $-p/q = [\alpha_0; \alpha_1, \dots, \alpha_k]$ and set

$$\frac{-p}{q} = [-\alpha_0; -\alpha_1, \dots - \alpha_k].$$

This definition for negative numbers is not the standard definition of [**14**] but works better in many applications including the one here. It gives more symmetry to the picture.

To complete the picture, for $n \neq 0$, if $p/q = 0/n$, we assign it the continued fraction $[0]$ and if $p/q = n/0 = \infty$ we assign it the continued fraction $[\infty] = [\emptyset]$. We also define the *level* of the continued fraction: the level of $[0]$ and the level of $[\infty]$ is 0. Otherwise, the level of $[\alpha_0; \alpha_1, \dots, \alpha_k]$ is $\sum_{i=0}^{k} \alpha_i$.

The notation for our $\mathcal{F}$-sequences looks very much like the continued fraction notation.

We justify this by identifying the rational p/q with continued fraction $[\alpha_0, \dots, \alpha_k]$ with the $\mathcal{F}-$sequence $[\alpha_0, \dots, \alpha_k]$. In this way we associate the rational p/q to the $\mathcal{F}$-word $W_{[\alpha_0, \dots \alpha_t]}(a, b)$ and set $W_{p/q} = W_{[\alpha_0, \dots \alpha_t]}(a, b)$. We add the convention $W_{1/0} = a_0$ and $W_{0/1} = b_0$. Note that because we defined the $\mathcal{F}$ words in terms of b_t, we have distinguished between b_t and $a_{t+1} = b_t^{-1}$. We thus have $W_{p/q}^{-1} = a_{t+1}$. This is summarized by

Remark 2.1. *These $W_{p/q}$ are not necessarily the same as the $W_{p/q}$ used in the Keen-Series papers* [**16, 17**]*, but are a variant corresponding to the algorithmic words.*

We also define the *$\mathcal{F}$-sequence pair* to mean the ordered pair

$$(W^{-1}_{[\alpha_0, \dots, \alpha_{t-1}]}, W_{[\alpha_0, \dots, \alpha_{t-1}, \alpha_t]}).$$

We will prove:

Theorem 2.1. *Up to conjugacy, there is a one to one correspondence between a pair consisting of a primitive element and its inverse, $\{W, W^{-1}\}$, and the extended rational numbers $\mathbb{Q} \cup \{\infty\}$.*

Remark 2.2. *This whole discussion depends on the generators as an ordered pair. Interchanging the order or replacing either generator by its inverse results in a change in the words in the $\mathcal{F}$-sequence as well a change in their identification with rationals.*

3. Word forms and primitive exponents

A word $W(a, b)$ in $F = \langle a, b \rangle$ is an expression of the form

$$a^{\eta_1} b^{\mu_1} \cdots a^{\eta_k} b^{\mu_k}$$

where the exponents are all integers and all are non-zero except perhaps the first, η_1 and the last μ_k. If the group is free, the expression is unique.

Definition 3. *Given a word $W(a, b) = a^{\eta_1} b^{\mu_1} \cdots a^{\eta_k} b^{\mu_k}$, the sequences of integers $\{\eta_1, \dots, \eta_k\}$, $\{\mu_1, \dots, \mu_k\}$, are called the* primitive exponent sequences *and the numbers η_i, μ_i are primitive exponents.*

In [**8**] and in [**10**], using different inductive techniques, we showed that up to conjugacy, inverse and cyclic order the primitive exponent sequences for primitive elements have special forms.

The first theorem shows that the special forms depend on whether p/q is positive or negative and whether its absolute value is greater or less than one.

THEOREM 3.1. *Up to conjugacy, every primitive element in $F = \langle a, b\rangle$ has one of the following forms where all the integers η_i, μ_i are assumed strictly positive:*
For p/q = 1/0

$$W(a,b) = a, \;\; W(a,b)^{-1} = a^{-1}$$

For p/q = 0/1,

$$W(a,b) = b, \;\; W(a,b)^{-1} = b^{-1}$$

For p/q = 1/1,

$$W(a,b) = a^{-1}b, \;\; W(a,b)^{-1} = b^{-1}a$$

For p/q = -1/1,

$$W(a,b) = ab, \;\; W(a,b)^{-1} = b^{-1}a^{-1}$$

For $0 < p/q < 1$,

$$W(a,b) = a^{-1}b^{\mu_1}a^{-1}b^{\mu_2}\dots a^{-1}b^{\mu_p}$$
$$W(a,b)^{-1} = b^{-\mu_p}ab^{-\mu_{p-1}}\dots ab^{-\mu_1}a$$
$$\text{where } \sum_{i=1}^{p}\mu_i = q \text{ and } |\mu_{i+1} - \mu_i| \leq 1.$$

For $-1 < p/q < 0$, the sign of the exponent of a changes

$$W(a,b) = ab^{\mu_1}ab^{\mu_2}\dots ab^{\mu_p}$$
$$W(a,b)^{-1} = b^{-\mu_p}a^{-1}b^{-\mu_{p-1}}\dots a^{-1}b^{-\mu_1}a^{-1}$$
$$\text{where } \sum_{1=1}^{p}\mu_i = q \text{ and } |\mu_{i+1} - \mu_i| \leq 1.$$

For $1 < p/q < \infty$ the roles of a and b and of p and q are reversed

$$W(a,b) = a^{-\eta_1}ba^{-\eta_2}b\dots a^{-\eta_q}b$$
$$W(a,b)^{-1} = b^{-1}a^{\eta_q}b^{-1}\dots a^{\eta_2}b^{-1}a^{\eta_1}$$
$$\text{where } \sum_{1=1}^{q}\mu_i = p \text{ and } |\eta_{i+1} - \eta_i| \leq 1.$$

Finally for $-\infty < p/q < -1$

$$W(a,b) = a^{\eta_1}ba^{\eta_2}b\dots a^{\eta_q}b$$
$$W(a,b)^{-1} = b^{-1}a^{-\eta_q}b^{-1}\dots a^{-\eta_2}b^{-1}a^{-\eta_1}$$
$$\text{where } \sum_{1=1}^{q}\mu_i = p \text{ and } |\eta_{i+1} - \eta_i| \leq 1.$$

PROOF. The theorem is true for $G \subset PSL(2,\mathbb{R})$ and is proved in [**17**]. The proof for F is given in section 6 and 7. $\square$

Note that in every case the exponent of the generator b in the word $W(a,b)$ is positive; that is $\mu_i > 0$. This implies that we don't get both a word and its inverse in this enumeration of the words $W(a,b)$. Moreover, in every case one of the exponent sequences is trivial in that it consists either of all 1's or all -1's. The primitive exponents in the other non-trivial exponent sequence all have the same sign and are either $\pm\alpha_0$ or $\pm(\alpha_0+1)$ where α_0 is the first entry in the continued fraction of p/q. We also remark that the words $W(a,b)$ have the property that their word length is as small as possible.

In [**8**] we gave the specific relationship between the continued fraction for p/q and the non-trivial primitive exponents of the word $W(a,b)$, We stated the theorem only for $p/q > 1$ and $W_{p/q}$. Using the above it is straightforward to write down the rules for $W_{p/q}^{-1}$ and the other cases for p/q.

We note that we can also enumerate all primitive pairs (see section 4) and in that enumeration each primitive element and its inverse appear. We extend theorems from [**8, 17, 19**] from G to F. The proof that the result extends is given in sections 6 and section 7. The statement of the extended result is

THEOREM 3.2. *Let F be a rank two free group with generators a and b. Given $p/q > 1$ with continued fraction expansion $[\alpha_0, \ldots, \alpha_k]$, expand the $\mathcal{F}$-words b_t, $t = 0, \ldots, k+1$, of the corresponding $\mathcal{F}$-sequence $W_{p/q}$ to obtain the primitive exponent sequences $\{\eta_1(t), \eta_2(t), \ldots, \eta_{q_t}(t)\}$ for the words*

$$b_t = W_{p_t/q_t}(a,b) = a^{-\eta_1(t)} b a^{-\eta_2(t)} b \ldots a^{-\eta_{q_t}(t)} b.$$

Then the non-trivial primitive exponent sequence

$$\{\eta_1(k+1), \ldots, \eta_{q_t}(k+1)\}$$

of W_{p_t/q_t} is related to the $\mathcal{F}$-sequence as follows:

If $t = 0$, then $\eta_0 = 0$ and $\eta_1(0) = \alpha_0$.
If $t = 1$, then $q_1 = \alpha_1$, $\eta_0(1) = 1$ and $\eta_i(1) = a_0$, $i = 1, \ldots, q_1$.
If $t = 2$ then $q_2 = \alpha_2\alpha_1 + 1$, $\eta_0(2) = 0$ and for $i = 1, \ldots, q_2$, $\eta_i(2) = a_0 + 1$ if $i \equiv 1 \mod q_2$ and $\eta_i(t) = \alpha_0$ otherwise.

For $2 < t \leq k+1$,

- *$\eta_0(t) = 0$ if t is even and $\eta_0(t) = 1$ if t is odd.*
- *For $i = 1 \ldots q_{t-2}$, $\eta_i(t) = \eta_i(t-2)$.*
- *For $i = q_{t-2}+1 \ldots q_t$, $\eta_i(t) = \alpha_0+1$ if $i \equiv 1+q_{k-1} \mod q_k$ and $\eta_i(t) = \alpha_0$ otherwise.*

Moreover any word $W(a,b)$ whose exponent sequences, up to cyclic permutation, satisfy the above conditions is primitive and conjugate to some $W_{p/q}$.

DEFINITION 4. *A pair of elements that generates F is called a* primitive pair *(but not every arbitrary pair of primitive elements form a primitive pair).*

It is clear that if (W,V) is a primitive pair, so is the inverse pair (V^{-1}, W^{-1}). In addition, the pairs (W, V^{-1}), (W^{-1}, V), (W^{-1}, V^{-1}) and their inverse pairs are also primitive pairs. This leads us to define the following notion for words either in G or in F.

DEFINITION 5. *The* pair class $\{W,V\}$ *consists of the eight primitive pairs: $(W,V), (W,V^{-1})$, (W^{-1},V), (W^{-1},V^{-1}) and their inverse pairs.*

An ordered pair of words (j,k) in a group is conjugate as a *pair* to another ordered pair (s,t) if there is a single element of the group that conjugates j to s and k to t. The rational numbers associated to any conjugate primitive pairs are the same. Thus a pair class determines a pair of rational numbers.

In [**8, 12**] we proved

THEOREM 3.3. *A pair class of primitive elements $\{W(A,B),V(A,B)\}$ in G contains primitive pairs if and only if the corresponding rationals satisfy $p/q,r/s$ satisfy $|ps-qr|=1$.*

Therefore, combining this theorem with the proofs of sections 6 and 7 we have

THEOREM 3.4. *A pair class of primitive elements $\{W(a,b),V(a,b)\}$ in F contains primitive pairs if and only if the corresponding rationals $\{p/q,r/s\}$ satisfy $|ps-qr|=1$.*

The primitive elements (a_t,b_t) formed from an $\mathcal{F}$-sequence are primitive pairs. These are ordered pairs. Note that the level of the continued fraction of a_t is never greater than the level of the continued fraction of b_t. Note further that none of the pairs of the pair class (a_t,b_t) appears as $(a_{t'},b_{t'})$ for a different t' in the $\mathcal{F}$-sequence construction because the level of a_t is never greater than the level of b_t. Moreover, from the construction we never have $a_t=a_{t'}^{-1}$ or $b_t=a_{t'}^{-1}$.

Thus, after lifting to F as in sections 6 and 7 we have

THEOREM 3.5. *Given a representation $\rho: F\to G\subset PSL(2,\mathbb{R})$ such that $A=\rho(a),B=\rho(b)$ are hyperbolics with disjoint axes, there is a distinguished set of three primitive elements in F, c,d,cd^{-1} depending upon $\rho(F)=G$ such that any pair of the three is a primitive pair and such that any primitive element in F is conjugate to a unique word given by an $\mathcal{F}$ sequence.*

4. Two generator subgroups of $PSL(2,\mathbb{R})$

We now turn to two generator subgroups of $PSL(2,\mathbb{R})$ and the geometric orientation of their elements.

The group $PSL(2,\mathbb{R})$ consists of isometries in the hyperbolic metric on the upper half plane $\mathbb{H}$. It is conjugate in $PSL(2,\mathbb{C})$ to the group of isometries of the unit disk $\mathbb{D}$ with its hyperbolic metric. By abuse of notation, we identify these groups and use whichever model is easier at the time. All of the results below are independent of the model we use. An isometry is called *hyperbolic* if it has two fixed points on the boundary of the half-plane or the disk. It leaves the hyperbolic geodesic joining them invariant; this geodesic is called the *axis* of the element. One of the fixed points is attracting and the other is repelling. This gives a natural orientation to the axis since points are moved along the axis toward the attracting fixed point. This natural orientation does not exist in the free group.

There is an analytic condition that determines whether or not the axes intersect. Note that however $A=\rho(A),B=\rho(B)$ are lifted to $\tilde{A},\tilde{B}\in SL(2,\mathbb{R})$, the sign of the trace of the multiplicative commutator $\mathrm{tr}[\tilde{A},\tilde{B}]$ is the same; we therefore write it as $\mathrm{tr}[A,B]$. The axes of A and B are disjoint if and only if $\mathrm{tr}[A,B]>2$.

We now will use the orientation of the axis of an element of $PSL(2,\mathbb{R})$ to define the notion of a coherently oriented pair of elements or axes of a subgroup $G=\langle A,B\rangle$. In section 6 we will lift this concept to the free group.

4.1. Coherently Oriented Generators.

Definition 6. *Let A and B be any pair of hyperbolic generators of the group G acting as isometries on the unit disk or the upper half-plane. Assume that they are given by representatives $\tilde{A}, \tilde{B} \in SL(2,\mathbb{R})$ with $tr\tilde{A} \geq tr\tilde{B} > 2$. Suppose the axes of A and B are disjoint. Let L be the common perpendicular geodesic to these axes oriented from the axis of A to the axis of B. We may assume that the attracting fixed point of A is to the left of L, replacing A by A^{-1} if necessary. We say A and B are* **coherently oriented** *if the attracting fixed point of B is also to the left of L and* **incoherently oriented** *otherwise.*

If (A, B) are coherently oriented, then (A, B^{-1}) and (B, A) are both incoherently oriented.

If $G = \langle A, B \rangle$ is discrete and free, and if the axes of A and B are disjoint, the quotient Riemann surface $\mathbb{D}/G$ is a sphere with three holes; that is, a pair of pants. The axes of all hyperbolic group elements project to closed geodesics on S. The length of the geodesic on S is determined by the trace of the element. This is another property that is lost when we lift to the free group, F.

4.2. Stopping generators . If G is an arbitrary two-generator non-elementary subgroup of $PSL(2,\mathbb{R})$ with disjoint axes, the Gilman-Maskit algorithm [**13**] goes through finitely many steps and at the last, or $k+1^{th}$ step, it determines whether or not the group is discrete and stops. We are concerned here with the case where it stops and the output is that the group is discrete and free. At each step, $t = 0, \ldots, k$, the algorithm determines an integer α_t and a new pair of generators (A_{t+1}, B_{t+1}); these integers form an $\mathcal{F}-$sequence and the pairs, (A_t, B_t), of *algorithmic words* are the $\mathcal{F}-$ words defined above in section 2. The final pair of generators $(C, D) = (A_{k+1}, B_{k+1})$ are called the *stopping generators*. It is shown in [**8**] that if the axes of the original generators are disjoint, the stopping generators have the geometric property that their axes, together with the axis of $A_{k+1}^{-1}B_{k+1}$, project to the three shortest closed geodesics on the quotient Riemann surface which is a three holed sphere. The projected geodesics are disjoint and the only simple closed curves on the quotient. [**8**].

Lemma 4.1. *If the pair (A, B) is coherently oriented, then either the pair (C, D) is coherently oriented or one of the pairs (D, C^{-1}) or (C, D^{-1}) is.*

Proof. We assume without loss of generality that the pair (A, B) is coherently oriented because if it is not, one of the pairs (A, B^{-1}) or (B, A^{-1}) or $B^{-1}, A^{-1})$ is coherently oriented and we can replace it with that one. We can analyze the steps in the algorithm and the orientations of the intermediate generators carefully and see that, if we start with a coherently oriented pair, at each step, up to the next to last, $t = k$, the pair we arrive at, (B_{t-1}^{-1}, B_t), is coherently oriented. We therefore need to check whether the last pair,

$$(C, D) = (A_{k+1}, B_{k+1}) = (B_k^{-1}, B_{k+1})$$

is coherently oriented.

The stopping condition is that the last word B_{k+1} have negative trace. We know $trB_{k-1} > trB_k$; we don't know the relation of $|trB_{k+1}|$ to these traces. We will have either

$$|trB_{k+1}| > trB_{k-1} > trB_k \text{ or}$$

$$trB_{k-1} > |trB_{k+1}| > trB_k \text{ or}$$
$$trB_{k-1} > trB_k > |trB_{k+1}|.$$

In the first case (B_{k-1}^{-1}, B_k) is coherently oriented. In the second case (B_k^{-1}, B_{k+1}) is incoherently oriented but $(D, C^{-1}) = (B_{k+1}^{-1}, B_k)$ is coherently oriented. In the third case, again (B_k^{-1}, B_{k+1}) is incoherently oriented but this time $(C, D^{-1}) = (B_k^{-1}, B_{k+1}^{-1})$ is coherently oriented. □

We note, but do not use the fact that if (C_0, D_0) denotes the ordered "shortest" pair of stopping generators with whatever orientation comes out, then at the last step the coherently ordered stopping generators are either (C^{-1}, D) or (D^{-1}, C) where $C = C_0$ and $D = D_0$. This comes from following the notation carefully to see that the *last pair*, the first case in the proof of the above lemma, actually has the stopping generators with k replacing $k+1$.

4.3. Winding and Unwinding. In [**8**] we studied the relationship between a given pair of generators for a free discrete two generator subgroup of $PSL(2,\mathbb{R})$ with disjoint axes and the stopping generators produced by the Gilman-Maskit algorithm. We found we could interpret the algorithm as an unwinding process, a process that at each step reduces the number of self-intersections of the corresponding curves on the quotient surface. In effect, it *unwinds* the way in which stopping generators have been *wound around* one another to obtain the original primitive pair.

Here is an example where we denote the original given pair of generators by (A, B) and the stopping generators by (C, D).

Example 1. *We begin with the (unwinding) $\mathcal{F}-$sequence $[3, 2, 4]$ and obtain the words*

$$(A_0, B_0) = (A, B)$$
$$(A_1, B_1) = (B^{-1}, A^{-1}B^3)$$
$$(A_2, B_2) = (B^{-3}A, BA^{-1}B^3A^{-1}B^3)$$

and

$$(A_3, B_3) = (B^{-3}AB^{-3}AB^{-1}, A^{-1}B^3 \cdot (BA^{-1}B^3A^{-1}B^3)^4) = (C, D).$$

Going backwards

$$(C_0, D_0) = (C, D)$$
$$(C_1, D_1) = (C_0^{-4}D_0^{-1}, C_0^{-1}) = (B^{-3}A, BA^{-1}B^3A^{-1}B^3)$$
$$(C_2, D_2) = (C_1^{-2}D_1^{-1}, C_1^{-1}) =$$
$$((B^{-3}A)^{-2} \cdot (BA^{-1}B^3A^{-1}B^3)^{-1}, A^{-1}B^3) = (B^{-1}, A^{-1}B^3)$$
$$(C_3, D_3) = (C_2^{-3}D_2^{-1}, C_2^{-1}) = (B^3B^{-3}A, B) = (A, B)$$

We can think of this as the (winding) sequence given by $[-4, -2, -3]$ and write

$$A = W_{[-4,-2,-3]}(C, D) \text{ and } B = W_{[-4,-2]}^{-1}(C, D).$$

Definition 7. *Let q be a positive integer. A* winding step *labeled by the integer $-q$ will send the pair (U, V) to the pair $(U^{-q}V^{-1}, U^{-1})$ and an* unwinding step *labeled by the integer q the will send the pair (M, N) to the pair $(N^{-1}, M^{-1}N^q)$.*

THEOREM 4.2. [**8**] *If $G = \langle A, B\rangle$ is a non-elementary, discrete, free subgroup of $PSL(2,\mathbb{R})$ where A and B are hyperbolic isometries with disjoint axes, then there exists an* unwinding *$\mathcal{F}$-sequence $[\alpha_0, ..., \alpha_k]$ such that the stopping generators (C, D) are obtained from the pair (A, B) by applying this $\mathcal{F}$-sequence. There is also a* winding *$\mathcal{F}$-sequence $[\beta_0, ..., \beta_k]$ such that the pair (A, B) is the final pair in the set of $\mathcal{F}$-words obtained by applying the winding $\mathcal{F}$-sequence to the pair (C, D).*

The sequences are related by $[\beta_0, ..., \beta_k] = [-\alpha_k, ..., -\alpha_0]$

The theorem suggests the following definitions.

DEFINITION 8. *(1) We call the $\mathcal{F}$-sequence $[\alpha_0, \alpha_1, \ldots, \alpha_k]$, determined by the discreteness algorithm that finds the stopping generators when the group is discrete, the* **unwinding** *$\mathcal{F}$-sequence.*

(2)We call the $\mathcal{F}$-sequence $[\beta_0, \beta_1, \ldots, \beta_k]$, that determines the original generators (A, B) from the stopping generators (C, D), the **winding** *$\mathcal{F}-$sequence.*

This justifies our modifying the classical definition of continued fractions for negative numbers. Note that the ambiguity in the definition of stopping generators corresponds exactly to the ambiguity in the definition of a continued fraction.

5. Primitive exponents

If X and Y are both primitive elements and together they generate the group they are termed a *primitive pair* or a pair of *primitive associates* and each is termed a *primitive associate* of the other. A given primitive word, of course, has many primitive associates.

It follows from Theorem 4.2 that up to conjugacy the stopping generators are independent of the given set of generators. This immediately implies

THEOREM 5.1. *Every primitive word in the group G is the last word in a winding $\mathcal{F}$-sequence and in particular, the forms of theorem 3.1 are correct.*

PROOF. If P is any primitive word in G, it has many primitive associates. Let Q be any one of these. After replacing (P, Q) by the coherently oriented pair if necessary, unwind according to the algorithm to find the stopping generators, (C, D). This unwinding determines an $\mathcal{F}$-sequence $[\alpha_0, \ldots, \alpha_k]$ which corresponds to a rational p/q. As in example 1, the unwinding sequence, in turn, determines another $\mathcal{F}$-sequence, the winding sequence $[\beta_0, \ldots, \beta_k]$. The $\mathcal{F}$-words formed from the winding sequence can be expanded into the form

$$C^{n_1}D^{m_1} \ldots C^{n_k}D^{m_k},\ n_i, m_i \in \mathbb{Z}, i = 1, \ldots, k.$$

It is easy to see that, starting with coherently oriented generators (C, D), and an $\mathcal{F}$-sequence with non-negative entries, the exponents of C and D in the $\mathcal{F}$-words always have opposite signs. If $\alpha_0 > 0$, and $p/q \geq 1$, we see that $D_1 = C^{-1}D^{\alpha_0}$ and, as we go through the $\mathcal{F}$-words, the exponent of C will always have absolute value 1. This agrees with the form of words for $p/q > 1$ in theorem 3.1. If, on the other hand, $\alpha_0 = 0$, and $0 < p/q < 1$, we see that $(C_1, D_1) = (D^{-1}, C^{-1})$ and the roles of C and D^{-1} and D and C^{-1} are interchanged, which again agrees with the corresponding form of theorem 3.1.

If we begin with an $\mathcal{F}$-sequence with non-positive entries, the negative entries always cause the exponents of C and D in the $\mathcal{F}$-words to have the same sign. Again, if $\alpha_0 < 0$, we see that $D_1 = C^{-1}D^{\alpha_0}$ and as we go through the $\mathcal{F}$-words, the exponent of C will always have absolute value 1. Similarly, if $\alpha_0 = 0$ the exponent of D will always have absolute value 1. Thus, here we also get agreement with the corresponding forms of theorem 3.1.

In either case, as we step from $t-1$ to t, we have $D_t = C_{t-1}^{-1}$ so that the signs of all the exponents change.

□

The non-trivial *primitive exponents* of the word $W(C,D)$ have the property that two adjacent primitive exponents differ by at most 1. This follows from looking closely at the $\mathcal{F}$-words. There are formulas for writing the primitive exponents in terms of the entries in the $(\mathcal{F})-$sequence that are derived in [**8**] and [**10**]. Using theorem 3.1 and replacing G by F in theorem 3.2, we obtain the corresponding formulas for F.

The identification of continued fractions for rationals to $\mathcal{F}$-sequences, together with Remark 2.2, immediately imply

Corollary 5.2. *There is a one-to-one map, τ from pairs of rationals $(p/q, r/s)$, with $|ps - rq| = 1$ to conjugacy classes of coherently oriented primitive pairs defined by $\tau : (p/q, r/s) \mapsto (A,B)$ where p/q is the rational with continued fraction expansion $[\alpha_0; \alpha_1, \ldots, \alpha_k]$ and r/s is the rational with continued fraction expansion $[\alpha_0, \alpha_1, \ldots, \alpha_{k-1}]$.*

Corollary 5.3. *Up to replacing a primitive word in G by its inverse, there is a one-to-one map from the set of conjugacy classes of primitive elements to the set of all rationals.*

In section 6 these will translate to corollaries 5.4 and 5.5 holding in the free group F. Namely,

Corollary 5.4. *There is a one-to-one map, τ from pairs of rationals $(p/q, r/s)$, with $|ps - rq| = 1$ to conjugacy classes of primitive pairs in F defined by τ : $(p/q, r/s) \mapsto (c,d)$ where p/q is the rational with continued fraction expansion $[\alpha_0; \alpha_1, \ldots, \alpha_k]$ and r/s is the rational with the continued fraction expansion $[\alpha_0, \alpha_1, \ldots, \alpha_{k-1}]$.*

Corollary 5.5. *Up to replacing a primitive word in F by its inverse, there is a one-to-one map from the set of conjugacy classes of primitive elements of F to the set of all rationals.*

6. Lifting to the free group

We can now achieve our goal which is to extend these results from a two-generator non-elementary discrete free subgroup G of $PSL(2,\mathbb{R})$ with disjoint axes to the free group, F on two generators. To do this first we take a faithful representation ρ of $F = \langle a,b \rangle$ into $PSL(2,\mathbb{R})$ such that $\rho(a) = A, \rho(b) = B$ and let (C,D) be a pair of coherently oriented stopping generators for the group $G = \langle A,B \rangle$. After that we take a second faithful representation ρ' of $F = \langle a,b \rangle$ into $PSL(2,\mathbb{R})$ with $\rho'(F) = G$ such that $\rho'(a) = C, \rho'(b) = D$ where (C,D) is the pair of coherently oriented stopping generators for the group G given by the first representation ρ.

We have

Theorem 6.1. *Given a free group $F = \langle a, b\rangle$ and a discrete faithful representation ρ of F into $PSL(2,\mathbb{R})$ such that $\rho(a) = A, \rho(b) = B$ where the axes of the images of a and b are disjoint, there is a distinguished pair of primitive associates c and d in F determined by the representation ρ such that, up to conjugacy, every pair of primitive associates in F can be written in the form $(W(c, d), V(c, d))$ where*

$$W(c, d) = W_{[\alpha_0,\dots,\alpha_k]}(c, d) \text{ and } V(c, d) = W^{-1}_{[\alpha_0,\dots,\alpha_{k-1}]}(a, b)$$

and is thus associated to a pair of rationals $(p/q, r/s)$ with $|ps - qr| = 1$.

Proof. Given the discrete faithful representation ρ of F into $PSL(2,\mathbb{R})$, let (C, D) be the stopping generators. Then A and B can be written as winding $\mathcal{F}$ words in C and D. Let $c = \rho^{-1}(C)$ and $d = \rho^{-1}(D)$. Further assume that $x \in F$ is any primitive element. Let y be any one of the many primitive associates of x and let $\rho(x) = X$ and $\rho(y) = Y$. Unwind the pair (X, Y) to obtain (up to conjugacy) the stopping generators C and D and then wind to obtain the $\mathcal{F}-$sequence for (X, Y) and (x, y). Note that we are speaking of a conjugacy that simultaneously conjugates both elements of one ordered pair to the elements of the other ordered pair. □

Theorem 6.2. *Every pair of primitive associates in $F = \langle a, b\rangle$, the free group on two generators, can be written in the form $(W(a, b), V(a, b))$ where*

$$W(a, b) = W_{[\alpha_0,\dots,\alpha_k]}(a, b) \text{ and } V(a, b) = W^{-1}_{[\alpha_0,\dots,\alpha_{k-1}]}(a, b)$$

and is thus associated to a pair of rationals $p/q, r/s$ with $|ps - qr| = 1$.

Proof. Given any faithful representation ρ of F into $PSL(2,\mathbb{R})$, let (C, D) be the stopping generators. Replace ρ by ρ' where $\rho'(a) = C$ and $\rho'(B) = D$ so that $a = \rho'^{-1}(C)$ and $b = \rho'^{-1}(D)$.

□

Note that for a given group F and elements c,d,a and b, the $\mathcal{F}$-sequences, the rationals and the primitive exponents in theorems 6.1 and 6.2 will be different for any given primitive word or primitive pair.

Combining these theorems yields proofs of corollary 5.4 and corollary 5.5.

7. The Geometries of Different Representations

In this section we turn our attention to representations ρ of $F = \langle a, b\rangle$ into $PSL(2,\mathbb{R})$ where $G = \rho(F)$ is discrete but either the generators are parabolic or their axes intersect.

If a generator is parabolic, it has only one fixed point and no invariant geodesic. We define its *axis* to be its fixed point. If one or both of the generators are parabolic and their axes are disjoint, all of the discussion above holds. The quotient $\mathbb{D}/G$ is still topologically a three holed sphere but the holes may have become punctures. The *projection of the axis* is the puncture.

Recall that the algebraic condition that determines whether or not the axes intersect depends on $\mathrm{tr}[A, B]$. The axes of A and B intersect if and only if $\mathrm{tr}[A, B] < 2$.

If $\mathrm{tr}[A, B] \leq -2$, G is free and discrete so no algorithm is needed to determine uniqueness. The quotient $\mathbb{D}/G$ is a torus with a hole or puncture. When the trace is between -2 and 2, the commutator is elliptic and the group is not free, but it may be discrete.

As noted in [**9**] (see section 8 of that paper), in the case $tr[A,B] < -2$, that is, even when one already knows G is discrete, one can follow the methods of [**7**] used to determine the discreteness, to find an *algorithmic* sequence of generators and an ordered set of *coherently oriented stopping generators* C and D which have the property that the axis of D projects to the unique shortest simple curve on the surface and the axis of C projects to the unique shortest simple curve that intersects C only once (assuming that C, D and CD^{-1} have different traces). Note that in this case, neither of the generators can be parabolic, because if one is, the generators share a fixed point and the group is not discrete.

One can then extend the proofs of theorems 3.1, 3.2, 3.5, 5.1, 6.1, 6.2, and corollaries 5.4 and 5.5 to this case. We have now proved the results in their most general form as they are stated in the introduction as theorems 1.1, 1.2, 1.3 and 1.4. We note that some, but not all, of the results are well known and have been proved using other techniques. The techniques here give new proofs of such results.

References

1. Bardakov, Sprilrain and Tolytykh, *On the palindromic and primitive widths in a free group*, J. Algebra 285 (2005) 574-585.
2. Buser, P.; Semmler, K.-D. *The geometry and spectrum of the one-holed torus.* Comment. Math. Helv. 63 (1988), no. 2, 259-274.
3. Cohen, P; Metzler, W; Zimmermann, B. *What does a basis of $F(a, b)$ look like?*, Math. Ann. 257 (4) (1981) 435-445.
4. Gilman, Jane, *Informative Words and Discreteness*, Contemp. Math **421**, (2007) 147-155. Cont Math.
5. Gilman, Jane, *Algorithms, Complexity and Discreteness Criteria in $PSL(2,\mathbb{C})$*, Journal D'Analyse Mathematique, Vol 73, (1997), 91-114.
6. Gilman, Jane *Complexity of a Turing Machine Algorithm*, Contemporary Math, volume 256, 165-171, 2000.
7. Gilman, Jane *Two-generator Discrete Subgroups of $PSL(2,\mathbb{R})$*, Memoirs of the AMS, Volume 117, No 561, 1995.
8. Gilman, Jane and Keen, Linda, *Word sequences and intersection numbers.* Complex manifolds and hyperbolic geometry (Guanajuato, 2001), 231-249, Contemp. Math., 311, Amer. Math. Soc., Providence, RI, 2002
9. Gilman, Jane and Keen, Linda, *The Geometry of Two-Generator Groups: Hyperelliptic Handlebodies* Geometriae Dedicata, 110 (2005), 159-190.
10. Gilman, Jane and Keen, Linda, *Cutting Sequences and Palindromes,Geometry of Riemann Surfaces* Series: London Mathematical Society Lecture Note Series (No. 368), 194-216 arXiv:0803.0234
11. Gilman, Jane and Keen, Linda, *Discreteness Criteria and the Hyperbolic Geometry of Palindromes*, Conformal Geometry and Dynamics, 13 (2009), 76-90 arXiv:0808.3488,
12. Gilman, Jane and Keen, Linda *Enumerating Palindromes and Primitives in Rank Two Free Groups*, Journal of Algebra, (2011), 1-13.
13. Gilman, J. and Maskit, B. *An algorithm for 2-generator Fuchsian groups* Michigan Math. J. **38** (1991) 13-32.
14. Hardy, G.H. and Wright, E. M., *An introduction to the theory of numbers* Oxford, Clarendon Press 1938.
15. Jiang, Yicheng, *Polynomial complexity of the Gilman-Maskit discreteness algorithm* Ann. Acad. Sci. Fenn. Math. 26 (2001), no. 2, 375-390.
16. Keen, Linda and Series, Caroline, Pleating Coordinates for Teichmüller Space, *Bull. AMS*,vol. 26, 1, 1992, 141-146
17. Keen, Linda and Series, Caroline, *Pleating Coordinates for the Maskit Embedding of Teichmüller space for a punctured torus*, Topology, Vol. **32** #4, (1993), 719-749.
18. Kassel, Christian; Reutenauer, Christophe *Sturmian morphisms, the braid group B_4, Christoffel words and bases of F_2.* Ann. Mat. Pura Appl. (4) 186 (2007), no. 2, 317-339.

19. Malik, Vidur, *Curves Generated on Surfaces by the Gilman-Maskit Algorithm*, Ph D thesis, Rutgers University, Newark, NJ (2007).
20. Malik, Vidur AMS Cont Math,
21. Magnus, Wilhelm; Karrass, Abraham; Solitar, Donald *Combinatorial group theory: Presentations of groups in terms of generators and relations* Interscience Publishers [John Wiley & Sons, Inc.], New York-London-Sydney (1966).
22. Osborne, R. P.; Zieschang, H. *Primitives in the free group on two generators* Invent. Math. 63 (1981), no. 1, 17-24.
23. Piggott, Adam, *Palindromic primitives and palindromic bases in the free group of rank two* J. Algebra 304 (2006), no. 1, 359-366.
24. Series, Caroline, *Non-euclidean geometry, continued fractions and ergodic theorey,* Math. Intelligencer #4,(1982), 24-31.
25. Series, Caroline *The modular surface and continued fractions*. J. London Math. Soc. 2, **31** (1985), 69-8.
26. Series, Caroline *The Geometry of Markoff Numbers*, Math. Intelligencer **7** #3,(1985), 20-29.
27. Vinogradov, I.M. *An Introduction to the Theory of Numbers*, (Enlgish translation by H. Popova) Pergamon Press, London-NY, (1955). MR # 0070644.
28. Wright, David J., *Searching for the cusp*, Spaces of Kleinian Groups, LMS Lecture Notes **329**, Cambridge U. Press (2004), 1-36.

Department of Mathematics, Rutgers University, Newark, NJ 07079
E-mail address: `gilman@rutgers.edu`

Department of Mathematics, CUNY, Lehman College and Graduate Center, Bronx, 10468
E-mail address: `linda.keen@lehman.cuny.edu`