1991

On identifying the identity in a group

Karlene R. Jenson
San Jose State University

Order Number 1344280

On identifying the identity in a group

Jensen, Karlene Rae, M.S.

San Jose State University, 1991

U·M·I
300 N. Zeeb Rd.
Ann Arbor, MI 48106

ON IDENTIFYING THE IDENTITY IN A GROUP

A Thesis

Presented to

The Faculty of the Department of Mathematics

San Jose State University

In Partial Fulfillment

of the Requirements for the Degree

Master of Sciences

By

Karlene R. Jensen

May, 1991

APPROVED fOR THE DEPARTMENT OF MATHEMATICS

Eloise Hamann

Dr. Eloise Hamann

Roger Alperin

Dr. Roger Alperin

Brian Peterson

Dr. Brian Peterson

APPROVED FOR THE UNIVERSITY

Serena W. Stanford

TABLE OF CONTENTS

ABSTRACT

ON IDENTIFYING THE IDENTITY IN A GROUP

by Karlene R. Jensen

This thesis addresses the following two questions. The word problem: Can one decide in a finite number of steps whether a word in a finitely generated group is trivial or not? This thesis will prove that there is a finitely presented group with an unsolvable word problem by embedding a recursively presented group with an unsolvable word problem in a finitely presented group.

The Burnside problem: Can a finitely generated group be such that every element has finite order, but the group is infinite? The focus is on the Burnside problem when the orders of elements are bounded. The methods discussed involve showing whether high order commutators are trivial or not. Finally, an example of a finitely generated 3-group which is infinite is given.

INTRODUCTION

Around the turn of the century two important group theoretical questions were raised. They both involve determining if a word in a group is equivalent to the identity. The historical developments of these two questions are chronicled below.

The first of these two questions was formulated by W. Burnside in 1902. Can a finitely generated group be such that every element has finite order, but the group is infinite?

Then in 1911, Max Dehn formulated the second question, the so called *word problem.* Let a group G be defined by means of a given presentation. For an arbitrary word w in the generators, can we decide in a finite number of steps whether w defines the identity element of G, or not?

During the 1930's and 1940's the finiteness of groups where every element has order a divisor of a specific n was studied. If n = 3, or 4, or 6, then the finitely generated group was shown to be finite. In 1950 W. Magnus restricted the scope of the general Burnside problem further by asking if there is a bound on the order of finite quotients of finitely generated groups where every element has order a divisor of a specific integer?

Dehn's word problem was proven to be unsolvable in general by Novikov in 1952 for recursively presented groups. Then in 1961, Higman proved that a recursively presented group can be embedded in a finitely presented group. Thus having a finite set of defining relations is insufficient for the word problem to be solvable, hence finitely presented is not enough to guarantee solvability of the word problem.

Finally, the general Burnside question was resolved by Golod, in 1964. He proved the existence of finitely generated infinite p-groups for all primes answering the general Burnside question in the positive.

Even though the general Burnside problem has been solved, the unsolvability of the word problem for certain groups and classes of finitely presented groups tells us that there is no procedure for solving the word problem which will work for every group. Since to show that a group is finite may well involve showing many words are the identity, we see the methods must be particular to the type of group. Thus, the Burnside problem seems to need special tools.

In part 1, we discuss the word problem in which we try to determine whether in a finite number of steps a word in a group G can be shown to be trivial or not. We also show the existence of a finitely presented group with an unsolvable word problem. The second part of this paper discusses the finiteness of the so called Burnside group. Here we will try to determine whether a specific type of word in the group, a high order commutator, is trivial or not. If the general Burnside question were false then there would be many more relations equivalent to the identity and the Burnside question would not be so complicated. In the last part of the paper we show that the answer to the General Burnside question is yes by proving the existence of a finitely generated infinite 3-group using tree automorphisms.

PART I: THE WORD PROBLEM

Introduction

A presentation $G = \langle a, b, c, \ldots; P, Q, R\rangle$, no matter how strange the defining relators, always determines a unique group (up to isomorphism). However, there may arise great difficulties as soon as we wish some more specific information about the group G, such as whether G is abelian or finite.

Part of the trouble is that the definition of equivalence of words used to obtain G is non-constructive. For example, if G is finitely generated, then G is abelian if and only if the words $aba^{-1}b^{-1}$, $aca^{-1}c^{-1}$, ..., $bcb^{-1}c^{-1}$, ... all define the identity element in G. If we have a constructive procedure for determining whether or not a word defines the identity element in G, we would be able to decide whether G is abelian.

Definition: A *decision procedure* for E a subset of A is a method by which, given any element $a \in A$ we can decide in a finite number of steps whether or not $a \in E$. Whether such a procedure exists is called the decision problem.

The decision problem is clearly equivalent to the following. Given a group G, can we find a method, by which given an element $g \in G$, we can decide in a finite number of steps whether or not $g = e$, or prove that no such method exists? This is what Dehn refers to as the word problem.

We show that the word problem for a finitely generated free group is solvable. Consider the free group generated by $\{x_1,\ldots,x_n\}$. Let $w = x_{v_1}^{\varepsilon_1}\ldots x_{v_p}^{\varepsilon_p}$ $(\varepsilon_i = \mp 1;\ v_i = 1,\ldots,n)$. We inductively define a process ρ whereby we freely reduce any consecutive occurrences of $x_v^{\varepsilon}x_v^{-\varepsilon}$ as follows:

$\rho(1) = 1$, $\rho(x_v^{\varepsilon}) = x_v^{\varepsilon}$ $(\varepsilon = \mp 1,\ v = 1,\ldots,n)$, and if

$\rho(U) = x_{u_1}^{\eta_1}\ldots x_{u_q}^{\eta_q}$ $(\eta_i = \mp 1;\ u_i = 1,\ldots,n)$ then

$$\rho(Ux_v^{\varepsilon}) = x_{u_1}^{\eta_1}\ldots x_{u_q}^{\eta_q}x_v^{\varepsilon} \text{ if } u_q \neq v \text{ or } \eta_q \neq -\varepsilon$$
$$= x_{u_1}^{\eta_1}\ldots x_{u_{q-1}}^{\eta_{q-1}} \text{ if } u_q = v \text{ and } \eta_q = -\varepsilon.$$

For example, let $w = x_1x_2^{-1}x_3x_3^{-1}x_2x_1$. Then $\rho(x_1) = x_1$,
$\rho(x_1x_2^{-1}) = x_1x_2^{-1}$, $\rho(x_1x_2^{-1}x_3) = x_1x_2^{-1}x_3$,
$\rho(x_1x_2^{-1}x_3x_3^{-1}) = x_1x_2^{-1}$, $\rho(x_1x_2^{-1}x_3x_3^{-1}x_2) = x_1$,
$\rho(x_1x_2^{-1}x_3x_3^{-1}x_2x_1) = x_1^2$. Since only trivial relations hold in a free group, we can determine in a finite number of steps whether or not $\rho(w) = 1$.

Let us introduce some terminology that will be used throughout the discussion. As there are many definitions and notations introduced throughout part 1, the reader may wish to use the material in the appendix as an aid in their reading.

Notation: Let [A] designate the free group on a set A.

A subset A of a group G is free if the homomorphism from [A] to G which is the identity on A is injective. In this case we identify the subgroup {A} (the subgroup generated by A) of G with [A]. This identification simplifies a number of discussions throughout the paper.

A relation on A is an expression X = Y where X and Y are words on A. This relation *holds* in a factor group [A]/ K if X and Y lie in the same coset of K (equivalently $XY^{-1} \in K$).

Let R be a set of relations on A. A relation on A is a *consequence* of R if it holds in every factor group of [A] in which all the relations in R hold. The set of consequences of R is denoted by C(R). There is a unique factor group [A]/ K_R of [A] in which the relations which hold are just the consequences of R; K_R is the normal subgroup generated by the XY^{-1} for X = Y in R. We call [A]/ K_R the group with the set of generators A and the set of defining relations R, and designate it by [A;R].

This notation [A;R] can be extended to allow several generators before the semicolon and several relations or sets of relations after the semicolon. Thus [A,t ; R,X=Y] has the set of generators A ∪ {t} and the set of defining relations R ∪ {X=Y}. It is understood that no generator is repeated. If A appears before the semicolon and a appears after the semicolon, it is understood that a varies through A.

Since [A] is a subgroup of [A,B] and K_R is a subgroup of $K_{R \cup S}$, there is a natural homomorphism from [A;R] to [A,B ; R,S] which maps the coset of a word on A into the coset of that word in [A,B ; R,S]. If this homomorphism is bijective, we identify the two groups.

A group G is isomorphic to a factor group of [G] and hence with the group [G;R_G] where R_G is the set of all relations on G.[1]

Definition: A group is *finitely presented* if it is isomorphic to a group [A;R] where both A and R are finite.

Definition: C(R) is *recursive* iff given any word w on A, there is some finite set of instructions that will decide whether or not $w \in C(R)$.

If C(R) is recursive then we can determine in a finite number of steps whether a word is a consequence of the defining relations or it is not.

Definition: The word problem for G = [A;R] is *solvable* iff C(R) is recursive.

Definition: C(R) is *recursively enumerable* iff there is some finite set of instructions such that given any word

---

[1] If G appears before the semicolon, it is understood that the relations in R are among the defining relations even if they do not appear explicitly after the semicolon.

w on A, will eventually determine if $w \in C(R)$.

If C(R) is recursively enumerable then given any word w in G, we may never be able to determine if w is not an element of C(R). That is, the procedure might produce the result $w \notin C(R)$, or it might go on forever without producing that $w \in C(R)$ if $w \notin C(R)$.

Definition: A group is *recursively presented* if it is isomorphic to a group [A;R] where A is finite and R is recursively enumerable.

Every recursive set is recursively enumerable. To see this, suppose R was a procedure that was recursive. Then upon every input it would respond with a yes or no response. If we restrict R to output only yes responses then R would be recursively enumerable. The converse is not true.

If G is a finitely generated group then G is isomorphic to [A;R] = [A;C(R)] with A finite. Therefore it suffices to talk about the solvability of the word problem for [A;R].

Suppose that [A;R] is a subgroup of [B;S] where both A and B are finite. We will show that C(R) is recursive if C(S) is recursive. Let ϕ be a monomorphism from [A;R] into [B;S], then X = Y in [A;R] iff $\phi(X) = \Phi(Y)$ in [B;S]. Let T be the procedure that takes the elements of A to words on B. T is recursive since both A and B are finite. Suppose that C(S) is recursive, then there is a procedure P that will decide in a finite number of steps whether a word w on B is an elements of C(S) or not. Now, let P′ be the following procedure: for a word w on A decide whether T(w) is an element of C(S) or not by the recursive procedure P. Then T(w) is an elements of C(S) iff w is an element of C(R). Hence P′ determines in a finite number of steps whether a word w on A is an element of C(R) or not, so C(R) must be recursive. As a consequence, if the word problem for [B;S] is solvable then the word problem for [A;R] is solvable.

Next we show that a finitely generated subgroup of a recursively presented group is recursively presented. Let G = [B;R] = [B;C(R)] where B is finite and R is recursively enumerable. Then C(R) is the set of relations on G closed under consequences and is recursively enumerable. There is a procedure T that will recursively enumerate the elements of C(R). That is, at step k T will produce $r_1, r_2, \ldots ,r_k$. Let H be a finitely generated subgroup of G. We wish to show that H = [A;C(S)] where A is finite and C(S) is recursively enumerable. Since the elements of A need not be a subset of B, then the relations of H must be on elements of A. Let L be the recursive procedure that lists all words on A of length 1, length 2, etc., where each letter x in A is written as a word on B. Create the procedure P as follows: at step i 1) enumerate the first i words in C(R) by the recursively enumerable procedure T, and 2) enumerate the first i words according to the recursive procedure L. Then a word w on the set B is in C(S) if $w \in C(R)$ and w is a word on A. Since P recursively enumerates the elements of C(S) then H is recursively presented.

A Finitely Presented Group with an Unsolvable Word Problem

The combined results of Novikov and Higman proved that the word problem is unsolvable in general for a finitely presented group G. In order to describe this group we must discuss some properties about the amalgamation of groups.

Let G and G′ be groups and let Φ be an isomorphism of a subgroup H of G and a subgroup H′ of G′. The free product of the groups G and G′ with the *amalgamation* Φ is the group

$$G *\Phi\ G' = [G, G'; h = \Phi(h)].$$

The natural mapping of G and G′ into G *Φ G′ are injective; so we identify G and G′ with their images under these mappings. Then H and H′ are identified via the isomorphism Φ. We have $G *\Phi\ G' = \{G, G'\}$ and

$$G \cap G' = H = H'.$$

This last group is called the *amalgam.*

Some useful properties about amalgams that will be used later in the discussion are presented below.

Let T consist of one element in each right coset of H in G other than H itself; and let T′ be formed similarly from H′ in G′. A word on $G \cup G'$ is in *normal form* if it is $ht_1t_2 \ldots t_n$ where $h \in H$; $t_1, t_2, \ldots t_n \in T \cup T'$ and $t_i \in T$ iff $t_{i+1} \in T'$ for $1 \le i < n$.

It can be shown that every right coset not equal to H in $G *_\Phi G'$ contains exactly one word in normal form. The existence of a word in normal form in each right coset is straightforward to see since every $w \in G *_\Phi G' = g_1 g_2 \cdots g_n$ where $g_i \in G$ iff $g_{i+1} \in G'$, and every $g_i = h_i t_j$ is in G so $g_{i-1} h_i \in G'$ and $w = h_{i-1} t'_k$ for some t'_k. The uniqueness follows from the use of Schreier's systems and Schreier's lemmas [Hall, Theory of Groups, 94-106].

Let $H \cong H'$ by Φ; let K and K' be subgroups of G and G' respectively such that $\Phi(H \cap K) = \Phi(H) \cap K'$. Then K and K' have the same intersection with the amalgam in $G *_\Phi G'$. Define $\varphi = \Phi|_{(H \cap K)}$. Then φ is an isomorphism between $H \cap K$ and $\Phi(H) \cap K'$. Thus we can form the amalgamation $K *_\varphi K'$ and there is a natural mapping λ from $K *_\varphi K'$ to $G *_\Phi G'$ whose image is $\{K,K'\}$. We show that λ is injective. Let T contain one element in each coset of $K/H \cap K$ other than $H \cap K$ itself. Let T' be formed similarly. Then the words on $K \cup K'$ in normal form are words among the words on $G \cup G'$ in normal form. Thus it follows from uniqueness that λ is injective.

We can thus identify $K *_\varphi K'$ with $\{K,K'\} \subset G *_\Phi G'$ and

$$G \cap \{K,K'\} = K. \tag{1}$$

To see this it suffices to show that $G \cap \{K,K'\} \leq K$. So let $g \in G \cap \{K,K'\}$. An element $g \in G$ is in normal form if $g = h$ or $g = ht$ with $t \in T$ where T consists of elements from cosets of G/H not including H. If g is in normal form in

$K *_\varphi K'$ then $h \in H \cap K$ and $t \in K$, so $g \in K$.

Notation: If Φ is the isomorphism of the zero subgroups, we write $G * G'$ for $G *_\Phi G'$ and call $G * G'$ the free product of G and G'. Thus $G * G' = [G,G']$. Now let G and G' be subgroups of some larger group, L. Let $H = G \cap G'$, and let Φ be the identity mapping from H to H. Then there is a unique homomorphism from $G *_\Phi G'$ to L which is the identity on G and G' and whose image is $\{G,G'\}$. If this homomorphism is injective, we identify $G *_\Phi G'$ and $\{G,G'\}$ and say that $\{G,G'\}$ is the free product of G and G' with the amalgam H.

Now we are ready to describe Novikov's group which is a recursively presented group with an unsolvable word problem. Let E be a recursively enumerable subset of the integers, which is not recursive. These sets are known to exist [Enderton; 235 - 238]. Let H be the subgroup of $G = [a,b]$ generated by the $a^n b a^{-n}$ for $n \in E$. Let Φ be the identity mapping from H to H. Letting G_1 be an isomorphic copy of G we have

$$G *_\Phi G_1 = [a,b,a_1,b_1 : a^n b a^{-n} = a_1^n b_1 a_1^{-n} \text{ for } n \in E]$$

which is clearly recursively presented.

In this group $a^n b a^{-n} = a_1^n b_1 a_1^{-n}$ iff $n \in E$. To see this, since the $a^m b a^{-m}$ are free then if $a^m b a^{-m} = a_1^m b_1 a_1^{-m}$, then $m \in E$ and if $n \in E$ then $a^n b a^{-n} = a_1^n b_1 a_1^{-n}$.

As a result of this relation, $a^n b a^{-n} = a_1^n b_1 a_1^{-n}$ iff

$n \in E$, the decision problem for E is equivalent to the word problem for $G *\Phi G' = [a,b,a_1,b_1;R]$ where $R = \{a^n b a^{-n} = a_1^n b a_1^{-n},\ n \in E\}$ is recursively enumerable. Recall that the word problem for [A;R] is the decision problem for C(R). Since C(R) is the set of relations holding in $G *\Phi G'$, this is also the word problem for $G *\Phi G'$. Therefore, since the relations R in [A;R] are nonrecursive (specifically only recursively enumerable), then C(R) is nonrecursive and so the word problem for $G *\Phi G'$ is unsolvable.

However, $G *\Phi G'$, or as we call Novikov's group is not a finitely presented group. We will, however, embed $G *\Phi G'$ in a finitely presented group. The rest of part 1 addresses the embedding problem.

Higman's Theorem

Higman's Theorem: A finitely generated group is embeddable in a finitely presented group iff it is recursively presented.

The forward direction of the proof is straightforward. By the work from the last section a finitely generated subgroup of a recursively presented group is recursively presented. Hence, if a finitely generated group is embedded in a finitely presented group then it is isomorphic to a recursively presented subgroup. Thus the embedeed group must be recursively presented since every finitely presented group is recursively presented.

The proof of the other direction will take the remainder of part 1.

Definition: A group is *Higman* if it is finitely generated and embeddable in a finitely presented group.

Two useful properties about direct products of Higman groups and amalgamations of Higman groups are presented below.

Lemma 1: If G and H are Higman groups, then $G \times H$ is Higman.

Proof: $G \times H = [G,H \mid gh = hg]$, thus $G \times H$ is finitely generated. If G and H are embeddable in finitely presented groups L and M respectively, then $G \times H$ is embeddable in $L \times M$.■

Lemma 2: If G and G' are Higman groups and Φ is an isomorphism from a finitely generated subgroup of G into G', then $G *_\Phi G'$ is Higman.

Proof: Clearly $G *_\Phi G'$ is finitely generated. Let G and G' be embeddable in the finitely presented groups K and K' respectively. Then $G *_\Phi G'$ is embeddable in $K *_\Phi K'$ which is finitely presented since Φ is an isomorphism between two finitely generated subgroups.■

Definition: If Φ is an isomorphism from a subgroup H of G into G then we define $G_\Phi = [G,t \,;\, tht^{-1} = \Phi(h)]$.

Clearly G can be naturally mapped into G_Φ since the relations of G_Φ intersect trivially with G. Therefore we can identify G with a subgroup of G_Φ. We also identify t with its coset in G_Φ and call t the Φ-*element*. If Φ is the identity mapping on a subgroup K of G then we say G_K for G_Φ.

First let us see how G_Φ will be used to prove Higman's theorem. Let $[A;R] = G/K$ where K is the normal subgroup generated by XY^{-1} for $X = Y$ in R, let $G_K = [G,t;\, tkt^{-1} = k] = G_i$ (where i is the identity mapping on K), and $\{G,tGt^{-1}\} = G *_i tGt^{-1} \subset G_i$. Clearly $\{G,tGt^{-1}\}$ is embedded in $G_i = G_K$. We next show that $\{G,tGt^{-1}\}$ is embedded in $G_K \times G/K$. First, define a mapping Φ from $\{G,tGt^{-1}\}$ to G/K by $\Phi(g) = gK$ and $\Phi(tgt^{-1}) = eK$. If we restrict the domain of Φ to the amalgam, then $\Phi(G \cap K) =$

$\Phi(tGt^{-1}) \cap K$. Now define a homomorphism ψ from $\{G, tGt^{-1}\}$ to $G_K \times G/K$ by $\psi(x) = (x, \Phi(x))$. We will show that ψ is an isomorphism. Since ψ is clearly injective, then it suffices to show that ψ is a homomorphism. Since Φ is a homomorphism, we have that

$$\psi(xy) = (xy, \Phi(x)\Phi(y)) = (x, \Phi(x))(y, \Phi(y)) = \psi(x)\psi(y)$$

so ψ is a homomorphism. Since G/K is embedded in $(G_K \times G/K)_\psi$, then if we can show that $(G_K \times G/K)_\psi$ is finitely presented for finitely generated G and recursively enumerable K we are done. However, one problem that immediately arises is that we don't know if G_K is finitely presented. If in this case we could show that G_K is finitely presented then we have a chance of showing that $(G_K \times G/K)_\psi$ is finitely presented since the relations that equate elements of K and {e} will be shown later to be among the relations in G_K. We begin this discussion by presenting three general properties about G_Φ.

Property 1: G_Φ is embeddable in a larger group where Φ is an isomorphism of a subgroup H of G into G.

In [G,r], $\{G, rHr^{-1}\}$ is the free product of G and rHr^{-1}. Let G_1 be a copy of G, then in $[G_1,s]$, $\{G_1, s\Phi(H)_1s^{-1}\}$ is the free product of G_1 and $s\Phi(H)_1s^{-1}$. Hence there is an isomorphism ψ of $\{G, rHr^{-1}\}$ and $\{G_1, s\Phi(H)_1s^{-1}\}$ defined by $\psi(g) = g_1$, $\psi(rhr^{-1}) = s\Phi(h)_1s^{-1}$. Then

$$[G,r] *_\psi [G_1,s] = [G,G_1,r,s \ ; \ g = g_1,\ rhr^{-1} = s\Phi(h)s^{-1}]$$

$$= [G,r,s \; ; \; rhr^{-1} = s\Phi(h)s^{-1}]$$
$$= [G,r,s,t \; ; \; rhr^{-1} = s\Phi(h)s^{-1}, \; t = s^{-1}r]$$
$$= [G,r,s,t \; ; \; tht^{-1} = \Phi(h), \; t = s^{-1}r]$$
$$= [G,r,s,t \; ; \; tht^{-1} = \Phi(h), \; r = st]$$
$$= [G,s,t \; ; \; tht^{-1} = \Phi(h)]$$
$$= [G_\Phi,s].$$

Thus G_Φ is embeddable in $[G,r] *\psi [G_1,s]$ and there is an isomorphism from G_Φ into $[G,r] *\psi [G_1,s]$ which maps the coset of g into g and maps t into $s^{-1}r$.

Since $\{G,rGr^{-1}\}$ is the free product of G and rGr^{-1} in $[G,r]$, we have similar to the results obtained from equation (1), page 10,

$$\{G,rHr^{-1}\} \cap rGr^{-1} = rHr^{-1}.$$

Similary, in $[G_1,s]$ we have

$$\{G_1,s\Phi(H)_1s^{-1}\} \cap sG_1s^{-1} = s\Phi(H)_1s^{-1}.$$

Then it follows that $rGr^{-1} *\psi sG_1s^{-1}$ is embedded in $[G,r] *\psi [G,s]$ as $\{rGr^{-1},sG_1s^{-1}\} = \{rGr^{-1},sGs^{-1}\}$ which is the free product of rGr^{-1} and sGs^{-1} with the amalgam $rHr^{-1} = s\Phi(H)s^{-1}$.

Recalling that $r^{-1}s = t$ and applying the inner automorphism under conjugation by r^{-1} on $\{rGr^{-1},sGs^{-1}\}$ we get that $\{G,tGt^{-1}\}$ is the free product of G and $t^{-1}Gt$ with the amalgam $\Phi(H) = tHt^{-1}$. Hence,

$$G \cap tGt^{-1} = H \text{ in } G_\Phi. \qquad (2)$$

Let G, Φ, and H be as above. A subgroup K of G is *invariant* under Φ if

$$\Phi(H \cap K) = \Phi(H) \cap K.$$

If K is invariant under Φ, then $\Phi' = \Phi|_{(H \cap K)}$ is an isomorphism in K. This leads us to the next property.

Property 2: $K_{\Phi'}$ is embedded in G_{Φ} where the above situation holds.

Since G_{Φ} is embedded in $[G,r] *\psi [G_1,s]$ by the proof of property 1 it can be shown similarly that $K_{\Phi'}$ is embedded in $[K,r] *\psi' [K_1,s]$ where $\psi' = \psi|_K$. Then it will suffice to show that there is a one to one mapping from $[K,r] *\psi' [K_1,s]$ to $[G,r] *\psi [G_1,s]$ which will make the following diagram commute.

$$\begin{array}{ccc} [K,r] *\psi' [K_1,s] & \dashrightarrow & [G,r] *\psi [G_1,s] \\ \text{1-1} \updownarrow & & \updownarrow \text{1-1} \\ K_{\Phi'} & \dashrightarrow & G_{\Phi} \end{array}$$

Clearly, $[K,r]$ is embedded in $[G,r]$ as $\{K,r\}$ and $[K_1,s]$ is embedded in $[G_1,s]$ as $\{K_1,s\}$. Hence we must check that $\{K,r\}$ and $\{K,s\}$ have the same intersection with the amalgam. Recall that the normal form of an element of the free product $\{G,rHr^{-1}\}$ is of the form $\ldots g_1rh_1r^{-1}g_2rh_2r^{-1}\ldots$. This is a normal form of a word in $[G,r]$ and is in $[K,r]$ iff g_i and h_i are in K. Thus

$$\{K,r\} \cap \{G,rHr^{-1}\} = \{K,r(H \cap K)r^{-1}\}. \qquad (3)$$

Similarly we get,

$$\{K_1,s\} \cap \{G_1,s\Phi(H)_1 s^{-1}\} = \{K_1,s(\Phi(H)_1 \cap K_1)s^{-1}\}. \qquad (4)$$

Since K is invariant under Φ,

$$\{K_1,s(\Phi(H)_1 \cap K_1)s^{-1}\} = \{K_1,s(\Phi(H \cap K\ )_1 s^{-1}\}$$
$$= \{K_1,\psi(r(H \cap K)r^{-1})\}$$
$$= \psi(\{K,r(H \cap K)r^{-1}\}).$$

Thus the right-hand sides of (3) and (4) correspond under ψ so that $\{K,s\}$ and $\{K_1,r\}$ agree when restricted to the amalgam as required. Hence $[K,r] *\psi' [K_1,s]$ is embedded in $[G,r] *\psi [G_1,s]$ and the diagram commutes so that K_{Φ}, is embedded in G_{Φ} as $\{K,t\}$. It follows from (1) of the previous section that

$$\{K,r,s\} \cap \{G,r\} = \{K,r\}. \qquad (5)$$

Since $\{K,r\} = K * [r]$ as a subgroup of $G * [r]$ then again by (1) we have

$$\{K,r\} \cap G = K.$$

Combining these with (5) we get that

$$\{K,r,s\} \cap G \subset K.$$

Thus since $K \subset \{K,r,s\} \cap G$ it follows that

$$\{K,t\} \cap G = K. \qquad (6)$$

Property 3: Suppose that we have a set Φ, ψ, ... of isomorphisms in G, then G is naturally embedded in $G_{\Phi,\psi,\ldots}$ where

$$G_{\Phi,\psi,\ldots} \equiv [G,t_{\Phi,\ldots}\ ;\ t_{\Phi}ht_{\Phi}^{-1} = \Phi(h),\ldots].$$

Suppose there is no natural embedding, then some relation $g = g'$ holds in $G_{\Phi,\psi,\ldots}$ which does not hold in G; and it must be a consequence of a finite number of defining relations. Therefore, we need only consider the case in which there are finitely many isomorphisms. This is easily proven by induction since

$$G_{\Phi_1,\Phi_2,\ldots,\Phi_n} = (G_{\Phi_1,\Phi_2,\ldots,\Phi_{n-1}})_{\Phi_n}.$$

If K is a subgroup of G invariant under all the Φ_1, $\Phi_2,\ldots$ then we will show that

$$\{K,t_1,t_2,\ldots\} \cap G = K$$

where t_i denotes t_{Φ_i}. Clearly the right hand side is included in the left. Since an element of $\{K,t_1,t_2,\ldots\}$ is already generated by K and a finite number of the t's, we need only prove the reverse inclusion for a finite number of isomorphisms. The case for n = 1 was (6). Assume true for n = j, then $\{K,t_1,t_2,\ldots,t_j\} \cap G = K$. Since each t_i is invariant under any other Φ_r, in particular Φ_{j+1} then by (6)

$$\{K,t_1,t_2,\ldots,t_{j+1}\} \cap G_{\Phi_1,\ldots\Phi_j} = \{K,t_1,t_2,\ldots,t_j\}$$

in $G_{\Phi_1,\ldots\Phi_{j+1}}$. Now intersecting both sides by G we get

$$\{K,t_1,t_2,\ldots,t_{j+1}\} \cap G \subset K.$$

Thus any subgroup K of G is invariant under all the Φ_i such that $\{K,t_1,t_2,\ldots\} \cap G = K$.

Let G be a Higman group. An isomorphism Φ in G is *benign* if G_Φ is Higman. A subgroup H of G is benign if G_H is Higman (ie: the identity mapping of H to H is Higman).

Some relevant lemmas about benign subgroups follow.

Lemma 3: If G is a Higman group, and Φ is an isomorphism of a finitely generated subgroup H of G into G, then Φ is benign in G.

Proof: Clearly, [G,r] and $[G_1,s]$ are Higman. Since G and rHr^{-1} are finitely generated then $[G,r] *\psi [G_1,s]$ is Higman where ψ is the isomorphism of $\{G,rHr^{-1}\}$ and $\{G_1,s\Phi(H)_1s^{-1}\}$ as in the proof of property 1. Hence its finitely generated subgroup G_Φ is Higman. It follows that a finitely generated subgroup of a Higman group G is benign in G.∎

Lemma 4: Let L be a Higman group and let G be a Higman subgroup of L. Then an isomorphism Φ in G is benign in G iff it is benign in L. Hence a subgroup of G is benign in G iff it is benign in L.

Proof: Suppose L_Φ is Higman. Then G_Φ is embeddable in L_Φ by property 2 and hence, is Higman. Going the other way, suppose that G_Φ is Higman. If $\psi(g) = g_1$, then $G_\Phi *\psi L_1$ is Higman. Let H be the domain of Φ, then

$$\begin{aligned} G_\Phi *\psi L_1 &= [G,t,L_1\colon tht^{-1} = \Phi(h),\ g = g_1] \\ &= [G_1,t,L_1\colon th_1t^{-1} = \Phi(h)_1,\ g = g_1] \\ &= [L_1,t : th_1t^{-1} = \Phi(h)_1] \cong L_\Phi.\blacksquare \end{aligned}$$

Lemma 5: If H and K are benign subgroups of the Higman group G, then 1) $H \cap K$ and 2) $\{H,K\}$ are benign in G.

Proof: First suppose K is finitely generated, hence

Higman (by Lemma 3). Then if Φ is the identity mapping on H then certainly K is invariant under Φ so $K_{H \cap K}$ is embedded in G_H and is Higman. Thus we have that $H \cap K$ is benign in K whence in G. Thus, 1) holds if K is finitely generated.

We show 2) also assuming that K is finitely generated. Now working in G_H, $\{G, tGt^{-1}\}$ is the free product of G and tGt^{-1} with the amalgam $H = tHt^{-1}$. Since $\{H,K\}$ and tGt^{-1} have the same intersection with the amalgam,

$$\{H,K,tGt^{-1}\} \cap G = \{H,K\},$$

and since $H \subset tGt^{-1}$ we have

$$\{K,tGt^{-1}\} \cap G = \{H,K\}.$$

By our assumption that K is finitely generated then $\{K,t^{-1}Gt\}$ is finitely generated in G_H. Thus by lemma 3 $\{K,t^{-1}Gt\}$ is benign. By the same argument G is benign in G_H. Thus $\{H,K\}$ is benign by our special case for 1) and we have the special case that 2) holds for K finitely generated. However, we need to prove these results without the assumption that K is finitely generated.

In general, we have that $G \cap tGt^{-1} = H$ in G_H; so

$$H \cap K = G \cap (tGt^{-1} \cap K).$$

Since tGt^{-1} is finitely generated then $K_{tGt^{-1} \cap K}$ is embedded in G_H and hence Higman. Thus $tGt^{-1} \cap K$ is benign by the truth for 1) if one subgroup is finitely generated. Similarly, $(tGt^{-1} \cap K)_{G \cap (tGt^{-1} \cap K)}$ is embedded in G_H. So $G \cap (tGt^{-1} \cap K)$ is benign and hence $H \cap K$ is benign, and 1) holds. Now $\{K, tGt^{-1}\}$ is benign since tGt^{-1} is finitely generated and benign. Thus $\{H,K\} = \{K, tGt^{-1}\} \cap G$ is the intersection of two benign subgroups and by 1) is therefore benign. Thus, 2) holds.■

Lemma 6: Let Φ be a homomorphism from the Higman group G to the Higman group L. If H is a benign subgroup of G, then $\Phi(H)$ is a benign subgroup of L. If M is a benign subgroup of L, then $\Phi^{-1}(M)$ is a benign subgroup of G.

Proof: We have shown by lemma 1 that $G \times L$ is Higman. Let Q be the subgroup of $G \times L$ consisting of all $(g, \Phi(g))$. Then Q is isomorphic to G by the mapping $(g, \Phi(g)) \rightarrow g$. Thus Q is finitely generated and benign in $G \times L$. If

$$\Phi(H) = \{\{H,L\} \cap Q, G\} \cap L \text{ in } G \times L, \text{ and}$$

$$\Phi^{-1}(M) = \{\{M,G\} \cap Q, L\} \cap G \text{ in } G \times L$$

then by the previous lemma $\Phi(H)$ and $\Phi^{-1}(M)$ are benign.

$$\begin{aligned}\{\{H,L\} \cap Q, G\} \cap L &= \{(H \times L) \cap Q, G\} \cap L \\ &= \{\{(h, \Phi(h))\}, G\} \cap L \\ &= [G \times \Phi(H)] \cap L \\ &= \Phi(H).\end{aligned}$$

Here G, H, and L have been identified with $G \times \{e\}$, $H \times \{e\}$, and $\{e\} \times L$. $\Phi^{-1}(M) = \{\{M,G\} \cap Q, L\} \cap G$ can be shown similarly.■

Lemma 7: If Φ is an isomorphism of the Higman group G into G and H is a benign subgroup of G then $\Phi|_H$ is benign in G.

Proof: G_Φ is Higman by lemma 3. Since $G_\Phi = [G,s\ ;\ \Phi(g) = sgs^{-1}]$ and $G_H = [G,t\ ;\ h = tht^{-1}]$, then G_H is embeddable in G_Φ by the function

$$\psi\colon G_H \to G_\Phi \text{ by } \psi(tht^{-1}) = shs^{-1} \text{ and } \psi(g) = g.$$

Thus H is benign in G_Φ which implies that $(G_\Phi)_H$ is Higman. But,

$$\begin{aligned}(G_\Phi)_H &= [G,s,t\ ;\ sgs^{-1} = \Phi(g),\ tht^{-1} = h] \\ &= [G,r,s,t\ ;\ sgs^{-1} = \Phi(g), stht^{-1}s^{-1} = \Phi(h),\ r = st] \\ &= [G,r,s,t\ ;\ rhr^{-1} = \Phi(h), sgs^{-1} = \Phi(g),\ t = s^{-1}r\ ] \\ &= [G,r,s\ ;\ rhr^{-1} = \Phi(h), sgs^{-1} = \Phi(g)] \\ &= [[G,r;\ rhr^{-1} = \Phi(h)],s\ ;\ sgs^{-1} = \Phi(g)] \\ &= (G_{\Phi|_H})_\Phi.\end{aligned}$$

Thus $G_{\phi|_H}$ is embedded in a Higman group and thus is Higman.∎

Definition: A set Φ, ψ,... of isomorphisms in a Higman group G is benign if $G_{\phi,\psi,\ldots}$ may be embedded in a Higman group H so that $\{t_\Phi,t_\psi,\ldots\}$ is a benign subgroup of H.

A finite set of benign isomorphisms in G is benign; we may take $H = G_{\phi,\psi,\ldots\eta}$ and use lemma 3.

Lemma 8: Let G be Higman, H a benign subgroup of G; Φ, ψ, ... a benign set of isomorphisms in G; K the smallest subgroup of G which includes H and is invariant under Φ, Ψ,..., then K is benign.

Proof: Embed $G_{\Phi,\psi\ldots}$ in a Higman group L so that $\{t_\Phi,t_\psi\ldots\}$ is benign. We know that

$$G \cap \{H, t_\Phi, t_\psi, \ldots\} \subset G \cap \{K, t_\Phi, t_\Psi, \ldots\} = K$$

by property 3. Clearly $K \subset G \cap \{H, t_\Phi, t_\psi, \ldots\}$ since the right hand side is invariant under $\Phi, \psi, \ldots$ and K was chosen as the smallest invariant subgroup. Thus we have that $K = G \cap \{H, t_\Phi, t_\psi, \ldots\}$. From Lemma 5 we have that $\{H, t_\Phi, t_\psi, \ldots\}$ is benign and $G \cap \{H, t_\Phi, t_\psi, \ldots\}$ is benign, thus K is benign.■

Benign Subgroups as Benign Subsets

Recall that we want to show that G_K is Higman for G finitely generated and K recursively enumerable. We will show that G_K is Higman by regarding K as a set and not as a subgroup, but first we must define benign subsets.

Let A be a finite set and choose an element z not in A. For P a set of words on A, E_P is the subgroup of [A,z] generated by the words XzX^{-1} for X in P. Since the words XzX^{-1} for X a word on A form a free set, then $XzX^{-1} \in E_P$ iff $X \in P$.

Definition: A subset P of [A] is benign in [A] if E_P is benign in [A,z].

Suppose that P a subgroup of [A], is benign as a subgroup, then $[A]_P$ is Higman, hence $[A,z]_P$ is Higman, so P is benign in [A,z]. Since [z] is embedded in [A,z] then by lemma 3 [z] is benign in [A,z]. Suppose $E_{[A]} = \langle XzX^{-1}$; X a word on A$\rangle$ was not the smallest subgroup of [A,z] containing z and invariant under the inner automorphisms of A. Let $F \subset E_{[A]}$ be that subgroup. If $F \neq E_{[A]}$ then choose $XzX^{-1} \notin F$ for X as short a word as possible in A such that $XzX^{-1} \notin F$. Then if $X = aY$ for some $a \in A$, $Y \in [A]$, Y is shorter so $YzY^{-1} \in F$ and $a(YzY^{-1})a^{-1} = XzX^{-1} \in F$. Thus by lemma 8, $E_{[A]}$ is benign.

Next we show that $E_P = \{P,z\} \cap E_{[A]}$. Clearly,

$E_P \subset \{P,z\} \cap E_{[A]}$. E_P contains z since $e \in P$, and E_P is invariant under the inner automorphisms through elements of P using the closure of P, therefore it is a normal subgroup of $\{P,z\}$.

Now since $z \in E_P$ the natural mapping of P to $\{P,z\}/_{E_P}$ is surjective. Then if $x \in \{P,z\}$, $x = py$ with $p \in P$ and $y \in E_P$. The homomorphism Φ from $[A,z]$ to $[A]$ defined by $\Phi(a) = a$, $\Phi(z) = e$ maps $E_{[A]}$ into the zero subgroup. So, if $x = py$ is in $E_{[A]}$ then $e = \Phi(x) = \Phi(py) = \Phi(p)\Phi(y) = p$, so $x = y$ and $x \in E_P$. Thus $E_P = \{P,z\} \cap E_{[A]}$ and by Lemma 5, E_P is benign. Thus, P is benign as a subset.

Now suppose that E_P is benign where P is a subgroup. Then we must show that P is benign as a subgroup. Let c and d be new elements not in A and form $[A,c,d]$. For X a word on A, let Φ_X be the isomorphism of $\{c\}$ and $\{dX\}$ defined by $\Phi_X(c) = dX$.

If we can show that the set of isomorphisms Φ_X for X in P is benign, then (by lemma 8) the smallest subgroup of $[A,c,d]$ which contains c and d and is invariant under the Φ_X for x in P is benign. This subgroup is $\{P,c,d\}$.

By lemma 5 since $P = \{P,c,d\} \cap [A]$ then P would be benign as a subgroup. It remains to show that

$$H = [A,c,d]_{\Phi_X,\Phi_Y,\ldots} \quad \text{(using all the words on A)}$$
$$= [A,c,d,t_X,t_Y,\ldots\ ;\ t_X c t_X^{-1} = dX,\ldots\ ]$$

where $t_X = t_{\Phi_X}$ is embeddable in a Higman group with the subgroup $\{t_X, \ldots\}$ for X in P benign.

Now suppose $A = \{a_1, \ldots, a_n\}$. Define an automorphism ψ_i of $[A, c, d, t_X, t_Y, \ldots]$ by $\psi_i(a) = a$, $\psi_i(c) = c$, $\psi_i(d) = da_i$, and $\psi_i(t_X) = t_{a_i X}$. Applying ψ_i to the relation $t_X c t_X^{-1} = dX$ gives $t_{a_i X} c t_{a_i X}^{-1} = da_i X$. Thus ψ_i permutes the defining relations of H and hence induces an automorphism of H.

Now we can embed H in a group K where

$K = [A, A', c, d, t_X, \ldots \ ; \ t_X c t_X^{-1} = dX,\ a_i' a a_i'^{-1} = a,$

$$a_i' c a_i'^{-1} = c,\ a_i' d a_i'^{-1} = da_i,\ a_i' t_X a_i'^{-1} = t_{a_i X}],$$

where $A' = \{a_1', \ldots, a_n'\}$. Define a mapping Ψ from H into K by

$$\Psi(a) = a$$

$$\Psi(c) = c$$

$$\Psi(d) = da_i$$

$$\Psi(t_X) = t_{a_i X}$$ and require linearity.

The only relations on H are the $t_X c t_X^{-1} = dX$ and since

$$\Psi(t_X c t_X^{-1}) = t_{a_i X} c t_{a_i X}^{-1} = da_i X,$$

and $\Psi(dX) = da_i X$ then Ψ is a well defined homomorphism. Also since K imposes no new relations on $[A, c, d, \{t_X\}]$ then Ψ is injective.

We show that K is finitely presented. Let $t = t_e$, and for X a word of A, let X′ be the word obtained from X by replacing each a_i by a_i'. By the relations

$$a_i' t_x a_i'^{-1} = t_{a_i x} \text{ we get}$$
$$X' t X'^{-1} = t_X$$

by replacing X by e and repeated application of the resulting $\{a_i' t a_i'^{-1} = t_{a_i}\}$. The equality $X'tX'^{-1} = t_X$ allows us to drop the generators t_X other than t, replace $t_X c t_X^{-1} = dX$ with $(X'tX'^{-1})c(X'tX'^{-1})^{-1} = dX$, and drop the relations $(a_i' t_x a_i'^{-1}) = t_{a_i x}$. Then

$$K = [A, A', c, d, t \; ; \; (X'tX'^{-1})c(X'tX'^{-1})^{-1} = dX,$$
$$a_i' a a_i'^{-1} = a,\ a_i' c a_i'^{-1} = c,\ a_i' d a_i'^{-1} = da_i]$$

which is finitely generated.

If we can show that $(X'tX'^{-1})c(X'tX'^{-1})^{-1} = dX$ is a result of the other relations then this implies that K is finitely presented and hence Higman. From $a = a_i' a a_i'^{-1}$, $c = a_i' c a_i'^{-1}$, and $da_i = a_i' a a_i'^{-1}$ we get $X'cX'^{-1} = c$ and $X'dX'^{-1} = dX$. Then applying the inner automorphism through X' to $tct^{-1} = d$ we get

$$X'tct^{-1}X'^{-1} = X'dX'^{-1} = dX$$
$$X't(X'^{-1}cX')t^{-1}X'^{-1} = dX$$
$$(X'tX'^{-1})c(X't^{-1}X'^{-1}) = dX,$$

so these are redundant.

Finally, we show that $\{t_X \; ; \; X \in P\}$ is benign in K. Since $E_{P'} = \{X'tX'^{-1} \; ; \; X' \in P'\}$ is benign in $[A', t]$, by lemma 6 $\{t_X \; ; \; X \in P\}$ is benign in K. Thus we have shown that the definition of benign for a subgroup P is the same as the definition of P as a set.

Our goal is to embed a recursively presented group in a finitely presented group. Recall that a recursively presented group [A;R] where A is finite and R is recursively presented can be written as G/K, where G is a free group on A and K is the recursively enumerable normal subgroup of G generated by the XY^{-1} for $X = Y$ in R.

We discuss, again, the group into which we embed G/K. Now in G_K, $\{G, tGt^{-1}\}$ is the free product of G and tGt^{-1} with the amalgam $K = tKt^{-1}$. The natural mapping from G to G/K and the mapping from tGt^{-1} to the zero subgroup of G/K agree when their domains are restricted to the amalgam.

Therefore we have a homomorphism Φ from $\{G, tGt^{-1}\}$ to G/K such that $\Phi(g) = gK$, $\Phi(tgt^{-1}) = eK$. Define a mapping ψ from $\{G, tGt^{-1}\}$ to $H \times G/K$ by $\psi(x) = (x, \Phi(x))$ where $H \geq G_K$. We will show that ψ is an isomorphism into $H \times G/K$. Since Φ is a homomorphism then

$$\psi(xy) = (xy, \Phi(x)\Phi(y)) = (x, \Phi(x))(y, \Phi(y)) = \psi(x)\psi(y)$$

so ψ is a homomorphism. Clearly ψ is injective.

If we can show that K is benign then we may embed G_K in a finitely presented group H. Then since G/K is embedded in $(H \times G/K)_\psi$, it will suffice to show that $(H \times G/K)_\psi$ is finitely presented.

Let us construct $(H \times G/K)_\psi$ from scratch.

$G_K = [G, t : tkt^{-1} = k] \leq [H ; R]$ and we may assume that the finite set of generators of H include t, a set of generators of G, and R contains the relations $\{tkt^{-1} = k\}$. Let G_1 be an isomorphic copy of G. Then $G_1/K_1 = [G_1 ; k_1 = e_1]$. Taking the direct product of H and G_1 we have

$$L = [H, G_1 ; g_1 h = h g_1].$$

Clearly $[G, tGt^{-1}]$ is a subgroup of H and hence a subgroup of L. Next we define mappings Φ^* and ψ^* from $[G, tGt^{-1}]$ to L such that

$$\Phi^*(g) = g_1,$$
$$\Phi^*(tgt^{-1}) = e_1,$$

and

$$\psi^*(x) = x\Phi^*(x).$$

The relations $\{g_1 h = h g_1\}$ guarantee that ψ^* is a homomorphism. Next let $L' = [L, s ; R, sxs^{-1} = \psi^*(x)]$ and we will show that $L' = (H \times G/K)_\psi$. First we show that in L', $k_1 = e_1$ for all $k_1 \in K_1$. We have in L' that

$$sks^{-1} = \psi^*(k) = k\Phi^*(k) = kk_1.$$

Also

$$sks^{-1} = stkt^{-1}s^{-1} = \psi^*(tkt^{-1}) = tkt^{-1}\Phi^*(tkt^{-1}) = ke_1.$$

Thus $kk_1 = ke_1$, and $k_1 = e_1$. Now, since ψ and Φ agree with ψ^* and Φ^* modulo the relations of L' then

$$(H \times G/K)_\psi = [H, G_1, s ; g_1 h = h g_1, sxs^{-1} = \psi(x), R] = L'.$$

Since there is a finite number of generators for H and G_1, there are finitely many relations that commute H and

G_1 and finitely many relations that equate $\psi(x)$ and sxs^{-1}; hence $(H \times G/K)_\psi$ is finitely presented and we are reduced to proving that K is benign. The benignness of a recursively enumerable subgroup P in [A] is known as the principle lemma and will be considered in the next section. By the results of this section we can view P as a subset.

The Principle Lemma

Principle Lemma: If A is finite and P is a recursively enumerable set of words on A, then P is benign.

Briefly let us state how we will prove the Principle Lemma. Recall that we must show that [A;R] = G/K is Higman, where G/K is recursively presented and G = [A]. Earlier we showed that it suffices to prove that G_K is embedded in a finitely presented group H, whence $(H \times G/K)_\psi$ will be finitely presented. Since to be benign as a subgroup agrees with benign as a subset, we will show that K is benign as a subset, P.

Let A′ consist of an element a′ for each a of A, Φ be the homomorphism from [A,A′] to [A] by Φ(a) = a, $\Phi(a') = a^{-1}$. The two properties that we will show are 1) P′ the set of positive words on A ∪ A′, is benign in [A,A′], and 2) There exists a mapping Φ so that Φ(P′) = P, and then P is benign in [A] which is what we want to show.

The following lemmas follow from similar lemmas about subgroups (Through the conclusion of part 1, A and B are finite sets.):

Lemma 9: Every finite subset of [A] is benign in [A].

Lemma 10: If A ⊂ B and P is a set of words on A, then P is benign in [A] iff P is benign in [B].

Lemma 11: If P and Q are benign subsets of [A], then

$P \cap Q$ and $P \cup Q$ are benign.

Definition: An *associate* of a mapping Φ (not necessarily a homomorphism) from [A] to [B] is a homomorphism from [A,z] to [B,z] such that $\psi(XzX^{-1}) = \Phi(X)z\Phi(X)^{-1}$ for X a word on A.

If Φ is a homomorphism, then it has an associate.

Definition: A bijective mapping from [A] to [A] is *nice* if it has an associate which is an automorphism of [A,z].

Definition: A word on A is *positive* if it does not contain any a^{-1} with $a \in A$ (in reduced form, of course).

Lemma 12: Let Φ be a mapping from [A] to [B] which has an associate. If P is a benign subset of [A] then $\Phi(P)$ is a benign subset of [B].

Proof: If ψ is an associate of Φ then $E_{\Phi(P)} = \psi(E_P)$. So by lemma 6, $\Phi(P)$ is a benign subset of [B].∎

The remainder of this chapter will show that the set of positive words is benign.

Definition: Let P and Q be subsets of [A], and let Φ be a mapping from [A] to [A]. We say that P is *(Φ,Q)-invariant* if for each X in Q, $X \in P$ iff $\Phi(X) \in P$. If $Q = [A]$, we say invariant under Φ for (Φ,Q)-invariant.

Lemma 13: Let P, $Q_1, \ldots, Q_n$ be benign subsets of [A]; $\Phi_1, \ldots, \Phi_n$ nice mappings from [A] to [A], R the smallest subset of [A] which includes P and is

(Φ_i, Q_i)-invariant for $i = 1, \ldots n$, then R is benign.

Proof: Let ψ_i be an automorphism of $[A,z]$ which is an associate of Φ_i. By lemma 7, $\psi_i|_{E_{Q_i}}$ is benign. Therefore, by lemma 8 the smallest subgroup which includes E_P and is invariant under the $\psi_i|_{E_{Q_i}}$ is benign. If this group is E_R then we are done. An element g of E_{Q_i} is a product of words $Xz^{\pm 1}X^{-1}$ with X in Q_i. We obtain $\psi_i(g)$ by replacing each X by $\Phi_i(X)$. Then $g \in E_R$ iff $\psi_i(g) \in E_R$ since R is (Φ_i, Q_i)-invariant. Thus E_R is invariant under $\psi_i|_{E_{Q_i}}$. Now an element of R is obtained from an element of P by repeatedly applying the Φ_i and Φ_i^{-1} subject to the condition that Φ_i is applied only to a word in Q_i and Φ_i^{-1} is applied only to a word in $\Phi_i(Q_i)$. It follows that if $X \in R$, then XzX^{-1} is in every subgroup which includes E_P and is invariant under $\psi_i|_{E_{Q_i}}$.∎

Lemma 14: Let $b_i = b^i a b^{-i}$, and let P be the set of all words $b_{i_1} b_{i_2} \cdots b_{i_n}$ with $0 \le i_1 < i_2 < \ldots < i_n$. Then P is a benign subset of $[a,b]$.

Proof: Let H, H^+, and H' be the subgroups generated by the b_i, the b_i for $i > 0$, and the b_i for $i \ge 0$ respectively. Since H is the smallest subgroup which contains a and is invariant under the inner automorphisms through powers of b, then H is benign by lemma 8. Consider homomorphisms Φ and λ from [a,b] to [a,b] by $\Phi(a) = a$, $\lambda(a) = bab^{-1}$, $\Phi(b) = \lambda(b) = b^2$. It is straightforward to show that Φ and λ are injective. So by lemma 7, $\Phi|_H$ and $\psi|_H$ are benign. Hence by lemma 8, it will suffice to show that H^+ is the smallest subgroup which contains b and is invariant under $\Phi|_H$ and $\psi|_H$. Since

$$\Phi(b_i) = \Phi(b^i ab^{-i}) = b^{2i}ab^{-2i} = b_{2i} \text{ and}$$
$$\lambda(b_i) = b^{2i}bab^{-1}b^{-2i} = b_{2i+1}$$

then it is a simple inductive argument to show that any subgroup which contains b_1 and is invariant under $\Phi|_H$ and $\lambda|_H$ will contain b_i for $i > 0$.

Next we show that H^+ is invariant under $\Phi|_H$ and $\lambda|_H$. Any element x of H is a product of the b_i and their inverses; $x \in H^+$ iff $i > 0$ for all the b_i. Then $x \in H^+$ implies $\Phi(x) \in H^+$ and $\lambda(x) \in H^+$. Thus H^+ is invariant under $\Phi|_H$ and $\lambda|_H$ so by lemma 8, H^+ is benign. Since $H' = \{H^+,a\}$, H' is benign by lemma 5.

Continuing, let ψ be the automorphism of [a,b] defined by $\psi(a) = bab^{-1}$, $\psi(b) = b$. Then $\psi(b_i) = b_{i+1}$. By lemma 13, it suffices to show that P is the smallest subset which contains e and is left multiplication by a of H^+, denoted La, (La,H^+)-invariant, and (ψ,H')-invariant. We show that P is (La,H^+)-invariant. An element h of H^+ is $b_{i_1}^{\pm 1} \cdots b_{i_n}^{\pm 1}$ with the i_j positive and not necessarily distinct. Then left multiplication by a is $b_0 b_{i_1}^{\pm 1} \cdots b_{i_n}^{\pm 1} = ah$. If the exponents are all +1 and $i_1 < \ldots < i_n$ then both h and ah are in P. If either of the two above conditions do not hold, then both h and ah are not in P since the b_i are free. Thus we get the desired results. The argument is similar for $(P, \psi|_H)$-invariant since $\psi(b_i^{\pm 1}) = b_{i+1}^{\pm 1}$.■

Lemma 15: The set of all positive words on A is benign.

Proof: Let $A = \{a_1, \ldots, a_n\}$. Define an automorphism Φ of [A,z] by $\Phi(a_i) = a_{i+1}$ for $i < n$, $\Phi(a_n) = a_1$, and $\Phi(z) = z$. $[A,z]_\Phi$ is Higman by lemma 3. Let t be the Φ-element, and let ψ be the homomorphism from [a,b,z] to $[A,z]_\Phi$ defined by $\psi(a) = a_1$, $\psi(b) = t$, and $\psi(z) = z$. If P is defined as it was in lemma 14, then $\psi(P)$ will be the set Q of positive words on A. To see this note that in $[A,z]_\Phi$ we have the following $a_{i+1} = ta_it^{-1}$ for $i < n$ and $a_1 = ta_nt^{-1}$ so

$$\psi(b_i) = \psi(b^iab^{-i}) = t^ia_1t^{-i} = a_{i+1} \text{ (mod n)}.$$

In addition, in $[A,z]_\Phi$ we have the relation that $t^na_it^{-n} = a_i$ so that any positive word on A can satisfy the ascending powers on the b_i in P. Thus $\psi(P) = Q$ and lemma 12 gives the result.■

Definition: An *n-ary predicate* is a subset of the set of n-tuples in A. $P(a_1, a_2, \ldots, a_n)$ means that the n-tuple

$\{a_1, a_2, \ldots, a_n\}$ is in P.

We can identify each k-tuple of natural numbers with a positive word on {a,b} by identifying $x_1, x_2, \ldots, x_n$ with $a^{x_1}ba^{x_2}b\ldots ba^{x_k}$. It then makes sense to say that a k-ary predicate of natural numbers is benign.

We collect some properties on benign predicates:

A) The predicates $\{(n,n)\} = P_=$, $\{(n,m,n+m)\} = P_+$, and $\{(n,m,nm)\} = P_.$ are benign.

B) If P is benign and Q is defined by $Q(\Omega,n) \Leftrightarrow P(n,\Omega)$, then Q is benign (where Ω is a sequence of letters in the predicate P).

C) If P is benign and Q is defined by $Q(n,\Omega) \Leftrightarrow P(\Omega)$, then Q is benign.

D) If P is benign and Q is defined by $Q(\Omega) \Leftrightarrow \exists n P(n,\Omega)$, then Q is benign.

E) If P is benign and Q is defined by $Q(n,\Omega) \Leftrightarrow \forall m<n\ P(m,\Omega)$, then Q is benign.

Definition: An *explicit* definition of a function or predicate contains only previously defined functions and predicates. Thus we can show that certain explicit definitions of predicates lead to benign predicates.

First, suppose that the definition only uses variables in benign predicates. Then an explicitly defined predicate P would be of the form

$$P(x_1, \ldots, x_n) \Leftrightarrow Q(x_{j_1}, \ldots, x_{j_p})$$

where the $x_{j_i} \in \{x_1, \ldots, x_n\}$ and with Q benign. We can rewrite this as

$$P(x_1, \ldots, x_n) \Leftrightarrow \exists y_1, \ldots, y_p(y_1 = x_1 \wedge \ldots \wedge y_p = x_{j_p} \wedge Q(y_1, \ldots, y_n)).$$

P is benign by D, lemma 11, and the fact that equals and Q are benign predicates of $y_1, \ldots, y_p, x_1, \ldots, x_k$ by B and C.[2]

By lemma 11, D, and E, we may also use $\wedge$, $\vee$, existential quantifiers, and bounded universal quantifiers in explicit definitions of benign predicates. We may also use constants. For example, we may replace ...0... by $\exists x(x = 0 \wedge \ldots x \ldots)$, and we know that $x = 0$ is a benign predicate by lemma 9.

Definition: A function F on $\mathbb{Z}$ is recursive if:

1) $F = I_i^n(a_1, \ldots, a_n) = a_i$ (projection map), $F = P_+$, $F = P_\cdot$, or $F = K_<$ where $K_<$ is the 2-place function defined by $K_<(a_1, a_2) = \{0 \text{ if } a_1 < a_2, 1 \text{ if } a_1 \geq a_2\}$.
2) $F(\Omega) = G(H_1(\Omega), \ldots, H_K(\Omega))$ where G, $H_1, \ldots, H_K$ are recursive functions.
3) If G is recursive and $\forall\Omega\exists x(G(\Omega,x) = 0)$, then $F(\Omega) = \mu x(G(\Omega,x) = 0)$ where $\mu x(G(\Omega,x) = 0) = x$ iff

---

[2] B is used to move the x_{j_i} around to their position if different in P than in Q, and C is used if $k \neq p$).

$\forall c < x\ G(\Omega,c) \neq 0$ and $G(\Omega,x) = 0$.[3]

A predicate is recursive if its representing function is recursive. Note that if $F(x_1, \ldots ,x_k) = y$ is recursive then $P_F = (x_1, \ldots ,x_k,y)$ is recursive where $F(x_1, \ldots ,x_k)$ is P_F's representing function.

Lemma 16: If F is a recursive function, then the predicate P_F is benign.

Proof: We proceed by induction on the complexity of F. If F is I_i^n, P_+, or $P_\cdot$ then it is benign by properties A, B, and C. For $F = K_<$, consider the predicate $X \neq 0$ by identifying it with $\{a^x ba^0;\ x \neq 0\}$. $\{a^x ba^0;\ x \neq 0\}$ is benign by lemmas 11, 12, 13, and 15 since this set is the image under left multiplication by a of the set $R \cap Q$ where R is the smallest subset of $A = [a,b]$ containing a^0ba^0 which is invariant under left multiplication by a and Q is the set of positive words in $A = [a,b]$. From this and the explicit definitions

$$x \leq y \Leftrightarrow \exists z\ P_+(x,z,y)$$

$$x < y \Leftrightarrow \exists z\ (z \neq 0 \wedge P_+(x,z,y)),$$

we see that $\leq$ and $<$ are benign. Hence we get explicitly

---

[3] $\mu x(\ldots x\ldots)$ denotes the smallest x for which ...x... is true.

that $P_F(x,y,z) \Leftrightarrow (x < y \wedge z = 0) \vee (y \leq x \wedge z = 1)$.[4]

Continuing the inductive process, suppose that F is defined by $F(\Omega) = G(H_1(\Omega), \ldots, H_k(\Omega))$ where G, $H_1, \ldots, H_k$ are benign. Then P_F has the explicit definition

$$P_F(\Omega,x) \Leftrightarrow \exists y_1 \ldots \exists y_k (P_{H_1}(\Omega,y_1) \wedge \ldots \wedge P_{H_k}(\Omega,y_k) \wedge P_G(y_1, \ldots, y_k, x))$$

and is benign by D and the fact P_{H_i} and P_G are benign.

Finally, suppose that F is defined by $F(\Omega) = \mu x(G(\Omega,x) = 0)$ where G is benign. Then P_F has the explicit definition

$$P_F(\Omega,x) \Leftrightarrow P_G(\Omega,x,0) \wedge \forall y<x\ \exists x(z \neq 0 \wedge P_G(\Omega,x,z)).$$

Thus P_F is benign by induction.∎

We claim that Q is recursively enumerable, not recursive, if there is a recursive predicate P such that

$$Q(\Omega) \Leftrightarrow \exists x\ P(\Omega,x) \text{ for all } \Omega.$$

Definition: K_P is the *representing partial functional* of predicate P defined on the same domain as P such that $K_P(\Omega) = 0$ if Ω is in P and $K_P(\Omega) = 1$ if Ω is not in P.

Lemma 17: Every recursively enumerable predicate is benign.

Proof: In view of D, it will suffice to consider a

---

[4]The constants are benign by lemma 9.

recursive predicate P. Since $P(\Omega) \Leftrightarrow P_{K_p}(\Omega,0)$, then by lemma 16, P is benign (P_{K_p} is the predicate from the recursive function K_p, the p-place function described earlier).■

Lemma 18: If Q is a recursively enumerable set of positive words on A, then Q is benign.

Proof: Let P be the set of all words $b_{i_1} \cdots b_{i_n}$ where $b_i = b^i ab^{-i}$, $0 \le i_1 < \ldots < i_n$ as in lemma 14. Let ψ be as in the proof of lemma 15 where ψ is the homomorphism from $[a,b,z]$ to $[A,z]_\Phi$ defined by $\psi(a) = a_1$, $\psi(b) = t$, and $\psi(z) = z$ where Φ is an automorphism of $[A,z]$ defined by $\Phi(a_i) = a_{i+1}$, $\Phi(a_n) = a_1$, and $\Phi(z) = z$. Since $\psi(P)$ is the set of positive words on A,

$$\psi(\psi^{-1}(Q) \cap P) = Q.$$

To see this, if a_i is an element in A, then $\psi^{-1}(a_i) = \psi^{-1}(t^{i-1}a_1t^{-i+1}) = b^{i-1}ab^{-i+1} = w$ which is an element of P, so $\psi^{-1}(w) \in P$ if w is a positive word. Thus, $\psi^{-1}(Q) \subseteq P$ and the results follow. From this equality we get $\psi(E_{\psi^{-1}(Q)\cap P}) = E_Q$ since

$$\psi(XzX^{-1}) = \psi(X)z\psi(X)^{-1} \text{ for } X \in E_{\psi^{-1}(Q)\cap P}.$$

It will therefore suffice to show that $\psi^{-1}(Q) \cap P$ is benign. Since $\psi^{-1}(Q) \cap P$ is clearly recursively enumerable, this will follow if we show that every recursively enumerable subset R of P is benign.

Let Φ be the homomorphism from $[a,z]$ to $[a,z]$ defined by $\Phi(a) = a^2$, $\Phi(z) = z$. Then Φ is injective. By lemma 3, $[a,z]_\Phi$ is Higman. Let b be the Φ-element, and let λ be the natural mapping from $[a,b,z]$ to $[a,z]_\Phi$. Since if $b_i = b^i ab^{-i}$ then $\lambda(b_i) = a^{2^i}$ by the relation $a^2 = bab^{-1}$ in $[a,z]_\Phi$ for $i \geq 0$. Hence if $X = b_{i_1} \ldots b_{i_n}$ is a word in P, then $\lambda(X) = a^y$ with $y = 2^{i_1} + \ldots + 2^{i_n}$; so $\lambda(XzX^{-1}) = a^y z a^{-y}$. Now a number y can be written in the form $2^{i_1} + \ldots + 2^{i_n}$ with $0 \leq i_1 < \ldots < i_n$ in only one way since its base 2 representation is unique. It follows that λ is injective on E_P; so $E_R = E_{P \cap \lambda^{-1}(\lambda(E_R))}$. Thus it will suffice to show that $\lambda(E_R)$ is benign.

Now $\lambda(E_R) = E_{\lambda(R)}$ where $\lambda(R)$ is a set of positive words on $\{a\}$. Since R is recursively enumerable, $\lambda(R)$ is a recursively enumerable 1-ary predicate. Hence $\lambda(R)$ is benign by lemma 17.∎

Now we can prove the principle lemma. Let P be a recursively enumerable set of words on A. Let A′ consist of an element a′ for each element a of A, and let Φ be the homomorphism from $[A,A']$ to $[A]$ defined by $\Phi(a) = a$, $\Phi(a') = a^{-1}$. Let P′ be the set of positive words X on $A \cup A'$ such that $\Phi(X) \in P$. Then P′ is recursively enumerable and hence benign by lemma 18. Clearly $\Phi(P') \subseteq P$. Let $p \in P$, if p is positive, then $p = \Phi(p)$. Suppose p is not positive, then replace each occurrence of a_i^{-1} in p by a_i' then p is a positive word in P'. Thus $P = \Phi(P')$, and P is benign by lemma 12.

In summary there were 3 main points in the discussion. First we showed that there is a recursively presented group with an unsolvable word problem. Next, we embedded a recursively presented group G/K in the group $(G_K \times G/K)_\psi$ where ψ is an isomorphism from $\{G, t^{-1}Gt\}$ into $G_K \times G/K$. But we needed to embed G_K in a finitely presented group H in order to show that $(G_K \times G/K)_\psi$ was finitely presented. The remainder of part 1 proved that K was benign so that G_K is Higman. Hence if a group is finitely presented this does not imply that the group has a solvable word problem. Indeed proving that an element is the identity in a finitely presented group is not a trivial task. In part two we consider different questions; however, the issue of whether certain types of elements are trivial or not is central to the discussion.

Part II: THE BURNSIDE PROBLEM

Introduction

Definition: Let A be a set of r elements, N be the normal subgroup of the free group on A denoted [A] generated by all nth powers of elements of A, then
$B(n,r) = [A]/N = [A \; ; \; w^n = e]$, and B(n,r) is called the *Burnside group* of order n with r generators. When we are referring to the Burnside group we shall call n the order.

Clearly, every group with r generators and elements of order dividing n will be a homomorphic image of the group B(n,r). We will in this section of the paper talk about the Burnside problem with respect to the Burnside group. We will discuss those groups where the orders are unbounded powers of a particular prime in the last section. Thus we restrict the general Burnside question to: "For which integers n and r are the groups B(n,r) finite?"

The case for B(1,r) is the trivial group, and B(n,1) is the cyclic group of order n. The group B(2,r) is abelian and hence finite. This is a classic problem in undergraduate algebra. B(3,r), B(4,r), and B(6,r) can also be shown to be finite. However, the question of the finiteness of B(5,2) is still unsettled.

Every finite group has a solvable word problem. Thus, if we could show that the word problem for B(n,r) was unsolvable then B(n,r) would be infinite. Thus solving the word problem for B(n,r) would seem like a reasonable approach for answering the Burnside question. Adian proved that the word problem is solvable for odd $n \geq 665$. He also proved for odd $n \geq 665$ that B(n,r) is infinite. However, solving the word problem for B(n,r) turns out to be a more difficult task than showing that an upper bound exists on products of commutators in B(n,r). We begin part 2 by discussing properties of commutators in B(n,r).

The Collection Problem and the Lower Central Series

There is a way of writing an expression y with n_1 x_1's, n_2 x_2's, ... , n_k x_k's as

$$y = x_1^{n_1} \; x_2^{n_2} \; \ldots \; x_k^{n_k} \; c_1 c_2 \; \ldots \; c_n$$

where c_i are commutators, and loosely speaking the higher the subscript the higher the commutator. Commutators of commutators are called higher commutators. Thus, a basic strategy for proving finiteness or obtaining bounds on the number of elements in a group, G, is to show that sufficiently high commutators must be trivial. This section gives a discussion of relevant results about commutators and higher commutator subgroups which yield the lower central series of G.

Definition: $(a,b) = a^{-1}b^{-1}ab$ and is called the commutator of a and b (in this order).

Definition: Let F be a group generated by x_1, ... , x_r:

1) $c_i = x_i$, i = 1, ... ,r are the commutators of weight 1; i.e. $w(x_i) = 1$, and are simply ordered by the rule $x_1 < x_2 < \ldots < x_r$. Call these commutators basic.

2) If c_i and c_j are commutators, then $c_k = (c_i, c_j)$ is a commutator and $w(c_k) = w(c_i) + w(c_j)$.

3) If basic commutators of weight less than n have

been defined and simply ordered, then (x,y) is a basic commutator of weight n, iff

a) x and y are basic commutators with $w(x) + w(y) = n$,

b) $x > y$,

c) if $x = (u,v)$, then $y \geq v$.

4) Commutators of weight n follow all commutators of weight less than n, and for weight n, $(x_1,y_1) < (x_2,y_2)$ if $y_1 < y_2$ or $y_1 = y_2$ and $x_1 < x_2$.

For example suppose x and y are basic commutators of weight 1 such that $x < y$. Then (x,y,x) is not basic since it does not satisfy 3c. Generally, any left normed commutator $(y,x,\ldots,x)$ is basic but $(x, \ldots ,x,y,x, \ldots ,x)$ is not basic since x cannot precede y.

Lemma 1 (Witt-Hall identities): $\forall\, a,b,c \in G$ where G is a group,

1) $(a,b)(b,a) = 1$

2) $(a,bc) = (a,c)(a,b)((a,b),c)$

3) $(ab,c) = (a,c)((a,c),b)(b,c)$

4) $((a,c),c^a)((c,a),b^c)((b,c),a^b) = 1$ where $a^b = b^{-1}ab$.

These identities are straightforward to prove.

Given any element $g \in B(n,r)$, g can be written as a product of commutators where the commutators are ordered in ascending weight by repeated applications of lemma 1 and the identity $ab = ba(a,b)$. Then

$g = x_{r1}^{a_1} \ldots x_{r2}^{a_r} (x_1,x_2)^{b_{12}} \ldots (x_i,x_j)^{b_{ij}} \ldots (x_{i_1},\ldots,x_{i_s})^m c_1 \ldots c_t$
where $\{c_i\}$ represent the bracket arrangements higher than s; a_i, b_{ij}, and m are positive integers less than n; and B(n,r) is generated by $\{x_1, \ldots, x_r\}$.

Suppose we could show in a group B(n,r) that all commutators of weight k+1 are trivial. Then $(x_{i_1},\ldots,x_{i_m}) = 1$ if $m > k$ and g reduces to
$g = x_1^{a_1} \ldots x_2^{a_r} (x_1,x_2)^{b_{12}} \ldots (x_i,x_j)^{b_{ij}} \ldots ((x_{i_1},\ldots,x_{ik}))^q$.
It can be shown that there are only finitely many bracket arrangements (on a finite number of generators) of weight k, thus there are only finitely many products of these bracket arrangements possible. Hence, B(n,r) must be finite in this case.

Two applications of the commutator identities on normal subgroups are presented below and will be useful later in the discussion.

If A and B are normal subgroups of G let (A,B) denote the subgroup generated by {(a,b)}, which is also normal. The normality follows from $g^{-1}(a,b)g = (g^{-1}ag, g^{-1}bg)$. The normality of A and B give us that (A,B) = (B,A). To see this let Z = (A,B) as a set. Since $wZw^{-1} = Z$ for all $w \in G$ then $b^{-1}a^{-1}ba = a^{-1}(ab^{-1}a^{-1}b)a \in Z$ so $(B,A) \leq Z$. Similarly, if $Z' = (B,A)$ then $Z' \geq (A,B)$.

Lemma 2: If A, B, C are normal subgroups of G, then ((A,B),C) is contained in ((B,C),A)((C,A),B).

Proof: Let $a \in A$, $b \in B$, $c \in C$. Since both B and A are normal subgroups, then $b^c \in B$ and $a^b \in A$. From the fourth Witt-Hall identity

$$((a,b),c^a)((c,a),b^c)((b,c),a^b) = 1$$

we have $((a,b),c^a) = ((b,c),a^b)^{-1} \cdot ((c,a),b^c)^{-1}$. Since c^a runs through all elements of C if c does, then the lemma is proved.■

Definition: Given $G = \langle x_1, x_2, \ldots, x_r \rangle$ define $G_n = \langle (y_1, y_2, \ldots, y_n) \mid y_i \in G \rangle$.[5] The series $G = G_1 \geq G_2 \ldots \geq G_n \ldots$ form the *lower central series* (LCS) of G.

G_i will be shown to contain all bracket arrangements of weight i. So showing that all commutators of weight i are trivial is equivalent to showing that G_i is trivial.

Definition: A group G for which $G_k = 1$ for some positive integer k is called *nilpotent*, and we say G is nilpotent of class k if k is the smallest integer such that $G_k = 1$.

At this point the Burnside question could be restated as "For what integers n,r are the groups B(n,r) nilpotent?".

There are some important facts about the groups of the

---

[5]Notation: $((a,b),c) = (a,b,c)$ and is inductively defined for larger products.

LCS that we present in the following theorem.

Theorem 1: (a) G_i is normal, (b) $G_{i+1} \subset G_i$, (c) $G_{k+1} = (G_k,G)$, d) $(G_k,G_m) \leq G_{k+m}$, and (e) G_i/G_{i+1} is abelian.

Proof (a): It suffices to show that a conjugate of a generator of G_i is in G_i. Let $x = c^{-1}d^{-1}cd = (c,d)$ where $c = (y_1,\ldots,y_{i-1})$. Then $g^{-1}xg = g^{-1}c^{-1}d^{-1}cdg = (g^{-1}c^{-1}gc)(c^{-1}g^{-1}d^{-1}cdg) = (c,g)^{-1}(c,dg) \in G_i$.

Proof (b): $G_{i+1} = \langle(a_1, \ldots, a_i, a_{i+1}) \mid a_k \in G\rangle$

$= \langle((a_1, \ldots, a_i), a_{i+1})\rangle$

$= \langle(g_i,a_{i+1}) \mid g_i \in G_i\rangle$, thus

$\forall x \in G_{i+1}$, $x = g_i^{-1}g^{-1}g_ig = g_i^{-1}(g^{-1}g_ig)$. But G_i is normal so $g^{-1}g_ig \in G_i$ which implies that $x \in G_i$.

Proof (c): We have $G_{k+1} \leq (G_k,G)$. To prove the inclusion in the other direction, we need the Witt-Hall identities. Using $(xy,z) = (x,z)^y(y,z)$ and setting $x = (a_1, \ldots ,a_k)$, $y = (a_1, \ldots ,a_k)^{-1}$, $z = a_{k+1}$ where $a_i \in G$, then

$$1 = (1,a_{k+1}) = (a_1, \ldots ,a_k,a_{k+1})^y((a_1, \ldots ,a_k)^{-1},a_{k+1})$$

and $(a_1, \ldots ,a_k,a_{k+1})^y \in G_{k+1}$ so

$$((a_1, \ldots ,a_k)^{-1},a_{k+1}) \in G_{k+1}.$$

Now, we can assume (G_k,G) is generated by elements $(u_1u_2\ldots u_n,g)$, where u_i is of the form $(a_1, \ldots ,a_k)$ or $(a_1, \ldots ,a_k)^{-1}$. By the work above, $(u_i,g) \in G_{k+1}$. We show by induction on n that $(u_1u_2\ldots u_n,g) \in G_{k+1}$. This is done by setting

$$x = u_1u_2\ldots u_{n-1},\ y = u_n,\ \text{and } z = g$$

in $(xy,z) = (x,z)^y(y,z)$ so that we have $(u_1u_2\ldots u_n,g) = (u_1u_2\ldots u_{n-1},g)^{u_n}(u_n,g)$. We have that $(u_1u_2\ldots u_{n-1},g)^{u_n}, (u_n,g) \in G_{k+1}$ by our inductive assumption. Therefore, $(u_1u_2\ldots u_{n-1},g) \in G_{k+1}$ as desired.

Proof (d): Let $m = 1$, then $G_{k+1} = (G_k,G)$ by part (c). Again we will use induction on m assuming that $(G_k,G_m) \subset G_{k+m}$ for any k, thus we have that $(G_{k+1},G_m) \subset G_{k+1+m}$. We know $(G_k,G_{m+1}) = (G_{m+1},G_k) = ((G_m,G_1),G_k) = ((G_1,G_m),G_k)$. By lemma 2 and part c of theorem 1

$$((G_1,G_m),G_k)) \subset ((G_m,G_k),G_1))((G_k,G_1),G_m) \text{ so}$$

$$(G_k,(G_m,G_1)) \subset ((G_k,G_m),G_1))((G_k,G_1),G_m).$$

By the induction hypothesis

$$((G_k,G_m),G_1) \subset (G_{k+m},G_1) = G_{k+m+1}$$

and

$$((G_k,G_1),G_m) = (G_{k+1},G_m) \subset G_{k+1+m}.$$

Hence, $(G_k,G_{m+1}) \subset G_{k+m+1}$ as desired.

Proof (e): $G_{i+1} \supset G_{2i} \supset (G_i,G_i)$. Thus G_i/G_{i+1} is abelian.■

Note that d) above implies that G_i contains all commutators of weight i no matter how the elements are associated.

Modulo the terms of the LCS, the commutator identities from lemma 1 take on a particularly useful form.

Theorem 2: Let $a,b,c \in G$, $k,m,n \in \mathbb{N}^+$ such that $a \in G_k$, $b \in G_m$, $c \in G_n$, then

1) $ab \equiv ba \pmod{G_{k+m}}$

2) $(a,bc) \equiv (a,b)(a,c) \pmod{G_{k+m+n}}$

3) $(ab,c) \equiv (a,c)(b,c) \pmod{G_{k+m+n}}$

4) $(a,b,c)(b,c,a)(c,a,b) \equiv 1 \pmod{G_{k+m+n+1}}$

Proof: (1) $ab = ba(a,b)$, thus it suffices to show that $(a,b) \in G_{k+m}$, but this is true by the last theorem.

(2) $(a,bc) = (a,c)(a,b)((a,b),c)$

$= (a,b)(a,c)((a,c),(a,b))((a,b),c)$. Clearly $(a,b,c) \in G_{k+m+n}$, $(a,c) \in G_{k+n}$, $(a,b) \in G_{k+m}$, so $((a,c),(a,b)) \in G_{2k+m+n} \subset G_{k+m+n}$.

(3) $((a,b),c^a)((c,a),b^c)((b,c),a^b) = 1$ from the Witt-Hall identities. Using this, first, we see that

$$(a,b,c^a) = ((a,b),a^{-1}ca) = ((a,b),cc^{-1}a^{-1}ca)$$

$$= ((a,b),c(c,a))$$

$$\equiv ((a,b),c)((a,b),(c,a)) \pmod{G_{2k+m+2n}}.$$

Now $((a,b),(c,a)) \in G_{2k+m+n}$ thus $(a,b,c^a) \equiv (a,b,c) \pmod{G_{2k+m+n}}$. Similarly, we get that $(c,a,b^c) \equiv (c,a,b) \pmod{G_{k+m+2n}}$ and $(b,c,a^b) \equiv (b,c,a) \pmod{G_{k+2m+n}}$. Since congruence modulo G_r implies congruence modulo G_s when $r \geq s$ then

$$(a,b,c^a) \equiv (a,b,c) \pmod{G_{k+m+n+1}}$$

$$(c,a,b^c) \equiv (c,a,b) \pmod{G_{k+m+n+1}}$$

$$(b,c,a^b) \equiv (b,c,a) \pmod{G_{k+m+n+1}}$$

so we get $(a,b,c)(c,a,b)(b,c,a) \equiv 1 \pmod{G_{k+m+n+1}}$.■

Any relations modulo a term of the LCS will be used to describe the elements of G_i and ultimately help us to determine if G_i is trivial or not. The following theorem, although relevant to the argument above, will be used later to show that a particular commutator $(y,x, \ldots ,x)$ will be trivial. It relates commutators involving products and inverses to products and inverses of commutators.

Theorem 3: If $g_1, \ldots, g_p \in G_k$, $g \in G_m$ and $\varepsilon_i = \pm 1$ then

$$\left(\prod_{i=1}^{p} g_i^{\varepsilon_i}, g\right) \equiv \prod_{i=1}^{p} (g_i,g)^{\varepsilon_i} \pmod{G_{2k+m}} \qquad (3\text{-}1)$$

and

$$\left(g, \prod_{i=1}^{p} g_i^{\varepsilon_i}\right) \equiv \prod_{i=1}^{p} (g,g_i)^{\varepsilon_i} \pmod{G_{2k+m}}. \qquad (3\text{-}2)$$

Proof: By induction on p we get $\left(\prod_{i=1}^{p} g_i^{\varepsilon_i}, g\right) \equiv \prod_{i=1}^{p} (g_i,g)^{\varepsilon_i} \pmod{G_{2k+m}}$ since $(g_1^{\varepsilon_1} g_2^{\varepsilon_2}, g) \equiv (g_1^{\varepsilon_1},g)(g_2^{\varepsilon_2},g) \pmod{G_{2k+m}}$. Now, $(g_i^{-1},g)(g_i,g) \equiv (g_i^{-1}g_i,g) = 1 \pmod{G_{2k+m}}$, hence it follows that $(g_i^{\varepsilon_i},g) \equiv (g_i,g)^{\varepsilon_i} \pmod{G_{2k+m}}$ and so we get (3-1). The proof of (3-2) follows similarly.■

If G_n/G_{n+1} is infinitely generated, then describing the elements of this group would be an almost impossible task. Thus showing that G_n/G_{n+1} is finitely generated, or better yet showing that the generators of G_n/G_{n+1} are cosets of commutators $(x_{i_1}, \ldots, x_{i_n})$, is important to our discussion.

Theorem 4: If G is generated by r elements $\{x_1, \ldots, x_r\}$, then G_n/G_{n+1} is generated by the cosets of the left-normed n-fold commutators

$$(x_{p_1}, \ldots, x_{p_n}) \text{ where } p_i \in \{1, \ldots, r\}. \qquad (4\text{-}1)$$

Proof: Let us proceed by induction on n using the results of the previous theorem. If n = 1, then (4-1) results in the generators of G and so the cosets of the generators of G yield the generators of G_1/G_2. Assuming that the cosets of (4-1) generate G_n/G_{n+1}, we wish to show that G_{n+1}/G_{n+2} is generated by $(x_{p_1}, \ldots, x_{p_{n+1}})G_{n+2}$. Theorem 1 gave us that $G_{n+1} = (G_n, G)$ is generated by (h,g) where $h \in G_n$, $g \in G$. Clearly G_{n+1}/G_{n+2} is generated by the cosets of all such (h,g). Since $h \in G_n$ by the inductive hypothesis we see that $h = \prod_{i=1}^{n} h_i^{\epsilon_i} h'$, $\epsilon_i = \pm 1$ where $h' \in G_{n+1}$, $h_i \in G_n$ and h_i is of the form (4-1). Using theorem 3 we see that

$$(h,g) = \left(\left[\prod_{i=1}^{n} h_i^{\epsilon_i} \right] h', g \right) \equiv \left(\prod_{i=1}^{n} h_i^{\epsilon_i}, g \right)(h',g) \pmod{G_{2n+1}}$$

$$\equiv \left(\prod_{i=1}^{n} (h_i \; ,g)^{\epsilon_i} \right)(h',g) \pmod{G_{2n+1}}.$$

Since $(h',g) \in G_{n+2}$ then

$$(h,g) \equiv \prod_{i=1}^{n} (h_i \; ,g)^{\epsilon_i} \pmod{G_{n+2}}.$$

Now $g = \prod_{j=1}^{s} x_{p_j}^{\epsilon_j}$ where $p_j \in \{1, \ldots ,r\}$ so

$$(h_i,g) \equiv (h_i, \prod_{j=1}^{s} x_{p_j}^{\epsilon_i}) \pmod{G_{n+2}} \equiv \prod_{j=1}^{s} (h_i, \; x_{p_j})^{\epsilon_i} \pmod{G_{n+2}}.$$

Therefore,

$$(h,g) \equiv \prod_{i=1}^{n} \left[\prod_{j=1}^{s} (h_i, \; x_{p_j})^{\epsilon_i} \right] \pmod{G_{n+2}}.$$

Since h_i is of the form (4-1) then (h_i,x_{p_j}) is also of the form (4-1) by replacing n by n+1 and we have our desired results.■

The Restricted Burnside Problem

In 1950 Magnus introduced a weaker version of Burnside's question: "Is there a bound on the orders of finite quotients of $B(n,r)$?" This is known as the restricted Burnside problem. Since the answer to this question comes from examining the LCS of the previous section, it fits in with our discussion. In addition, if $B(n,r)$ fails to be finite, but a bound on finite quotients of $B(n,r)$ does exist we will be able to focus on an obstruction, a term of the LCS, to the finiteness of $B(n,r)$.

If $p^k|n$ for some prime p, then since $B(n,r)$ has $B(p^k,r)$ as a factor group, $B(n,r)$ is infinite if $B(p^k,r)$ is infinite, and $B(p^k,r)$ will be finite if $B(n,r)$ is finite. Therefore, the case of $n = p^k$ deserves special attention.

Definition: A group is a *p-group* if every element of G has order a power of p, a prime.

Theorem 5: If $q = p^k$, where p is a prime, and if $B(q,r)$ is finite, then $B(q,r)$ is nilpotent.

Proof: Every finite p-group is nilpotent. We know that every element of $B(q,r)$ has order that divides q, thus $B(q,r)$ is a p-group.∎

Suppose that $B(p^k,r)$'s LCS terminates after a finite number of steps with a group $\hat{B}(p^k,r)$ which is infinite, then the quotient group

$$B^*(p^k,r) = \frac{B(p^k,r)}{\hat{B}(p^k,r)}$$ will be shown to be finite.

B^* would then have the property of being maximal in the sense that every finite group with r generators where $w^{p^k} = 1$, will have order $\leq |B^*|$. To see this, first note that $\frac{B_i(p^k,r)}{B_{i+1}(p^k,r)}$ must be finite since every element has order that divides p^k and it is finitely generated and abelian. To show that $B^*(p^k,r)$ is finite we use an inductive argument, and show $\frac{B(p^k,r)}{B_i(p^k,r)}$ is finite for all i.

In the case where $i = 0$ we have that $\frac{B(p^k,r)}{B_1(p^k,r)}$ is finite.

Assume $\frac{B(p^k,r)}{B_{i-1}(p^k,r)}$ is finite. Then by the third isomorphism theorem we have

$$\frac{B(p^k,r)}{B_{i-1}(p^k,r)} \cong \frac{B(p^k,r)\big/B_i(p^k,r)}{B_{i-1}(p^k,r)\big/B_i(p^k,r)}$$

but $B_{i-1}(p^k,r) \Big/ B_i(p^k,r)$ is finite, thus $\dfrac{B(p^k,r)}{B_i(p^k,r)}$ is finite

and since $\hat{B}(p^k,r) = B_i(p^k,r)$ for some i then $B*(p^k,r)$ is finite.

Next we show that $B*(p^k,r)$ has the maximal property. Let G be a group, finite, which is generated by r elements where $g^{p^k} = e \ \forall g \in G$. There exists a homomorphism from $B(p^k,r)$ onto G. Recall that G is nilpotent. Let B_i represent the ith group in $B(p^k,r)$'s LCS and G_i represent G similarly. Calculating their LCS we get

$$B_1 \supset B_2 \supset \ldots \supset B_n = \hat{B} = B_{n+1}$$

$$G_1 \supset G_2 \supset \ldots \supset G_i = \{e\} \text{ for some } i \geq 1.$$

Let Φ be the onto homomorphism $\Phi\colon B_1 \Rightarrow G_1$. Then $\Phi|_{B_2}$ will be an onto homomorphism $\Phi|_{B_2}\colon B_2 \Rightarrow G_2$. etc. Since G's LCS terminates at $G_i = \{e\}$ and B's LCS terminates at B_n, then we claim that $i \leq n$. To see this we note that since $B_n = B_{n+1}$ then $\Phi|_{B_n}(B_n) = \Phi|_{B_{n+1}}(B_{n+1})$. So $G_n = G_{n+1}$, but this is true only when $n \geq i$. Thus $B_n \subseteq \text{Ker } \Phi$ and by the third isomorphism theorem $G \cong B* \ {}_{\text{Ker}\Phi}\ {}_{B_n}$ and G is a homomorphic image of

$B* = {}^{B}1/B_n$. Further suppose there exists a maximal finite quotient for $B(p^k,r)$. If the LCS of $B(p^k,r)$ does not stabilize after a finite number of steps, then the sequence

$\{B_1/B_2,\ B_1/B_3,\ \ldots\}$ forms a sequence of finite quotients with strictly increasing order. But this sequence must be finite, therefore $B(p^k,r)$'s LCS stabilizes after a finite number of steps.

Now, suppose that $B(p^k,r)$ is infinite but its LCS reaches, after a finite number of steps, a group $B_i(p^k,r)$. $B_i(p^k,r)$ is nilpotent since it is a p-group. By the word above $B^*(p^k,r) = B(p^k,r)/B_i(p^k,r)$ is maximal in the sense described earlier. Thus when $n = p^k$ the restricted Burnside problem takes the form: " Does the lower central series of $B(p^k,r)$ become stationary after a finite number of steps?".

If we can show that for every such group $G = B(p^k,r)$ there is an integer $s = s(p^k,r)$ such that $G_s = G_{s+1}$, then we shall have solved the restricted Burnside problem for exponent $n = p^k$. The finiteness of G then reduces to the finiteness of G_s. Of course G_s can be infinite or finite, but knowing this integer, s, and maximal bound N on finite quotients will tell us that if we find N + 1 distinct elements in the group, then the group must be infinite.

The answer to the restricted Burnside question is known to be yes for k = 1. This comprehensive finding is known as Kostrikin's Theorem. His arguments show that certain theorems about finitely generated Lie rings lead to a bound on the orders of the finite quotient groups of

B(p,r).[6]

Next, we will discuss how the nilpotency of the Lie ring is used to solve the restricted Burnside problem.

---

[6]Recently E. I. Zelmanov solved the restricted Burnside problem for groups of prime power exponent.

The Lie Ring

Briefly let us show how the Lie Ring of B(q,r), denoted L(B(q,r)), is used to solve the restricted Burnside problem for $q = p^k$. We showed that if $B_i = B_{i+1}$ for some $i \geq 1$ then B*(q,r) is finite and we will show that this implies that the jth term of the LCS of L(B(q,r)) is zero for $j \geq i$, L(B(q,r)) is finite and has the same order and nilpotency class as B*(q,r). Hence if L(B(q,r)) is infinite, then there is no bound on the orders of the quotient groups $B(q,r)/B_i(q,r)$ and hence no bound on the orders of finite r generator groups of exponent q.

In an associative ring R let us define a Lie product [x,y] by the rule [x,y] = xy - yx. Then with respect to the addition in R and the Lie product, the elements of R form a Lie ring L.

A Lie ring L satisfies the following laws:

L1: Addition x + y, and Lie product [x,y] are well defined operations.

L2: L, + is an abelian group.

L3: $[x+y,z] = [x,z] + [y,z]$, $[x,y+z] = [x,y] + [x,z]$.

L4: $[x,x] = 0$.

L5: $[[x,y],z] + [[y,z],x] + [[z,x],y] = 0$.

It is straight forward to show that the Lie product $[x,y] = xy - yx$ satisfies the above laws.

From L3 and L4 we find

$0 = [x+y,x+y] = [x,x] + [x,y] + [y,x] + [y,y]$
$= [x,y] + [y,x]$ whence we get that $[x,y] = -[y,x]$.

If R is generated by elements $x_1, \ldots, x_r$ then the elements generated from $x_1, \ldots, x_r$ by addition and the Lie product $[x,y]$ will not in general include all the elements generated in R by addition and the associative product (Consider the ring $\mathbb{Z}_5[x]$, the Lie product of any two elements will always be linear.).

The elements generated by the Lie product are called *Lie elements*. Thus x_1^2 is not a Lie element, but
$x_1^2x_2 - 2x_1x_2x_1 + x_2x_1^2 = x_1(x_1x_2-x_2x_1) - (x_1x_2 - x_2x_1)x_1$
$= [x_1, x_1x_2 - x_2x_1] = [x_1,[x_1,x_2]]$ is a lie element. It may, of course, happen that x_1^2 is equal to a Lie element because of relations in R.

We may take the laws L1, L2, L3, L4, L5, as the definition of a Lie ring L.

If G is a group with lower central series, $G = G_1 \geq \ldots \geq G_n \geq \ldots$, then the *associative Lie ring* L of G is formed in the following way:

L1) L is the Cartesian sum of the additively written factor groups G_i/G_{i+1}. The Cartesian sum gives the addition in L

$$L(G) = \Sigma_{i=m}^{\infty} \; G_i/G_{i+1} = G_1/G_2 \oplus G_2/G_3 \oplus \cdots \quad \text{where } G_i/G_{i+1}$$

are called *homogeneous* components. The Lie product

$[aG_{i+1}, bG_{j+1}] = (a,b)G_{i+j+1}$ is well defined by theorem 1 where $a \in G_i$ and $b \in G_j$. Also we know from theorem 1 that $(a,b) \in G_{i+j}$ so $(a,b)G_{i+j+1} \in G_{i+j}/G_{i+j+1}$ and is inductively defined for larger products. More general Lie products are defined by requiring the distributive law.

L2) Since each G_i/G_{i+1} is abelian addition is commutative.

L3) It suffices to show

$[gG_{i+1} + hG_{i+1}, kG_{j+1}] = [gG_{i+1}, kG_{j+1}] + [hG_{i+1}, kG_{j+1}]$.

$$\begin{aligned} [gG_{i+1} + hG_{i+1}, kG_{j+1}] &= [ghG_{i+1}, kG_{j+1}] \\ &= (gh,k)G_{i+j+1} \\ &= (g,k)(h,k)G_{i+j+1} \text{ since } i+j+1 \leq 2i+j \\ &= (g,k)G_{i+j+1} + (h,k)G_{i+j+1} \\ &= [gG_{i+1}, kG_{j+1}] + [hG_{i+1}, kG_{j+1}]. \end{aligned}$$

The proof for

$[gG_{i+1}, hG_{j+1} + kG_{j+1}] = [gG_{i+1}, hG_{j+1}] + [gG_{i+1}, kG_{j+1}]$

is similar.

L4) $[gG_{i+1}, gG_{i+1}] = (g,g)G_{2i+1} = eG_{2i+1}$ which is the zero element in the 2i+1'st component under $\oplus$.[7]

L5) From L3 we only need to show $[[x,y],z] + [[y,z],x] + [[z,x],y] = 0$ for homogeneous x,y,z. But $[[gG_{i+1}, hG_{j+1}], kG_{l+1}] + [[hG_{j+1}, kG_{l+1}], gG_{i+1}] + [[kG_{l+1}, gG_{i+1}], hG_{j+1}] = 0$ follows from lemma 2. Thus

---

[7] $0 \in L(G)$ is denoted as $0 = eG_2 + eG_3 + \ldots$.

$L(G)$ is a Lie Ring and has the anti-commutative property $[gG_{i+1},hG_{j+1}] = -[hG_{j+1},gG_{i+1}]$.

In a Lie Ring L let us write monomials in left normed form, ie., write x_1x_2 for $[x_1,x_2]$ and recursively $x_1x_2\ldots x_n$ for $[x_1,x_2, \ldots , x_n]$.

The lower central series of $L(G)$ is defined analogously to be the LCS of G where $L^1(G) = L(G)$, $L^{i+1}(G) = [L^i(G),L(G)]$ $i \geq 1$. Note that in $L(G) = \sum_{i=m}^{\infty} G_i/G_{i+1}$ elements are such that only a finite number of terms may be not 0. To show that $L^2(G) = \sum_{i=m}^{\infty} G_i/G_{i+1}$ we see given gG_2, $hG_2 \in G/G_2$ that $[gG_2,hG_2] = (g,h)G_3 \in G_2/G_3$, thus elements of $L^2(G)$ have zero component in G/G_2. Assuming that $L^m(G) = \sum_{i=m}^{\infty} G_i/G_{i+1}$ for $m \geq 2$, an arbitrary element $[gG_{m+1},hG_2] = (g,h)G_{m+2}$ in $L^{m+1}(G)$, thus elements of $L^{m+1}(G)$ have zero component in G_m/G_{m+1}.

Theorem 6 : $L^{i+1}(G)$ is generated by all left normed Lie elements $[x_{p_1}G_2 , \ldots, x_{p_{i+1}}G_2]$ where the x_i are generators of G and $p_k \in \{1, \ldots r\}$.

Proof: From theorem 4 we have that G_n/G_{n+1} is generated by the cosets of the simple n-fold commutator $(x_{p_1}, \ldots , x_{p_n})$.

$L^1(G) = L(G)$ and is generated by

$\{x_1G_2, x_2G_2, \ldots ,x_rG_2\} = \{x_iG_2 \mid i \in \{1,, \ldots ,r\}\}$.

$L^2(G)$ is generated by the

$$[x_iG_2,x_jG_2] = (x_i,x_j)G_3 = \{(x_i,x_j)G_3 \mid i,j \in \{1, \ldots ,r\}\}$$

by theorem 2. Assume $L^k(G)$ is generated by

$[x_{p_1}G_2, \ldots ,x_{p_k}G_2]$.

Recalling that $[x_{p_1}G_2, \ldots ,x_{p_k}G_2] = (x_{p_1}, \ldots ,x_{p_k})G_{k+1}$

then $L^k(G)$ is generated by

$$\{(x_{p_1}, \ldots ,x_{p_k})G_{k+1} \mid p_i \in \{1, \ldots ,r\}\}.$$

To see that $L^{k+1}(G)$ is generated by

$$\{(x_{p_1}, \ldots ,x_{p_{k+1}})G_{k+2} \mid p_i \in \{1, \ldots ,r\}\}$$

recall that $L^{k+1}(G) = [L^k(G) ,L(G)]$ where a generator is of the form $[(x_{p_1}, \ldots , x_{p_k})G_{k+1}, x_{p_i}G_2], \ p_i \in \{1, \ldots ,r\}$.

This in turn is equal to $(x_{p_1}, \ldots ,x_{p_k},x_{p_i})G_{k+2}$

$$= (x_{p_1}, \ldots ,x_{p_{k+1}})\ G_{k+2},\ p_i \in \{1, \ldots ,r\}$$

$$= [x_{p_1}G_2, \ldots,x_{p_{k+1}}G_2].\blacksquare$$

Next, since the factor group B(n,r) and the Lie ring L(B(n,r)) share many properties, if we could show that the LCS of B(n,r) stabilizes after the kth term when the kth term of the LCS of L(B(n,r)) is trivial then we will have answered the restricted Burnside question for B(n,r). This equivalence is advantageous since showing that higher commutators are trivial will be an easier task to accomplish in L(B(n,r)).

Theorem 7: $G_n = G_{n+1}$ iff $L^n(G) = 0$.

Proof: If $G_n = G_{n+1}$ then $L(G) = \sum_{i=1}^{n} {}^{G_i}/G_{i+1}$ where n is finite. By the work above $L^n(G) = \sum_{i=n}^{n} {}^{G_i}/G_{i+1} = {}^{G_n}/G_{n+1}$ $= 0_L = \{e_G\}$.

Going the other way, if $L^n(G) = 0$ then $L^n(G) = \sum_{i=n}^{\infty} {}^{G_i}/G_{i+1} = 0_L$ which implies that ${}^{G_n}/G_{n+1} = 0_L$ implying $G_n = G_{n+1}$.∎

Definition: If $L^n(G) = 0$ for some $n \geq 1$, then L(G) is *nilpotent*, and we say that L(G) is nilpotent of class n.

Some of the theorems that will be useful in L(B(p,r)) follow from theorems about basic commutators. The collection formula, whereby basic commutators are collected in order of their weight, developed by P. Hall leads to the following theorem.

Theorem 8: We may collect the product $(a_1a_2...a_r)^n$ in the form

$$(a_1a_2...a_r)^n = a_1^n a_2^n ... a_r^n c_{r+1}^{e_{r+1}} ... c_i^{e_i} R_1 ... R_t,$$

where $c_{r+1}, \ldots ,c_i$ are the basic commutators on $a_1, \ldots ,a_r$ in order, and $R_1, \ldots ,R_t$ are basic commutators later than c_i in the ordering. For $1 \leq j \leq i$, the exponent e_j is of the form

$$e_j = b_1 n + b_2 n^{(2)} + \ldots + b_m n^{(m)},$$

where m is the weight of c_j, the b's are non-negative integers and do not depend on n but only on c_j. Here $n^{(k)} = n(n-1)\ldots(n-k+1)/k! = \binom{n}{k}$.

The proof consists of keeping track of from which occurrence of $a_1, a_2, \ldots$ a commutator arises. For example in the product

$$\begin{aligned}(xy)^5 = xyxyxyxyxy &= x^2y(y,x)yxyxyxy \\ &= x^2y(y,x)xy(y,x)yxyxy \\ &= x^2yx(y,x)(y,x,x)y(y,x)yxyxy \\ &= x^3y(y,x)^2(y,x,x)y(y,x)yxyxy\end{aligned}$$

(y,x,x) is labeled as $C_{yxx}(1,2,3)$ since it arose from the first y and the second and third x's. It can be shown that whether an arbitrary commutator will occur only depends on the inequalities that hold between coordinates. For example, if (2,3,4) is a label that occurs, so is (a,b,c) for all a,b,c such that $a < b < c \leq n$. If these all occur, then there are $\binom{n}{3}$ of these labels so $\binom{n}{3}$ of $C_{yxx}(a,b,c)$ types occur.

Theorem 9: If $G = B(p,r)$, then $(y,x, \ldots ,x) \equiv 1 \pmod{G_{p+1}}$ ($p - 1$ x's).

Proof: In the collecting process above as applied to $(xy)^n$ we have $(xy)^n = x^n y^n c_1^{a_1(n)} \ldots c_t^{a_t(n)} R_1 \ldots R_t$ where if c_i is of weight m, then its exponent, $a_i(n)$ is of the form:

$$b_i n + b_{i_2}\binom{n}{2} + \ldots + b_{i_m}\binom{n}{m}.$$

And if c_i is of the form $c_i = (y,x,\ldots,x)$ (where x occurs s times), the exponent $a_i(n)$ is the number of ways of choosing indices $j_1, j_2, \ldots, j_{s+1}$ such that in $(y_{j_1}, x_{j_2}, \ldots, x_{j_{s+1}})$ we have $j_1 < j_2, \ldots < j_{s+1}$, and $1 \le j_k \le n$. But this is merely the number of ways of choosing $s + 1$ distinct numbers from $1,2,\ldots,n$ and is $\binom{n}{s+1}$.

If $n = p$ is a prime, the exponents for commutators of weights at most $p - 1$, the $a_i(p)$ are all multiples of p since the binomial coefficients $\binom{p}{i}$ with $1 \le i \le p - 1$ are all multiples of p. But for the commutator $(y,x, \ldots ,x)$ ($p-1$ occurrences of x), the exponent is $\binom{p}{p} = 1$. Hence in a group G of exponent p we have

$1 = (xy)^p = (y,x, \ldots ,x)v_1 \ldots v_t$ ($p - 1$ occurrences of x), where $x < y$ and $v_1, \ldots ,v_t$ are commutators of weight at least p, and for those of weight p the weight in y is at least 2.

This gives the relation in G_p/G_{p+1}

$$(y,x, \ldots ,x)v_1 \ldots v_s \equiv 1 \pmod{G_{p+1}}$$
$$(p - 1 \text{ occurrences of } x). \qquad (9\text{-}1)$$

where $v_1, \ldots , v_s$ are commutators of weight p in x and y, and of weight at least 2 in y and at most $p-2$ in x. From theorem 3 we have generally in any group that if (u,v) is of weight m, then $(u^i,v^j) \equiv (u,v)^{ij} \pmod{G_{m+1}}$.

Using this we find that if a v_i in (9-1) is of weight r in x the replacement of x by x^i in (9-1) can be viewed as replacing v by v^{i^r} where $v_i = (y,y,\ldots,y,x,x,\ldots,x)$ is of weight r in x. Theorem 4 implies that v_i is of the form involving only x's and y's. The collection process with $x < y$ on basic commutators implies that the y's occur to the left of the x's.

Since the choice of y and x was arbitrary in (9-1) then replacing each occurrence of x by x^i will not change the equivalence relation. Then we can let

$$v_0 = (y,x,x,\ldots,x) \quad (p\text{-}1\ x\text{'s})$$

and $w_i = v_0^{i^{p-1}} v_1^{i^{r_1}} \ldots v_s^{i^{r_s}}$ where r_j is the weight of x in v_j. By multiplying w_1 through w_{p-1} together we get $w_1 w_2 \ldots w_{p-1} \equiv 1 \pmod{G_{p+1}}$ since $w_i \in G_{p+1}$. By the identity $ab = ba(a,b)$ we can collect all the v_j's together and we get the following

$$v_0^{u_0} v_1^{u_1} \ldots v_s^{u_s} p_1 p_2 \ldots p_m \equiv 1 \pmod{G_{p+1}}$$

where $u_i = 1 + 2^{r_i} + \ldots + (p-1)^{r_i}$ and p_j is a commutator of weight $\geq p+1$. Since we have congruence modulo G_{p+1}, the relation becomes $v_0^{u_0} v_1^{u_1} \ldots v_s^{u_s} \equiv 1 \pmod{G_{p+1}}$. Now,

$$1^r + 2^r + \ldots + (p-1)^r \equiv 0 \pmod p \text{ for } 1 \leq r \leq p-2,$$

so $u_i \equiv 0 \pmod p$ for $1 \leq r_i \leq p-2$; $i^r \equiv 1 \pmod p$ when $r = p-1$ so $u_0 = p - 1 \pmod p$ and (9-1) becomes

$$(y,x,x,\ldots,x)^{p-1} \equiv 1 \pmod{G_{p+1}} \text{ and so}$$

$$(y,x,x,\ldots,x) \equiv 1 \pmod{G_{p+1}}$$

since $z^{p-1} = z^{-1} = 1$ implies $z = 1$.∎

Definition: A ring R has characteristic n if there is a least positive integer n such that na = 0 for all $a \in R$.

Lemma 3: L(G) has characteristic p, for G = (p,r).

Proof: Let L(G) be the Lie Ring of B(p,r). Let x be an arbitrary element in L(G) where $x = (x_1, x_2, \ldots)$ then $px = (x_1^p, x_2^p, \ldots) = 0$ thus L(G) has characteristic p.∎

The realization of (y,x,...,x) is not easily distinguishable in G. If we can show that $yx^{p-1} = 0$ in L(G) then the consequences of this relation are more easily recognized in L(G).

Corollary 9-1: The Lie Ring of a group of prime exponent p satisfies the identical relation $yx^{p-1} = 0$.

Proof: L(G) is of characteristic p. Since $(y,x,\ldots,x)^{p-1}$ is $(p-1)yx^k$ (k occurrences of x) in L(G) by definition then $yx^{p-1} = 0$ by Theorem 9.∎

Let us call the relation $yx^{p-1} = 0$ the (p-1)-*Engel condition*.

Thus we have shown that if L(B(q,r)) is finite, then there is a bound on the orders of finite r generator groups of exponent $q = p^k$, and the largest of these groups has the same order and nilpotency class as L(B(q,r)). This fact is essential to Kostrikin's solution to the restricted Burnside problem for exponent p in which he proves that L(B(p,r)) is nilpotent.

The Finiteness of $B(3,r)$

As we stated earlier, Kostrikin solved the Restricted Burnside problem for prime exponent. We will prove that $B(3,r)$ is finite by first proving Kostrikin's theorem for $p = 3$.

Let $x,y,z,t \in L(B(3,r))$. By corollary 9-1 we have

$$xy^2 = xz^2 = x(y + z)^2 = 0.$$

So $x(y+z)^2 = (xy + xz)(y + z) = xy^2 + xyz + xzy + xz^2$ and we see that

$$xyz + xzy = 0. \tag{9-2}$$

Since $xy + yx = 0$ by the anticommutativity of $L(B(3,r))$ then we also have

$$xyz + yxz = 0. \tag{9-3}$$

Combining the results from (9-2) and (9-3) we see that

$$xyz = yzx = zxy = -yxz = -xzy = -zyx. \tag{9-4}$$

Applying the Jacoby identity $xyz + yzx + zxy = 0$ to (9-4) we get

$$3xyz = 0. \tag{9-5}$$

Now by using (9-4) repeatedly we have

$$\begin{aligned} xyzt &= (xy)zt \\ &= zt(xy) \\ &= -(xy)(zt) \quad \text{(by anticommutativity)} \\ &= y(zt)x + (zt)xy \quad \text{(by the Jacoby identity)} \\ &= (zt)xy - (zt)yx \end{aligned}$$

$$= 2(zt)xy$$
$$= 2ztxy.$$

Also

$$\begin{aligned} xyzt &= (xyz)t \\ &= (zxy)t \\ &= (zx)yt \\ &= -(zx)ty \\ &= (ztx)y \\ &= ztxy. \end{aligned}$$

Thus we see that $2ztxy = ztxy$ so $ztxy = 0$. So we have that $L(B(3,r))$ is nilpotent. and the Restricted Burnside problem for $B(3,r)$ has been solved.

Since the identities

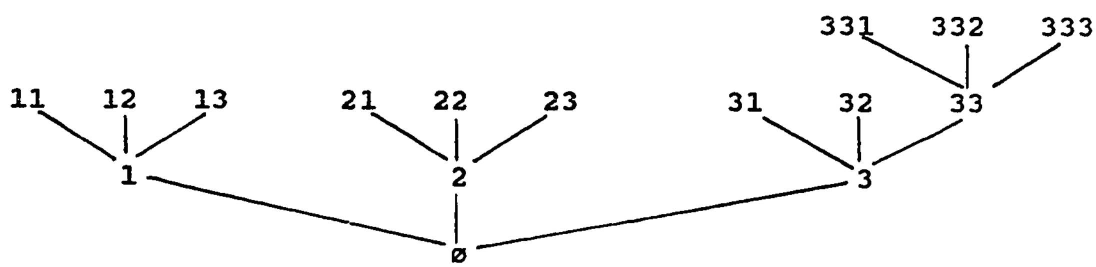
$$[x,y,z,t] = 1$$
$$[x,y,z] = [y,z,x] = [z,x,y] = [x,z,y]^{-1}$$
$$= [z,y,x]^{-1} = [y,x,z]^{-1}$$

follow immediately from the Lie identities, then all groups of exponent 3 are nilpotent and hence finite, if finitely generated. Thus $B(3,r)$ is finite.

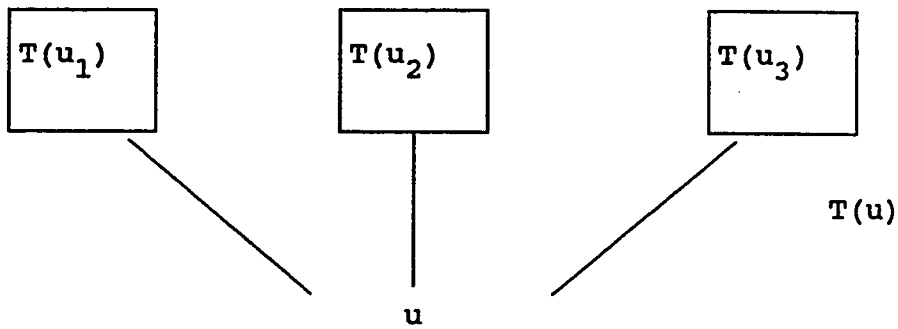
The Existence of a Finitely Generated Infinite 3-group

The General Burnside problem was resolved in 1964 by Golod. Based on his joint work with Shafarevich, Golod proved the existence of finitely generated infinite p-groups of all primes p. We will, here, give the construction, due to Gupta and Sidki, of a 2-generator, infinite 3-group using tree automorphisms (as described in AMJ April 1989).

Let T be a tree with root denoted "ø" such that from ø and from the end of each branch precisely 3 new branches grow upwards, and subscript as below.



For any vertex u of T let T(u) denote the subtree with root "u". Then T = T(ø) is an infinite (everbranching) 3-regular tree with the property that T(ø) ≅ T(u) for all u (note that $T(u) = (T(u_1),T(u_2),T(u_3))$ since u can be described in terms of its branches u_1, u_2, u_3).



For each vertex u we define an automorphism t_u(= [t_u: T(u) → T(u)]) of T(u) by mapping $T(u_1)$ onto $T(u_2)$, $T(u_2)$ onto $T(U_3)$, and $T(u_3)$ onto $T(u_1)$ (Note: this automorphism can be thought of as grafting the branch starting at u_1 onto the branch where u_2 was previously located. Otherwise, $t_{u_{i1\ldots in}}(v)$ alters only the n+1st subscript so $t_{u_{i1\ldots in}}(v) = v$ if v has fewer or the same number of subscripts or if the first n subscripts of v differ from those of $u_{i1\ldots in}$). Clearly t_u has order 3. Using these automorphisms as a tool we next define an automorphism a_u(= [a_u: T(u) → T(u)]) by its action on the subtrees $T(u_1)$, $T(u_2)$, and $T(u_3)$ as follows. We set $a_u(u)=u$ and $a_u(v) = v$ if v is not above u, and $a_u = (t_{u1}, t_{u2}^2, a_{u3})$ with each component representing the action on the corresponding subtree. Since T(u) ≅ T(Φ) we can describe the action a_u from the initial node Φ. For example, we compute the image of v = 3321, and w=123 under $a = a_\emptyset \cong a_u$ as

$$a_\emptyset(w) = t_1(123) = 133$$

$a_\emptyset(v) = a_3(3321) = a_{33}(3321) = t_{332}^2(3321) = 3323.$

Note that 3 acts like the identity on a level (ie. $a_u(3333) = a_{3333}(3333) = 3333$).

Since we can compare componentwise $a_u^3 = (1,1, a_{u3}^3)$ it follows inductively that a_u has order a power of 3. We set $G_u = \langle a_u, t_u \rangle$ to be the subgroup of the automorphism group of T(u) generated by a_u and t_u (note that $G_\emptyset$ and G_u are isomorphic for each vertex u). We proceed to show that each G_u so constructed is an infinite 3-group. We set

$$b_u = t_u^{-1} a_u t_u = (t_u^{-1} t_{u2}^2 t_u,\ t_u^{-1} a_{u3} t_u,\ t_u^{-1} t_{u1} t_u),$$

$$c_u = t_u^{-2} a_u t_u^2 = (t_u^{-2}\ a_{u3} t_u^2,\ t_u^{-2} t_{u1} t_u^2,\ t_u^{-2} t_{u2}^2 t_u^2)$$

so that

$$a_u = (t_{u1}, t_{u2}^2, a_{u3}),$$

$$b_u = (t_{u1}^2, a_{u2}, t_{u3}),$$

$$c_u = (a_{u1}, t_{u2}, t_{u3}^2).$$

Let $H_u = \langle a_u, b_u, c_u \rangle$. We show that H_u is a proper normal subgroup of G_u of index 3. First note that H_u fixes u1 (t_{u1} and a_{u1} leave u1 fixed) but t_u permutes {u1,u2,u3}. Thus H_u is proper.

Next, we show that H_u is normal. It suffices to look at the generators of G_u and H_u. $a_u h a_u^{-1} \in H$ since $a_u \in H_u$. To see that $t_u h t_u^{-1} \in H_u$ we need to look at the generators of H_u in turn:

$$t_u a_u t_u^{-1} = t_u^{-2} a_u t_u^2 = c_u \in H,$$

$$t_u b_u t_u^{-1} = t_u^2 t_u a_u t_u t_u^{-1} = t_u^3 a_u = a_u \in H,$$

$$t_u c_u t_u^{-1} = t_u^2 a_u t_u^2 t_u^{-1} = t_u^2 a_u t_u = b_u \in H.$$

Thus H_u is normal.

Finally, let $\bar{t}_u \in G_u/H_u$. We know $\bar{t}_u^3 = \bar{1}$ and $\bar{t}_u \neq 1$ since $t_u \notin H_u$. Therefore, $\bar{t}_u$ has order 3. So H_u has index 3 in G_u/H_u. Since the action of H_u on $T(u_1)$ is generated by $\langle a_{u_1}, t_{u_1}\rangle = G_{u_1} \cong G_u$, then G_u has a proper subgroup isomorphic to itself, and so G_u must be infinite. Thus to finish the proof we must show that G_u is a 3-group.

First, observe that

$G_u = \{w_u t_u^{\alpha(u)}$, where $w_u \in H_u$ and $\alpha(u) \in \{0,1,2\}\}$.

For each $g_u = w_u t_u^{\alpha(u)}$ we define its formal length $|g_u|$ as $\lambda(w_u)$ if $\alpha(u) \equiv 0 \bmod(3)$ and as $\lambda(w_u) + 1$ if $\alpha(u) \not\equiv 0 \bmod(3)$, where $\lambda(w_u)$ the formal syllable length is defined as follows:

If $w_u = v_1^{u_1} \ldots v_r^{u_r}$ where $v_i \in \{a_u, b_u, c_u\}$ and $v_i \neq v_{i+1}$, then $\lambda(w_u) = r$.

To prove that G_u is a 3-group it suffices to prove by induction on the formal length $|g_u| = n$ that g_u has order dividing 3^n. If $|g_u| = 1$, then $g_u = a_u^\alpha$ or b_u^α or c_u^α or t_u^α for some α, and it follows that g_u has order 3. Let $|g_u| = n+1$, $n \geq 1$, and assume the results for elements of formal length up to n. If g_u is of the form $g_u = w_u$, then, as an element of H_u, then $g_u = (g_{u1}, g_{u2}, g_{u3})$ where each g_{ui}

has length at most n. If $g_{ui} \in H_{ui}$ then the facts that $a_u t_u = t_u b_u$, $a_u t_u^2 = t_u^2 c_u$ are used to "herd" the t_u's together such that the length of g_u never increases. If $g_{ui} \in H_{ui}$ after "herding" the t_u's, they appear with exponent a multiple of 3 and so drop out, and there is at least one fewer syllable and we are done by induction. Otherwise, $g_{ui} = w_{ui} t_{ui}^{\alpha(i)}$ with $w_{ui} \in H_{ui}$, $|w_{ui}| \le n$, and $\alpha(i) \in \{1,2\}$.

Thus without loss of generality, we may assume that g_u itself has the form $g_u = w_u t_u^{\alpha}$ with $w_u \in H_u$, $|w_u| = n$ and $\alpha \in \{1,2\}$. Then g_u^3 is an element of H_u since H_u has index 3 in G_u. It can be expressed in the following form:

$$\begin{aligned} g_u^3 &= w_u t_u^{\alpha} w_u t_u^{\alpha} w_u t_u^{\alpha} \\ &= w_u (t_u^{\alpha} w_u t_u^{-\alpha})(t_u^{2\alpha} w_u t_u^{-2\alpha}) \\ &= w_u\, \Pi_1(w_u)\, \Pi_2(w_u) \quad \text{where } \Pi_i \text{ are permutations} \end{aligned}$$

of the letters of w_u. and $\Pi_2 = \Pi_1^2 = \Pi_1^{-1}$. As an example of this let $w_u = a_u^{\kappa} b_u^{\beta} c_u^{\lambda}$ and let $\alpha = 1$, $\kappa,\beta,\lambda \in \{0,1,2\}$ then

$$\begin{aligned} \Pi_1(w_u) &= t_u a_u^{\kappa} b_u^{\beta} c_u^{\lambda} t_u^{-1} \\ &= (t_u a_u^{\kappa} t_u^{-1}) t_u (t_u^{-1} a_u t_u)^{\beta} (t_u^{-2} a_u t_u)^{\lambda} t_u^{-1} \\ &= c_u^{\kappa} a_u^{\beta} t_u t_u^{-2} a_u^{\lambda} t_u \\ &= c_u^{\kappa} a_u^{\beta} b_u^{\lambda}. \end{aligned}$$

Clearly $\Pi_2 = \Pi_1^2$. In general $\Pi_1(w_u)$ is a word where a_u's are replaced with c_u's, b_u's by a_u's and c_u's by b_u's, and $\Pi_2(w_u) = \Pi_1^2(w_u)$ similarly permutes a_u, b_u, and c_u. This means the word g_u^3 has as many a_u^{α} 's as b_u^{β} 's as c_u^{χ} 's. If $|w_u| = k$, g_u^3 will have k a_u^{α} 's, k b_u^{β} 's, and k c_u^{χ} 's.

Now, consider any word with k a_u^{α} 's, k b_u^{β} 's, and k c_u^{χ} 's. Componentwise, each component will be a product of k a_{ui}^{α} types and 2k t_{ui}^{β} types since one of the components is an a-type and the other 2 are t-types. (Note: it does not matter whether the exponent is α, β, or χ since we are concerned only with the formal length). Thus each component is an alternating product of at most k a_{ui}^{α} types and 2k t_{ui}^{β}. Now, $t_{ui}^{-1} a_{ui}^{\alpha} t_{ui} = b_{ui}^{\alpha}$ and $t_{ui}^{-2} a_{ui}^{\alpha} t_{ui}^{2} = c_{ui}^{\alpha}$ so that

$$a_{ui}^{\alpha} t_{ui} = t_{ui} b_{ui}^{\alpha}.$$

and

$$a_{ui}^{\alpha} t_{ui}^{2} = t_{ui}^{2} c_{ui}^{\alpha}.$$

Using these relations we can herd together all of the t_{ui} to the left. Then the number of t_{ui} will be a multiple of 3. To see this, if w_u has l a_u's, m b_u's and n c_u's, component 1 will have $l + 2m$ t's from w_u $m + 2n$ t's from $\Pi_1(w_u)$ and $n + 2l$ t's from $\Pi_2(w_u)$ for a total of $3(l + m + n)$ t's. By the relations above we will still have at most k syllables to the right of the t_u's. Therefore, $|w_{ui}| \le k$ where $g_u^3 = (w_{u1}, w_{u2}, w_{u3})$. By the induction hypothesis it follows that g_u has order dividing 3^{k+1} as was to be proved. Thus, the general Burnside question is answered.

In summary, we have shown in the beginning of part 2 that if B(n,r) is nilpotent, then B(n,r) is finite. In the specific case where $n = p^k$, B(n,r) is nilpotent, the LCS terminates in an infinite group $B_i(n,r)$, or the LCS does not terminate. If the LCS terminates in an infinite group

$B_i(n,r)$, then $B(n,r)$ modulo this group $B_i(n,r)$ will be a maximal finite group on r generators where every element has order dividing p^k. Thus the restricted Burnside problem, a weaker version of the Burnside problem, "Is there a bound on these finite groups?" was shown to be equivalent to "Does the LCS of $B(p^k,r)$ terminate after a finite number of steps?". However determining if the LCS terminates with the identity or even showing that it becomes stationary after a finite number of steps is still a difficult task. We have shown many similarities between the group $B(n,r)$ and the Lie ring $L(B(n,r))$ where commutator calculations are easier to work with and in particular that the nth term of the LCS of $L(B(n,r))$ implies that the n+1st group of the LCS of $B(n,r)$ becomes stationary. Next, we showed that $B(3,r)$ is finite. Finally we showed that the answer of the Burnside question in general is no by proving the existence of a finitely generated infinite 3-group.

BIBLIOGRAPHY

Adian, S. 1979. The Burnside Problem and Identities in Groups, Springer-Verlag.

Enderton, H. 1972. A Mathematical Introduction to Logic, Academic Press.

Gupta, N. 1989. "On groups in which every element has finite order," Amer. Math. Monthly 4.

Hall, M. 1959. The Theory of Groups, MacMillan.

Kostrikin, A. 1964. "The Burnside problem", Amer. Math. Soc. Translation 36.

Magnus, W., Karass, A., Solitar, D. 1976. Combinatorial Group theory: Presentations of Groups in Terms of Generators and Relations, 2d ed., Dover.

Shoenfield, J. 1976. Mathematical Logic, Addision-Wesley.

Vaughan-Lee, M. 1990. The Restricted Burnside Problem, Oxford University.

APPENDIX

WORD PROBLEM DEFINITIONS

Definition (1): A decision procedure for E a subset of A is a method by which given any element $a \in A$ we can decide in a finite number of steps whether or not $a \in E$. The decision problem is whether such a procedure exists.

Definition (2): A group is *finitely presented* if it is isomorphic to a group [A;R] where both A and R are finite.

Definition (3): C(R) is *recursive* if given any word w on A, there is some finite set of instructions that will decode whether or not $w \in C(R)$.

Definition(4): C(R) is *recursively enumerable* if there is some finite set of instructions such that given any word w on A, will determine if $w \in C(R)$.

Definition (5): A group is *recursively presented* if it is isomorphic to a group [A;R] where A is finite and R is recursively enumerable.

Definition (6):Let G and G′ be groups and let Φ be an isomorphism of a subgroup H of G and a subgroup H′ of G′. The free product of the groups G and G′ with the *amalgamation* Φ is the group $G *\Phi G' = [G,G'; h=\Phi(h)]$. The natural mapping of G and G′ into $G *\Phi G'$ are injective; so we identify G and G′ with their images under these mappings. Then H and H′ are identified via the isomorphism Φ. We have $G *\Phi G' = \{G,G'\}$ (the subgroup generated by $G \cup G'$) and $G \cap G' = H = H'$. This last group is called the *amalgam.*

Definition (7): A group is *Higman* if it is finitely generated and embeddable in a finitely presented group.

Definition (8): If Φ is an isomorphism from a subgroup H of G into G then we define $G_\Phi = [G,t \; ; \; tht^{-1} = \Phi(h)]$ and call t the *Φ-element.*

Definition (9): *A subgroup K of G is invariant* under Φ if $\Phi(H \cap K) = \Phi(H) \cap K$.

Definition (10): Let G be a Higman group. An isomorphism Φ in G is *benign* if G_Φ is Higman. If Φ is the identity isomorphism of H then we write G_H for G_Φ.

Definition (11): A set Φ ,ψ,... of isomorphisms in a

Higman group G is benign if $G_{\phi,\psi,\ldots}$ may be embedded in a Higman group H so that $\{t_\Phi, t_\psi, \ldots\}$ is a benign subgroup.

Definition (12): A subset P of [A] is benign in [A] if E_P is benign in [A,z] where E_P is the subgroup of [A,z] generated by the words XzX^{-1} for X in P.

Definition (13): An *associate* of a mapping from [A] to [B] is a homomorphism from [A,z] to [B,z] such that $\psi(XzX^{-1}) = \Phi(X)z\Phi(X)^{-1}$ for X a word on A.

Definition (14): A bijective mapping from [A] to [A] is *nice* if it has an associate which is an automorphism of [A,z].

Definition (15): A word on A is *positive* if it does not contain any a^{-1} for $a \in A$.

Definition (16): Let P and Q be subsets of [A], and let Φ be a mapping from [A] to [A]. We say that P is (Φ,Q)-*invariant* if for each X in Q, $X \in P$ iff $\Phi(X) \in P$. If Q = [A], we say invariant under Φ for (Φ,Q)-invariant.

Definition (17): An n-*ary predicate* is a subset of the set of n-tuples in A. $P(a_1,a_2, \ldots,a_n)$ means an n-tuple in the predicate P.

Definition (18): An *explicit* definition of a function or predicate contains only previously defined functions and predicates.

Definition (19): A function F is recursive if:

1) $F = I_i^n(a_1, \ldots,a_n) = a_i$ (projection map), $F = P_+$, $F = P_\cdot$, or $F = K_<$ where $K_<$ is the 2-place function defined by $K_<(a_1,a_2) = \{ 0 \text{ if } a_1<a_2, 1 \text{ if } a_1 \geq a_2\}$.

2) $F(\Omega) = G(H_1(\Omega), \ldots,H_K(\Omega))$ where G, $H_1, \ldots,H_K$ are recursive functions.

3) If G is recursive and $\forall\Omega\exists x(G(\Omega,x) = 0)$, then $F(\Omega) = \mu x(G(\Omega,x) = 0)$ where $\mu x(G(\Omega,x) = 0) = x$ if for all $c < x$ $G(\Omega,c) \neq 0$ and $G(\Omega,x) = 0$.

Definition (20): K_P is a *representing partial functional* of predicate P defined on the same domain as P such that $K_P(\Omega) = 0$ if Ω is in P and $K_P(\Omega) = 1$ if Ω is not in P.

NOTATIONS

[A] is the free group on a set A.

{A} is a subgroup of G such that if the homomorphism from [A] to G which is the identity on A is injective then we identify the subgroup {A} of G with [A].

[A;R] is the group generated by the elements of A and the set of defining relations R.

$G *_\Phi H$: See definition 6.

$G * G' = [G,G'] = G *_\Phi G'$ if Φ is the isomorphism of the zero subgroups.

$G_\Phi = [G,t\ ;\ tht^{-1} = \Phi(h)]$: See defintion 10.

$G_H = G_\Phi$ if Φ is the identity isomorphism of H a subgroup of G.

$P_=$ is the predicate $\{(n,n)\}$.

P_+ is the predicate $\{(n,m,n+m)\}$.

$p_\cdot$ is the predicate $\{(n,m,nm)\}$.

P_F is the predicate $\{(x_1,\ldots,x_k,y)\}$ where $F(x_1,\ldots,x_k) = y$.

E_P: See definition 12.

$K_<$: See definition 19.

(Φ,H)-invariant: See definition 16.

K_P: See definition 20.