Counting primitive elements of a free group

Vladimir Shpilrain

ABSTRACT. We show that the number of primitive elements of length n in a free group of rank $r \geq 3$ is bounded from above by $c \cdot \lambda^n$, where λ is the greatest real root of the polynomial $\lambda(\lambda^2-1)(\lambda-(2r-2))+1$ and c is some constant. To obtain this estimate, we use some well known facts from graph theory together with a counting technique based on the theory of linear recurrence relations.

1 Introduction

Let F_r be the free group of a finite rank $r \geq 2$ with a set $X = \{x_i\}$, $1 \leq i \leq r$, of free generators. An element $g \in F_r$ is called *primitive* if it is a member of some free basis of F_r. Or, equivalently, if there is an automorphism of F_r that takes g to x_1.

Let $P(r, n)$ be the number of primitive elements of length n in F_r. This paper addresses the following problem of M. Wicks (see [1, Problem (F17)]):

Problem. What is the growth of $P(r, n)$ as a function of n, with r fixed?

For $r = 2$, the number $P(2, n)$ grows like $(\sqrt{3})^n$; this follows from [3, Proposition 4.1], as observed by Rivin [6]. We also note that the *precise* number of *cyclically reduced* primitive elements of length n in F_2 was given in [5]; this number has linear growth as a function of n. This case however is exceptional, and it is easy to see that if $r \geq 3$, then the growth of the number of primitive elements (cyclically reduced or not) is exponential, say, λ^n. The problem is therefore to determine λ (as a function of r).

It was shown in [3] that $\lambda \leq \mu(r) > 2r-2$, where $\mu(r)$ is asymptotically approaching $2r-2$. In [2], it was shown that $\lambda \leq 2r-2$. In both papers, crucial for the counting arguments was the fact that the Whitehead graph

2000 Mathematics Subject Classification: Primary 20E05, 20F28; Secondary 05C25.

of any primitive element of length > 2 has either an isolated edge or a cut vertex, i.e., a vertex that, having been removed from the graph together with all incident edges, increases the number of connected components of the graph.

In the present paper, we again exploit this fact to sharpen the estimate for λ:

Theorem. If $r \geq 3$, then, for some constants c_1, c_2, one has $c_1 \cdot n \cdot (2r-3)^n \leq P(r,n) \leq c_2 \cdot \lambda^n$, where λ is the greatest real root of the polynomial $\lambda(\lambda^2-1)(\lambda-(2r-2))+1$.

Obviously, λ in the Theorem is smaller than $2r-2$, although it is asymptotically approaching $2r-2$. It seems that the above estimate exhausts the potential of the "cut vertex" approach, and further improvements would require brand new ideas. As for the ultimate result, we make the following

Conjecture. If $r \geq 3$, then $P(r,n) = O(n \cdot (2r-3)^n)$.

We note that $n \cdot (2r-3)^n$ is (up to a factor that does not depend on n) the number of "obvious" primitive elements of length n having the form $u \cdot x_i^{\pm 1} \cdot v$, where u, v are arbitrary elements that do not depend on x_i. Thus, our conjecture says that, for $r \geq 3$, "most" primitive elements are of that form.

Our proof uses a refined analysis of the Whitehead graph of a primitive element and a new ingredient, namely, systems of linear recurrence relations, which is described in the following section. We believe this technique can be used for other counting problems in (free) groups as well.

Acknowledgement. I am grateful to the referee for helpful comments, in particular for pointing out a computational error in the original version of the paper.

2 The Whitehead graph, Whitehead tree and transition matrix

The Whitehead graph $Wh(u)$ of a (cyclically reduced) word $u \in F_r$ is obtained as follows. The vertices of this graph correspond to the elements of the free generating set X and their inverses. For each occurrence of a subword $x_i x_j$ in the word u, there is an edge in $Wh(u)$ that connects the vertex x_i to the vertex x_j^{-1}; if u has a subword $x_i x_j^{-1}$, then there is an edge connecting x_i to x_j, etc. There is one more edge (the external edge) included in the definition of the Whitehead graph: this is the edge that connects the vertex corresponding to the last letter of u to the vertex corresponding to the inverse of the first letter.

It was observed by Whitehead himself that the Whitehead graph of any primitive element of length > 2 has either an isolated edge or a cut vertex,

i.e., a vertex that, having been removed from the graph together with all incident edges, increases the number of connected components of the graph.

Both [2] and [3] exploited this fact to get upper bounds for $P(r, n)$. In the present paper, we refine these upper bounds based on the following simple observation (see e.g. [7, Exercise 5.7]):

Suppose a simple graph Γ has the property that any two vertices can be included in a simple circuit. Then Γ does not have a cut vertex.

Our strategy therefore will be to produce an upper bound for the number of elements $u \in F_r$ whose Whitehead graph (or, rather, the underlying simple graph) does *not* have the property alluded to in the previous observation.

Our counting technique is best visualized by introducing the *Whitehead tree* $WT(u)$ associated to the graph $Wh(u)$. The Whitehead tree $WT(u)$ is an infinite rooted labeled tree; the root (level 0) is labeled 1; $2r$ vertices at level 1 are labeled by x_i or x_i^{-1}, $1 \le i \le r$, and a parent vertex at a level $k \ge 1$ labeled x_i is connected to a child vertex at the level $(k+1)$ labeled x_j if and only if there is an edge from the vertex x_i to the vertex x_j^{-1} in the graph $Wh(u)$ (or, equivalently, if u has a subword $x_i x_j$). Thus, by computing the growth function of the tree $WT(u)$ (i.e., by counting elements at a level n as a function of n), we find (or estimate) the number of words u of length n having the Whitehead graph with a particular underlying simple graph.

Now the problem of finding the growth function of the tree $WT(u)$ can be translated into a system of (linear) recurrence relations as follows. Let j_n (resp. $\overline{j_n}$) be the number of vertices labeled x_j (resp. x_j^{-1}) at the level n of the tree $WT(u)$. Then, based on the Whitehead graph $Wh(u)$, it is easy to write down recurrence relations for all j_{n+1} and $\overline{j_{n+1}}$ in terms of appropriate i_n and $\overline{i_n}$. All these recurrence relations are obviously linear, so one can employ a well studied theory of systems of linear recurrence relations to solve for all j_n and $\overline{j_n}$.

Solving a system like that basically amounts to finding eigenvalues of the matrix of this system, usually called the *transition matrix*. (Note that all entries of this matrix are nonnegative.) In fact, since we are only interested in the *growth* of $\sum_n (j_n + \overline{j_n})$, we only need the maximum real positive eigenvalue (the Perron-Frobenius eigenvalue) of the transition matrix; this will determine the growth type of the tree $WT(u)$.

Of course, a system like that is, in general, too big; it has $2r$ equations. In most practical situations however the set of vertices of the Whitehead graph $Wh(u)$ can be split into a union of a few (large) sets, and then one can write recurrence relations (still linear) for the numbers of elements in these sets, thus getting a reasonable number of equations. We illustrate this in the following section.

Finally, we mention that some sets of elements of F_r can be interpreted as Markov processes whose transition matrices arise in a way similar to

what we described above (we refer to [4] for details). It is conceivable that sets like that are precisely *graphic sets* in the sense of [3].

3 Proof of the main result

Let $u \in F_r$, and let $\overline{Wh(u)}$ be the underlying simple graph of the Whitehead graph $Wh(u)$ (in particular, $\overline{Wh(u)}$ is not oriented and has no loops or multiple edges).

There are two principal cases to consider:

Case 1. There is a vertex of degree 1 in $\overline{Wh(u)}$.

Case 2. The degree of any vertex of the graph $\overline{Wh(u)}$ is ≥ 2.

In Case 1, suppose that, say, the vertex of $\overline{Wh(u)}$ corresponding to the generator x_1 has degree 1. That means u, considered as a cyclic word, has the form $u = u(x_1 x_j, x_2, ..., x_r)$ for some $j \neq 1$. Then the vertex corresponding to x_j^{-1} may have any degree $\leq 2r-1$, whereas other vertices have degrees $\leq 2r-2$.

Thus, the greatest possible number of edges in the graph $\overline{Wh(u)}$ occurs if $\overline{Wh(u)}$ has one vertex of degree 1, one vertex of degree $2r-1$, and $2r-2$ vertices of degree $2r-2$. To produce the corresponding transition matrix, we let a_n be the number of vertices labeled x_1 in the nth level of the Whitehead tree $WT(u)$, b_n the number of vertices labeled x_j^{-1}, c_n the number of vertices labeled x_j, and r_n the number of vertices labeled by other letters. Then we have the following system of linear recurrence relations:

$$\begin{cases} a_{n+1} = b_n + c_n + r_n \\ b_{n+1} = b_n + r_n \\ c_{n+1} = a_n + c_n + r_n \\ r_{n+1} = b_n \cdot (2r-3) + c_n \cdot (2r-4) + r_n \cdot (2r-4) \end{cases} \tag{1}$$

Here we are assuming that $n \geq 1$ and use the initial conditions $a_1 = b_1 = c_1 = 1$, and $r_1 = 2r-3$.

To explain, say, the last recurrence relation, we note that, given the assumptions of Case 1, u cannot have a subword $x_j x_1^{-1}$. Then, since r_{n+1} is the number of vertices labeled by letters other than x_1, x_j, x_j^{-1}, we see that a vertex at the level n labeled by x_j may have (at most) $2r-4$ children at the level $(n+1)$, which is why c_n is multiplied by $2r-4$ in the last recurrence relation.

We also note that the actual value of r_{n+1} is smaller than $b_n \cdot (2r-3) + c_n \cdot (2r-4) + r_n \cdot (2r-4)$ because, say, some vertices labeled x_j may be connected to vertices labeled x_j, and not to vertices labeled by "other"

letters. However, since we are looking for an upper bound, we are allowed to replace the actual value of r_{n+1} by a greater one.

The transition matrix of the system (1) is

$$\begin{pmatrix} 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 2r-3 & 2r-4 & 2r-4 \end{pmatrix}.$$

The characteristic polynomial of this matrix is $\lambda(\lambda^2-1)(\lambda-(2r-2))+1$, which completes the proof in Case 1.

In Case 2, we start with a simple

Lemma 3.1. Let $r \geq 2$. Suppose the degree of any vertex of a simple graph Γ with $2r$ vertices is ≥ 2. If Γ has either at least two vertices of degree $2r-2$ or at least one vertex of degree $2r-1$, then any two vertices of Γ can be included in a simple circuit.

Proof. Let v_1 and v_2 be two vertices of degree $2r-2$. If they are not adjacent, then they both must be adjacent to all other vertices of the graph Γ. Then, given any two vertices w_1 and w_2 of Γ, we can include them in the simple circuit $w_1 \to v_2 \to w_2 \to v_1 \to w_1$.

If v_1 and v_2 are adjacent, then there might be a vertex w which is not adjacent to either v_1 or v_2 (or both). Suppose w_1 and w_2 are two vertices of Γ. If they both are different from w, then they obviously can be included in a simple circuit. Now suppose, say, $w_1 = w$. Consider two cases:

(a) w is adjacent to either v_1 or v_2; without loss of generality assume that w is adjacent to v_1. Since the degree of any vertex of Γ is ≥ 2, w must be adjacent to at least one other vertex. If w is adjacent to w_2, we get a simple circuit $w \to w_2 \to v_2 \to v_1 \to w$. If w is adjacent to a vertex $w_3 \neq w_2$, we get a simple circuit $w \to w_3 \to v_2 \to w_2 \to v_1 \to w$.

(b) w is *not* adjacent to either v_1 or v_2. Since the degree of any vertex of Γ is ≥ 2, w must be adjacent to at least two vertices w_3 and w_4. The case where w is adjacent to w_2 is easy (cf. (a) above), so suppose $w_3 \neq w_2$, $w_4 \neq w_2$. Then we get a simple circuit $w \to w_4 \to v_1 \to w_2 \to v_2 \to w_3 \to w$.

The case where Γ has a vertex of degree $2r-1$ is similar. $\square$

From Lemma 3.1, we see that if $u \in F_r$ is a primitive element, then at most one vertex of the graph $\overline{Wh(u)}$ can have degree $2r-2$, and there are no vertices of degree $2r-1$. If there are no vertices of degree $2r-2$, then the number of elements of length n with the graph $\overline{Wh(u)}$ like that is obviously bounded by $(2r-3)^n$, so there is nothing to prove.

Thus, the greatest possible number of edges in $\overline{Wh(u)}$ occurs if $\overline{Wh(u)}$ has one vertex of degree $2r-2$, and $2r-1$ vertices of degree $2r-3$. We note in passing that, in fact, this cannot happen because, if all vertices of

$\overline{Wh(u)}$ have degrees $\geq 2r-3$, then, since $2r-3 \geq \frac{2r}{2}$ when $r \geq 3$, $\overline{Wh(u)}$ must be Hamiltonian by a classical result of Ore (see e.g. [7, Theorem 7.1, Corollary 7.2]). A Hamiltonian graph cannot have a cut vertex. However, since we are looking for an upper bound, this is legitimate.

Let now the vertex of degree $2r-2$ have label x_1. It is easy to see (by induction on the level number) that, for any element u whose graph $\overline{Wh(u)}$ has properties mentioned above, at every level of the Whitehead tree $WT(u)$ one has at least $2r-4$ times as many vertices labeled $x_i, i \neq 1$, as one does vertices labeled x_1. We therefore have the following inequalities for the numbers r_n of vertices at level n:

$$r_{n+1} \leq \frac{1}{2r-3} \cdot r_n \cdot (2r-2) + \frac{2r-4}{2r-3} \cdot r_n \cdot (2r-3) = r_n \cdot (2r-3+\frac{1}{2r-3}).$$

Thus, $r_n \leq c \cdot (2r-3+\frac{1}{2r-3})^n$ for some constant c in this case. Since, if $r \geq 3$, $2r-3+\frac{1}{2r-3}$ is smaller than the greatest real root of $\lambda(\lambda^2-1)(\lambda-(2r-2))+1$, this completes the proof in Case 2.

Finally, we note that in the course of our proof we have actually counted *cyclically reduced* primitive elements of F_r. The result however holds for the number $P(r,n)$ of *all* primitive elements as well because for $r \geq 3$, the number of cyclically reducible primitive elements of a given length n is easily seen to be smaller than the number of cyclically reduced primitive elements of the same length (cf. [5]). This completes the proof of the theorem. $\square$

References

[1] G. Baumslag, A. G. Myasnikov, V. Shpilrain, *Open problems in combinatorial group theory. Second edition*, Contemp. Math., Amer. Math. Soc. **296** (2002), 1–38.

[2] A. Borovik, A. G. Myasnikov, and V. Shpilrain, *Measuring sets in infinite groups*, Contemp. Math., Amer. Math. Soc. **298** (2002), 21–42.

[3] J. Burillo, E. Ventura, *Counting primitive elements in free groups*, Geom. Dedicata **93** (2002), 143–162.

[4] I. Kapovich, P. Schupp, V. Shpilrain, *Generic properties of the Whitehead algorithm, stabilizers in $Aut(F_k)$ and one-relator groups*, preprint.
http://arxiv.org/abs/math.GR/0303386

[5] A. G. Myasnikov, V. Shpilrain, *Automorphic orbits in free groups*, J. Algebra **269** (2003), 18–27.

[6] I. Rivin, *A Remark on "Counting primitive elements in free groups" (by J. Burillo and E. Ventura)*, Geom. Dedicata, to appear.

[7] R. J. Wilson, *Introduction to Graph Theory*, Pearson, 1996.

Department of Mathematics, The City College of New York, New York, NY 10031
e-mail address: shpil@groups.sci.ccny.cuny.edu
http://www.sci.ccny.cuny.edu/˜shpil/