1

Cutting Sequences and Palindromes

Jane Gilman and Linda Keen

Rutgers University, Newark, NJ and Lehman College and Graduate Center, CUNY

This paper is dedicated to Bill Harvey on the occasion of his 65th birthday.

1.1 Introduction

In this paper we discuss several more or less well-known theorems about primitive and palindromic words in two generator free groups. We describe a geometric technique that ties all of these theorems together and gives new proofs of all but the last of them, which is an enumerative scheme for palindromic words. This geometric approach and the enumerative scheme will be useful in applications. These applications will be studied elsewhere [GKgeom].

The main object here is a two generator free group which we denote by $G = \langle A, B \rangle$.

Definition 1 *A word* $W = W(A,B) \in G$ *is* primitive *if there is another word* $V = V(A,B) \in G$ *such that* W *and* V *generate* G. V *is called a* primitive associate *of* W *and the unordered pair* W *and* V *is called a* pair of primitive associates*.*

We remark that if W, V is a pair of primitive associates then both WV and WV^{-1} are primitive and $W, WV^{\pm 1}$ and $V, WV^{\pm 1}$ are both primitive pairs.

Definition 2 *A word* $W = W(A,B) \in G$ *is a* palindrome *if it reads the same forward and backward.*

In [GKwords] we found connections between a number of different forms of primitive words and pairs of primitive associates in a two generator free group. These were obtained using both algebra and geometry. The theorems that we discuss, Theorems 1.2.1, 1.2.2 and 1.2.3, can be found in [GKwords] and Theorem 1.2.4 can be found in [Piggott].

Theorem 1.2.5, the enumeration scheme, along with another proof of Theorem 1.2.4 can be found in [GKenum].

There are several different geometric objects that can be associated to two generator free groups; among them are the punctured torus, the three holed sphere and the genus two handlebody. Here we focus on the punctured torus and use "cutting sequences" for simple curves to obtain proofs of Theorems 1.2.1, 1.2.2 and 1.2.4.

A similar treatment can be made using the three holed sphere. Looking at the technique developed in Vidur Malik's thesis [Malik] for the three holed sphere representation of two generator groups we first noticed that the palindromes and products of palindromes were inherent in the geometry. The concept of a geometric center of a primitive word was inherent in his work. We thank him for his insight.

1.2 Notation and Definitions

In this section we establish the notation and give the definitions needed to state five theorems and we state them. Note that our statements of these theorems gather together results from several places into one theorem. Thus, for example, a portion of the statements in Theorem 1.2.3 appears in [KS] while another portion appears in [GKwords].

We assume that the reader is familiar with standard group theory terminology as found in Magnus-Karass-Solitar [MKS], but we review some terms here. We give fuller details of well known terms related to continued fraction expansions and Farey sequences as we work intensely with these.

A word $W = W(A,B) \in G$ is an expression $A^{n_1}B^{m_1}A^{n_2}\cdots B^{n_r}$ for some set of $2r$ integers $n_1, ..., n_r, m_1, ..., n_r$.

A word $X_1X_2X_3\cdots X_{n-1}X_n$ in G is *freely reduced* if each X_i is a generator of G and $X_i \neq X_{i+1}^{-1}$. It is *cyclically reduced* if it is freely reduced and $X_1 \neq X_n^{-1}$. We note that given a cyclically reduced word $X_1X_2X_3\cdots X_{n-1}X_n$, a *cyclic permutation* of the word is a word of the form $X_rX_{r+1}\cdots X_nX_1X_2X_3\cdots X_{r-1}$ where $1 \leq r \leq n$. A cyclic permutation of such a word is also cyclically reduced and is conjugate to the initial word.

Our ultimate aim is to characterize the exponents that occur in $W = W(A,B)$ when W is primitive. These will be called *primitive exponents*. Before we do that we associate to each rational $p/q \in \mathbb{Q}$, where p and q are relatively prime integers, a set of words which we denoted by $\{W_{p/q}\}$ as follows:

Definition 3 *If $p/q \geq 1$ set*

$$\{W_{p/q}\} = \{B^{n_0}AB^{n_1}AB^{n_2}\dots AB^{n_q}\} \tag{1.1}$$

where $n_0 \geq 0$, $n_i > 0, i = 1, \dots q$ and $p = \sum_{i=1}^{q} n_i$.

If $p/q \leq -1$, then replace A by A^{-1} in (1.1) and if $|p/q| < 1$, interchange both A and B and p and q in (1.1) so that after the interchanges $q = \sum_{i=1}^{p} n_i$.

Note that because the exponents of A and the exponents of B always have the same sign, each word in $\{W_{p/q}\}$ must be cyclically reduced and thus, there are no shorter words in its conjugacy class. Also note that in the union of the sets $\{W_{p/q}\}$ over all p/q, we never have both a word and its inverse.

After we recall some elementary number theory in the next section, we will be able to state Theorem 1.2.3 which gives necessary and sufficient conditions on the exponents n_i so that a particular word $W_{p/q} \in \{W_{p/q}\}$ is primitive.

Using the notation [ ] for the greatest integer function, one immediate corollary of Theorem 1.2.3 is

Corollary 1.2.1 *If $W_{p/q} \in \{W_{p/q}\}$ is primitive, then the primitive exponents satisfy $n_j = [|p/q|]$ or $n_j = [|p/q|] + 1$, $0 < j \leq p$.*

Another immediate corollary of Theorem 1.2.3 is

Corollary 1.2.2 *The primitive word $W_{p/q} \in \{W_{p/q}\}$ is unique up to cyclic permutation and inverse.*

In what follows, we will pick unique representatives for elements in the set $\{W_{p/q}\}$ using iteration. These will be termed the W-iteration, the V-iteration and the E-iteration schemes. The W iteration scheme is patterned on Farey sequences. We will show:

We can characterize pairs of primitive associates as follows:

Corollary 1.2.3 *Two primitive words $W_{p/q}$ and $W_{r/s}$ that occur in the W-iteration scheme are a pair of primitive associates if and only if $|ps - qr| = 1$.*

We will see that this corollary also holds for the V- and E-iteration schemes.

1.2.1 Farey arithmetic

In the rest of this section we work only with rationals $r/s \in [0,\infty]$ where we assume $r,s \geq 0$, but not simultaneously 0, and that they are relatively prime, which we denote by $(r,s) = 1$. We use the notation $1/0$ to denote the point at infinity. We use $\mathbb{Q}^+$ to denote these rational numbers and we think of them as points on the real axis in the extended complex plane.

To state the second theorem, we need the concept of Farey addition for fractions in $\mathbb{Q}^+$.

Definition 4 *If $\frac{p}{q}, \frac{r}{s} \in \mathbb{Q}^+$, the* Farey sum *is*

$$\frac{p}{q} \oplus \frac{r}{s} = \frac{p+r}{q+s}$$

Two fractions are called Farey neighbors *or simply neighbors if* $|ps-qr = 1|$*; the corresponding words are also called* neighbors.

Note that the Farey neighbors of $1/0$ are the rationals $n/1$. If $\frac{p}{q} < \frac{r}{s}$ then it is a simple computation to see that

$$\frac{p}{q} < \frac{p}{q} \oplus \frac{r}{s} < \frac{r}{s}$$

and that both pairs of fractions

$$(\frac{p}{q}, \frac{p}{q} \oplus \frac{r}{s}) \text{ and } (\frac{p}{q} \oplus \frac{r}{s}, \frac{r}{s})$$

are neighbors if $(p/q, r/s)$ are.

We can create the diagram for the Farey tree by marking each fraction by a point on the real line and joining each pair of neighbors by a semi-circle orthogonal to the real line in the upper half plane. The points $n/1$ are joined to their neighbor $1/0$ by vertical lines. The important thing to note here is that because of the properties above none of the semi-circles or lines intersect in the upper half plane. To simplify the exposition when we talk about a point or a vertex we also mean the word corresponding to that rational number. Each pair of neighbors together with their Farey sum form the vertices of a curvilinear or hyperbolic triangle and the interiors of two such triangles are disjoint. Together the set of these triangles forms a tessellation of the hyperbolic plane which is known as the Farey tree.

Fix any point ζ on the positive imaginary axis. Given a fraction, $\frac{p}{q}$, there is a hyperbolic geodesic γ from ζ to $\frac{p}{q}$ that intersects a minimal number of these triangles.

Definition 5 *The* Farey level *or the* level *of p/q, $Lev(p/q)$, is the number of triangles traversed by γ*

Note that the curve (line) γ joining ζ to either $0/1$ or $1/0$ does not cross any triangle so these rationals have level 0. The geodesic joining ζ to $1/1$ intersects only the triangle with vertices $1/0, 0/1$ and $1/1$ so the level of $1/1$ is 1. Similarly the level of $n/1$ is n.

We emphasize that we now have two different and independent orderings on the rational numbers: the ordering as rational numbers and the ordering by level. That is, given $\frac{p}{q}$ and $\frac{r}{s}$, we might, for example, have as rational numbers $\frac{p}{q} \leq \frac{r}{s}$, but $Lev(\frac{r}{s}) \leq Lev(\frac{p}{q})$. If we say one rational is larger or smaller than the other, we are referring to the standard order on the rationals. If we say one rational is higher or lower than the other, we are referring to the *levels* of the fractions.

Definition 6 *We determine a* Farey sequence for $\frac{p}{q}$ *inductively by choosing the new vertex of the next triangle in the sequence of triangles traversed by γ.*

The Farey sequence for $\frac{8}{5}$ is shown in Figure 1.1.

Given p/q, we can find the smallest and largest rationals m/n and r/s that are its neighbors. These also have the property that they are the only neighbors with lower level. That is, as rational numbers $m/n < p/q < r/s$ and the levels satisfy $Lev(m/n) < Lev(p/q)$ and $Lev(r/s) < Lev(p/q)$, and if u/v is any other neighbor $Lev(u/v) > Lev(p/q)$. Thinking of the Farey diagram as a tree whose nodes are the triangles of the diagram leads us to define

Definition 7 *The smallest and the largest neighbors of the rational p/q are the* parents *of p/q.*

Note that we can tell which parent r/s is smaller (respectively larger) than p/q by the sign of $rq - ps$.

Farey sequences are related to continued fraction expansions of fractions (see for example, [HardyWright]). In particular, write

$$\frac{p}{q} = a_0 + \cfrac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \ldots + \frac{1}{a_k}}}} = [a_0, \ldots, a_k]$$

where $a_j > 0$, $j = 1 \ldots k$.

The level of p/q can be expressed in terms of the continued fraction

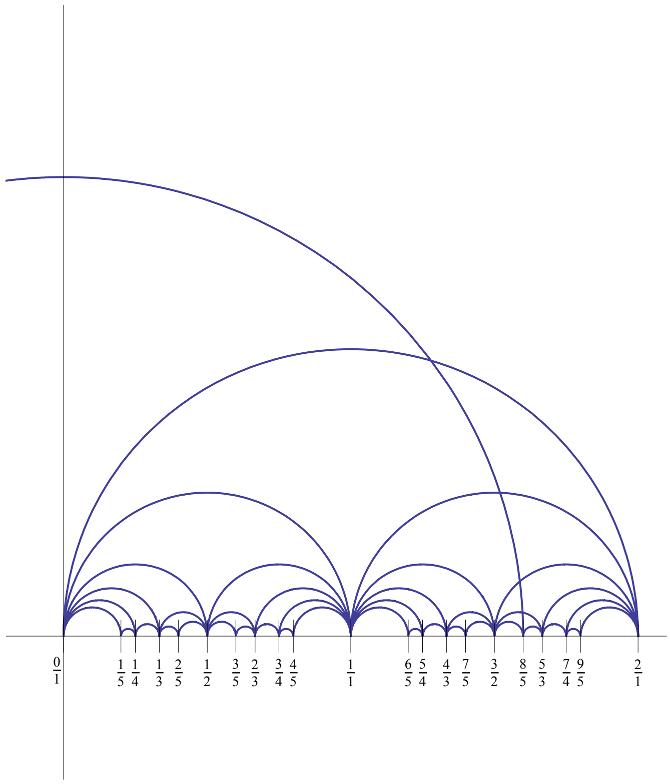

Fig. 1.1. Farey sequence for 8/5

expansion by the formula

$$Lev(p/q) = \sum_{j=0}^{k} a_j.$$

The parents of p/q have continued fractions

$$[a_0, \ldots, a_{k-1}] \text{ and } [a_0, \ldots, a_{k-1}, a_k - 1].$$

1.2.2 Farey words, continued fraction expansions and algorithmic words

In this section we relate primitive words with their associated rationals p/q to Farey sequences. We tacitly assume $p/ \in \mathbb{Q}^+$; for negative p/q we use the transformation rules in Definition 3.

The next theorem gives a recursive enumeration scheme for primitive words using Farey sequences of rationals. This is the W iteration scheme.

Theorem 1.2.1 (The W-iteration scheme) ([GKwords, KS]) *The primitive words in $G = \langle A, B \rangle$ can be enumerated inductively by using Farey sequences as follows: set*

$$W_{0/1} = A, \quad W_{1/0} = B.$$

Given p/q, consider its Farey sequence. Let $\frac{m}{n}$ and $\frac{r}{s}$ be its parents labeled so that

$$\frac{m}{n} < \frac{p}{q} < \frac{r}{s}.$$

Then

$$W_{\frac{p}{q}} = W_{\frac{m}{n} \oplus \frac{r}{s}} = W_{r/s} \cdot W_{m/n}.$$

A pair $W_{p/q}, W_{r/s}$ is a pair of primitive associates if and only if $\frac{p}{q}, \frac{r}{s}$ are neighbors, that is, $|ps - qr| = 1$.

Because a product of primitive associates is always primitive, it is clear that the words we obtain in the theorem are primitive. As we will see when we give the proofs of the theorems, the words $W_{p/q}$ in the theorem belong to the set $\{W_{p/q}\}$ we defined above so the notation is consistent.

We note that the two products $W_{m/n} \cdot W_{r/s}$ and $W_{r/s} \cdot W_{m/n}$ are always conjugate in G. In this W-iteration scheme we always choose the product where the larger subscript comes first. The point is that in order for the scheme to work the choice has to be made consistently.

We emphasize that $W_{p/q}$ always denotes the word obtained using this enumeration scheme.

The other enumeration schemes are the V-scheme where the words come from the algorithm discussed below and the E-enumeration scheme that gives the words in a palindromic form or a canonical product palindromic form. While it might seem that we have introduced more notation here than necessary, we have done so because want to emphasize the different ways in which the primitive words can arise.

The $W_{p/q}$ words can be rewritten using the entries in the continued fraction expansion instead of the primitive exponents. Since this is the form in which the words arise in the $PSL(2,\mathbb{R})$ discreteness algorithm [G3, Compl, YCJiang, Malik], the rewritten form is also known as *algorithmic form* of the primitive words.

The algorithm begins with a pair of generators (X_0, Y_0) for a subgroup of $PSL(2,\mathbb{R})$ and runs through a sequence of primitive pairs of generators. At each step the algorithm either replaces a generating pair (X, Y) with a new generating pair (XY, Y), called a "linear step" and or it replaces a generating pair with the pair (Y, XY) called a "Fibonacci step". There can be many linear steps between Fibonacci steps; the replacement pair after N linear steps is $(X^N Y, X)$. Each Fibonacci step, however, occurs between two linear steps. The algorithm thus generates new pairs of primitive associates at each step, and as we will see, the entries of the continued fraction are visible in the form of the words generated.

The main point of the discreteness algorithm, however, is not only to generate new pairs of primitive generators but to decide whether a particular pair of matrices generates a discrete group. Therefore, at each step a "stopping condition" is tested for and when it is reached, the algorithm prints out either: *the group is discrete* or *the group is not discrete*. The pair of generators given by the algorithm when it stops are called the *stopping generators*. Associated to any implementation of the algorithm is a sequence of integers, the F-sequence, or Fibonacci sequence, which gives the number of linear steps that occur between consecutive Fibonacci steps at the point the algorithm stops. The F-sequence is usually denoted by $[a_1, ..., a_k]$. The stopping generators can be determined from the F-sequence.

The algorithm can be run backwards from the stopping generators when the group is discrete and free, and any primitive pair can be obtained from the stopping generators using the backwards F-sequence.

The F-sequence of the algorithm is used in [G3] and [YCJiang] to determine the computational complexity of the algorithm. In [G3] it is shown that most forms of the algorithm run in polynomial time and in [YCJiang] it is shown that all forms do.

The entries in the F-sequence, also called the *algorithmic exponents.* In [GKwords] it is shown that they are also the the entries in the continued fraction expansion of the rational corresponding to that primitive word determined by the algorithm — hence the same notation. Some of theorems below are stated in [GKwords] with the term F-sequence instead of the equivalent term, the continued fraction expansion.

The next theorem exhibits the primitive words with the continued fraction expansion exponents in its most concise form.

If $p/q = [a_0, \ldots, a_k]$, set $\frac{p_j}{q_j} = [a_0, \ldots, a_j]$, $j = 0, \ldots k$. These fractions, called the *approximants* of p/q, can be computed recursively from the continued fraction for p/q as follows:

$$p_0 = a_0, q_0 = 1 \text{ and } p_1 = a_0 a_1 + 1, q_1 = a_1$$

$$p_j = a_j p_{j-1} + p_{j-2} \ , q_j = a_j q_{j-1} + q_{j-2} \ j = 2, \ldots, k.$$

Theorem 1.2.2 ([GKwords]) *If $[a_0, \ldots, a_k]$ is the continued fraction expansion of p/q, the primitive word $W_{p/q}$ can be written inductively using the continued fraction approximants $p_j/q_j = [a_0, \ldots, a_j]$.*

Set

$$W_{0/1} = A, \ W_{1/0} = B \text{ and } W_{1/1} = BA.$$

For $j = 1, \ldots, k$ if $p_{j-2}/q_{j-2} > p/q$ set

$$W_{p_j/q_j} = W_{p_{j-2}/q_{j-2}} (W_{p_{j-1}/q_{j-1}})^{a_j}$$

and set

$$W_{p_j/q_j} = (W_{p_{j-1}/q_{j-1}})^{a_j} W_{p_{j-2}/q_{j-2}}$$

otherwise.

The relationship between the Farey sequence and the approximants of p/q is that the Farey sequence contains the approximating fractions as a subsequence. The points of the Farey sequence between $\frac{p_j}{q_j}$ and $\frac{p_{j+1}}{q_{j+1}}$ have continued fraction expansions

$$[a_0, a_1, \ldots a_j + 1], [a_0, a_1, \ldots, a_j + 2], \ldots, [a_0, a_1, \ldots a_j + a_{j+1} - 1].$$

As real numbers, the approximants are alternately larger and smaller than $\frac{p}{q}$. The number a_j counts the number of times the new endpoint in the Farey sequence lies on one side of the old one. Theorem 1.2.2 is thus an easy consequence of Theorem 1.2.1.

We have an alternative recursion scheme which reflects the form of the words as they show up in the algorithm; this is not quite the same as the form in Theorem 1.2.2. Words at linear steps are formed as in Theorem 1.2.2 but words that occur at Fibonacci steps are slightly different; they are a cyclic permutation of the words in Theorem 1.2.2. We use the notation V for these words. To define the V-scheme, assume without loss of generality that $p/q > 1$ and write $p/q = [a_0, \dots a_k]$. By assumption $a_0 > 0$. Set $V_{-1} = B$ and $V_0 = W_{p_0/q_0} = AB^{a_0}$. Then for $j = 1, \dots, k$, set

$$V_j = V_{j-2}[V_{j-1}]^{a_j}.$$

In the V words we see the entries of the continued fraction occurring as exponents. When we expand the word as a product of A's and B's, we see the primitive exponents. The next theorem gives us formulas for the primitive exponents in terms of the entries of the continued fraction expansion and hence necessary and sufficient conditions to recognize primitive words in $\{W_{p/q}\}$.

The notation here is a bit cumbersome because there are several indices to keep track of. When we expand the word V_j as a product of A's and B's, we need to keep track both of the index j and the primitive exponents of V_j so we denote them $n_i(j)$.

Theorem 1.2.3 ([GKwords, Malik]) *Given $p/q > 1$, expand the words V_j into*

$$V_j = B^{n_0(j)} AB^{n_1(j)} \dots AB^{n_{t_j}(j)}$$

for $j = 0, \dots, k$. Then $V_k \in \{W_{p/q}\}$; it is primitive and its exponents are related to the continued fraction of $p/q = [a_0, \dots, a_k]$ or the F-sequence as follows:

If $j = 0$, then $t_0 = 1 = q_0$, $n_0 = 0$ and $n_1(0) = a_0$.
If $j = 1$, then $t_1 = a_1 = q_1$, $n_0(1) = 1$ and $n_i(1) = a_0$, $i = 1, \dots, t_1$.
If $j = 2$ then $t_2 = a_2 a_1 + 1 = q_2$, $n_0(2) = 0$ and for $i = 1, \dots, t_2$, $n_i(2) = a_0 + 1$ if $i \equiv 1 \mod t_2$ and $n_i(j) = a_0$ otherwise
For $j > 2, \dots, k$,

- *$n_0(j) = 0$ if j is even and $n_0(j) = 1$ if j is odd.*
- *$t_j = q_j$.*

- *For* $i = 1 \dots t_{j-2}$, $n_i(j) = n_i(j-2)$.
- *For* $i = t_{j-2} + 1 \dots t_j$, $n_i(j) = a_0 + 1$ *if* $i \equiv 1 + t_{k-2}$ *mod* t_{k-1} *and* $n_i(j) = a_0$ *otherwise.*

Moreover any word in $\{W_{p/q}\}$ *whose exponents, up to cyclic permutation, satisfy the above conditions is primitive.*

There is an ambiguity because $[a_0, \dots, a_k] = [a_0, \dots, a_k - 1, 1]$ and these continued fractions give different words. One, however, is a cyclic permutation of the other.

Using the recursion formulas for the exponents in theorem, we obtain a new proof of the following corollary which was originally proved in [BuserS]. We omit the proof as it is a fairly straightforward induction argument on the Farey level.

Corollary 1.2.4 ([BuserS]) *In the expression for a primitive word* $W_{p/q}$, *for any integer* m, $0 < m < p$, *the sums of any* m *consecutive primitive exponents* n_i *differ by at most* ± 1.

We note that the authors in [BuserS] also prove that this exponent condition is also sufficient for a word to be primitive.

The following theorem was originally proved in [OZ] and in [Piggott] and [KR].

Theorem 1.2.4 ([GKenum, KR, OZ, Piggott]) *Let* $G = \langle A, B \rangle$ *be a two generator free group. Then any primitive element* $W \in G$ *is conjugate to a cyclic permutation of either a palindrome in* A, B *or a product of two palindromes. In particular, if the length of* W *is* $p + q$, *then, up to cyclic permutation,* W *is a palindrome if and only if* $p + q$ *is odd and is a product of two palindromes otherwise.*

We note that this can be formulated equivalently using the parity of pq which is what we do below.

In the pq odd case, the two palindromes in the product can be chosen in various ways. We will make a particular choice in the next theorem.

1.2.3 E-Enumeration

The next theorem, proved in [GKenum], gives yet another enumeration scheme for primitive words, again using Farey sequences. The new scheme to enumerate primitive elements is useful in applications, especially geometric applications. These applications will be studied elsewhere [GKgeom]. Because the words we obtain are cyclic permutations of the words $W_{p/q}$, we use a different notation for them; we denote them as $E_{p/q}$.

Theorem 1.2.5 (The E-iteration scheme) ([GKenum]) *The primitive elements of a two generator free group can be enumerated recursively using their Farey sequences as follows. Set*

$$E_{0/1} = A,\ E_{1/0} = B, \quad \textit{and } E_{1/1} = BA.$$

Given p/q with parents $m/n, r/s$ such that $m/n < r/s$,

- *if pq is odd, set $E_{p/q} = E_{r/s}E_{m/n}$ and*
- *if pq is even, set $E_{p/q} = E_{m/n}E_{r/s}$. In this case $E_{p/q}$ is the unique palindrome cyclically conjugate to $W_{p/q}$.*

$E_{p/q}$ and $E_{p'/q'}$ are primitive associates if and only if $pq' - qp' = \pm 1$.

Note that when pq is odd, the order of multiplication is the same as in the enumeration scheme for $W_{p/q}$ but when pq is even, it is reversed. This theorem says that if pq is even, $E_{p/q}$ is the unique palindrome cyclically conjugate to $W_{p/q}$. If pq is odd, then $E_{p/q}$ is a product of a uniquely determined pair of palindromes.

In this new enumeration scheme, Farey neighbors again correspond to primitive pairs but the elements of the pair $(W_{p/q}, W_{p'/q'})$ are not necessarily conjugate to the elements of the pair $(E_{p/q}, E_{p'/q'})$ by the same element of the group. That is, they are not necessarily conjugate as pairs.

1.3 Cutting Sequences

We represent G as the fundamental group of a punctured torus and use the technique of *cutting sequences* developed by Series (see [S, KS, Nielsen]) as the unifying theme. This representation assumes that the group G is a discrete free group. Cutting sequences are a variant on Nielsen boundary development sequences [Nielsen]. In this section we outline the steps to define cutting sequences.

- It is standard that $G = \langle A, B \rangle$ is isomorphic to the fundamental group of a punctured torus S. Each element of G corresponds to a free homotopy class of curves on S. The primitive elements are free homotopy classes of simple curves that do not simply go around the puncture. Primitive pairs are classes of simple closed curves with a single intersection point.

- Let $\mathcal{L}$ be the lattice of points in $\mathbb{C}$ of the form $m+ni$, $m, n \in \mathbb{Z}$ and let $\mathcal{T}$ be the corresponding lattice group generated by $a = z \mapsto z+1, b = z \mapsto z+i$. The (unpunctured) torus is homeomorphic to the quotient $\mathbb{T} = \mathbb{C}/\mathcal{T}$. The horizontal lines map to longitudes and the vertical lines to meridians on $\mathbb{T}$.

  The punctured torus is homeomorphic to the quotient of the plane punctured at the lattice, $(\mathbb{C} \setminus \mathcal{L})/\mathcal{T}$. Any curve in $\mathbb{C}$ whose endpoints are identified by the commutator $aba^{-1}b^{-1}$ goes around a puncture and is no longer homotopically trivial.
- The simple closed curves on $\mathbb{T}$ are exactly the projections of lines joining pairs of lattice points (or lines parallel to them). These are lines $L_{p/q}$ of rational slope p/q. The projection $l_{p/q}$ consists of p longitudinal loops q meridional loops. We assume that p and q are relatively prime; otherwise the curve has multiplicity equal to the common factor.

  For the punctured torus, any line of rational slope, not passing through the punctures projects to a simple closed curve and any simple closed curve, not enclosing the puncture, lifts to a curve freely homotopic to a line of rational slope.
- Note that, in either case, if we try to draw the projection of $L_{p/q}$ as a simple curve, the order in which we traverse the loops on $\mathbb{T}$ (or S) matters. In fact there is, up to cyclic permutation and reversal, only one way to draw the curve. We will find this way using cutting sequences. This is the content of Theorem 1.2.3. Below, we assume we are working on $\mathbb{T}$.
- Choose as fundamental domain (for S or $\mathbb{T}$) the square D with corners (puncture points) $\{0, 1, 1+i, i\}$. Label the bottom side B and the top side $\bar{B}$; label the left side A and the right side $\bar{A}$. Note that the transformation a identifies A with $\bar{A}$ and b identifies B with $\bar{B}$. Use the translation group to label the sides of all copies of D in the plane.
- Assume for simplicity that $p/q \geq 0$. We will be indicate how to modify the discussion otherwise. Choose a fundamental segment of the line $L_{p/q}$ and pick one of its endpoints as initial point. It passes through $p+q$ copies of the fundamental domain. Call the segment in each copy a strand.

  Because the curve is simple, there will either be "vertical" strands joining the sides B and $\bar{B}$, or "horizontal" strands joining the sides A and $\bar{A}$, but not both.

  Call the segments joining a horizontal and vertical side corner strands. There are four possible types of corner strands: from left to bottom, from left to top, from bottom to right, from top to right. If all four types were to occur, the projected curve would be trivial on $\mathbb{T}$. There cannot be only one or three different types of corner strands because the curve would not close up. Therefore the only corner strands occur on one pair of opposite corners and there are an equal number on each corner.

- Traversing the fundamental segment from its initial point, the line goes through or "cuts" sides of copies of D. We will use the side labeling to define a *cutting sequence* for the segment. Since each side belongs to two copies it has two labels. We have to pick one of these labels in a consistent way. As the segment passes through, there is the label from the copy it leaves and the label from the copy it enters. We always choose the label from the copy it enters. Note that the cyclic permutation depends on the starting point.
- If $p/q > 1$, the resulting cutting sequence will contain p B's and q A's and there will be $p-q$ horizontal strands and q corner strands; if $0 \leq p/q < 1$, the resulting cutting sequence will contain q B's, p A's and there will be $q-p$ vertical strands and p corner strands. If $p/q < 0$ we either replace A by $\bar{A}$ or B by $\bar{B}$. We identify the cutting sequence with the word in G interpreting the labels A, B and the generators and the labels $\bar{A}, \bar{B}$ as their inverses.
- Given an arbitrary word $W = A^{m_1}B^{n_1}A^{m_2}B^{n_2}\ldots A^{m_p}B^{n_p}$ in G, we form a cutting sequence for it by drawing strands from the word through successive copies of D. We then draw translates of the resulting strands by elements of the lattice group so that they all lie in the fundamental domain D. The strands in D are all disjoint up to homotopy if and only if the word is primitive.

Let us illustrate with three examples. In the first two, we draw the cutting sequences for the fractions $\frac{p}{q} = \frac{1}{1}$ and $\frac{p}{q} = \frac{3}{2}$. In the third, we construct the cutting sequence for the word A^2B^3. See figure **??**.

- A fundamental segment of $l_{1/1}$ can be chosen to begin at a point on the left (A) side and pass through D and the adjacent copy above D; There will be a single corner strand connecting the A side to a $\bar{B}$ side and another connecting a B side to an $\bar{A}$ side.

  To read off the cutting sequence begin with the point on A and write A. Then as we enter the next (and last) copy of D we have an B side. The word is thus AB.

  Had we started on the bottom, we would have obtained the word BA.

- A fundamental segment of $L_{3/2}$ passes through 5 copies of the fundamental domain. (See Figure 2.) There is one "vertical" segment joining a B and a $\bar{B}$, 2 corner segments joining an A and a $\bar{B}$ and two joining the opposite corners. Start on the left side. Then, depending on where on this side we begin we obtain the word $ABABB$ or $ABBAB$.

  If we start on the bottom so that the vertical side is in the last copy we encounter we get $BABAB$.
- To see that the word $AABBB$ cannot correspond to a simple loop, draw the a vertical line of length 3 and join it to a horizontal line of length 2. Translate it one to the right and one up. Clearly the translate intersects the curve and projects to a self-intersection on the torus. This will happen whenever the horizontal segments are not separated by a vertical segment.

  Another way to see this is to try to draw a curve with two meridian loops and three longitudinal loops on the torus. You will easily find that if you try to connect them arbitrarily the strands will cross on $\mathbb{T}$, but if you use the order given by the cutting sequence they will not. Start in the middle of the single vertical strand and enter a letter every time you come to the beginning of a new strand. We get $BABAB$.
- Suppose $W = B^3A^2$. To draw the cutting sequence, begin on the bottom of the square and, since the next letter is B again, draw a vertical strand to a point on the top and a bit to the right. Next, since we have a third B, in the copy above D draw another vertical strand to the top and again go a bit to the right. Now the fourth letter is a A so we draw a corner strand to the right. Since we have another A we need to draw a horizontal strand. We close up the curve with a last corner strand from the left to the top.

  Because we have both horizontal and vertical strands, the curve is not simple and the word is not primitive.

1.4 Proofs

Proof of Theorem 1.2.3.

A word is primitive if and only if its cutting sequence defines a curve with no intersecting strands in the fundamental domain. The word corresponding to the cutting sequence is determined up to cyclic permutation, depending on which strand is chosen as the first one, and inverse, depending on the direction. It therefore corresponds to a line of rational slope p/q. This means that given a word in $\{W_{p/q}\}$ we can check whether it is primitive by drawing its cutting sequence.

We start with a line of slope p/q and find its cutting sequence. This process will determine conditions on the form of the corresponding word that will be necessary and sufficient for the word to be primitive.

The cases $p/q = 0/1, 1/0$ are trivial. We suppose first that $p/q \geq 1$ and treat that case. The other cases follow in the same way, either interchanging A and B or replacing B by $\overline{B}$.

Set $p/q = [a_0, \ldots a_k]$. Since $p/q > 1$ we know that $a_0 > 0$. Note that there is an ambiguity in this representation; we have $[a_0, \ldots a_k - 1, 1] = [a_0, \ldots a_k]$. We can eliminate this by assuming $a_k > 1$. With this convention, the parity of k is well defined.

Assume first k is even; choose as starting point the lowest point on an A side. The line $L_{p/q}$ has slope at least 1 so there will be at least one vertical strand and no horizontal strands. Because there are no horizontal strands, we must either go up or down; assume we go up. The first letter in the cutting sequence is A and since the strand must be a corner strand, the next letter is B. As we form the cutting sequence we see that because there are no horizontal strands, no A can be followed by another A. Because we always go up or to the right, no strand begins with $\bar{B}$. Because we started at the lowest point on A, the last strand we encounter before we close up must start at the rightmost point on a B side. Since there are $p + q$ strands, this means the sequence, and hence the word belongs to $\{W_{p/q}\}$. Since we begin with an A, $n_0 = 0$ and the word looks like

$$AB^{n_1}AB^{n_2}A \ldots B^{n_q}, \sum_{i=1}^{q} n_i = p$$

with all $n_i > 0$. If we use the translation group to put all the strands into one fundamental domain, the endpoints of the strands on the sides are ordered. We see that if we are at a point on the B side, the next time we come to the B side we are at a point that is q to the right mod(p).

Let us see exactly what the exponents are. Since we began with the lowest point on the left, the first B comes from the q^{th} strand on the bottom. There are p strands on the bottom; the first (leftmost) $p - q$ strands are vertical and the last q are corner strands. Since we move to the right p strands at a time, we can do this $a_0 = [p/q]$ times. The word so far is AB^{a_0}.

At this point we have a corner strand so the next letter will be an A.

Define r_1 by $p = a_0 q + r_1$. The corner strand ends at the right endpoint $r_1 + 1$ from the bottom and the corresponding corner strand on the A side joins with the $(q - r_1)^{th}$ vertical strand on the bottom. We again move to the right q strands at a time, a_0 times, while $a_0 q - r_1 > p - q$. After repeating this some n times, $a_0 q - r_1 \leq p - q$. This number, n, will satisfy $q = r_1 n + r_2$ and $r_2 < r_1$. Notice that this is the first step of the Euclidean algorithm for the greatest common denominator of p and q and it generates the continued fraction coefficients at each step. Thus $n = a_1$ and the word at this point is $[AB^{a_0}]^{a_1}$. Since we are now at a corner strand, the next letter is an "extra" B. We repeat the sequence we have already obtained a_3 times where $r_1 = a_3 r_2 + r_3$ and $r_3 < r_2$. The word at this point is $[AB^{a_0}]^{a_1} B [[AB^{a_0}]^{a_1}]^{a_3}$ which is the word V_3 in the V-recursion scheme.

We continue in this way. We see that the Euclidean algorithm tells us that each time we have an extra B, the sequence up to that point repeats as many times as the next a_i entry in the continued fraction expansion of p/q. When we come to the last entry a_k, we have used all the strands and are back to our starting point. The exponent structure is thus forced on us by the number p/q and the condition that the strands not intersect.

If we had intersecting strands we might have a horizontal strand violating the condition on the A exponents. If a vertical strand intersected either another vertical strand or a corner strand, or if two corner strands intersected, the points on the top or bottom would not move along q at a time and the exponents wouldn't satisfy the rules above.

If k is odd, we begin the process at the rightmost bottom strand and begin the word with B and obtain the recursion.

Note that had we chosen a different starting point we would have obtained a cyclic permutation of $W_{p/q}$, or, depending on the direction, its inverse.

For $0 < p/q < 1$ we have no vertical strands and we interchange the roles of A and B. We use the continued fraction $q/p = [a_0, \ldots, a_k]$ and argue as above, replacing "vertical" by "horizontal".

For $p/q < 0$, we replace A or B by $\bar{A}$ or $\bar{B}$ as appropriate.

Thus, we have proved that if we have a primitive word its exponents satisfy the conditions in Theorem 1.2.3 up to to cyclic permutation. In addition, if the exponents n_i of a word $W \in \{W_{p/q}\}$, or some cyclic permutation of it, do not satisfy the exponent conditions, the strands of its cutting sequence must either intersect somewhere or they do not close up properly and the word is not primitive. The conditions are therefore both necessary and sufficient for the word to be primitive and Theorem 1.2.3 follows. □

It is obvious that the only primitive exponents that can occur are a_0 and a_0+1. This gives the simple necessary conditions of Corollary 1.2.1. □

For the proof of Corollary 1.2.3 we want to to see when two primitive words $W_{p/q}$ and $W_{r/s}$ are associates. Note the vectors joining zero with $m+ni$ and $r+si$ generate the lattice $\mathcal{L}$ if and only if $|ps-qr|=1$; or equivalently, if and only if $(p/q, r/s)$ are neighbors. Fundamental segments of lines $L_{p/q}, L_{r/s}$ correspond to primitive words in $\{W_{p/q}\}$ and $\{W_{r/s}\}$. If we choose words $W_{p/q}$ and $W_{r/s}$ and draw their cutting sequences they both start at a point closest to the left bottom corner. Connecting the strands for each word we see that they become generators for the lattice and hence associates if and only if $(p/q, r/s)$ are neighbors. □

Proof of Theorem 1.2.1 and 1.2.2. Although Theorem 1.2.1 and 1.2.2 can be deduced from the proof above, we give an independent proof.

The theorems prescribe a recursive definition of a primitive word associated to a rational p/q. We assume $p/q \geq 0$ and that m/n and r/s are parents with

$$\frac{m}{n} < \frac{p}{q} < \frac{r}{s}.$$

We need to show that if we draw the strands for the cutting sequences of $W_{m/n}$ and $W_{r/s}$ in the same diagram, then the result is the cutting sequence of the product.

Note again that if $r/s, m/n$ are neighbors, the vectors joining zero with $m+ni$ and $r+si$ generate the lattice $\mathcal{L}$. Draw a fundamental segment $s_{m/n}$ for $W_{m/n}$ joining 0 to $m+ni$ and a fundamental segment $s_{r/s}$ for $W_{r/s}$ joining $m+ni$ to $(m+r)+(n+s)i$. The straight line s joining 0 to $(m+r)+(n+s)i$ doesn't pass through any of the lattice points because by the neighbor condition $rn-sm=1$, $s_{m/n}$ and $s_{r/s}$ generate the lattice. We therefore get the same cutting sequence whether we follow $s_{m/n}$ and $s_{r/s}$ in turn or follow the straight line s. This means that the cutting sequence for $W_{p/q}$ is the concatenation of the cutting sequences of $W_{r/s}$ and $W_{m/n}$ which is what we had to show.

If $p/q < 0$, reflect the lattice in the imaginary axis. This corresponds to applying the rules in Definition 3.

We note that proving Theorem 1.2.2 is just a matter of notation.

□

Proof of Theorem 1.2.4.

We prove the theorem for $0 < p/q < 1$. The other cases follow as above by interchanging the roles of A and B or replacing B by $\overline{B}$. The idea is to choose the starting point correctly.

Suppose pq is even. We want to show that there is a unique cyclic permutation of $W_{p/q}$ that is a palindrome.

Draw a line of slope p/q. By assumption, there are horizontal but no vertical strands and $p - q > 0$ must be odd. This implies that in a fundamental segment there are an odd number of horizontal strands. In particular, if we pull all the strands of a fundamental segment into one copy of D, one of the horizontal strands is the middle strand. Choose the fundamental segment for the line in the lattice so that it is centered about this middle horizontal strand.

To form the cutting sequence for the corresponding word W, begin at the right endpoint of the middle strand and take as initial point the leftpoint that it corresponds to. Now go to the other end of the middle strand on the left and take as initial point the rightpoint that it corresponds to and form the cutting sequence for a word V. By the symmetry, since we began with a middle strand, V is W with all the A's replaced by $\overline{A}$'s and all the B's replaced by $\overline{B}$'s. Since $V = W^{-1}$, we see that W must be a palindrome which we denote as $W = P_{p/q}$. Moreover, since it is the cutting sequence of a fundamental segment of the line of slope p/q, it must is a cyclic permutation of $W_{p/q}$.

Note that since we began with a horizontal strand, the first letter in the sequence is an A and, since it is a palindrome, so is the last letter.

When $q/p > 1$, there are horizontal and no vertical strands, and there is a middle horizontal strand. This time we choose this strand and go right and left to see that we get a palindrome. The first and last letters in this palindrome will be B.

If $p/q < 0$, we argue as above but either A or B is replaced by respectively $\bar{A}$ or $\bar{B}$. □

Heuristic for the enumeration, Theorem 1.2.5.

The proof of the enumeration theorem, Theorem 1.2.5, involves purely algebraic manipulations and can be found in [GKenum]. We do not reproduce it here but rather give a heuristic geometric idea of the enumeration and the connection with palindromes that comes from the $PSL(2, \mathbb{R})$ discreteness algorithm [G2, G3].

Note that the absolute value of the trace of an element $X \in PSL(2,\mathbb{R})$, $|\mathrm{trace}(X)|$, is well-defined. Recall that X is elliptic if $|\mathrm{trace}(X)| < 2$ and hyperbolic if $|\mathrm{trace}(X)| > 2$. As an isometry of the upper half plane, each hyperbolic element has an invariant geodesic called its *axis*. Each point on the axis is moved a distance $l(X)$ towards one endpoint on the boundary. This endpoint is called the attractor and the distance can be computed from the trace by the formula $\cosh \frac{l(X)}{2} = \frac{1}{2}|\mathrm{trace}(X)|$. The other endpoint of the axis is a repeller.

For convenience we use the unit disk model and consider elements of $PSL(2,\mathbb{R})$ as isometries of the unit disk. In the algorithm one begins with a representation of the group where the generators A and B are (appropriately ordered) hyperbolic isometries of the unit disk. The algorithm applies to any non-elementary representation of the group where the representation is not assumed to be free or discrete. The axes of A and B may be disjoint or intersect. We illustrate the geometric idea using intersecting axes.

If the axes of A and B intersect, they intersect in unique point p. In this case one does not need an algorithm to determine discreteness or non-discreteness as long as the multiplicative commutator, $ABA^{-1}B^{-1}$, is not an elliptic isometry. However, the geometric steps used in determining discreteness or non-discreteness in the case of an elliptic commutator still make sense. We think of the representation as being that of a punctured torus group when the group is discrete and free.

Normalize at the outset so that the translation length of A is smaller than the translation length of B, the axis of A is the geodesic joining -1 and 1 with attracting fixed point 1 and the axis of B is the line joining $e^{i\theta}$ and $-e^{i\theta}$. This makes the point p the origin. Replacing B by its inverse if necessary, we may assume the attracting fixed point of B is $e^{i\theta}$ and $-\pi/2 < \theta \leq \pi/2$.

The geometric property of the palindromic words is that their axes all pass through the origin.

Suppose $(p/q, p'/q')$ is a pair of neighbors with pq and $p'q'$ even and $p/q < p'/q'$. The word $W_{r/s} = W_{p'/q'}W_{p/q}$ is not a palindrome or conjugate to a palindrome. Since it is a primitive associate of both $W_{p'/q'}$ and $W_{p/q}$ the axis of $Ax_{W_{r/s}}$ intersects each of the axes $Ax_{W_{p/q}}$ and $Ax_{W_{p'/q'}}$ in a unique point; denote these points by $q_{p/q}$ and $q_{p'/q'}$ respectively. Thus, to each triangle, $(p/q, r/s, p'/q')$ we obtain a triangle in the disk with vertices $(0, q_{p/q}, q_{p'/q'})$.

The algorithm provides a method of choosing a next neighbor and next associate primitive pair so that at each step the longest side of the triangle is replaced by a shorter side. The procedure stops when the sides are as short as possible. Of course, it requires proof to see that this procedure will stop and thus will actually give an algorithm.

There is a similar geometric description of the algorithm and palindromes in the case of disjoint axes.

The first author would like to thank the Rutgers Research Council and Yale University for support. The second author would like to thank PSC-CUNY for support.

Bibliography

[BuserS] Buser, P.; Semmler, K.-D. (1988). The geometry and spectrum of the one-holed torus. *Comment. Math. Helv.* **63, no. 2**, 259–274.

[CMZ] Cohen, P; Metzler, W; Zimmermann, B. (1981). What does a basis of $F(a,b)$ look like?, *Math. Ann.* **257 (4)**, 435–445.

[G2] Gilman, Jane (2001). Alternate Discreteness tests, *Birman Conf. Proceedings, AMS/IP Studies in Advanced Mathematics*, **24**, 41–47.

[G3] Gilman, Jane (1995). Two-generator Discrete Subgroups of $PSL(2, \mathbf{R})$, *Memoirs of the AMS,* **561**

[Compl] Gilman, Jane (1997). Algorithms, Complexity and Discreteness Criteria in $PSL(2, \mathbb{C})$, *Journal D'Analyse Mathematique*, **73**, 91–114.

[GKwords] Gilman, Jane and Keen, Linda (2002). Word Sequence and Intersection Numbers, *Contemporary Math*, **311** 331–349.

[GKenum] Gilman, Jane and Keen, Linda Enumerating Plaindromes in Rank Two Free Groups, to appear.

[GKgeom] Gilman, Jane and Keen, Linda Palindromes and discreteness for Kleinian groups, submitted.

[HardyWright] Hardy, G.H. and Wright, E. M. (1938). *An introduction to the theory of numbers Oxford, Clarendon Press*

[YCJiang] Jiang, Yichang (2001). Complexity of the Fuchsian Group Discreteness Algorithm, *Ann Acad Sci Fenn*, **26** 375–390.

[KR] Kassel, Christian and Reutenauer, Christophe (2007). Sturmian morphisms, the braid group B_4, Christoffel words and bases of F_2. *Ann. Mat. Pura Appl.* **(4) 186 no. 2**, 317–339.

[KS] Keen, Linda and Series, Caroline, (1993). Pleating Coordinates for the Maskit Embedding of Teichmüller space for a punctured torus, *Topology*, **32** #4, 719–749.

[MKS] Magnus, Wilhelm; Karass, Abraham; and Solitar, Donald (1966). it Combinatorial Group Theory, *John Wiley & Sons, NYC.*

[Malik] Malik, Vidur (2007). Curves Generated on Surfaces by the Gilman-Maskit Algorithm, *Ph D thesis, Rutgers University, Newark, NJ.*

[Nielsen] Nielsen, Jacob (1927), (1927), (1932). Untersuchengen zur Topolie der geschlossenen zweiseitigen Flächen, I, II III, *Acta Math.* **50** 189–358; **53** 1–76, **58** 87–167.

[OZ] Osborne, R. P.; Zieschang, H. (1981). Primitives in the free group on two generators, *Invent. Math.***63 no. 1**, 17–24.

[Piggott] Piggott, Adam (2006). Palindromic primitives and palindromic bases in the free group of rank two *J. Algebra*, **304 no. 1**, 359–366.

[S] Series, Caroline (1985). The Geometry of Markoff Numbers, *Math. Intelligencer* **7** #3, 20–29.

[Wr] Wright, David J. (2004). Searching for the cusp, in *Spaces of Kleinian Groups, LMS Lecture Notes* **329**, *Cambridge U. Press* 1–36.

Jane Gilman,

Department of Mathematics, Rutgers University, Newark, NJ 07079, USA

Email: gilman@andromeda.rutgers.edu

Linda Keen,

Department of Mathematics, Lehman College and Graduate Center, CUNY, Bronx, 10468 and Department of Mathematics, CUNY Graduate Center, New York, NY 10016, USA

Email: linda.keen@lehman.cuny.edu