CHAPTER 12

The Word Problem

Introduction

Novikov, Boone, and Britton proved, independently, that there is a finitely presented group $\mathcal{B}$ for which no computer can ever exist that can decide whether an arbitrary word on the generators of $\mathcal{B}$ is 1. We shall prove this remarkable result in this chapter.

Informally, if $\mathcal{L}$ is a list of questions, then a decision process (or algorithm) for $\mathcal{L}$ is a uniform set of directions which, when applied to any of the questions in $\mathcal{L}$, gives the correct answer "yes" or "no" after a finite number of steps, never at any stage of the process leaving the user in doubt as to what to do next.

Suppose now that $G$ is a finitely generated group with the presentation

$$G = (x_1, \ldots, x_n | \gamma_j = 1, j \geq 1);$$

every (not necessarily reduced) word $\omega$ on $X = \{x_1, \ldots, x_n\}$ determines an element of $G$ (namely, $\omega R$, where $F$ is the free group with basis $X$ and $R$ is the normal subgroup of $F$ generated by $\{r_j, j \geq 1\}$). We say that $G$ has a solvable word problem if there exists a decision process for the set $\mathcal{L}$ of all questions of the form: If $\omega$ is a word on $X$, is $\omega = 1$ in $G$? (It appears that solvability of the word problem depends on the presentation. However, it can be shown that if $G$ is finitely generated and if its word problem is solvable for one presentation, then it is solvable for every presentation with a finite number of generators.)

Arrange all the words on $\{x_1, \ldots, x_n\}$ in a list as follows: Recall that the length of a (not necessarily reduced) word $\omega = x_1^{e_1} \ldots x_n^{e_m}$, where $e_i = \pm 1$, is $m$. For example, the empty word 1 has length 0, but the word $xx^{-1}$ has length 2. Now list all the words on $X$ as follows: first the empty word, then the
words of length 1 in the order $x_1, x_1^{-1}, \ldots, x_n, x_n^{-1}$, then the words of length 2 in "lexicographic" order (as in a dictionary): $x_1 x_1 < x_1 x_1^{-1} < x_1 x_2 < \cdots < x_1^{-1} x_1 < x_1^{-1} x_1^{-1} < \cdots < x_n^{-1} x_n^{-1}$, then the words of length 3 in lexicographic order, and so forth. Use this ordering of words: $\omega_0, \omega_1, \omega_2, \ldots$ to define the list $\mathcal{L}$ whose $k$th question asks whether $\omega_k = 1$ in $G$.

We illustrate by sketching a proof that a free group

$$G = (x_1, \ldots, x_n | \emptyset)$$

has a solvable word problem. Here is a decision process.

1. If $\text{length}(\omega_k) = 0$ or 1, proceed to Step 3. If $\text{length}(\omega_k) \geq 2$, underline the first adjacent pair of letters, if any, of the form $x_i x_i^{-1}$ or $x_i^{-1} x_i$; if there is no such pair, underline the final two letters; proceed to Step 2.
2. If the underlined pair of letters has the form $x_i x_i^{-1}$ or $x_i^{-1} x_i$, erase it and proceed to Step 1; otherwise, proceed to Step 3.
3. If the word is empty, write $\omega_k = 1$ and stop; if the word is not empty, write $\omega_k \neq 1$ and stop.

The reader should agree, even without a formal definition, that the set of directions above is a decision process showing that the free group $G$ has a solvable word problem.

The proof of the Novikov–Boone–Britton theorem can be split in half. The initial portion is really Mathematical Logic, and it is a theorem, proved independently by Markov and Post, that there exists a finitely presented semigroup $S$ having an unsolvable word problem. The more difficult portion of the proof consists of constructing a finitely presented group $\mathcal{B}$ and showing that if $\mathcal{B}$ had a solvable word problem, then $S$ would have a solvable word problem. Nowhere in the reduction of the group problem to the semigroup problem is a technical definition of a solvable word problem used, so that the reader knowing only our informal discussion above can follow this part of the proof. Nevertheless, we do include a precise definition below. There are several good reasons for doing so: the word problem can be properly stated; a proof of the Markov–Post theorem can be given (and so the generators and relations of the Markov–Post semigroup can be understood); a beautiful theorem of G. Higman (characterizing the finitely generated subgroups of finitely presented groups) can be given. Here are two interesting consequences: Theorem 12.30 (Boone–Higman): there is a purely algebraic characterization of groups having a solvable word problem; Theorem 12.32 (Adian–Rabin): given almost any interesting property $P$, there is no decision process which can decide, given an arbitrary finite presentation, whether or not the presented group enjoys $P$.

**Exercises**

12.1. Sketch a proof that every finite group has a solvable word problem.

12.2. Sketch a proof that every finitely generated abelian group has a solvable word
problem. (Hint. Use the fundamental theorem of finitely generated abelian groups.)

12.3. Sketch proofs that if each of $G$ and $H$ have a solvable word problem, then the same is true of their free product $G \ast H$ and their direct product $G \times H$.

12.4. Sketch a proof that if $G = (x_1, \ldots, x_n|r_j = 1, j \geq 1)$ has a solvable word problem and if $H$ is a finitely generated subgroup of $G$, then $H$ has a solvable word problem. (Hint. If $H = \langle h_1, \ldots, h_m \rangle$, write each $h_i$ as a word in the $x$.)

Turing Machines

Call a subset $E$ of a (countable) set $\Omega$ "enumerable" if there is a computer that can recognize every element of $E$ and no others. Of course, the nature of such a well-behaved subset $E$ should not depend on any accidental physical constraints affecting a real computer; for example, it should not depend on the number of memory cells being less than the total number of atoms in the universe. We thus define an idealized computer, called a Turing machine, after its inventor A. Turing (1912–1954), which abstracts the essential features of a real computer and which enumerates only those subsets $E$ that, intuitively, "ought" to be enumerable.

Informally, a Turing machine can be pictured as a box with a tape running through it. The tape consists of a series of squares, which is as long to the left and to the right as desired. The box is capable of printing a finite number of symbols, say, $s_0, s_1, \ldots, s_M$, and of being in any one of a finite number of states, say, $q_0, q_1, \ldots, q_N$. At any fixed moment, the box is in some state $q_i$ as it "scans" a particular square of the tape that bears a single symbol $s_j$ (we agree that $s_0$ means blank). The next move of the machine is determined by $q_i$ and $s_j$ and its initial structure: it goes into some state $q_i$ after obeying one of the following instructions:

1. Replace the symbol $s_j$ by the symbol $s_k$ and scan the same square.
2. Move one square to the right and scan this square.
3. Move one square to the left and scan this square.

The machine is now ready for its next move. The machine is started in the first place by being given a tape, which may have some nonblank symbols printed on it, one to a square, and by being set to scan some one square while in "starting state" $q_1$. The machine may eventually stop (we agree that $q_0$ means "stop"; that is, the machine stops when it enters state $q_0$) or it may continue working indefinitely.

Here are the formal definitions; after each definition, we shall give an informal interpretation. Choose, once and for all, two infinite lists of letters:

$s_0, s_1, s_2, \ldots$ and $q_0, q_1, q_2, \ldots$
Definition. A quadruple is a 4-tuple of one of the following three types:

\[ q_i s_j s_k q_l, \]
\[ q_i s_j R q_l, \]
\[ q_i s_j L q_l. \]

A Turing machine \( T \) is a finite set of quadruples no two of which have the same first two letters. The alphabet of \( T \) is the set \( \{s_0, s_1, \ldots, s_M\} \) of all \( s \)-letters occurring in its quadruples.

The three types of quadruples correspond to the three types of moves in the informal description given above. For example, \( q_i s_j R q_l \) may be interpreted as being the instruction: “When in state \( q_i \) and scanning symbol \( s_j \), move right one square and enter state \( q_l \).” The “initial structure” of the Turing machine is the set of all such instructions.

Recall that a word is positive if it is empty or if it has only positive exponents. If an alphabet \( A \) is a disjoint union \( S \cup T \), where \( S = \{s_i : i \in I\} \), then an \( s \)-word is a word on \( S \).

Definition. An instantaneous description \( \alpha \) is a positive word of the form \( \alpha = \sigma q_l \tau \), where \( \sigma \) and \( \tau \) are \( s \)-words and \( \tau \) is not empty.

For example, the instantaneous description \( \alpha = s_2 s_0 q_1 s_5 s_2 s_2 \) is to be interpreted: the symbols on the tape are \( s_2 s_0 s_5 s_2 s_2 \), with blanks everywhere else, and the machine is in state \( q_1 \) scanning \( s_5 \).

Definition. Let \( T \) be a Turing machine. An ordered pair \( (\alpha, \beta) \) of instantaneous descriptions is a basic move of \( T \), denoted by

\[ \alpha \rightarrow \beta, \]

if there are (possibly empty) positive \( s \)-words \( \sigma \) and \( \sigma' \) such that one of the following conditions hold:

(i) \( \alpha = \sigma q_i s_j \sigma' \) and \( \beta = \sigma q_i s_k \sigma' \), where \( q_i s_j s_k q_l \in T \); 
(ii) \( \alpha = \sigma q_i s_j s_k \sigma' \) and \( \beta = \sigma s_j q_i s_k \sigma' \), where \( q_i s_j R q_l \in T \); 
(iii) \( \alpha = \sigma q_i s_j \sigma \) and \( \beta = \sigma s_j q_i s_0 \), where \( q_i s_j R q_l \in T \); 
(iv) \( \alpha = \sigma s_k q_i s_j \sigma' \) and \( \beta = \sigma q_i s_k s_j \sigma' \), where \( q_i s_j L q_l \in T \); and 
(v) \( \alpha = q_i s_j \sigma' \) and \( \beta = q_i s_0 s_j \sigma' \), where \( q_i s_j L q_l \in T \).

If \( \alpha \) describes the tape at a given time, the state \( q_i \) of \( T \), and the symbol \( s_j \) being scanned, then \( \beta \) describes the tape, the next state of \( T \), and the symbol being scanned after the machine’s next move. The proviso in the definition of a Turing machine that no two quadruples have the same first two symbols
means that there is never ambiguity about a machine’s next move: if \( \alpha \to \beta \)
and \( \alpha \to \gamma \), then \( \beta = \gamma \).

Some further explanation is needed to interpret basic moves of types (iii)
and (v). Tapes are finite, but when the machine comes to an end of the tape,
the tape is lengthened by adjoining a blank square. Since \( s_0 \) means blank,
these two rules thus correspond to the case when \( T \) is scanning either the last
symbol on the tape or the first symbol.

**Definition.** An instantaneous description \( \alpha \) is **terminal** if there is no instantaneous
description \( \beta \) with \( \alpha \to \beta \). If \( \omega \) is a positive word on the alphabet of \( T \),
then \( T \) **computes** \( \omega \) if there is a finite sequence of instantaneous descriptions
\( \alpha_1 = q_1 \omega, \alpha_2, \ldots, \alpha_t, \) where \( \alpha_i \to \alpha_{i+1} \), for all \( i \leq t - 1 \), and \( \alpha_t \) is terminal.

Informally, \( \omega \) is printed on the tape and \( T \) is in starting state \( q_1 \) while
scanning the first square. The running of \( T \) is a possibly infinite sequence of
instantaneous descriptions \( q_1 \omega \to \alpha_2 \to \alpha_3 \to \cdots \). This sequence stops if \( T \)
computes \( \omega \); otherwise, \( T \) runs forever.

**Definition.** Let \( \Omega \) be the set of all positive words on symbols \( S = \{ s_1, \ldots, s_M \} \).
If \( T \) is a Turing machine whose alphabet contains \( S \), define
\[
e(T) = \{ \omega \in \Omega : T \text{ computes } \omega \},
\]
and say that \( T \) **enumerates** \( e(T) \). A subset \( E \) of \( \Omega \) is **r.e.** (recursively
enumerable) if there is some Turing machine \( T \) that enumerates \( E \).

The notion of an r.e. subset of \( \Omega \) can be specialized to subsets of the natural
numbers \( \mathbb{N} = \{ n \in \mathbb{Z} : n \geq 0 \} \) by identifying each \( n \in \mathbb{N} \) with the positive word
\( s_1^{n+1} \). Thus, a subset \( E \) of \( \mathbb{N} \) is an r.e. subset of \( \mathbb{N} \) if there is a Turing machine
\( T \) with \( s_1 \) in its alphabet such that \( E = \{ n \in \mathbb{N} : T \text{ computes } s_1^{n+1} \} \).

Every Turing machine \( T \) defines an r.e. subset \( E = e(T) \subset \Omega \), the set of all
positive words on its alphabet. How can we tell whether \( \omega \in \Omega \) lies in \( E \)? Feed
\( q_1 \omega \) into \( T \) and wait; that is, perform the basic moves \( q_1 \omega \to \alpha_2 \to \alpha_3 \to \cdots \).
If \( \omega \in E \), then \( T \) computes \( \omega \) and so \( T \) will eventually stop. However, for a
given \( \omega \), there is no way of knowing, a priori, whether \( T \) will stop. Certainly
this is unsatisfactory for an impatient person, but, more important, it
suggests a new idea.

**Definition.** Let \( \Omega \) be the set of all positive words on \( \{ s_0, s_1, \ldots, s_M \} \). A subset
\( E \) of \( \Omega \) is **recursive** if both \( E \) and its complement \( \Omega - E \) are r.e. subsets.

If \( E \) is recursive, there is never an “infinite wait” to decide whether or not
a positive word \( \omega \) lies in \( E \). If \( T \) is a Turing machine with \( e(T) = E \) and if \( T' \)
is a Turing machine with \( e(T') = \Omega - E \), then, for each \( \omega \in \Omega \), either \( T \) or \( T' \)
computes \( \omega \). Thus, it can be decided in a finite length of time whether or not
a given word \( \omega \) lies in \( E \): just feed \( \omega \) into each machine and let \( T \) and \( T' \) run simultaneously.

Recall the informal discussion in the introduction. If \( \mathcal{L} \) is a list of questions, then a decision process for \( \mathcal{L} \) is a uniform set of directions which, when applied to any of the questions in \( \mathcal{L} \), gives the correct answer "yes" or "no" after a finite number of steps, never at any stage of the process leaving the user in doubt as to what to do next. It is no loss of generality to assume that the list \( \mathcal{L} \) has been encoded as positive words on an alphabet, that \( E \) consists of all words for which the answer is "yes," and that its complement consists of all words for which the answer is "no." We propose that recursive sets are precisely those subsets admitting a decision process. Of course, this proposition (called Church's thesis) can never be proved, for it is a question of translating an intuitive notion into precise terms. There have been other attempts to formalize the notion of decision process (e.g., using a Turing-like machine that can read a two-dimensional tape; or, avoiding Turing machines altogether and beginning with a notion of computable function). So far, every alternative definition of "decision process" which recognizes all recursive sets has been proved to recognize only these sets.

**Theorem 12.1.** There exists an r.e. subset of the natural numbers \( \mathbb{N} \) that is not recursive.

**Proof.** There are only countably many Turing machines, for a Turing machine is a finite set of quadruples based on the countable set of letters \( \{R, L, s_0, s_1, \ldots; q_0, q_1, \ldots\} \). Assign natural numbers to these letters in the following way:

\[
\begin{align*}
R &\mapsto 0; \quad L \mapsto 1; \quad q_0 \mapsto 2; \quad q_1 \mapsto 4; \quad q_2 \mapsto 6; \quad \cdots \\
&\quad s_0 \mapsto 3; \quad s_1 \mapsto 5; \quad s_2 \mapsto 7; \quad \cdots.
\end{align*}
\]

If \( T \) is a Turing machine having \( m \) quadruples, juxtapose them in some order to form a word \( w(T) \) of length \( 4m \); note that \( T \neq T' \) implies \( w(T) \neq w(T') \). Define the Gödel number

\[
G(T) = \prod_{i=1}^{4m} p_i^{e_i},
\]

where \( p_i \) is the \( i \)th prime and \( e_i \) is the natural number assigned above to the \( i \)th letter in \( w(T) \). The Fundamental Theorem of Arithmetic implies that distinct Turing machines have distinct Gödel numbers. All Turing machines can now be enumerated: \( T_0, T_1, \ldots, T_n, \ldots \); let \( T \) precede \( T' \) if \( G(T) < G(T') \).

Define

\[
E = \{n \in \mathbb{N}: \text{there exists } m \text{ such that } T_m \text{ computes } n^{n+1}\}
\]

(thus, \( n \in E \) if and only if the \( n \)th Turing machine computes \( n \)).

We claim that \( E \) is an r.e. set. Consider the following figure reminiscent of
the proof that the set of all rational numbers is countable:

\[
\begin{array}{ccccc}
T_0 & T_1 & T_2 & T_3 & T_4 \\
q_1s_1 & q_1s_1^2 & q_1s_1^3 & q_1s_1^4 & q_1s_1^5 \\
\downarrow & \nearrow & \nearrow & \nearrow & \nearrow \\
\alpha_{12} & \alpha_{22} & \alpha_{32} & \alpha_{42} \\
\swarrow & \nearrow & \nearrow & \nearrow \\
\alpha_{13} & \alpha_{23} & \alpha_{33} \\
\downarrow & \nearrow \\
\alpha_{14} & \alpha_{24}
\end{array}
\]

The \( n \)th column consists of the sequence of basic moves of the \( n \)th Turing machine \( T_n \) beginning with \( q_1s_1^{n+1} \). It is intuitively clear that there is an enumeration of the natural numbers \( n \) lying in \( E \): follow the arrows in the figure, and put \( n \) in \( E \) as soon as one reaches a terminal instantaneous description \( \alpha_{ni} \) in column \( n \). A Turing machine \( T^* \) can be constructed to carry out these instructions (by Exercise 12.11 below, such a \( T^* \) exists having stopping state \( q_0 \); that is, terminal instantaneous descriptions, and only these, involve \( q_0 \).) Thus, \( E \) is an r.e. subset of \( \mathbb{N} \).

The argument showing that \( E \) is not recursive is a variation of Cantor's diagonal argument proving that the set of reals is uncountable. It suffices to prove that the complement

\[
E' = \{ n \in \mathbb{N} : n \notin E \} = \{ n \in \mathbb{N} : T_n \text{ does not compute } s_1^{n+1} \}
\]

is not an r.e. subset of \( \mathbb{N} \). Suppose there were a Turing machine \( T' \) enumerating \( E' \); since all Turing machines have been listed, \( T' = T_m \) for some \( m \in \mathbb{N} \). If \( m \in E' = e(T') = e(T_m) \), then \( T_m \) computes \( s_1^{m+1} \), and so \( m \in E \), a contradiction. If \( m \notin E' \), then \( m \in E \) and so \( T_m \) computes \( s_1^{m+1} \) (definition of \( E \)); hence \( m \in e(T_m) = e(T') = E' \), a contradiction. Therefore, \( E' \) is not an r.e. set and \( E \) is not recursive. 

**Exercises**

12.5. Prove that there are subsets of \( \mathbb{N} \) that are not r.e. (*Hint*. There are only countably many Turing machines.)

12.6. Prove that the set of all even natural numbers is r.e.

12.7. Give an example of a Turing machine \( T \) having \( s_1 \) in its alphabet, which does not compute \( s_1 \).

12.8. Let \( \Omega \) be the set of all positive words on \( \{s_0, s_1, \ldots, s_M\} \). If \( E_1 \) and \( E_2 \) are r.e. subsets of \( \Omega \), then both \( E_1 \cup E_2 \) and \( E_1 \cap E_2 \) are also r.e. subsets.

12.9. Let \( \Omega \) be the set of all positive words on \( \{s_0, s_1, \ldots, s_M\} \). If \( E_1 \) and \( E_2 \) are...
recursive subsets of $\Omega$, then both $E_1 \cup E_2$ and $E_1 \cap E_2$ are also recursive subsets. Conclude that all recursive subsets of $\Omega$ form a Boolean algebra.

12.10. If $E_1$ and $E_2$ are recursive subsets of $\mathbb{N}$, then $E_1 \times E_2$ is a recursive subset of $\mathbb{N} \times \mathbb{N}$. \textit{(Hint.} First imbed $\mathbb{N} \times \mathbb{N}$ into $\mathbb{N}$ by “encoding” the ordered pair $(m, n)$ as $2^m3^n$.)

12.11. If $T$ is a Turing machine enumerating a set $E$, then there is a Turing machine $T^*$ having the same alphabet and with stopping state $q_0$ that also enumerates $E$.

The Markov–Post Theorem

We now link these ideas to algebra.

If $\Gamma$ is a semigroup with generators $X = \{x_1, \ldots, x_n\}$ and if $\Omega$ is the set of all positive words on $X$, then the semigroup $\Gamma$ has a \textit{solvable word problem} if there is a decision process to determine, for an arbitrary pair of words $\omega, \omega' \in \Omega$, whether $\omega = \omega'$ in $\Gamma$. This (informal) definition gives a precise definition of unsolvability.

\textbf{Definition.} Let $\Gamma$ be a semigroup with generators $X = \{x_1, \ldots, x_n\}$, and let $\Omega$ be the set of all positive words on $X$. The semigroup $\Gamma$ has an \textit{unsolvable word problem} if there is a word $\omega_0 \in \Omega$ such that $\{\omega \in \Omega : \omega = \omega_0 \text{ in } \Gamma\}$ is not recursive.

If $F$ is the free group with basis $X = \{x_1, \ldots, x_n\}$, then we shall view the set $\Omega$ of all (not necessarily positive) words on $X$ as the set of all positive words on the alphabet

$$\{x_1, x_1^{-1}, \ldots, x_n, x_n^{-1}\}.$$  

\textbf{Definition.} Let $G$ be a group with presentation $(x_1, \ldots, x_n | \Delta)$, and let $\Omega$ be the set of all words on $x_1, \ldots, x_n$ (viewed as the set of positive words on $\{x_1, x_1^{-1}, \ldots, x_n, x_n^{-1}\}$). Then $G$ has a \textit{solvable word problem} if $\{\omega \in \Omega : \omega = 1 \text{ in } G\}$ is recursive.

The distinction between r.e. sets and recursive sets persists in group theory.

\textbf{Theorem 12.2.} Let $G$ be a finitely presented group with presentation

$$G = (x_1, \ldots, x_n | r_1, \ldots, r_m).$$

If $\Omega$ is the set of all words on $x_1, \ldots, x_n$, then $E = \{\omega \in \Omega : \omega = 1 \text{ in } G\}$ is r.e.

\textbf{Proof.} List the words $\omega_0, \omega_1, \ldots$ in $\Omega$ as we did in the Introduction: first the empty word, then the words of length 1 in order $x_1, x_1^{-1}, \ldots, x_n, x_n^{-1}$, then the
words of length 2 in lexicographic order, then the words of length 3 in lexicographic order, and so forth. Similarly, list all the words on \( \{r_1, \ldots, r_m\} \): \( \rho_0, \rho_1, \ldots \). As in the proof of Theorem 12.1, following the arrows in the figure below enumerates \( E \).

\[
\begin{array}{cccc}
\omega_0 \rho_0 \omega_0^{-1} & \omega_0 \rho_1 \omega_0^{-1} & \omega_0 \rho_2 \omega_0^{-1} & \omega_0 \rho_3 \omega_0^{-1} \\
\downarrow & \searrow & \nearrow & \\
\omega_1 \rho_0 \omega_1^{-1} & \omega_1 \rho_1 \omega_1^{-1} & \omega_1 \rho_2 \omega_1^{-1} & \\
\searrow & \nearrow & \\
\omega_2 \rho_0 \omega_2^{-1} & \omega_2 \rho_1 \omega_2^{-1} & \\
\downarrow & \nearrow & \\
\omega_3 \rho_0 \omega_3^{-1} & \\
\end{array}
\]

It follows that a finitely presented group \( G \) has solvable word problem if and only if \( \{\omega \in \Omega: \omega \neq 1 \text{ in } G\} \) is r.e.

Recall the following notation introduced in Chapter 11. If \( \omega \) and \( \omega' \) are (not necessarily reduced) words on an alphabet \( X \), then we write

\[ \omega \equiv \omega' \]

if \( \omega \) and \( \omega' \) have exactly the same spelling.

Suppose that a semigroup \( \Gamma \) has a presentation

\[ \Gamma = (X | \alpha_j = \beta_j, j \in J). \]

If \( \omega \) and \( \omega' \) are positive words on \( X \), then it is easy to see that \( \omega = \omega' \) in \( \Gamma \) if and only if there is a finite sequence

\[ \omega \equiv \omega_1 \rightarrow \omega_2 \rightarrow \cdots \rightarrow \omega_t \equiv \omega', \]

where \( \omega_i \rightarrow \omega_{i+1} \) is an \textit{elementary operation}; that is, either \( \omega_i \equiv \sigma \alpha_j \tau \) and \( \omega_{i+1} \equiv \sigma \beta_j \tau \) for some \( j \), where \( \sigma \) and \( \tau \) are positive words on \( X \) or \( \omega_{i+1} \equiv \sigma \beta_j \tau \) and \( \omega_i \equiv \sigma \alpha_j \tau \).

Let us now associate a semigroup to a Turing machine \( T \) having stopping state \( q_0 \). For notational convenience, assume that the \( s \)-letters and \( q \)-letters involved in the quadruples of \( T \) are \( s_0, s_1, \ldots, s_M \), and \( q_0, q_1, \ldots, q_N \). Let \( q \) and \( h \) be new letters.

\textbf{Definition.} If \( T \) is a Turing machine having stopping state \( q_0 \), then its \textit{associated semigroup} \( \Gamma(T) \) has the presentation:

\[ \Gamma(T) = (q, h, s_0, s_1, \ldots, s_M, q_0, q_1, \ldots, q_N | R(T)), \]

where the relations \( R(T) \) are
The Markov–Post Theorem

\[ q_i s_j = q_i s_k \quad \text{if} \quad q_i s_j s_k a \in T, \]

for all \( \beta = 0, 1, \ldots, M: \)

\[ q_i s_j s_\beta = s_j q_i s_\beta \quad \text{if} \quad q_i s_j s_\beta a \in T; \]
\[ q_i s_j h = s_j q_i s_\omega h \quad \text{if} \quad q_i s_j s_\omega h \in T; \]
\[ s_\omega q_i s_j = q_i s_\omega s_j \quad \text{if} \quad q_i s_j s_\omega h \in T; \]
\[ h q_i s_j = h q_i s_\omega s_j \quad \text{if} \quad q_i s_j s_\omega h \in T; \]
\[ q_\alpha s_\beta = q_\alpha, \]
\[ s_\omega q_\omega h = q_\omega h, \]
\[ h q_\omega h = q. \]

The first five types of relations are just the obvious ones suggested by the basic moves of \( T; \) the new letter \( h \) enables one to distinguish basic move (ii) (in the definition of a Turing machine) from basic move (iii) and to distinguish basic move (iv) from basic move (v). One may thus interpret \( h \) as marking the ends of the tape, so that the following words are of interest.

**Definition.** A word is \textit{h-special} if it has the form \( h_\omega h \), where \( \omega \) is an instantaneous description.

Since \( T \) has stopping state \( q_0 \), each \( h_\omega h \) (with \( \omega \) terminal) has the form \( h_\sigma q_\omega \tau h \), where \( \sigma \) and \( \tau \) are \( s \)-words and \( \tau \) is not empty. Therefore, the last three relations allow us to write \( h_\omega h = q \) in \( \Gamma(T) \) whenever \( \omega \) is terminal.

**Lemma 12.3.** Let \( T \) be a Turing machine with stopping state \( q_0 \) and associated semigroup

\[ \Gamma(T) = (q, h, s_0, s_1, \ldots, s_M, q_0, q_1, \ldots, q_n|R(T)). \]

\( \text{(i)} \) Let \( \omega \) and \( \omega' \) be words on \( \{s_0, s_1, \ldots, s_M, q_0, q_1, \ldots, q_n\} \) with \( \omega \neq q \) and \( \omega' \neq q. \) If \( \omega \rightarrow \omega' \) is an elementary operation, then \( \omega \) is \textit{h-special} if and only if \( \omega' \) is \textit{h-special}.

\( \text{(ii)} \) If \( \omega = h_\omega h \) is \textit{h-special}, \( \omega' \neq q, \) and \( \omega \rightarrow \omega' \) is an elementary operation of one of the first five types, then \( \omega' \equiv h_\beta h, \) where either \( \alpha \rightarrow \beta \) or \( \beta \rightarrow \alpha \) is a basic move of \( T. \)

**Proof.** (i) This is true because the only relation that creates or destroys \( h \) is \( h q_\omega h = q. \)

(ii) By the first part, we know that \( \omega' \) is \textit{h-special}, say, \( \omega' \equiv h_\beta h. \) Now an elementary move in a semigroup is a substitution using an equation in a defining relation; such a relation in \( \Gamma(T) \) of one of the first five types corresponds to a quadruple of \( T, \) and a quadruple corresponds to a basic move. Thus, either \( \alpha \rightarrow \beta \) or \( \beta \rightarrow \alpha. \]

**Lemma 12.4.** Let \( T \) be a Turing machine with stopping state \( q_0, \) let \( \Omega \) be the set
of all positive words on the alphabet of $T$, and let $E = e(T)$. If $\omega \in \Omega$, then
\[
\omega \in E \text{ if and only if } hq_1 \omega h = q \text{ in } \Gamma(T).
\]

**Proof.** If $\omega \in E$, then there are instantaneous descriptions $\alpha_1 = q_1 \omega, \alpha_2, \ldots, \alpha_t$, where $\alpha_i \rightarrow \alpha_{i+1}$, and $\alpha_t$ involves $q_0$. Using the elementary operations in $\Gamma(T)$ of the first five types, one sees that $hq_1 \omega h = h\alpha_t h$ in $\Gamma(T)$; using the last three relations, one sees that $h\alpha_t h = q$ in $\Gamma(T)$.

The proof of sufficiency is of a different nature than the proof of necessity just given, for equality in $\Gamma(T)$ is, of course, a symmetric relation, whereas $\alpha \rightarrow \beta$ a basic move does not imply that $\beta \rightarrow \alpha$ is a basic move.

If $hq_1 \omega h = q$ in $\Gamma(T)$, then there are words $\omega_1, \ldots, \omega_t$ on $\{h, s_0, s_1, \ldots, s_M, q_0, q_1, \ldots, q_N\}$ and elementary operations
\[
hq_1 \omega h \equiv \omega_1 \rightarrow \omega_2 \rightarrow \cdots \rightarrow \omega_t \equiv hq_0 h \rightarrow q.
\]

By Lemma 12.3(i), each $\omega_i$ is $h$-special: $\omega_i \equiv h\alpha_t h$ for some instantaneous description $\alpha_i$. By Lemma 12.3(ii), either $\alpha_i \rightarrow \alpha_{i+1}$ or $\alpha_{i+1} \rightarrow \alpha_i$. We prove, by induction on $t \geq 2$, that all the arrows go to the right; that is, for all $i \leq t - 1$, $\alpha_i \rightarrow \alpha_{i+1}$. It will then follow that $q_1 \omega \rightarrow \alpha_2 \rightarrow \cdots \rightarrow \alpha_t$ is a sequence of basic moves with $\alpha_t$ terminal (for $\alpha_t$ involves $q_0$, the stopping state); hence $T$ computes $\omega$ and $\omega \in E$. It is always true that $\alpha_{t-1} \rightarrow \alpha_t$, for $\alpha_t$ is terminal and hence $\alpha_{t-1} \leftarrow \alpha_t$ cannot occur. In particular, this shows that the induction begins when $t = 2$. Suppose that $t > 2$ and some arrow goes to the left. Since the last arrow $\alpha_{t-1} \rightarrow \alpha_t$ points right, moving backward until one reaches an arrow pointing left gives an index $i$ with
\[
\alpha_{i-1} \leftarrow \alpha_i \rightarrow \alpha_{i+1}.
\]

But there is never ambiguity about the next move of a Turing machine, so that $\alpha_{i-1} \equiv \alpha_{i+1}$ and $\omega_{i-1} \equiv h\alpha_{i-1} h \equiv h\alpha_{i+1} h \equiv \omega_{i+1}$. We may thus eliminate $\omega_i$ and $\omega_{i+1}$, thereby reducing $t$, and the proof is completed by induction.

**Theorem 12.5 (Markov–Post, 1947).**

(i) There is a finitely presented semigroup
\[
\gamma = \langle q, h, s_0, s_1, \ldots, s_M, q_0, q_1, \ldots, q_N | R \rangle
\]
with an unsolvable word problem.

(ii) There is no decision process which determines, for an arbitrary $h$-special word $hzh$, whether $hzh = q$ in $\gamma$.

**Proof.** (i) If $T$ is a Turing machine with stopping state $q_0$ and with alphabet $A = \{s_0, s_1, \ldots, s_M\}$, then let $\Omega$ be all the positive words on $A$ and let $E = e(T) \subset \Omega$. Define $\overline{\Omega}$ to be all the positive words on $A \cup \{q, h, q_0, q_1, \ldots, q_N\}$, where $q_0, q_1, \ldots, q_N$ are the $q$-letters occurring in the quadruples of $T$, and
define
\[ \bar{E} = \{ \bar{\omega} \in \bar{\Omega} : \bar{\omega} = q \text{ in } \Gamma(T) \}. \]

Define \( \phi : \Omega \rightarrow \bar{\Omega} \) by \( \omega \rightarrow hq_1 \omega h \), and identify \( \Omega \) with its image \( \Omega_1 \subset \bar{\Omega} \); the subset \( E \) of \( \Omega \) is now identified with
\[ E_1 = \{hq_1 \omega h : \omega \in E\}. \]

It is plain that \( E_1 \) is a recursive subset of \( \Omega_1 \) if and only if \( E \) is a recursive subset of \( \Omega \). In this notation, Lemma 12.4 reads:
\[ E_1 = \bar{E} \cap \Omega_1. \]

Now assume that \( T \) is the Turing machine \( T^* \) (with stopping state \( q_0 \)) of Theorem 12.1, so that \( E \), hence \( E_1 \), is r.e. but not recursive. Were \( E \) recursive, then Exercise 12.9 would give \( E_1 \), hence \( E \), recursive, and this is a contradiction. Therefore, \( \gamma = \Gamma(T^*) \) has an unsolvable word problem.

(ii) Define
\[ \bar{S} = \{ h \text{-special words } hzh : hzh = q \text{ in } \Gamma(T^*) \}. \]

Were \( S \) a recursive subset of \( \bar{\Omega} \), then \( \bar{S} \cap \Omega_1 \) would be a recursive subset of \( \Omega_1 \), by Exercise 12.9. But \( \bar{S} \cap \Omega_1 = E_1 \). ☐

For later use, we rewrite the generators and relations of the Markov–Post semigroup \( \gamma(T^*) \).

**Corollary 12.6.**

(i) There is a finitely presented semigroup
\[ \Gamma = (q, q_0, \ldots, q_N, s_0, \ldots, s_M | F_i q_i, G_i = H_i q_i K_i, i \in I), \]
with an unsolvable word problem, where \( F_i, G_i, H_i, K_i \) are (possibly empty) positive \( s \)-words and \( q_i, q_i \in \{q_0, \ldots, q_N\} \).

(ii) There is no decision process which determines, for arbitrary \( q_i \) and positive \( s \)-words \( X \) and \( Y \), whether \( X q_i Y = q \) in \( \Gamma \).

**Proof.** (i) Regard the generator \( h \) of the semigroup \( \gamma = \Gamma(T^*) \) as the last \( s \)-letter and re-index these \( s \)-letters so that \( h = s_M \). The rewritten relations in \( R(T^*) \) now have the described form.

(ii) Let \( \Omega_2 \) be the set of all positive words on the rewritten generators of \( \Gamma \), let
\[ \bar{\Lambda} = \{ X q_i Y : X, Y \text{ are positive words on rewritten } s \text{-letters and } X q_i Y = q \text{ in } \Gamma \}, \]
and let
\[ \bar{S}_2 = \{ s_M x s_M : x = \sigma q_i \tau, \text{ where } \sigma \text{ and } \tau \text{ are positive words on } s_0, \ldots, s_{M-1} \text{ and } s_M x s_M = q \text{ in } \Gamma \}. \]
The Novikov–Boone–Britton Theorem: Sufficiency of Boone’s Lemma

The word problem for groups was first considered by M. Dehn (1910) and by A. Thue (1914). The solution was given by P.S. Novikov (1955) and, independently, by W.W. Boone (1954–1957) and by J.L. Britton (1958). In 1959, Boone exhibited a much simpler finitely presented group than any of those previously given, and he proved it has an unsolvable word problem. In contrast to the “combinatorial” proofs of Novikov and Boone, Britton’s proof relies on properties of HNN extensions (which led him to discover Britton’s lemma). In 1963, Britton gave a much simpler and shorter proof for Boone’s group; we present his proof here, incorporating later improvements of Boone, D.J. Collins, and C.F. Miller, III. We assure the reader that all the Mathematical Logic required in the proof has already appeared; we need only Corollary 12.6, a paraphrase of the Markov–Post theorem, that exhibits a particular finitely presented semigroup \( \Gamma \) with an unsolvable word problem.

Remember that the proof is going to reduce equality of words in a group to equality of words in a semigroup. It is thus essential to keep track of exponents, for while arbitrary words make sense in a group, only positive words make sense in a semigroup.

Notation. If \( X = s_{\beta_1}^{{e_1}} \cdots s_{\beta_m}^{{e_m}} \) is a (not necessarily positive) s-word, then \( X^* = s_{\beta_1}^{-{e_1}} \cdots s_{\beta_m}^{-{e_m}} \). Note that if \( X \) and \( Y \) are s-words, then \( (X^*)_Y = X \) and \( (X Y)^* = X^* Y^* \).

Recall, for every Turing machine \( T \), that there is a semigroup \( \Gamma = \Gamma(T) \) with the presentation

\[
\Gamma = (q, q_0, \ldots, q_N, s_0, \ldots, s_M | F_i q_i, G_i = H_i q_{i_2} K_i, i \in I),
\]

where \( F_i, G_i, H_i, K_i \) are (possibly empty) positive s-words and \( q_i, q_{i_2} \in \{q, q_0, \ldots, q_N\} \).

For every Turing machine \( T \), we now define a group \( \mathcal{A} = \mathcal{A}(T) \) that will be shown to have an unsolvable word problem if \( T \) is chosen to be the Turing machine \( T^* \) in the Markov–Post theorem. The group \( \mathcal{A}(T) \) has the presentation:
The Novikov–Boone–Britton Theorem: Sufficiency of Boone’s Lemma

 generators: \( q, q_0, \ldots, q_N, s_0, \ldots, s_M, r_i, i \in I, x, t, k; \)

 relations: for all \( i \in I \) and all \( \beta = 0, \ldots, M, \)

\[

x s_\beta = s_\beta x^2, \quad \Delta_1 \]
\[
r_i s_\beta = s_\beta x r_i x, \quad \Delta_2 \]
\[
r_i^{-1} F_i^\# q_i G_i r_i = H_i^\# q_i K_i, \quad \Delta_2 \]
\[
tr_i = r_i t, \quad \Delta_3 \]
\[
t x = x t, \quad \Delta_3 \]
\[
k r_i = r_i k, \]
\[
k x = x k, \]
\[
k (q^{-1} t q) = (q^{-1} t q) k. \]

The subsets \( \Delta_1 \subset \Delta_2 \subset \Delta_3 \) of the relations are labeled for future reference.

If \( X \) and \( Y \) are s-words, define

\[
(X q_j Y)^* \equiv X^* q_j Y, \]

where \( q_j \in \{q, q_0, \ldots, q_N\}. \)

**Definition.** A word \( \Sigma \) is **special** if \( \Sigma \equiv X^* q_j Y, \) where \( X \) and \( Y \) are positive s-words and \( q_j \in \{q, q_0, \ldots, q_N\}. \)

If \( \Sigma \) is special, then \( \Sigma \equiv X^* q_j Y, \) where \( X \) and \( Y \) are positive s-words, and so \( \Sigma^* \equiv (X^* q_j Y)^* \equiv X q_j Y \) is a positive word; therefore, \( \Sigma^* \) determines an element of the semigroup \( \Gamma. \)

The reduction to the Markov–Post theorem is accomplished by the following lemma:

**Lemma 12.7 (Boone).** Let \( T \) be a Turing machine with stopping state \( q_0 \) and associated semigroup \( \Gamma = \Gamma(T) \) (rewritten as in Corollary 12.6). If \( \Sigma \) is a special word, then

\[
k (\Sigma^{-1} t \Sigma) = (\Sigma^{-1} t \Sigma) k \quad \text{in} \quad \mathcal{B} = \mathcal{B}(T) \]

if and only if \( \Sigma^* = q \) in \( \Gamma(T). \)

**Theorem 12.8 (Novikov–Boone–Britton).** There exists a finitely presented group \( \mathcal{B} \) with an unsolvable word problem.

**Proof.** Choose \( T \) to be the Turing machine \( T^* \) of the Markov–Post theorem. If there were a decision process to determine, for an arbitrary special word \( \Sigma, \)

whether \( k \Sigma^{-1} t \Sigma k^{-1} \Sigma^{-1} t \Sigma = 1 \) in \( \mathcal{B}(T^*), \) then this same decision process determines whether \( \Sigma^* = q \) in \( \Gamma(T^*). \) But Corollary 12.6(ii) asserts that no such decision process for \( \Gamma(T^*) \) exists. \( \blacksquare \)
Corollary 12.9. Let $T$ be a Turing machine with stopping state $q_0$ enumerating a subset $E$ of $\Omega$ (the set of all positive words on the alphabet of $T$). If $\omega \in \Omega$, then $\omega \in E$ if and only if $k(h^{-1}q_1\omega h) = (h^{-1}q_1\omega h)k$ in $B(T)$.

**Proof.** By Lemma 12.4, $\omega \in E$ if and only if $hq_1\omega h = q$ in $\Gamma(T)$. But, in $B(T)$, $(hq_1\omega h)^* = h^{-1}q_1\omega h$ (which is a special word), and Boone's lemma shows that $(h^{-1}q_1\omega h)^* = hq_1\omega h = q$ in $\Gamma(T)$ if and only if $k(h^{-1}q_1\omega h) = (h^{-1}q_1\omega h)k$ in $B(T)$.

The proof below is valid for any Turing machine $T$ with stopping state $q_0$. We abbreviate $B(T)$ to $B$ and $\Gamma(T)$ to $\Gamma$.

The proof of Boone's lemma in one direction is straightforward.

**Lemma 12.10.**

(i) If $V$ is a positive s-word, then

$$r_i V = VR \quad \text{in } B$$

and

$$r_i^{-1} V = VR' \quad \text{in } B,$$

where $R$ and $R'$ are words on $\{r_i, x\}$ with $R$ positive.

(ii) If $U$ is a positive s-word, then

$$U^* r_i = LR^* \quad \text{in } B$$

and

$$U^* r_i^{-1} = L'U^* \quad \text{in } B,$$

where $L$ and $L'$ are words on $\{r_i, x\}$.

**Proof.** We prove that $r_i V = VR$ in $B$ by induction on $m \geq 0$, where $V \equiv s_{\beta_1} \ldots s_{\beta_m}$. This is certainly true when $m = 0$. If $m > 0$, write $V \equiv V' s_{\beta_m}$; by induction, $r_i V \equiv r_i V' s_{\beta_m} = V' R' s_{\beta_m}$, where $R'$ is a positive word on $\{r_i, x\}$. Using the relations $x s_{\beta} = s_{\beta} x^2$ and $r_i s_{\beta} = s_{\beta} x r_i x$, we see that there is a positive word $R$ on $\{r_i, x\}$ with $s_{\beta_m} R = R' s_{\beta_m}$ in $B$.

The proofs of the other three equations are similar.

**Proof of Sufficiency in Boone's Lemma.** If $\Sigma$ is a special word with $\Sigma^* \equiv Xq_j Y = q$ in $\Gamma$, then there is a sequence of elementary operations

$$\Sigma^* \equiv \omega_1 \to \omega_2 \to \cdots \to \omega_n \equiv q \quad \text{in } \Gamma,$$

where, for each $v$, one of the words $\omega_v$ and $\omega_{v+1}$ has the form $U F_i q_i G_i V$ with $U$ and $V$ positive s-words, and the other has the form $U H_i q_i K_i V$. By the lemma, there are equations in $B$:

$$U^* (H_i^* q_i K_i) V = U^* (r_i^{-1} F_i^* q_i G_i r_i) V$$

$$= L' U^* (F_i^* q_i G_i) VR',$$

where $L'$ and $R'$ are words on $\{r_i, x\}$. In a similar manner, one sees that there are words $L''$ and $R''$ on $\{r_i, x\}$ with

$$U^* (F_i^* q_i G_i) V = U^* (r_i H_i^* q_i K_i r_i^{-1}) V = L'' U^* (H_i^* q_i K_i) VR''.$$
Since \( \omega_v = \omega_{v+1} \) in \( \Gamma \) implies \( \omega_v^* = \omega_{v+1}^* \) in \( \mathcal{B} \), by the relations labeled \( \Delta_2 \), it follows, for each \( v \), that

\[
\omega_v^* = L_v \omega_{v+1}^* R_v \quad \text{in } \mathcal{B}
\]

for words \( L_v \) and \( R_v \) on some \( r_i \) and \( x \). The words \( L \equiv L_1 \ldots L_{n-1} \) and \( R \equiv R_{n-1} \ldots R_1 \) are thus words on \( \{ x, r_i \} \), and

\[
\omega_1^* = L \omega_n^* R \quad \text{in } \mathcal{B}.
\]

But \( \omega_1^* \equiv (\Sigma^*)^* \equiv \Sigma \) and \( \omega_n^* \equiv q^* \equiv q \), so that

\[
\Sigma = LqR \quad \text{in } \mathcal{B}.
\]

Since the generators \( t \) and \( k \) commute with \( x \) and all the \( r_i \), they commute with \( L \) and \( R \). Therefore,

\[
k \Sigma^{-1} t \Sigma k^{-1} \Sigma^{-1} t^{-1} \Sigma = k R^{-1} q^{-1} L^{-1} t L q R k^{-1} R^{-1} q^{-1} L^{-1} t^{-1} L q R \\
= k R^{-1} q^{-1} t q k^{-1} q^{-1} t^{-1} q R \\
= R^{-1} (k q^{-1} t q k^{-1} q^{-1} t^{-1} q) R \\
= 1,
\]

because the last word is a conjugate of a relation. □

Observe that the last relation of the group \( \mathcal{B} \) appears only in the last step of the proof.

## Cancellation Diagrams

We interrupt the proof of Boone's lemma (and the Novikov–Boone–Britton theorem) to discuss a geometric method of studying presentations of groups, essentially due to R. Lyndon, that uses diagrams in the plane. Since we are only going to use diagrams in a descriptive way (and not as steps in a proof), we may write informally. For a more serious account, we refer the reader to Lyndon and Schupp (1977, Chap. V) with the caveat that our terminology does not always coincide with theirs.

When we speak of a polygon in the plane, we mean the usual geometric figure including its interior; of course, its boundary (or perimeter) consists of finitely many edges and vertices. A directed polygon is a polygon each of whose (boundary) edges is given a direction, indicated by an arrow. Finally, given a presentation \((X|\Delta)\) of a group, a labeled directed polygon is a directed polygon each of whose (directed) edges is labeled by a generator in \( X \).

Given a presentation \((X|\Delta)\) of a group, we are going to construct a labeled directed polygon for (almost) every word

\[
\omega \equiv x_1^{e_1} \ldots x_n^{e_n},
\]

where \( x_1, \ldots, x_n \) are (not necessarily distinct) generators and each \( e_i = \pm 1 \). For technical reasons mentioned below, \( \omega \) is restricted a bit.
Definition. Let $F$ be a free group with basis $X$. A word $\omega = x_1^{e_1} \cdots x_n^{e_n}$ on $X$ with each $e_i = \pm 1$ is called \textit{freely reduced} if it contains no subwords of the form $xx^{-1}$ or $x^{-1}x$ with $x \in X$.

A \textit{cyclic permutation} of $\omega = x_1^{e_1} \cdots x_n^{e_n}$ is a word of the form $x_1^{e_1} \cdots x_n^{e_n} x_1^{e_1} \cdots x_n^{e_n}$ (by Exercise 3.8, a cyclic permutation of $\omega$ is a conjugate of it). A word $\omega$ is \textit{cyclically reduced} if every cyclic permutation of it is freely reduced.

If $\omega = x_1^{e_1} \cdots x_n^{e_n}$ is cyclically reduced, construct a labeled directed polygon as follows: draw an $n$-gon in the plane; choose an edge and label it $x_1$; label successive edges $x_2, x_3, \ldots, x_n$ as one proceeds counterclockwise around the boundary; direct the $i$th edge with an arrow according to the sign of $e_i$ (we agree that the positive direction is counterclockwise). For example, if $k$ and $x$ commute, then the labeled directed polygon is the square in Figure 12.1; we read the word $k^{-1}xkx^{-1}$ as we travel counterclockwise around the boundary.

![Figure 12.1](image1)

As a second example, consider the last relation in Boone's group $\mathcal{B}$: $\omega = $ first edge is the top $k$-edge in Figure 12.2, for the boundary word is $kq^{-1}tqk^{-1}q^{-1}t^{-1}q$. If $\omega$ is not cyclically reduced, this construction gives a polygon having two adjacent edges with the same label and which point in opposite directions, and such polygons complicate proofs. However, there is no loss in generality in assuming that every relation in a
presentation is cyclically reduced, for every word has some cyclically reduced conjugate, and one may harmlessly replace a relation by any of its conjugates. Every cyclically reduced relation thus yields a labeled directed polygon called its \textit{relator polygon}.

We can now draw a picture of a presentation \((X|\Delta)\) of a group \(G\) (with cyclically reduced relations \(\Delta\)) by listing the generators \(X\) and by displaying a relator polygon of each relation in \(\Delta\). These polygons are easier to grasp (especially when viewing several of them simultaneously) if distinct generators are given distinct colors. The presentation of the group \(\mathcal{B}\) in Boone’s lemma is pictured in Plate 1 (inside front cover). There are six types of generators: \(q; s; r; x; t; k\), and each has been given a different color.

There is a presentation of a group called \(\mathcal{B}_6\) which is pictured in Plate 3. This group will occur in our proof of the Higman imbedding theorem.

Another example is provided by an HNN extension: a relation involving a stable letter \(p\) has the form \(ap^ebp^{-c}\), where \(e = \pm 1\). If the corresponding relator polygon is drawn so that the \(p\)-edges are parallel, then they point in the same direction.

Let \(D\) be a labeled directed polygon. Starting at some edge on the boundary of \(D\), we obtain a word \(\omega\) as we read the edge labels (and the edge directions) while making a complete (counterclockwise) tour of \(D\)’s boundary. Such a word \(\omega\) is called a \textit{boundary word} of \(D\). (Another choice of starting edge gives another boundary word of \(D\), but it is just a cyclic permutation, hence a conjugate, of \(\omega\). A clockwise tour of \(D\)’s boundary gives a conjugate of \(\omega^{-1}\).)

\textbf{Definition.} A \textit{diagram} is a labeled directed polygon whose interior may be subdivided into finitely many labeled directed polygons, called \textit{regions}; we insist that any pair of edges which intersect do so in a vertex.

We quote the fundamental theorem in this context; a proof can be found in Lyndon and Schupp.

\textbf{Fundamental Theorem of Combinatorial Group Theory.} \textit{Let} \(G\) \textit{have a finite presentation} \((X|\Delta)\), \textit{where} \(\Delta\) \textit{satisfies the following conditions}:

(i) \textit{each} \(\delta \in \Delta\) \textit{is cyclically reduced};
(ii) \textit{if} \(\delta \in \Delta\), \textit{then} \(\delta^{-1} \in \Delta\);
(iii) \textit{if} \(\delta \in \Delta\), \textit{then every cyclic permutation of} \(\delta\) \textit{lies in} \(\Delta\).

\textit{If} \(\omega\) \textit{is a cyclically reduced word on} \(X\), \textit{then} \(\omega = 1\) \textit{in} \(G\) \textit{if and only if there is a diagram having a boundary word} \(\omega\) \textit{and whose regions are relator polygons of relations in} \(\Delta\).

An immediate consequence of this theorem is a conjugacy criterion. Assume that \(\omega\) and \(\omega'\) are cyclically reduced words on \(X\), and consider the annulus with outer boundary word \(\omega'\) and inner boundary word \(\omega\), as in Figure 12.3.
Corollary. The elements $\omega$ and $\omega'$ are conjugate in $G$ if and only if the interior of the annulus can be subdivided into relator polygons.

The proof consists in finding a path $\beta$ from $\omega'$ to $\omega$ and cutting along $\beta$ to form a diagram as in Figure 12.4. A boundary word of the new diagram is $\omega' \beta \omega^{-1} \beta^{-1}$, and the fundamental theorem says that this word is 1 in $G$. Conversely, if $\omega' \beta \omega^{-1} \beta^{-1} = 1$ in $G$, one may form an annulus by identifying the edges labeled $\beta$; that is, start with the diagram on the above right and glue the $\beta$'s together to obtain the annulus on the left.

An example will reveal how these diagrams can illustrate the various steps taken in rewriting a word using the relations of a given presentation. The proof of sufficiency of Boone's lemma requires one to prove, for a special word $\Sigma$, that

$$w(\Sigma) = k \Sigma^{-1} t \Sigma k^{-1} \Sigma^{-1} t^{-1} \Sigma = 1 \quad \text{in } B.$$
The hypothesis provides a sequence of elementary operations

\[ \Sigma^* \equiv \omega_1 \rightarrow \omega_2 \rightarrow \cdots \rightarrow \omega_n \equiv q \quad \text{in } \Gamma. \]

The proof begins by showing that each \( \omega_v^* \) has the form \( U_v q_i V_v \), where \( v \leq n - 1 \) and \( U_v \) and \( V_v \) are positive s-words; moreover, there are words \( L_v \) and \( R_v \) on \( \{ x, r_i, i \in I \} \) such that, for all \( v \),

\[ \omega_v^* = L_v \omega_{v+1}^* R_v \quad \text{in } \mathcal{B}. \]

Figure 12.5 pictures all of these equations; we have not drawn the subdivision of each interior polygon into relator polygons, and we have taken the liberty of labeling segments comprised of many s-edges by a single label \( Y, X, V, \) or \( U \).

The reader should now look at Plate 2; it is a diagram having \( w(\Sigma) \) as a boundary word. In the center is the octagon corresponding to the octagonal relation \( w(q) \equiv k q^{-1} t q^{-1} t^{-1} q \), and there are four (almost identical) quadrants as drawn above, involving either \( \Sigma \) or \( \Sigma^{-1} \) on the outer boundary and \( q \) or \( q^{-1} \) on the octagon (actually, adjacent quadrants are mirror images). The commutativity of \( k \) with \( x \) and each \( r_i \) allows one to insert sequences of squares connecting \( k \)-edges on the outer boundary to \( k \)-edges on the octagon; similarly, the commutativity of \( t \) with \( x \) and each \( r_i \) inserts sequences connecting \( t \)-edges on the outer boundary with \( t \)-edges on the octagon. Since the quadrants have already been subdivided into relator polygons, the four quadrants together with the four border sequences, form a diagram. Therefore, \( w(\Sigma) = 1 \) in \( \mathcal{B} \), as asserted by the fundamental theorem.
Define $\mathcal{B}^\Delta$ to be the group having the same presentation as $\mathcal{B}$ except that the octagonal relation is missing. Now regard Plate 2 as an annulus having the octagonal relation as the inner boundary word. This annulus has just been subdivided into relator polygons, and so the corollary of the fundamental theorem says that $w(\Sigma)$ is conjugate to $w(q)$ in $\mathcal{B}^\Delta$. This last result is a reflection of the fact that the octagonal relation enters the given proof of the sufficiency of Boone's lemma at the last step.

The Novikov–Boone–Britton Theorem: Necessity of Boone's Lemma

We now turn to the proof of the more difficult half of Boone's lemma. Geometrically, the problem is to subdivide the labeled directed polygon with boundary word $w(\Sigma)$ into a diagram whose regions are relator polygons of $\mathcal{B}$. The conjugacy of $w(\Sigma)$ and the octagonal relation $w(q)$ in the group $\mathcal{B}^\Delta$ (mentioned above) suggests a strategy to prove the necessity of Boone's lemma: subdivide the annulus with outer boundary $w(\Sigma)$ and inner boundary $w(q)$ using the relations of $\mathcal{B}^\Delta$ (thereby allowing us to avoid further use of the octagonal relation $w(q)$), trying to make the annulus look like Plate 2. We shall give formal algebraic proofs, but, after the proof of each lemma, we shall give informal geometric descriptions. (It was the idea of E. Rips to describe this proof geometrically, and he constructed the diagrams for the Novikov–Boone–Britton theorem as well as for the coming proof of the Higman embedding theorem. He has kindly allowed me to use his description here.)

Define groups $\mathcal{B}_0, \mathcal{B}_1, \mathcal{B}_2,$ and $\mathcal{B}_3$ as follows:

$\mathcal{B}_0 = (x; \varnothing)$, the infinite cyclic group with generator $x$;

$\mathcal{B}_1 = (\mathcal{B}_0; s_0, \ldots, s_M; \Delta_1)$

(recall that we labeled certain subsets of the relations of $\mathcal{B}$ as $\Delta_1 \subset \Delta_2 \subset \Delta_3$ when we defined $\mathcal{B}$; recall also that this notation means that we are adjoining the displayed generators and relations to the given presentation of $\mathcal{B}_0$);

$\mathcal{B}_2 = (\mathcal{B}_1 \ast \mathcal{Q}; r_i, i \in I; \Delta_2)$,

where $\mathcal{Q}$ is free with basis $\{q, q_0, \ldots, q_N\}$;

$\mathcal{B}_3 = (\mathcal{B}_2; t; \Delta_3)$.

Lemma 12.11. In the chain

$$\mathcal{B}_0 \leq \mathcal{B}_1 \leq \mathcal{B}_1 \ast \mathcal{Q} \leq \mathcal{B}_2 \leq \mathcal{B}_3 \leq \mathcal{B},$$

each group is an HNN extension of its predecessor; moreover, $\mathcal{B}_1 \ast \mathcal{Q}$ is an HNN extension of $\mathcal{B}_0$. In more detail:
(i) \( \mathcal{B}_1 \) is an HNN extension with base \( \mathcal{B}_0 \) and stable letters \( \{s_0, \ldots, s_M\} \);
(ii) \( \mathcal{B}_1 \ast Q \) is an HNN extension with base \( \mathcal{B}_0 \) and stable letters \( \{s_0, \ldots, s_M\} \cup \{q, q_0, \ldots, q_N\} \);
(iii) \( \mathcal{B}_2 \) is an HNN extension with base \( \mathcal{B}_1 \ast Q \) and stable letters \( \{r_i; \ i \in I\} \);
(iv) \( \mathcal{B}_3 \) is an HNN extension with base \( \mathcal{B}_2 \) and stable letter \( t \); and
(v) \( \mathcal{B} \) is an HNN extension with base \( \mathcal{B}_3 \) and stable letter \( k \).

**Proof.** (i) The presentation

\[ \mathcal{B}_1 = (x, s_0, \ldots, s_M; s_\beta^{-1}xs_\beta = x^2, \text{all } \beta) \]

shows that \( \mathcal{B}_1 \) has base \( \langle x \rangle = \mathcal{B}_0 \) and stable letters \( \{s_0, \ldots, s_M\} \). Since \( x \) has infinite order, \( A_\beta = \langle x \rangle \cong \langle x^2 \rangle = B_\beta \), and so \( \varphi_\beta: A_\beta \to B_\beta \), defined by \( x \mapsto x^2 \), is a isomorphism for all \( \beta \). Therefore, \( \mathcal{B}_1 \) is an HNN extension.

(ii) The presentation of \( \mathcal{B}_1 \ast Q \),

\[ (x, s_0, \ldots, s_M, q, q_0, \ldots, q_N; s_\beta^{-1}xs_\beta = x^2, q^{-1}xq = x, q_\beta^{-1}xq_\beta = x), \]

shows that \( \mathcal{B}_1 \ast Q \) has base \( \mathcal{B}_0 \) and stable letters \( \{s_0, \ldots, s_M\} \cup \{q, q_1, \ldots, q_N\} \). Since \( x \) has infinite order, \( A_\beta = \langle x \rangle \cong \langle x^2 \rangle = B_\beta \), and so the maps \( \varphi_\beta \) are isomorphisms, as above; also, the maps \( \varphi_{q_i} \) are identity maps, where \( A_{q_i} = \langle x \rangle = B_{q_i} \). Thus, \( \mathcal{B}_1 \ast Q \) is an HNN extension with base \( \mathcal{B}_0 \) and stable letters \( \{s_0, \ldots, s_M\} \cup \{q, q_0, \ldots, q_N\} \).

(ii) Since \( Q \) is free with basis \( \{q, q_0, \ldots, q_N\} \), Example 11.10 now shows that \( \mathcal{B}_1 \ast Q \) is an HNN extension with base \( \mathcal{B}_1 \) and stable letters \( \{q, q_0, \ldots, q_N\} \).

(iii) The presentation

\[ \mathcal{B}_2 = (\mathcal{B}_1 \ast Q; r_i, i \in I| r_i^{-1}(F_i^* q_i, G_i) = H_i^* q_i K_i, r_i^{-1}(s_\beta x) r_i = s_\beta x^{-1}) \]

shows that \( \mathcal{B}_2 \) has base \( \mathcal{B}_1 \ast Q \) and stable letters \( \{r_i, i \in I\} \). Now, for each \( i \), the subgroup \( A_i \) is \( \langle F_i^* q_i, G_i, s_\beta x, \text{all } \beta \rangle \) and the subgroup \( B_i \) is \( \langle H_i^* q_i K_i, s_\beta x^{-1}, \text{all } \beta \rangle \). We claim that both \( A_i \) and \( B_i \) are free groups with bases the displayed generating sets. First, use Exercise 11.8 to see that \( \langle s_\beta x, \text{all } \beta \rangle \) is free with basis \( \{s_\beta x, \text{all } \beta\} \); map \( \langle s_\beta x, \text{all } \beta \rangle \) onto the free group with basis \( \{s_0, \ldots, s_M\} \) by setting \( x = 1 \); then observe that \( A_i = \langle F_i^* q_i G_i, s_\beta x, \text{all } \beta \rangle \cong \langle F_i^* q_i G_i \rangle \ast \langle s_\beta x, \text{all } \beta \rangle \leq \mathcal{B}_1 \ast Q \) (because \( F_i^* q_i G_i \) involves a \( q \)-letter and elements of the free group \( \langle s_\beta x, \text{all } \beta \rangle \) do not). A similar argument applies to \( B_i \), and so there is an isomorphism \( \varphi_i: A_i \to B_i \) with \( \varphi_i(F_i^* q_i, G_i) = H_i^* q_i K_i \) and \( \varphi_i(s_\beta x) = s_\beta x^{-1} \) for all \( \beta \). Thus, \( \mathcal{B}_2 \) is an HNN extension with base \( \mathcal{B}_1 \ast Q \).

(iv) Note that \( \mathcal{B}_3 \) has base \( \mathcal{B}_2 \) and stable letter \( t \):

\[ \mathcal{B}_3 = (\mathcal{B}_2; t| t^{-1}r_i t = r_i, t^{-1}x t = x) \]

Since \( t \) commutes with the displayed relations, \( \mathcal{B}_3 \) is an HNN extension of \( \mathcal{B}_2 \), as in Example 11.11.
(v) Note that $\mathcal{B}$ has base $\mathcal{B}_3$ and stable letter $k$:

$$\mathcal{B} = (\mathcal{B}_3; k|k^{-1}r_ik = r_i, i \in I, k^{-1}xk = x, k^{-1}(q^{-1}tq)k = q^{-1}tq).$$

As in Example 11.11, $\mathcal{B}$ is an HNN extension of $\mathcal{B}_3$. ■

**Corollary 12.12.**

(i) The subgroup $\langle s_1x, \ldots, s_Mx \rangle \leq \mathcal{B}_1$ is a free group with basis the displayed letters.

(ii) There is an automorphism $\psi$ of $\mathcal{B}$, with $\psi(x) = x^{-1}$ and $\psi(s_\beta) = s_\beta$ for all $\beta$.

**Proof.** (i) This was proved in part (iii) of the above lemma.

(ii) The function on the generators sending $x \mapsto x^{-1}$ and $s_\beta \mapsto s_\beta$ for all $\beta$ preserves all the relations. ■

The reader should view Lemma 12.11 as preparation for the remainder of the proof; it will allow us to analyze words using Britton's lemma, Theorem 11.81.

**Lemma 12.13.** Let $\Sigma$ be a fixed special word satisfying the hypothesis of Bonne's lemma:

$$w(\Sigma) \equiv k\Sigma^{-1}t\Sigma k^{-1}\Sigma^{-1}t^{-1}\Sigma = 1 \quad \text{in } \mathcal{B}.$$ 

Then there are freely reduced words $L_1$ and $L_2$ on $\{x, r_i, i \in I\}$ such that

$$L_1\Sigma L_2 = q \quad \text{in } \mathcal{B}_2.$$ 

**Proof.** Since $\mathcal{B}$ is an HNN extension with base $\mathcal{B}_3$ and stable letter $k$, Britton's lemma applies to the word $k\Sigma^{-1}t\Sigma k^{-1}\Sigma^{-1}t^{-1}\Sigma$; it says that $k\Sigma^{-1}t\Sigma k^{-1}$ is a pinch and that $\Sigma^{-1}t\Sigma = C$ in $\mathcal{B}_3$, where $C$ is a word on $\{x, q^{-1}tq, r_i, i \in I\}$. (Since the stable letter $k$ commutes with $\{x, q^{-1}tq, r_i, i \in I\}$, we are in the simple case of Example 11.11 when the subgroups $A$ and $B$ are equal and the isomorphism $\varphi: A \to B$ is the identity.) Therefore, there exist words $\omega$ of the form $\Sigma^{-1}t\Sigma C^{-1} = 1$ in $\mathcal{B}_3$; in detail,

$$\omega \equiv \Sigma^{-1}t\Sigma R_0(q^{-1}t^{e_1}q)R_1(q^{-1}t^{e_2}q)R_2 \ldots (q^{-1}t^{e_n}q)R_n = 1 \quad \text{in } \mathcal{B}_3,$$

where the $R_j$ are (possibly empty) freely reduced words on $\{x, r_i, i \in I\}$ and $e_j = \pm 1$. We assume $\omega$ is such a word chosen with $n$ minimal.

Since $\mathcal{B}_3$ is an HNN extension with base $\mathcal{B}_2$ and stable letter $t$, Britton's lemma applies again, showing that $\omega$ contains a pinch $t^eDt^{-e}$, and there is a word $R$ on $\{x, r_i, i \in I\}$ with $D = R$ in $\mathcal{B}_2$.

If the pinch involves the first occurrence of the letter $t$ in $\omega$, then $t^eDt^{-e} = t\Sigma R_0q^{-1}t^{e_1}$. Hence $e = +1, e_1 = -1, t\Sigma R_0q^{-1}t^{e_1} = tRt^{-1}$, and

$$\Sigma R_0q^{-1} = R \quad \text{in } \mathcal{B}_2;$$

equivalently,

$$R^{-1}\Sigma R_0 = q \quad \text{in } \mathcal{B}_2,$$

which is of the desired form.
If the initial $t^e$ in the pinch is $t^{e_j}$, where $j \geq 1$, then $t^eDt^{-e} \equiv t^{e_j}qR_jq^{-1}t^{e_{j+1}}$ with $qR_jq^{-1} = R$ in $B_2$ for some word $R$ on $\{x, r_i, i \in I\}$. Since $B_2 \leq B_3$, by Theorem 11.78, we may view this as an equation in $B_3$:

$$t^{e_j}qR_jq^{-1}t^{e_{j+1}} = t^eR_jq^{-1}t^{-e} = t^eR t^{-e} \in B_3.$$ 

But the stable letter $t$ in $B_3$ commutes with $x$ and all $r_i$, so there is an equation

$$qR_jq^{-1} = R \quad \text{in} \quad B_3.$$ 

Hence, in $B_3$,

$$(q^{-1}t^{e_j}q)R_j(q^{-1}t^{e_{j+1}}q) = q^{-1}t^eR t^{-e}q$$

$$= q^{-1}Rq \quad \text{(for} \ t \ \text{commutes with} \ x, r_i)$$

$$= q^{-1}(qR_jq^{-1})q$$

$$= R_j.$$ 

There is thus a factorization of $\omega$ in $B_3$ having smaller length, contradicting the choice of $n$ being minimal. Therefore, this case cannot occur. 

![Figure 12.6](image)

Geometrically, we have shown that the labeled directed annulus with outer boundary word $w(\Sigma)$ and inner boundary word the octagon $w(q)$ contains a "quadrant" involving $\Sigma$ on the outer boundary, $q$ on the inner boundary, and internal paths $L_1$ and $L_2$ which are words on $\{x, r_i, i \in I\}$. Of course, there are two such quadrants as well as two "mirror images" of these quadrants which involve $\Sigma^{-1}$ on the outer boundary and $q^{-1}$ on the inner boundary. Moreover, the regions subdividing these quadrants are relator polygons corresponding to the relations $\Delta_2$. 
Finally, there is no problem inserting the “border sequences” connecting $k$-edges (and $t$-edges) on the outer boundary with $k$-edges (and $t$-edges) on the inner boundary, for the internal paths of the quadrants involve only $x$ and $r_i$'s, all of which commute with $k$ and with $t$.

Recall that $\Sigma = X^* q_j Y$, where $X$ and $Y$ are positive $s$-words and $q_j \in \{ q, q_0, \ldots, q_N \}$. We have just shown that

$$ L_1 X^* q_j Y L_2 = q \quad \text{in } \mathcal{A}_2 $$

for some freely reduced words $L_1$ and $L_2$ on $\{ x, r_i, i \in I \}$. Rewrite this last equation as

$$ L_1 X^* q_j = q L_2^{-1} Y^{-1} \quad \text{in } \mathcal{A}_2. $$

**Lemma 12.14.** Each of the words $L_1 X^* q_j$ and $q L_2^{-1} Y^{-1}$ is $r_i$-reduced for every $i \in I$.

**Proof.** Suppose, on the contrary, that $L_1 X^* q_j$ contains a pinch $r_i^e C r_k^{-e}$ as a subword. Since $X^*$ is an $s$-word, this pinch is a subword of $L_1$, a word on $\{ x, r_i, i \in I \}$. Since $L_1$ is freely reduced, $C = x^m$ for some $m \neq 0$. Since $\mathcal{A}_2$ is an HNN extension with base $\mathcal{A}_1 \ast Q$ and stable letters $\{ r_i, i \in I \}$, Britton's lemma says that there is a word $V$ in $\mathcal{A}_1 \ast Q$, where $Q = \langle q, q_1, \ldots, q_N \rangle$, such that

$$ V \equiv \omega_0 (F_i^* q_i G_i)^{e_1} \omega_1 \ldots (F_i^* q_i G_i)^{e_n} \omega_n, $$

$$ e_j = \pm 1, \omega_j \text{ is a word on } \{ s_1 x, \ldots, s_M x \} \text{ for all } j, V \text{ is reduced as a word in the free product, and} $$

$$ x^m = V \quad \text{in } \mathcal{A}_1 \ast Q. $$

Since $x^m \in \mathcal{A}_1$, one of the free factors of $\mathcal{A}_1 \ast Q$, we may assume that $V$ does not involve any $q$-letters; in particular, $V$ does not involve $F_i^* q_i G_i$. Therefore,

$$ x^m = \omega_0 \equiv (s_{\beta_1} x)^{f_1} \ldots (s_{\beta_p} x)^{f_p} \quad \text{in } \mathcal{A}_1, $$

where each $f_v = \pm 1$. Since $\mathcal{A}_1$ is an HNN extension with base $\mathcal{A}_0 = \langle x \rangle$ and stable letters $\{ s_0, \ldots, s_M \}$, another application of Britton’s lemma says that the word $x^{-m} \omega_0$, which is 1 in $\mathcal{A}_1$, contains a pinch of the form $s_{\beta_1}^f x^e s_{\beta_2}^{-f}$, where $e = \pm 1$. Now inspection of the spelling of $\omega_0$ shows that it contains no such subword; we conclude that $\omega_0 = 1$, hence $x^m = 1$. But $x$ has infinite order (since $\mathcal{A}_0 \leq \mathcal{A}_1$), and this contradicts $m \neq 0$. We conclude that $L_1$, and hence $L_1 X^* q_j$, is $r_i$-reduced.

A similar proof shows that $q L_2^{-1} Y^{-1}$ is also $r_i$-reduced. ■

We know that the boundary word of each of the four quadrants is 1, so that each quadrant is subdivided into relator polygons. The two words in the lemma are sub-boundary words that do not flank either of the two $q$-edges; that is, neither of the $q$-edges is surrounded by other (boundary) edges on both sides. As we are working within $\mathcal{A}^2$, the octagonal relator polygon is not inside a quadrant. The only other relator involving a $q$-letter is the eight-
The Novikov–Boone–Britton Theorem: Necessity of Boone's Lemma

Figure 12.7

Figure 12.8

sided “petal” in $\Delta_2$ (Figure 12.7). There must be such a petal involving the $q$-letter on the quadrant's boundary. The lemma shows that the petal's boundary must contain edges in $Y$ and edges in $X^*$ (Figure 12.8).

The following lemma completes the proof of Boone's lemma and, with it, the Novikov–Boone–Britton theorem. In view of a further application of it in the next section, however, we prove slightly more than we need now.

**Lemma 12.15.** Let $L_1$ and $L_2$ be words on $\{x, r_i, i \in I\}$ that are $r_i$-reduced for all $i \in I$. If $X$ and $Y$ are freely reduced words on $\{s_0, \ldots, s_M\}$ and if

$$L_1 X^* q_j Y L_2 = q \quad \text{in } \mathcal{R}_2,$$

then...
then both $X$ and $Y$ are positive and

$$Xq_jY \equiv (X \# q_j Y)^* = q \quad \text{in } \Gamma.$$ 

**Remark.** In our case, both $X$ and $Y$ are freely reduced, for $X$ and $Y$ are positive (because $\Sigma \equiv X \# q_j Y$ is special), and positive words are necessarily freely reduced.

**Proof.** The previous lemma shows that $L_1 X \# q_j = q L_2^{-1} Y^{-1}$ in $B_2$ and that both words are $r_i$-reduced. By Corollary 11.82, the number $\rho \geq 0$ of $r$-letters in $L_1$ is the same as the number of $r$-letters in $L_2$ (because no $r$-letters occur outside of $L_1$ or $L_2$); the proof is by induction on $\rho$.

If $\rho = 0$, then the equation $L_1 X \# q_j Y L_2 = q$ is

$$x^m X \# q_j Y x^n = q \quad \text{in } B_2.$$ 

This equation involves no $r$-letters, and so we may regard it as an equation in $B_1 \ast Q \leq B_2$, where $Q = \langle q, q_0, \ldots, q_N \rangle$. But the normal form theorem for free products (Theorem 11.52) gives $q_j = q$ and $x^m X^* = 1 = Y x^n$ in $B_1$. Since $B_1$ is an HNN extension with base $B_0 = \langle x \rangle$ and stable letters $\{s_0, \ldots, s_M\}$, it follows from Britton's lemma that $m = 0 = n$ and that both $X$ and $Y$ are empty. Thus, $X$ and $Y$ are positive and $X q_j Y = q_j \equiv q$ in $\Gamma$.

Assume now that $\rho > 0$. By Lemma 12.14, the words $L_1 X \# q_j$ and $q L_2^{-1} Y^{-1}$ are $r_i$-reduced for all $i$. Since $B_2$ is an HNN extension with base $B_1 \ast Q$ and stable letters $\{r_i, i \in I\}$, Britton's lemma gives subwords $L_3$ of $L_1$ and $L_4$ of $L_2$ such that

$$L_1 X \# q_j Y L_2 = L_3(r_i^e x^m X \# q_j Y x^n r_i^{-e}) L_4 = q \quad \text{in } B_2,$$

where the word in parentheses is a pinch; moreover, either $e = -1$ and

$$x^m X \# q_j Y x^n \in A_i = \langle F_i^* q_i G_i, s^_g x, \text{all } \beta \rangle,$$

or $e = +1$ and

$$x^m X \# q_j Y x^n \in B_i = \langle H_i^* q_{i_2} K_i, s^_g x^{-1}, \text{all } \beta \rangle.$$

In the first case,

$$q_j = q_{i_1},$$

for the membership holds in the free product $B_1 \ast Q$; in the second case, $q_j = q_{i_2}$. We consider only the case

$$e = -1,$$

leaving the similar case $e = +1$ to the reader. There is a word

$$\omega \equiv x^m X \# q_j Y x^n u_0 (F_i^* q_j G_i)^{s_1} u_1 \cdots (F_i^* q_j G_i)^{s_t} u_t = 1 \quad \text{in } B_1 \ast Q,$$

where $x_j = \pm 1$ and the $u_j$ are possibly empty words on $\{s^_g x, \text{all } \beta\}$. Of all such words, we assume that $\omega$ has been chosen with $t$ minimal. We may
The Novikov–Boone– Britton Theorem: Necessity of Boone’s Lemma

445

further assume that each \( u_i \) is a reduced word on \( \{ s_{\beta} x, \text{ all } \beta \} \), for Corollary 12.12(i) says that this set freely generates its subgroup. Since \( \omega = 1 \) in \( \mathcal{B}_1 \ast Q \), the normal form theorem for free products (Theorem 11.52) shows that each “syllable” of \( \omega \) between consecutive \( q_i \)'s is equal to 1 in \( \mathcal{B}_1 \). However, if one views \( \mathcal{B}_1 \ast Q \) as an HNN extension with base \( \mathcal{B}_1 \) and stable letters \( \{ q, q_0, \ldots, q_n \} \) (as in Example 11.10, in which case the subgroups \( A \) and \( B \) are 1), then Britton’s lemma says that \( \omega \) contains a pinch \( q_j C q_j^{-1} \) as a subword with \( C = 1 \) in \( \mathcal{B}_1 \) (of course, this case of Britton’s lemma is very easy to see directly).

If a pinch involves the first occurrence of \( q_j \), then \( -\varepsilon = \alpha_1 = -1 \) and

\[
Yx^*u_0 G_i^{-1} = 1 \quad \text{in } \mathcal{B}_1.
\]

We claim that a pinch cannot occur at any other place in \( \omega \). Otherwise, there is an index \( v \) with a pinch occurring as a subword of \( (F_1 x^* q G_1)^v u (F_1 x^* q G_1)^{v+1} \).

If \( \alpha_v = +1 \), then \( \alpha_{v+1} = -1 \), the pinch is \( q_j G_i u_i G_i^{-1} q_j^{-1} \), and \( G_i u_i G_i^{-1} = 1 \) in \( \mathcal{B}_1 \); if \( \alpha_v = -1 \), then \( \alpha_{v+1} = +1 \), the pinch is \( q_j^{\alpha} F_1^{-1} u_i F_1^{\alpha} q_j \), and \( F_1^{-1} u_i F_1^{\alpha} = 1 \) in \( \mathcal{B}_1 \). In either case, we have \( u_v = 1 \) in \( \mathcal{B}_1 \). But \( u_v \) is a reduced word on the basis \( \{ s_{\beta} x, \text{ all } \beta \} \), and so \( u_v = 1 \), contradicting the minimality of \( t \). We conclude that \( t = 1, \alpha_1 = -1, \) and

\[
\omega \equiv x^* X^* q_j Y x^* u_0 G_i^{-1} q_j^{-1} F_i^{-1} u_1 = 1 \quad \text{in } \mathcal{B}_1 \ast Q.
\]

We have already seen that

\[
Yx^*u_0 G_i^{-1} = 1 \quad \text{in } \mathcal{B}_1,
\]

and so it follows from \( \omega \) being in the free product that

\[
F_i^{-1} u_i x^* X^* = 1 \quad \text{in } \mathcal{B}_1.
\]

We rewrite these last two equations, by conjugating, into more convenient form:

\[
\begin{aligned}
x^*u_0 G_i^{-1} Y &= 1 \quad \text{in } \mathcal{B}_1, \\
x^* F_i^{-1} u_1 x^* &= 1 \quad \text{in } \mathcal{B}_1.
\end{aligned}
\]

(2)

Recall that \( G_i \) is a positive \( s \)-word. Let us show, after canceling all subwords of the form \( s_{\beta} s_{\beta} \) or \( s_{\beta}^{-1} s_{\beta} \) (if any), that the first surviving letter of \( G_i^{-1} Y \) is positive; that is, there is enough cancellation so that the whole of \( G_i \) is eaten by \( Y \). Otherwise, after cancellation, \( G_i^{-1} Y \) begins with \( s_{\beta} \) for some \( \beta \). Since \( \mathcal{B}_1 \) is an HNN extension with base \( \langle x \rangle \) and stable letters \( \{ s_0, \ldots, s_M \} \), then \( x^* u_0 G_i^{-1} Y = 1 \) in \( \mathcal{B}_1 \) implies, by Britton’s lemma, that its post-cancellation version contains a pinch \( s_{\lambda} D s_{\lambda} \equiv s_{\lambda} x^h s_{\lambda} \), where \( 0 \leq \lambda \leq M \). Now \( u_0 \) is a reduced word on \( \{ s_0 x, \ldots, s_M x \} \), say,

\[
u_0 = (s_{\beta_1} x)^{p_1} \cdots (s_{\beta_p} x)^{p_p},
\]

where \( g_v = \pm 1 \). The pinch is not a subword of \( x^* u_0 \). It follows that the last letter \( s_{\lambda} \) of the pinch \( s_{\lambda} x^h s_{\lambda} \) is the first surviving letter \( s_{\beta} \) of \( G_i^{-1} Y \). Thus, \( \lambda = \beta = \beta_p, f = +1 = g_p \), and \( s_{\beta} x^h s_{\beta}^{-1} = s_{\beta} x s_{\beta}^{-1} \); that is, \( h = 1 \). But \( x =
In a similar manner, one sees, after canceling all subwords of the form \( s_\beta x s_\beta^{-1} \) or \( s_\beta^{-1} x s_\beta \) (if any), that the first surviving letter of \( X^* F_i^* x^{-1} \) is negative; that is, there is enough cancellation so that the whole of \( F_i^* x^{-1} \) is eaten by \( X^* \). The proof is just as above, inverting the original equation \( X^* F_i^* x^{-1} u_1 x^m = 1 \) in \( B_1 \). There is thus a subword \( X_1 \) of \( X \) with \( X_1^* \) ending in a negative letter and such that \( X \equiv X_1 F_i \).

We have proved, in \( B_1 \), that \( 1 = x^n u_0 G_i^{-1} Y = x^n u_0 G_i^{-1} G_i Y_1 \), and so

\[
u_0^{-1} = Y_1 x^n \quad \text{in } B_1.
\]

Define

\[
u_0^{-1} = r_i^{-1} u_0^{-1} r_i.
\]

Since \( u_0 \) is a word on \( s_\beta x \)'s and \( r_i^{-1} s_\beta x r_i = s_\beta x^{-1} \) for all \( \beta \), the element \( v_0^{-1} \) is a word on \( \{ s_0 x^{-1}, \ldots, s_M x^{-1} \} \). But we may also regard \( u_0^{-1} \) and \( v_0^{-1} \) as elements of \( B_2 \), \( \langle x, s_0, \ldots, s_M \rangle \). By Corollary 12.12(ii), there is an automorphism \( \psi \) of \( B_1 \) with \( \psi(x) = x^{-1} \) and \( \psi(s_\beta) = s_\beta \) for all \( \beta \). Hence, \( v_0^{-1} = \psi(u_0^{-1}) = \psi(Y_1 x^n) = Y_1 x^{-n} \); that is,

\[
u_0^{-1} = Y_1 x^{-n} \quad \text{in } B_1.
\]

If one defines \( v_1^{-1} = r_i^{-1} u_1^{-1} r_i \), then a similar argument gives

\[
u_1^{-1} = x^{-m} X_1^*,
\]

where \( X_1 \) is the subword of \( X \) defined above.

Let us return to the induction (remember that we are still in the case \( e = -1 \) of the beginning equation (1)):

\[
L_1 X^* q_j Y L_2 \equiv L_3 (r_i x^m X^* q_j Y x^n r_i^{-1}) L_4 = q \quad \text{in } B_2.
\]

There are equations in \( B_2 \),

\[
q = L_1 X^* q_j Y L_2 \equiv L_3 r_i^{-1} (x^m X^*) q_j (Y x^n) r_i L_4 \\
= L_3 r_i^{-1} (u_1^{-1} F_i^*) q_j (G_i u_0^{-1}) r_i L_4 \quad \text{Eq. (2)} \\
= L_3 v_i^{-1} r_i^{-1} (F_i^* q_j G_i) r_i v_0^{-1} L_4 \\
= L_3 v_i^{-1} (r_i^{-1} F_i^* q_j G_i) r_i v_0^{-1} L_4 \\
= (L_3 v_i^{-1}) H_i^* q_i K_i (v_0^{-1} L_4) \\
= (L_3 x^{-m} X_i^*) H_i^* q_i K_i (Y_1 x^{-n} L_4) \quad \text{Eqs. (3), (4).}
\]

Therefore,

\[
L_3 x^{-m} (X_i^* H_i^* q_i K_i Y_1) x^{-n} L_4 = q \quad \text{in } B_2.
\]

Now \( L_3 x^{-m} \) and \( x^{-n} L_4 \) are words on \( \{ x, r_i, i \in I \} \) having at most \( \rho - 1 \) occurrences of various \( r \)-letters. In order to apply the inductive hypothesis, we
must see that \( X_i^* H_i^* \) and \( K_i Y_1 \) are freely reduced; that is, they contain no “forbidden” subwords of the form \( s_\beta s_\beta^{-1} \) or \( s_\beta^{-1} s_\beta \). Now \( K_i \) is a positive word on \( s \)-letters, so that it contains no forbidden subwords; further, \( Y_1 \equiv G_i^{-1} Y \) is just a subword of \( Y \) (since the whole of \( G_i \) is eaten by \( Y \)), hence has no forbidden subwords, by hypothesis. Therefore, a forbidden subword can occur in \( K_i Y_1 \) only at the interface. But this is impossible, for we have seen that \( Y_1 \) begins with a positive letter, namely, “the first surviving letter” above. A similar argument shows that \( X_i^* H_i^* \) is freely reduced.

By induction, both \( X_i H_i \) and \( K_i Y_1 \) are positive. Hence, their subwords \( X_i \) and \( Y_1 \) are also positive, and hence \( X \equiv X_i F_i \) and \( Y \equiv G_i Y_1 \) are positive. The inductive hypothesis also gives

\[
(X_i^* H_i^* q_{i_1} K_i Y_1)^* = q \quad \text{in } \Gamma.
\]

Since \((X_i^* H_i^*)^* = X_i H_i\), we have

\[
(5) \quad X_i H_i q_{i_1} K_i Y_1 = q \quad \text{in } \Gamma
\]

(it is only now that we see why the “sharp” operation \( \ast \) was introduced; had we used inversion instead, we would now have \( H_i X_i q_{i_2} K_i Y_1 = q \) in \( \Gamma \), and we could not finish the proof). Thus,

\[
X q_j Y \equiv X_i F_i q_j G_i Y_1
\]

\[
\equiv X_i F_i q_{i_1} G_i Y_1 = X_i H_i q_{i_2} K_i Y_1 \quad \text{in } \Gamma.
\]

Combining this with (5) gives

\[
X q_j Y = q \quad \text{in } \Gamma,
\]

as desired. The case \( e = +1 \) at the beginning of the inductive step is entirely similar, and the proof of Boone’s lemma and the Novikov–Boone–Britton theorem is complete. \( \square \)

Here is some geometric interpretation of the long proof of this last lemma. At the end of the previous lemma, we had shown that a quadrant involving \( \Sigma \equiv X^* q_{i_1} Y \) on the outer boundary and a \( q \) on the inner boundary must have a “petal” relator polygon next to \( q_{i_1} \). Now there is another \( q \)-letter on this petal which is now in the interior of the quadrant. As petals are the only relator polygons involving \( q \)-letters (for we are working in \( \mathscr{B}^A \)), there must be a sequence of such petals (involving various \( q \)-letters) from the outer boundary of the quadrant to the \( q \) on the inner boundary (Figure 12.9).

Do any other \( q \)-edges occur on interior regions of the quadrant? The only other possibility is a flower whose eight-sided petals arise from a petal relator regions (Figure 12.10). We have not drawn the relator polygons that subdivide the eye of the flower, but we may assume that the eye contains no relator regions having \( q \)-edges (otherwise the eye contains a smaller such flower and we examine it). The boundary word of the flower’s eye involves \( r_i \)'s and \( s_\beta \)'s, and this word is \( 1 \) in \( \mathscr{B}_2 \). By Britton’s lemma, this word contains a pinch of
12. The Word Problem

Figure 12.9

Figure 12.10
the form $r_i^e C r_i^{-e}$. There are thus two adjacent petals whose $r$-edges point in opposite directions, and this contradicts the orientation of these petals (note how the geometry of the plane enters).

Now focus on the top portion of the quadrant. The remainder of the proof shows that the dashed paths comprised of $s$-edges can be drawn (actually, the proof shows that the rightward path is $X_1^e$ (followed by $x^{-m}$, which is incorporated into $L_3$) and the leftward path is $Y_1$ (followed by $x^n$, which is incorporated into $L_4$). Induction says that one can repeat this construction, so that the petals move down to the bottom $q$; thus the whole quadrant can be subdivided into relator regions.

Aside from the group-theoretic proof just given (which is a simplification of Britton's original proof), there are several other proofs of the unsolvability of the word problem for groups: the original combinatorial proofs of Novikov and of Boone; a proof of G. Higman's, which is a corollary of his imbedding theorem. The proof of Higman's imbedding theorem that we shall give in the next section uses our development so far, whereas Higman's original proof does not depend on the Novikov–Boone–Britton theorem.

We must mention an important result here (see Lyndon and Schupp (1977) for a proof). W. Magnus (1930) proved the Freiheitsatz. If $G$ is a finitely generated group having only one defining relation $r$, say, $G = \langle x_1, \ldots, x_n | r \rangle$, then any subset of $\{x_1, \ldots, x_n\}$ not containing all the $x_i$ involved in $r$ freely generates its subgroup. As a consequence, he showed (1932) that $G$ has a solvable word problem.

There are other group-theoretic questions yielding unsolvable problems; let us consider another such question now.

**Definition.** A finitely generated group $G = \langle X | \Delta \rangle$ has a solvable conjugacy problem if there is a decision process to determine whether an arbitrary pair of words $\omega$ and $\omega'$ on $X$ are conjugate elements of $G$. 
When \( G \) is finitely presented, it can be shown that its having a solvable conjugacy problem does not depend on the choice of finite presentation. A group with a solvable conjugacy problem must have solvable word problem, for one can decide whether an arbitrary word \( \omega \) is (a conjugate of) \( 1 \); the converse is false. We now indicate how this result fits into our account.

**Corollary 12.16.** The group \( B^A \) has solvable word problem and unsolvable conjugacy problem.

**Proof.** Recall that \( B^A \) is Boone's group \( B \) without the octagonal relation \( w(q) \). A.A. Fridman (1960) and Boone, independently, proved that \( B^A \) has solvable word problem (we will not present this argument).

The following three statements are equivalent for any special word \( \Sigma \):

(i) \( w(\Sigma) = 1 \) in \( B \);
(ii) \( \Sigma^* = q \) in \( \Gamma \);
(iii) \( w(\Sigma) \) is conjugate to \( w(q) \) in \( B^A \).

The necessity of Boone's lemma is (i) \( \Rightarrow \) (ii); in geometric terms, we have already seen that the labeled directed annulus with outer boundary word \( w(\Sigma) \) and inner boundary word \( w(q) \) can be subdivided into relator polygons corresponding to relations other than \( w(q) \); that is, using relations of \( B^A \). This proves (ii) \( \Rightarrow \) (iii). Finally, (iii) \( \Rightarrow \) (i) is obviously true, because \( w(q) = 1 \) in \( B \). The equivalence of (i) and (iii) shows that \( B^A \) has a solvable conjugacy problem if and only if \( B \) has a solvable word problem. By the Novikov–Boone–Britton theorem, \( B^A \) has an unsolvable conjugacy problem. 

**The Higman Imbedding Theorem**

When can a finitely generated group be imbedded in a finitely presented group? The answer to this purely group-theoretic question reveals a harmonic interplay of Group Theory and Mathematical Logic. The proof we present here is due to S. Aanderaa (1970).

The following technical lemma is just a version of the "trick" which allows an arbitrary word on an alphabet to be viewed as a positive word on a larger alphabet.

**Lemma 12.17.** Every group \( G \) has a presentation

\[
G = (Y|\Psi)
\]

in which every relation is a positive word on \( Y \). If \( G \) is finitely generated (or finitely presented), there is such a presentation in which \( Y \) (or both \( Y \) and \( \Psi \)) is finite.

**Proof.** If \( G = (X|\Delta) \) is a presentation, define a new set \( X' \) disjoint from \( X \) and
The Higman Imbedding Theorem

in bijective correspondence with it via \( x \mapsto x' \),
\[
X' = \{ x' | x \in X \},
\]
and define a new presentation of \( G \):
\[
G = (X \cup X'|\Delta', xx', x \in X),
\]
where \( \Delta' \) consists of all the words in \( \Delta \) rewritten by replacing every occurrence of every \( x^{-1} \) by \( x' \).

**Definition.** A group \( R \) is **recursively presented** if it has a presentation
\[
R = (u_1, \ldots, u_m | \omega = 1, \omega \in E),
\]
where each \( \omega \) is a positive word on \( u_1, \ldots, u_m \), and \( E \) is an r.e. set.

The lemma shows that the positivity assumption, convenient for notation, is no real restriction on \( R \).

**Exercises**

12.12. If a group \( R \) is recursively presented, then it has a presentation whose relations form a recursive set of positive words. (*Hint.* If the given presentation is
\[
R = (u_1, \ldots, u_m | \omega_k = 1, k \geq 0),
\]
where \( \{ \omega_k = 1, k \geq 0 \} \) is an r.e. set of positive words, define a new presentation
\[
(u_1, \ldots, u_m, y | y = 1, y^k \omega_k = 1, k \geq 0).)
\]

12.13. Every finitely generated subgroup of a finitely presented group is recursively presented. (*Hint.* Consider all words that can be obtained from 1 by a finite number of elementary operations.)

12.14. Every recursively presented group can be imbedded in a two-generator recursively presented group. (*Hint.* Corollary 11.80.)

**Theorem 12.18 (G. Higman, 1961).** Every recursively presented group \( R \) can be imbedded in a finitely presented group.

With Exercise 12.13, Higman's theorem characterizes finitely generated subgroups of finitely presented groups.

Assume that \( R \) has a presentation
\[
R = (u_1, \ldots, u_m | \omega = 1, \omega \in E),
\]
where \( E \) is an r.e. set of positive \( u \)-words. There is thus a Turing machine \( T \) (with alphabet \( \{ s_0, \ldots, s_M \} \) containing \( \{ u_1, \ldots, u_m \} \)) enumerating \( E \); moreover, by Exercise 12.11, we may assume that \( T \) has stopping state \( q_0 \). We are going to use the group \( \mathcal{B}(T) \), constructed in Boone's lemma, arising from the semigroup \( \Gamma(T) \). Now the original Markov–Post semigroup \( \gamma(T) \) was rewrit-
ten as $\Gamma(T)$ for the convenience of the proof of the unsolvability of the word problem. For Higman’s theorem, we shall rewrite $\gamma(T)$ another way. Of course, this will engender changes in the generators and relations of $B(T)$, and so we review the construction. Beginning with a Turing machine $T$ with stopping state $q_0$, we constructed $\gamma(T)$ with generators $q, h, q_0, \ldots, q_N, s_0, \ldots, s_M$, and certain relations. The semigroup $\Gamma(T)$ renamed $h$ as the last $s$-letter; thus, $\Gamma(T)$ has generators $q$’s and $s$’s and relations those of $\gamma$ rewritten accordingly. Returning to the original notation (with $h$ no longer an $s$-letter) gives a group $B(T)$ with generators:

$$q, h, q_0, \ldots, q_N, s_0, \ldots, s_M, r_i, i \in I, x, k, t$$

and relations those of the original $B(T)$ but with the relations $\Delta_2$ rewritten accordingly:

$$\Delta_2': \quad \text{for all } \beta = 0, \ldots, M \text{ and } i \in I,$$

$$s_{\beta}^{-1}xs_{\beta} = x^2, \quad h^{-1}xh = x^2,$$

$$r_i^{-1}s_{\beta}xr_i = xs_{\beta}^{-1}, \quad r_i^{-1}hxr_i = xh^{-1},$$

$$r_i^{-1}F_i^#q_iG_i = H_i^#q_iK_i.$$

By Corollary 12.9, a positive $s$-word $w$ lies in $E$ if and only if $w(h^{-1}q_1w) = 1$ in $B(T)$; that is, $\omega \in E$ if and only if

$$(6) \quad k(h^{-1}\omega^{-1}q_1^{-1}hth^{-1}q_1^{-1}w) = (h^{-1}\omega^{-1}q_1^{-1}hth^{-1}q_1^{-1}w)k \quad \text{in } B(T).$$

Let us introduce new notation to simplify this last equation. First, define $B_2(T)$ as the group with the presentation

$$B_2(T) = (q, h, q_0, \ldots, q_N, s_0, \ldots, s_M, r_i, i \in I | \Delta_2').$$

Now introduce new symbols:

$$\tau = q_1^{-1}hth^{-1}q_1 \quad \text{and} \quad \kappa = hkh^{-1}.$$

Define a new group $B_3(T)$ by the presentation

$$B_3'(T) = (B_2(T); \tau | \tau^{-1}(q_1^{-1}hr_1h^{-1}q_1)\tau = q_1^{-1}hr_1h^{-1}q_1, \tau^{-1}(q_1^{-1}hth^{-1}q_1)\tau = q_1^{-1}hth^{-1}q_1).$$

Note that $B_3'(T)$ is just another presentation of the group

$$B_3 = (B_2(T); t | tr_i = r_it, i \in I, tx = xt),$$

as can be quickly seen by replacing $\tau$ by its definition. Similarly, we define

$$B'(T) = (B_3'(T); \kappa | \kappa^{-1}(hr_1h^{-1})\kappa = hr_1h^{-1}, \kappa^{-1}(hth^{-1})\kappa = hth^{-1}, \kappa^{-1}(hq^{-1}h^{-1}q_1q_1^{-1}hqh^{-1}) = hq^{-1}h^{-1}q_1q_1^{-1}hqh^{-1}).$$

Replacing $\kappa$ by its definition shows that $B'(T)$ is another presentation of

$$B(T) = (B_3'(T); k | kr_i = r_i, i \in I, kx = xk, k(q^{-1}tq) = (q^{-1}tq)k).$$
Lemma 12.19.
(i) $B'_3(T)$ is an HNN extension with base $B_3(T)$ and stable letter $\tau$.
(ii) $B'(T) \cong B(T)$, and $B'(T)$ is an HNN extension with base $B'_3(T)$ and stable letter $\kappa$.

Proof. As the proof of Lemma 12.11. ■

The next lemma shows how $B'(T)$ simplifies (6).

Lemma 12.20. If $\omega$ is a positive word on $s_0, \ldots, s_m$, then $\omega \in E$ if and only if
$\kappa(\omega^{-1} \tau \omega) = (\omega^{-1} \tau \omega) \kappa$ in $B'(T)$.

Proof. The equation $\omega(h^{-1} q_1 \omega h) = 1$ in $B(T)$ has this simpler form in $B'(T)$
when $t$ and $k$ are replaced by $\tau$ and $\kappa$, respectively. ■

Form the free product $B'(T) \ast R$. Recall that $R$ is generated by
$\{u_1, \ldots, u_m\}$. At the outset, the Turing machine $T$ enumerating the relations
of $R$ was chosen so that its alphabet $\{s_0, \ldots, s_m\}$ contains $\{u_1, \ldots, u_m\}$. Of
course, the generating sets of the free factors of $B'(T) \ast R$ must be disjoint.
Let us, therefore, introduce new letters $\{a_1, \ldots, a_m\} \subset \{s_0, \ldots, s_m\} \subset B'(T)$
for the replica of $\{u_1, \ldots, u_m\} \subset R$. Henceforth, we will regard the r.e. set $E$
comprised of certain positive words on $\{a_1, \ldots, a_m\} \subset \{s_0, \ldots, s_m\}$. Our re-
writing is completed.

Now define new groups $B_4$, $B_5$, and $B_6$ as follows (these also depend on
$T$, but we abbreviate notation):

$B_4 = (B'(T) \ast R; b_1, \ldots, b_m | b_i^{-1} u_j b_i = u_j, b_i^{-1} a_j b_i = a_j,$
$\quad b_i^{-1} \kappa b_i = \kappa u_i^{-1}, \text{ all } i, j = 1, \ldots, m);$  
$B_5 = (B_4; d | d^{-1} \kappa d = \kappa, d^{-1} a_i b_i d = a_i, i = 1, \ldots, m);$  
$B_6 = (B_5; \sigma | \sigma^{-1} \tau \sigma = \tau d, \sigma^{-1} \kappa \sigma = \kappa, \sigma^{-1} a_i \sigma = a_i, i = 1, \ldots, m).$

Aanderaa’s proof of Higman’s theorem is in two steps. The first step shows
that each of these groups is an HNN extension of its predecessor:

$R \leq B'(T) \ast R \leq B_4 \leq B_5 \leq B_6;$

by Theorem 11.78, each group is imbedded in its successor, and so $R$ is a
subgroup of $B_6$. The second step shows that $B_6$ is finitely presented. After the
proof is completed, we shall see that the diagram in Plate 4 partially explains
how the generators and relations of the groups $B_4$, $B_5$, and $B_6$ arise.

Lemma 12.21. The subgroups $\langle a_1, \ldots, a_m, \kappa \rangle$ and $\langle a_1, \ldots, a_m, \tau \rangle$ of $B'(T) \ast R$
are free groups with respective bases the displayed generating sets.

Proof. Recall our analysis of $B(T)$ in Lemma 12.11: $B_1$ is an HNN extension
with base $B_0$ and stable letters $\{s_0, \ldots, s_M\}$; in our present notation, $B_1$ has stable letters $\{h, s_0, \ldots, s_M\}$. It follows from Lemma 11.76 that $\langle h, s_0, \ldots, s_M \rangle$ is a free group with basis $\{h, s_0, \ldots, s_M\}$. Since $B_1 \leq B'(T)$, this last statement holds in $B'(T) \ast R$. But $\{a_1, \ldots, a_m\} \subseteq \{s_0, \ldots, s_M\}$, so that $\langle a_1, \ldots, a_m \rangle$ is free with basis $\{a_1, \ldots, a_m\}$.

We now show that $\{a_1, \ldots, a_m, \kappa\}$ freely generates its subgroup (a similar argument that $\{a_1, \ldots, a_m, \tau\}$ freely generates its subgroup is left to the reader). Otherwise, there is a word

$$\omega = c_0 \kappa c_1 \kappa^{-1} \cdots c_{n-1} \kappa^{-n} = 1 \quad \text{in} \quad B'(T) \ast R,$$

where $e_v = \pm 1$ and $c_v$ are (possibly empty) freely reduced words on $\{a_1, \ldots, a_m\}$; we may further assume, of all such words $\omega$, that $n$ is chosen minimal. Since $\omega$ involves no $u$-letters, we have $\omega = 1$ in $B'(T)$. As $B'(T)$ is an HNN extension with base $B'_3(T)$ and stable letter $\kappa$, Britton's lemma says that either $\omega$ does not involve $\kappa$ or $\omega$ contains a pinch $\kappa^oc_\kappa \kappa^{-e}$, where $c_v$ is a word on $\{hr,h^{-1}, i \in I, hxx^{-1}, hq^{-1}h^{-1}q_1h_{q_1}^{-1}h_{q_1}h^{-1}\}$. But the relations in $B'(T)$ show that $\kappa$ commutes with $c_v$, so that $\kappa^oc_\kappa \kappa^{-e} = c_v$ in $B'(T) \leq B'(T) \ast R$, and this contradicts the minimality of $n$. It follows that $\omega$ does not involve $\kappa$; that is, $\omega$ is a reduced word on $\{a_1, \ldots, a_m\}$. But we have already seen that $\langle a_1, \ldots, a_m \rangle$ is free with basis $\{a_1, \ldots, a_m\}$, so that $\omega = 1$. ■

Lemma 12.22. $B_4$ in an HNN extension with base $B'(T) \ast R$ and stable letters $\{b_1, \ldots, b_m\}$.

Proof. It suffices to show there are isomorphisms $\phi_i: A_i \rightarrow B_i$, where

$$A_i = \langle u_1, \ldots, u_m, a_1, \ldots, a_m, \kappa \rangle,$$

$$B_i = \langle u_1, \ldots, u_m, a_1, \ldots, a_m, \kappa u_i^{-1} \rangle,$$

and $\phi_i(u_j) = u_j$, $\phi_i(a_j) = a_j$, and $\phi_i(\kappa) = \kappa u_i^{-1}$. Note that $A_i = B_i$.

It is easy to see, in $B'(T) \ast R$, that

$$A_i = \langle a_1, \ldots, a_m, \kappa \rangle \ast \langle u_1, \ldots, u_m \rangle$$

$$= \langle a_1, \ldots, a_m, \kappa \rangle \ast R.$$

By Lemma 12.21, $\langle a_1, \ldots, a_m, \kappa \rangle$ is freely generated by $\{a_1, \ldots, a_m, \kappa\}$, so that $\phi_i$ is a well defined homomorphism. Similarly, the map $\psi_i: B_i \rightarrow A_i$, given by $\psi_i(u_j) = u_j$, $\psi_i(a_j) = a_j$, and $\psi_i(\kappa) = \kappa u_i$, is a well defined homomorphism. But $\psi_i$ is the inverse of $\phi_i$, so that $\phi_i$ is an isomorphism and $B_4$ is an HNN extension. ■

Lemma 12.23. $B_5$ is an HNN extension with base $B_4$ and stable letter $d$.

Proof. It suffices to show that there is an isomorphism

$$\phi: A = \langle \kappa, a_1b_1, \ldots, a_mb_m \rangle \rightarrow B = \langle \kappa, a_1, \ldots, a_m \rangle$$

with $\phi(\kappa) = \kappa$ and $\phi(a_ib_j) = a_i$ for all $i$. 

\[\]
Since \( \kappa^{-1}b_{i}\kappa = b_{i}u_{i} \) in \( \mathcal{B}_{s} \), the function \( \theta: \mathcal{B}_{s} \to \mathcal{B}(T) \ast R \), defined by sending each \( b_{i} \) to 1, each \( u_{i} \) to 1, and all other generators to themselves, is a well defined homomorphism (it preserves all the relations: \( b_{i} = 1 \) implies \( 1 = \kappa^{-1}b_{i}\kappa = b_{i}u_{i} = u_{i} \)). The map \( \theta \) takes each of \( \langle \kappa, a_{1}, b_{1}, \ldots, a_{m}, b_{m} \rangle \) and \( \langle \kappa, a_{1}, \ldots, a_{m} \rangle \) onto the subgroup \( \langle \kappa, a_{1}, \ldots, a_{m} \rangle \leq \mathcal{B}(T) \ast R \) which, by the preceding lemma, is free on the displayed generators. By Exercise 11.8, each of the two subgroups \( A \) and \( B \) of \( \mathcal{B}_{s} \) is free on the displayed generators, and so the map \( \phi: A \to B \) given above is a well defined isomorphism. ■

The next lemma will be needed in verifying that \( \mathcal{B}_{s} \) is an HNN extension of \( \mathcal{B}_{s} \).

**Lemma 12.24.** The subgroup \( A = \langle \kappa, a_{1}, \ldots, a_{m}, \tau \rangle \leq \mathcal{B}(T) \) has the presentation

\[
A = (\kappa, a_{1}, \ldots, a_{m}, \tau | \kappa^{-1}\omega^{-1}1\omega \kappa = \omega^{-1}1\tau \omega, \omega \in E).
\]

**Remark.** Recall our change in notation: although \( E \) was originally given as a set of positive words on \( \{u_{1}, \ldots, u_{m}\} \), it is now comprised of positive words on \( \{a_{1}, \ldots, a_{m}\} \).

**Proof.** By Lemma 12.20, the relations \( \kappa^{-1}\omega^{-1}1\omega \kappa = \omega^{-1}1\tau \omega \), for all \( \omega \in E \), do hold in \( \mathcal{B}(T) \), and hence they hold in the subgroup \( A \leq \mathcal{B}(T) \). To see that no other relations are needed, we shall show that if \( \zeta \) is a freely reduced word on \( \{\kappa, a_{1}, \ldots, a_{m}, \tau\} \) with \( \zeta = 1 \) in \( A \), then \( \zeta \) can be transformed into 1 via elementary operations using only these relations.

**Step 1.** \( \zeta \) contains no subword of the form \( \tau^{e}\omega \kappa^{\eta} \), where \( e = \pm 1, \eta = \pm 1 \), and \( \omega \in E \).

It is easy to see that the given relations imply

\[
\tau^{e}\omega \kappa^{\eta} = \omega \kappa^{\eta} \omega^{-1}1\tau \omega.
\]

If \( \zeta \) contains a subword \( \tau^{e}\omega \kappa^{\eta} \), then

\[
\zeta \equiv \zeta_{1} \tau^{e}\omega \kappa^{\eta} \zeta_{2} \rightarrow \zeta_{1} \omega \kappa^{\eta} \omega^{-1}1\tau \omega \zeta_{2}
\]

is an elementary operation. Cancel all subwords (if any) of the form \( \gamma \gamma^{-1} \) or \( \gamma^{-1} \gamma \), where \( \gamma \equiv \tau, \kappa, \) or some \( a_{j} \). With each such operation, the total number of occurrences of \( \tau^{e} \) which precede some \( \kappa^{\eta} \) goes down. Therefore, we may assume that \( \zeta \) is freely reduced and contains no subwords of the form \( \tau^{e} \omega \kappa^{\eta} \).

**Step 2.** \( \zeta \) involves both \( \kappa \) and \( \tau \).

If \( \zeta \) does not involve \( \kappa \), then it is a word on \( \{a_{1}, \ldots, a_{m}, \tau\} \). But this set freely generates its subgroup, by Lemma 12.21, and so \( \zeta \) being freely reduced and \( \zeta = 1 \) imply \( \zeta \equiv 1 \). A similar argument shows that \( \zeta \) involves \( \tau \) as well.

Since \( \mathcal{B}(T) \) is an HNN extension with base \( \mathcal{B}_{s}(T) \) and stable letter \( \kappa \), Britton's lemma says that \( \zeta \) contains a pinch \( \kappa^{e}V_{\kappa^{-e}} \), where \( e = \pm 1 \), and
there is a word \( D \) on \( \{hr_i h^{-1}, i \in I, h x h^{-1}, h q^{-1} h^{-1} q_1 \tau q_1^{-1} h q h^{-1} \} \) with
\[ V = D \quad \text{in} \quad B_3(T). \]
Choose \( D \) so that the number of occurrences of \( \tau \) in it is minimal.

**Step 3.** \( D \) is \( \tau \)-reduced.

Now \( B_3(T) \) is an HNN extension with base \( B_2(T) \) and stable letter \( \tau \). Let us write
\[ \delta = h q^{-1} h^{-1} q_1, \]
so that
\[ h q^{-1} h^{-1} q_1 \tau q_1^{-1} h q h^{-1} \equiv \delta \tau \delta^{-1}. \]
If \( D \), which is now a word on \( \{hr_i h^{-1}, i \in I, h x h^{-1}, \delta \tau \delta^{-1} \} \), is not \( \tau \)-reduced, then it contains a pinch. Since an occurrence of \( \tau \) can only arise from an occurrence of \( \delta \tau \delta^{-1} \), it follows that
\[ D \equiv D_1 \delta \tau f \delta^{-1} D_2 \delta \tau^{-f} \delta^{-1} D_3, \]
where \( D_2 \) does not involve the stable letter \( \tau \) (just check the cases \( f = 1 \) and \( f = -1 \) separately); moreover, there is a word \( W \) on \( \{q_1^{-1} h r_i h^{-1} q_1, i \in I, q_1^{-1} h x h^{-1} q_1 \} \) with
\[ \delta^{-1} D_2 \delta = W \quad \text{in} \quad B_2(T) \]
(the subgroups \( A \) and \( B \) in the HNN extension are here equal, and so we need not pay attention to the sign of \( f \)). From the presentation of \( B_3(T) \), we see that \( \tau \) and \( W \) commute. Therefore,
\[ D = D_1 \delta \tau f W \tau^{-f} \delta^{-1} D_3 = D_1 \delta W \delta^{-1} D_3 \quad \text{in} \quad B_3(T), \]
contradicting our choice of \( D \) having the minimal number of occurrences of \( \tau \). It follows that \( D \) is \( \tau \)-reduced.

**Step 4.** \( V \) is \( \tau \)-reduced.

Otherwise, \( V \) contains a pinch \( \tau^\theta C \tau^{-\theta} \), where
\[ C = W \quad \text{in} \quad B_2(T) \]
and \( W \), a word on \( \{q_1^{-1} h r_i h^{-1} q_1, i \in I, q_1^{-1} h x h^{-1} q_1 \} \) (as above), commutes with \( \tau \) in \( B_3(T) \). Now \( V \) does not involve \( \kappa \), so its subword \( C \) involves neither \( \kappa \) nor \( \tau \). Since \( \zeta \), hence its subword \( V \), is a word on \( \{\kappa, a_1, \ldots, a_m, \tau \} \), it follows that \( C \) is a word on \( \{a_1, \ldots, a_m\} \). But \( \langle \tau, a_1, \ldots, a_m \rangle \leq B'(T) \ast R \) is a free group with basis the displayed generators, by Lemma 12.21, and so \( C \) commutes with \( \tau \) if and only if \( C \equiv 1 \). Therefore, the pinch \( \tau^\theta C \tau^{-\theta} \equiv \tau^\theta \tau^{-\theta} \), contradicting \( \zeta \) being freely reduced.

**Step 5.** Both \( V \) and \( D \) involve \( \tau \).

Since \( V = D \) in \( B_3(T) \) and both are \( \tau \)-reduced, Corollary 11.82 applies to show that both of them involve the same number of occurrences of the stable
letter $\tau$. Assume now that neither $V$ nor $D$ involves $\tau$. Then $V$ is a word on \{a_1, \ldots, a_m\} and $D$ is a word on \{hr_i h^{-1}, i \in I, hxh^{-1}\}; we may assume that $D$ has been chosen so that the total number of occurrences of $r$-letters is minimal; moreover, we may assume that all adjacent factors equal to $hxh^{-1}$ are collected as $hx^m h^{-1}$. It follows that the equation $V = D$ holds in the subgroup $\mathcal{B}_2(T)$, which is an HNN extension with base $\mathcal{B}_1 \ast \langle q, q_0, \ldots, q_N \rangle$ and stable letters \{r_i, i \in I\}.

Now $V$ is $r_i$-reduced for all $i$ because $V$, being a word on \{a_1, \ldots, a_m\}, does not even involve any $r$-letters. We claim that $D$ is also $r_i$-reduced for all $i$. Otherwise, $D$ (a word on \{hr_i h^{-1}, i \in I, hxh^{-1}\}) contains a pinch: there is thus an index $i$ with $$D \equiv \Delta_1 hr_i h^{-1} \Delta_2 hr_i^{-1} h^{-1} \Delta_3,$$
where $l = \pm 1$ and $\Delta_2$ involves no $r$-letters (just check the cases $l = 1$ and $l = -1$ separately); hence, $\Delta_2 \equiv hx^m h^{-1}$ (since it is freely reduced), and $$D \equiv \Delta_1 hr_i x^m r_i^{-1} h^{-1} \Delta_3.$$ The pinch in $D$ is thus $r_i^lx^m r_i^{-1}$, and Britton’s lemma concludes, depending on the sign of $l$, that $x^m$ is equal in $\mathcal{B}_1 \ast \langle q, q_0, \ldots, q_N \rangle$ either to a word on \{$F_i q_i, G_i, s_0 x, \ldots, s_M x$\} or to a word on \{$H_i q_i K_i, s_0 x^{-1}, \ldots, s_M x^{-1}$\}. As $D$ does not involve $q$-letters, $x^m$ is equal in $\mathcal{B}_1$ to a word on either \{s_0 x, \ldots, s_M x\} or \{s_0 x^{-1}, \ldots, s_M x^{-1}\}, and we have already seen, in the proof of Lemma 12.14, that this forces $m = 0$. Therefore, the pinch is $r_i^l r_i^{-1}$, contradicting our choice of $D$ involving the minimal number of $r$-letters. We conclude that both $V$ and $D$ are $r_i$-reduced for all $i$. By Corollary 11.82, $D$ involves no $r$-letters (because $V$ involves none), and $D$ is a word on $hxh^{-1}$; that is, $D = hx^m h^{-1}$ in $\mathcal{B}_1$. In this step, $V$ is assumed to be a word on \{a_1, \ldots, a_m\} $\subseteq$ \{s_0, \ldots, s_M\}, so that the equation $V = D$ holds in $\mathcal{B}_1$ and $$Vhx^{-n}h^{-1} = 1 \text{ in } \mathcal{B}_1.$$ Recall that $\mathcal{B}_1$ is an HNN extension with base $\langle x \rangle$ and stable letters \{h, s_0, \ldots, s_M\} If $V$ involves $a_j$ for some $j$, then Britton’s lemma gives a pinch $a_j^r U a_j^{-r}$, where $r = \pm 1$ and $U$ is a power of $x$ (for $a_j$ is a stable letter). Now $h \neq a_j$, for $h \notin \{s_0, \ldots, s_M\}$, so that this pinch must be a subword of $V$. But $V$ does not involve $x$, and so $U \equiv 1$; therefore $a_j^r a_j^{-r}$ is a subword of $V$, contradicting $\zeta$ and its subword $V$ being freely reduced. It follows that $V$ involves no $a_j$; as $V$ is now assumed to be a word on $a$-letters, we have $V \equiv 1$. Recall that $V$ arose in the pinch $k^e V k^{-e}$, a subword of $\zeta$, and this, too, contradicts $\zeta$ being freely reduced.

**Step 6.** $V$ contains a subword $\tau^e V_p$, where $V_p$ is a positive $a$-word lying in the r.e. set $E$.

Since $D$, a word on \{hr_i h^{-1}, i \in I, hxh^{-1}, hq^{-1} h^{-1} q_1 \tau q_1^{-1} hqh^{-1}\}, involves $\tau$, it must involve $hq^{-1} h^{-1} q_1 \tau q_1^{-1} hqh^{-1}$. Write $$D \equiv \Lambda (hq^{-1} h^{-1} q_1 \tau q_1^{-1} hqh^{-1}) \Lambda,$$
where \( \alpha = \pm 1 \) and the word in parentheses is the final occurrence of the long word involving \( \tau \) in \( D \); thus, \( \Lambda \) is a word on \( \{ hr_i h^{-1}, i \in I, h x h^{-1} \} \).

Since \( V \) involves \( \tau \), we may write

\[
V \equiv V_0 \tau^e_1 V_1 \ldots V_{p-1} \tau^e_p V_p,
\]

where \( e_i = \pm 1 \) and each \( V_i \) is a freely reduced word on \( a \)-letters. By Steps 3 and 4, both \( D \) and \( V \) are \( \tau \)-reduced, so that Corollary 11.82 says that

\[
\tau^e_p V_p \Lambda^{-1} h q^{-1} h^{-1} q_1 \tau^{-e}
\]

is a pinch. Thus, there is a word \( Z \) on \( \{ q_1^{-1} h r_i h^{-1} q_1, q_i^{-1} h x h^{-1} q_1 \} \) with

\[
V_p \Lambda^{-1} h q^{-1} h^{-1} q_1 = Z \quad \text{in } B_2(T);
\]

of course, we may choose

\[
Z \equiv q_1^{-1} h L_1 h^{-1} q_1,
\]

where \( L_1 \) is a word on \( \{ x, r_i, i \in I \} \); similarly, since \( \Lambda \) is a word on \( \{ hr_i h^{-1}, i \in I, h x h^{-1} \} \), we may write

\[
\Lambda^{-1} = h L_2 h^{-1} \quad \text{in } B_2(T),
\]

where \( L_2 \) is a word on \( \{ x, r_i, i \in I \} \). Substituting, we see that

\[
V_p h L_2 h^{-1} h q^{-1} h^{-1} q_1 = q_1^{-1} h L_1 h^{-1} q_1 \quad \text{in } B_2(T),
\]

and we rewrite this equation as

\[
L_1^{-1} h^{-1} q_1 V_p h L_2 = q \quad \text{in } B_2(T).
\]

Note that \( V_p h \) is freely reduced, for \( V_p \) is a freely reduced word on \( a \)-letters, and \( h \) is not an \( s \)-letter, hence not an \( a \)-letter. By Lemma 12.15 (with \( X \equiv h \) and \( Y \equiv V_p h \)), we have \( Y \) a positive word, so that its subword \( V_p \) is a positive word on \( a \)-letters; moreover,

\[
h q_1 V_p h = q \quad \text{in } \gamma(T).
\]

By Lemma 12.4, \( V_p \in E \). Returning to (7), the birthplace of \( V_p \), we see that \( \tau^e_p V_p \) is a subword of \( V \). Indeed, \( V \equiv V \tau^e_p V_p \), where \( V \) is the initial segment of \( V \).

**Step 7.** Conclusion.

Recall that \( V \) arose inside the pinch \( \kappa^e V \kappa^{-e} \), which is a subword of \( \zeta \). From the previous step, we see that \( \kappa^e V \tau^e_p V_p \kappa^{-e} \) is a subword of \( \zeta \). In particular, \( \zeta \) contains a subword of the form \( \tau^e \omega \kappa^e \), where \( \varepsilon = \pm 1 \), \( \eta = \pm 1 \), and \( \omega \in E \). But we showed, in Step 1, that \( \zeta \) contains no such subword. This completes the proof. ■

**Lemma 12.25.**

(i) \( B_6 \) is an HNN extension with base \( B_5 \) and stable letter \( \sigma \).

(ii) \( R \) is imbedded in \( B_6 \).
Proof. (i) It suffices to show that there is an isomorphism

\[ \varphi: A = \langle \kappa, \tau, a_1, \ldots, a_m \rangle \to B = \langle \kappa, \tau d, a_1, \ldots, a_m \rangle \]

with \( \varphi(\kappa) = \kappa, \varphi(\tau) = \tau d, \) and \( \varphi(a_j) = a_j \) for all \( j. \) Since

\[ H(T) \leq H_4 \leq H_5, \]

the subgroup \( A \) is precisely the subgroup whose presentation was determined in the previous lemma:

\[ A = (\kappa, a_1, \ldots, a_m, \tau | \kappa^{-1} \omega^{-1} \tau \omega \kappa = \omega^{-1} \tau \omega, \omega \in E). \]

To see that \( \varphi \) is a well defined homomorphism, we must show that it preserves all the relations; that is, if \( \omega \in E, \) then

\[ \kappa^{-1} \omega^{-1} \tau \omega \kappa = \omega^{-1} \tau \omega \quad \text{in } B. \]

We shall show that this last equation does hold in \( H_5, \) and hence it holds in \( B \leq H_5. \)

Let us introduce notation. If \( \omega \) is a word on \( \{a_1, \ldots, a_m\}, \) write \( \omega_b \) to denote the word obtained from \( \omega \) by replacing each \( a_j \) by \( b_j, \) and let \( \omega_u \) denote the word obtained from \( \omega \) by replacing each \( a_j \) by \( u_j. \) If \( \omega \in E, \) then \( \omega_u = 1, \) for \( \omega_u \) is one of the original defining relations of \( R. \) For \( \omega \in E, \) each of the following equations holds in \( H_5: \)

\[ \kappa^{-1} \omega^{-1} \tau \omega \kappa = \kappa^{-1} \omega^{-1} \tau(d \omega d^{-1})d \kappa \]

\[ = \kappa^{-1} \omega^{-1} \tau \omega \omega_b d \kappa \]

(for \( da_i d^{-1} = a_i b_i \) in \( H_5 \) and \( a_i \) and \( b_j \) commute in \( H_4 \leq H_5). \) Since \( \kappa \) and \( d \)

commute in \( H_5, \) we have

\[ \kappa^{-1} \omega^{-1} \tau \omega \omega_b d \kappa = \kappa^{-1} \omega^{-1} \tau \omega \omega_b \kappa d \]

\[ = \kappa^{-1} \omega^{-1} \tau \omega \kappa(\kappa^{-1} \omega_b \kappa) d \]

\[ = \kappa^{-1} \omega^{-1} \tau \omega \kappa \omega_b \omega_u d \]

(because \( b_i \) and \( u_j \) commute and \( \kappa^{-1} b_i \kappa = b_i u_j \))

\[ = \kappa^{-1} \omega^{-1} \tau \omega \kappa \omega_b d \]

(because \( \omega_u = 1). \) We have shown that

\[ \kappa^{-1} \omega^{-1} \tau \omega \omega_b d \kappa = (\kappa^{-1} \omega^{-1} \tau \omega \kappa) \omega_b d \]

\[ = \omega^{-1} \tau \omega \omega_b d. \]

On the other hand,

\[ \omega^{-1} \tau \omega = \omega^{-1}(d \omega d^{-1})d \]

\[ = \omega^{-1} \tau \omega \omega_b d, \]
as we saw above. Therefore,
\[ \kappa^{-1} \omega^{-1} \tau \omega \kappa = \omega^{-1} \tau \omega \quad \text{in } \mathcal{R}_5 \]
and \( \varphi: A \to B \) is a well defined homomorphism.

To see that \( \varphi \) is an isomorphism, we construct a homomorphism \( \psi: \mathcal{R}_5 \to \mathcal{R}_5 \) whose restriction \( \psi|B \) is the inverse of \( \varphi \). Define \( \psi \) by setting \( \psi| \mathcal{B}'(T) \) to be the identity map and
\[ \psi(d) = \psi(b_i) = \psi(u_i) = 1. \]

Inspection of the various presentations shows that \( \psi \) is a well defined homomorphism. Since \( \psi(\kappa) = \kappa, \psi(a_i) = a_i, \) and \( \psi(\tau d) = \tau, \) we see that \( \psi|B \) is the inverse of \( \varphi \).

(ii) This follows from several applications of Theorem 11.78. ■

The following lemma completes the proof of the Higman imbedding theorem:

**Lemma 12.26.** \( \mathcal{R}_6 \) is finitely presented.

**Proof.** The original presentation of \( R \) is

\[ R = (u_1, \ldots, u_m| \omega = 1, \omega \in E), \]

where \( E \) is an r.e. set of positive words on \( \{u_1, \ldots, u_m\} \). Recall the notation introduced in the proof of Lemma 12.25: if \( \omega \) is a word on \( \{a_1, \ldots, a_m\} \), then \( \omega_u \) and \( \omega_b \) are obtained from \( \omega \) by replacing each \( a_i \) by \( u_i \) or \( b_i \), respectively. With this notation, the presentation of \( R \) can be rewritten:

\[ R = (u_1, \ldots, u_m| \omega_u = 1, \omega \in E). \]

Now \( \mathcal{B}'(T) \ast R \) is a finitely generated group having a finite number of relations occurring in the presentation of \( \mathcal{B}'(T) \) together with the (possibly infinitely many) relations above for \( R \). Each step of the construction of \( \mathcal{R}_6 \) from \( \mathcal{B}'(T) \ast R \) contributes only finitely many new generators and relations. Thus, \( \mathcal{R}_6 \) is finitely generated, and it is finitely presented if we can show that every relation of the form \( \omega_u = 1, \) for \( \omega \in E, \) is a consequence of the remaining relations in \( \mathcal{R}_6 \).

By Lemma 12.20, \( \kappa^{-1} \omega^{-1} \tau \omega \kappa = \omega^{-1} \tau \omega \) for all \( \omega \in E. \) Hence
\[ \sigma^{-1} \kappa^{-1} \omega^{-1} \tau \omega \kappa \sigma = \sigma^{-1} \omega^{-1} \tau \omega \sigma. \]

Since \( \sigma \) commutes with \( \kappa \) and with all \( a_i, \) this gives
\[ \kappa^{-1} \omega^{-1} \sigma^{-1} \tau \sigma \omega \kappa = \omega^{-1} \sigma^{-1} \tau \sigma \omega. \]

As \( \sigma^{-1} \tau \sigma = \tau d, \) this gives
\[ \kappa^{-1} \omega^{-1} \tau d \omega \kappa = \omega^{-1} \tau d \omega. \]
Inserting $\omega \kappa \kappa^{-1} \omega^{-1}$ and $\omega \omega^{-1}$ gives

$$(\kappa^{-1} \omega^{-1} \tau \omega \kappa) \kappa^{-1} \omega^{-1} d \omega \kappa = (\omega^{-1} \tau \omega) \omega^{-1} d \omega.$$  

The terms in parentheses are equal (Lemma 12.20 again), so that canceling gives

$$(8) \quad \kappa^{-1} \omega^{-1} d \omega \kappa = \omega^{-1} d \omega.$$  

Now the relations $da_i d^{-1} = a_i b_i$ and $a_i b_j = b_j a_i$, all $i, j$, give

$$d \omega d^{-1} = \omega \omega_b,$$

hence

$$\omega = d^{-1} \omega \omega_b d,$$

for every word $\omega$ on $\{a_1, \ldots, a_m\}$, and so

$$(9) \quad \omega^{-1} d \omega = \omega^{-1} d d^{-1} \omega \omega_b d = \omega_b d.$$  

Substituting (9) into (8) gives

$$\omega_b = \kappa^{-1} (\omega^{-1} d \omega) \kappa d^{-1} = \kappa^{-1} \omega_b d \kappa d^{-1}.$$  

Since $\kappa$ and $d$ commute,

$$(10) \quad \kappa^{-1} \omega_b \kappa = \omega_b.$$  

On the other hand, the relations $\kappa^{-1} b_i \kappa = b_i u_i$ and $b_i u_j = u_j b_i$, all $i, j$, give

$$\kappa^{-1} \omega_b \kappa = \omega_b \omega_u.$$  

This last equation coupled with (10) gives

$$\omega_b \omega_u = \omega_b,$$

and so $\omega_u = 1$, as desired. ■

Let us review the proof of Higman's theorem to try to understand Aanderaa's construction. Certainly, some of the relations of $\mathcal{B}_6$ are present to guarantee a chain of HNN extensions, for this gives an imbedding of $R$ into $\mathcal{B}_6$. The proof of the last lemma, showing that $\mathcal{B}_6$ is finitely presented, amounts to proving, for $\omega \in E$, that $\omega_u = 1$ follows from the other relations; that is, one can subdivide the labeled directed polygon with boundary word $\omega_u$ into relator polygons corresponding to the other relations in $\mathcal{B}_6$. E. Rips has drawn a diagram (Plate 4) that helps explain the construction of $\mathcal{B}_6$.

Before we examine Plate 4, let us discuss diagrams in the plane from a different viewpoint. Regard the plane as lying on the surface of a sphere, and assume that the north pole, denoted by $\infty$, lies outside a given diagram. Otherwise said, we may regard a given planar diagram $D$ having $n$ regions to actually have $n + 1$ regions, the new "unbounded" region (containing $\infty$) being the outside of $D$. We now propose redrawing a diagram so that the unbounded region is drawn as an interior region. For example, assume that
Figure 12.12 shows that $\omega \equiv aba^{-1}b^2 = 1$ in some group. Figure 12.13 is a redrawn version of Figure 12.12 with $\infty$ marking the old unbounded region.

To redraw, first number all the vertices, then connect them as they are connected in the original diagram. Note that all the (bounded) regions are relator regions corresponding to the inverses of the original relations, with the exception of that containing $\infty$. The boundary word of the region with $\infty$ is $sbt$, as in the original diagram. In general, every (not necessarily bounded) region in the redrawn diagram is a relator polygon save the new region containing $\infty$ whose boundary word is $\omega$. Such a diagram will show that $\omega = 1$ if every region (aside from that containing $\infty$) is a relator polygon and the boundary word of the diagram is 1 in the group.

Let us return to $B_6$. For a word $\omega \in E$, draw a diagram, new version, showing that $\omega_\omega = 1$ in $B_6$ (using only the other relations of $B_6$). By Lemma 12.20, $\omega \in E$ gives

$$\kappa^{-1} \omega^{-1} \tau \omega \kappa^{-1} \omega^{-1} \tau^{-1} \omega = 1.$$
We begin, therefore, with a labeled directed octagon for this word as well as with a "balloon" region (containing $\infty$) inside having boundary word $\omega_u$. To subdivide, draw a second octagon inside it, and yet a third octagon perturbed by two $d$-edges. Now complete this picture, adding $\sigma$-edges and the subdivision of the bottom, to obtain Plate 4, the diagram showing that $\omega_u = 1$ follows from the other relations.

Let us indicate, briefly, how the Novikov–Boone–Britton theorem follows from the Higman theorem. It is not difficult to construct a recursively
presented group $G$ having an unsolvable word problem. For example, let $G$ be a variant of the group in Theorem 11.85: if $F$ is a free group with basis $\{a, b\}$, let

$$G = (a, b, p|p^{-1} \omega_n p = \omega_n \text{ for all } n \in E),$$

where the commutator subgroup $F'$ is free with basis $\{\omega_0, \omega_1, \ldots, \omega_n, \ldots\}$ and $E$ is an r.e. set in $\mathbb{Z}$ that is not recursive. By Higman's theorem, there is a finitely presented group $G^*$ containing $G$. If $G^*$ had a solvable word problem, then so would all its finitely generated subgroups, by Exercise 12.4, and this contradicts the choice of $G$.

Some Applications

Higman's theorem characterizes those finitely generated groups $G$ that can be imbedded in finitely presented groups. Of course, any (perhaps nonfinitely generated) group $G$ that can be so imbedded must be countable. In Theorem 11.71, we saw that every countable group $G$ can be imbedded in a two-generator group $G'^{\infty}$.

**Lemma 12.27.** If $G$ is a countable group for which $G'^{\infty}$ is recursively presented, then $G$ can be imbedded in a finitely presented group.

**Proof.** Higman's theorem shows that $G'^{\infty}$ can be imbedded in a finitely presented group. ■

At this point, we omit some details which essentially require accurate bookkeeping in order to give an explicit presentation of $G'^{\infty}$ from a given presentation of $G$. We assert that there is a presentation of the abelian group

$$G = \sum_{i=1}^{\infty} D_i,$$

where $D_i \cong \mathbb{Q} \oplus (\mathbb{Q}/\mathbb{Z})$ for all $i$, such that $G'^{\infty}$ is recursively presented.

**Theorem 12.28.** There exists a finitely presented group containing an isomorphic copy of every countable abelian group as a subgroup.

**Proof.** By Exercise 10.29, every countable abelian group can be imbedded in $G = \sum_{i=1}^{\infty} D_i$, where $D_i \cong \mathbb{Q} \oplus (\mathbb{Q}/\mathbb{Z})$ for all $i$. Lemma 12.27, with the assertion that $G'^{\infty}$ is recursively presented, gives the result. ■

There are only countably many finitely presented groups, and their free product is a countable group $H$ having a presentation for which $H'^{\infty}$ is recursively presented.
Some Applications

Theorem 12.29. There exists a universal finitely presented group $\mathcal{U}$; that is, $\mathcal{U}$ is a finitely presented group and $\mathcal{U}$ contains an isomorphic copy of every finitely presented group as a subgroup.

Proof. The result follows from Lemma 12.27 and our assertion about the group $H^{II}$. ■

Groups with a solvable word problem admit an algebraic characterization. In the course of proving this, we shall encounter groups which are not finitely generated, yet over whose presentations we still have some control. Let $G$ be a group with presentation

$$G = (x_i, i \geq 0 | \Delta)$$

in which each $\delta \in \Delta$ is a (not necessarily positive) word on $\{x_i, i \geq 0\}$, let $\Omega$ be the set of all words on $\{x_i, i \geq 0\}$, and let $R = \{\omega \in \Omega : \omega = 1 \text{ in } G\}$. Encode $\Omega$ in $\mathbb{N}$ using Gödel numbers: associate to the word $\omega \equiv x_1^{i_1} \cdots x_n^{i_n}$ the positive integer $g(\omega) = \prod_{k=1}^{n} p_k^{i_k}$, where $p_0 < p_1 < \cdots$ is the sequence of primes (note that $1 + e_k \geq 0$). The Gödel image of this presentation is

$$g(R) = \{g(\omega) : \omega \in R\}.$$

Definition. A presentation $(x_i, i \geq 0 | \Delta)$ is r.e. if its Gödel image $g(R)$ is an r.e. subset of $\mathbb{N}$; this presentation has a solvable word problem if $g(R)$ is recursive.

Definition. A group $G$ is r.e. or has a solvable word problem if it has some presentation which is either r.e. or has a solvable word problem.

We remarked at the beginning of this chapter that a finitely generated group $G$ having a solvable word problem relative to one presentation with a finite number of generators has a solvable word problem relative to any other such presentation. The analogue of this statement is no longer true when we allow nonfinitely generated groups. For example, let $G$ be a free group of infinite rank with basis $\{x_i, i \geq 0\}$. Now $g(R)$ is recursive (this is not instantly obvious, for $R$ is an infinite set of nonreduced words; list its elements lexicographically and according to length), and so this presentation, and hence $G$, has a solvable word problem. On the other hand, if $E$ is an r.e. subset of $\mathbb{N}$ that is not recursive, then

$$(x_i, i \geq 0 | x_i = 1 \text{ if and only if } i \in E)$$

is another presentation of $G$, but $g(R)$ is not recursive; this second presentation has an unsolvable word problem.

We wish to avoid some technicalities of Mathematical Logic (this is not the appropriate book for them), and so we shall shamelessly declare that certain groups arising in the next proof are either r.e. or have a solvable word problem; of course, the serious reader cannot be so cavalier.
A.V. Kuznetsov (1958) proved that every recursively presented simple group has a solvable word problem.

**Theorem 12.30 (Boone–Higman, 1974).** A finitely generated group \( G \) has a solvable word problem if and only if \( G \) can be imbedded in a simple subgroup of some finitely presented group.

**Sketch of Proof.** Assume that

\[ G = \langle g_1, \ldots, g_n \rangle \leq S \leq H, \]

where \( S \) is a simple group and \( H \) is finitely presented; say,

\[ H = \langle h_1, \ldots, h_m | \rho_1, \ldots, \rho_q \rangle. \]

Let \( \Omega' \) denote the set of all words on \( \{ h_1, \ldots, h_m \} \), and let \( R' = \{ \omega' \in \Omega' : \omega' = 1 \} \); let \( \Omega \) denote the set of all words on \( \{ g_1, \ldots, g_n \} \), and let \( R = \{ \omega \in \Omega : \omega = 1 \} \). Theorem 12.2 shows that \( R' \) is r.e. If one writes each \( g_i \) as a word in the \( h_j \), then one sees that \( R = \Omega \cap R' \); since the intersection of r.e. sets is r.e. (Exercise 12.8), it follows that \( R \) is r.e. We must show that its complement \( \{ \omega \in \Omega : \omega \neq 1 \} \) is also r.e. Choose \( s \in S \) with \( s \neq 1 \). For each \( \omega \in \Omega \), define \( N(\omega) \) to be the normal subgroup of \( H \) generated by \( \{ \omega, \rho_1, \ldots, \rho_q \} \). Since \( S \) is a simple group, the following statements are equivalent for \( \omega \in \Omega \): \( \omega \neq 1 \) in \( G \); \( N(\omega) \cap S \neq 1 \); \( S \leq N(\omega) \); \( s = 1 \) in \( H/N(\omega) \). As \( H \) is finitely presented, Theorem 12.2 shows that the set of all words in \( \Omega \) which are equal to 1 in \( H/N(\omega) \) is an r.e. set. A decision process determining whether \( \omega = 1 \) in \( G \) thus consists in checking whether \( s = 1 \) in \( H/N(\omega) \).

To prove the converse, assume that \( G = \langle g_1, \ldots, g_m \rangle \) has a solvable word problem. By Exercise 12.10,

\[ \{ (u, v) \in \Omega \times \Omega : u \neq 1 \text{ and } v \neq 1 \} \]

is a recursive set; enumerate this set \( (u_0, v_0), (u_1, v_1), \ldots \) (each word \( u \) or \( v \) has many subscripts in this enumeration). Define \( G_0 = G \), and define

\[ G_1 = (G; x_1, t_i, i \geq 0 | t_i^{-1}u_i x_1^{-1} u_i x_1 t_i = v_i x_1^{-1} u_i x_1, i \geq 0). \]

It is plain that \( G_1 \) has base \( G \ast \langle x_1 \rangle \) and stable letters \( \{ t_i, i \geq 0 \} \); it is an HNN extension because, for each \( i \), both \( A_i = \langle u_i x_1^{-1} u_i x_1 \rangle \) and \( B_i = \langle v_i x_1^{-1} u_i x_1 \rangle \) are infinite cyclic. Thus, \( G \leq G_1 \). One can show that this presentation of \( G_1 \) has a solvable word problem (note that \( G_1 \) is no longer finitely generated).

We now iterate this construction. For each \( k \), there is an HNN extension \( G_k \) with base \( G_{k-1} \ast \langle x_k \rangle \), and we define \( S = \bigcup_{k \geq 1} G_k \); clearly \( G \leq S \). To see that \( S \) is simple, choose \( u, v \in S \) with \( u \neq 1 \) and \( v \neq 1 \). There is an integer \( k \) with \( u, v \in G_{k-1} \). By construction, there is a stable letter \( p \) in \( G_k \) with

\[ p^{-1} u x_k^{-1} u x_k p = v x_k^{-1} u x_k. \]

Therefore,

\[ v = (p^{-1} u p)(p^{-1} u x_k^{-1} u x_k p)(x_k^{-1} u^{-1} x_k) \]
lies in the normal subgroup generated by \( u \). Since \( u \) and \( v \) are arbitrary nontrivial elements of \( S \), it follows that \( S \) is simple.

It can be shown that \( S \) is recursively presented. By Theorem 11.71, there is a two-generator group \( S'' \) containing \( S \); moreover, \( S'' \) is recursively presented. The Higman imbedding theorem shows that \( S'' \), hence \( S \), and hence \( G \), can be imbedded in a finitely presented group \( H \). ■

It is an open question whether a group with a solvable word problem can be imbedded in a finitely presented simple group (the simple group \( S \) in the proof is unlikely to be finitely generated, let alone finitely presented).

Our final result explains why it is often difficult to extract information about groups from presentations of them. Before giving the next lemma, let us explain a phrase occurring in its statement. We will be dealing with a set of words \( \Omega \) on a given alphabet and, for each \( \omega \in \Omega \), we shall construct a presentation \( \mathcal{P}(\omega) \) involving the word \( \omega \). This family of presentations is uniform in \( \omega \) if, for each \( \omega' \in \Omega \), the presentation \( \mathcal{P}(\omega') \) is obtained from \( \mathcal{P}(\omega) \) by substituting \( \omega' \) for each occurrence of \( \omega \). A presentation \( (X|\Delta) \) is called finite if both \( X \) and \( \Delta \) are finite sets; of course, a group is finitely presented if and only if it has such a presentation.

**Lemma 12.31 (Rabin, 1958).** Let \( G = (\Sigma|\Delta) \) be a finite presentation of a group and let \( \Omega \) be the set of all words on \( \Sigma \). There are finite presentations \( \{\mathcal{P}(\omega)\} \), uniform in \( \omega \), such that if \( R(\omega) \) is the group presented by \( \mathcal{P}(\omega) \), then

(i) if \( \omega \neq 1 \) in \( G \), then \( G \leq R(\omega) \); and

(ii) if \( \omega = 1 \) in \( G \), then \( \mathcal{P}(\omega) \) presents the trivial group \( 1 \).

**Proof (C.F. Miller, III).** Let \( \langle x \rangle \) be an infinite cyclic group; by Corollary 11.80, \( G \ast \langle x \rangle \) can be imbedded in a two-generator group \( A = \langle a_1, a_2 \rangle \) in which both generators have infinite order. Moreover, one can argue, as in Exercise 11.82, that \( A \) can be chosen to be finitely presented: there is a finite set \( \Delta \) of words on \( \{a_1, a_2\} \) with

\[
A = (a_1, a_2|\Delta).
\]

Define

\[
B = (A; b_1, b_2|b_{1}^{-1}a_1b_1 = a_{1}^{2}, b_{2}^{-1}a_2b_2 = a_{2}^{2}).
\]

It is easy to see that \( B \) is an HNN extension with base \( A \) and stable letters \( \{b_1, b_2\} \), so that \( G \leq A \leq B \). Define

\[
C = (B; c|c^{-1}b_1c = b_{1}^{2}, c^{-1}b_2c = b_{2}^{2}).
\]

Clearly \( C \) has base \( B \) and stable letter \( c \); \( C \) is an HNN extension because \( b_1 \) and \( b_2 \), being stable letters in \( B \), have infinite order. Thus, \( G \leq A \leq B \leq C \).

If \( \omega \in \Omega \) and \( \omega \neq 1 \) in \( G \), then the commutator

\[
[\omega, x] = \omega x \omega^{-1} x^{-1}
\]

has infinite order in \( A \) (because \( G \ast \langle x \rangle \leq A \)).
We claim that $\langle c, [\omega, x] \rangle \leq C$ is a free group with basis $\{c, [\omega, x]\}$. Suppose that $V$ is a nontrivial freely reduced word on $\{c, [\omega, x]\}$ with $V = 1$ in $C$. If $V$ does not involve the stable letter $c$, then $V \equiv [\omega, x]^n$ for some $n \neq 0$, and this contradicts $[\omega, x]$ having infinite order. If $V$ does involve $c$, then Britton's lemma shows that $V$ contains a pinch $c^eWc^{-e}$ as a subword, where $e = \pm 1$ and $W \in \langle b_1, b_2 \rangle$. But $V$ involves neither $b_1$ nor $b_2$, so that $W \equiv 1$ and $c^eWc^{-e} \equiv c^e(c^{-e})$, contradicting $V$ being freely reduced. Therefore, $V$ must be trivial.

We now construct a second tower of HNN extensions. Begin with an infinite cyclic group $\langle r \rangle$, define

$$S = (r, s | s^{-1}rs = r^2),$$

and define

$$T = (S; t | t^{-1}st = s^2).$$

Since both $r$ and $s$ have infinite order, $S$ is an HNN extension with base $\langle r \rangle$ and stable letter $s$, and $T$ is an HNN extension with base $S$ and stable letter $t$. Britton's lemma can be used, as above, to show that $\langle r, t \rangle$ freely generates its subgroup in $T$.

Since both $\langle r, t \rangle \leq T$ and $\langle c, [\omega, x] \rangle \leq C$ are free groups of rank 2, there is an isomorphism $\varphi$ between them with $\varphi(r) = c$ and $\varphi(t) = [\omega, x]$. Form the amalgam $R(\omega) = T*_{\varphi} C$ with presentation

$$\mathcal{P}(\omega) = (T*_{\varphi} C | r = c, t = [\omega, x]).$$

We conclude from Theorem 11.67(i) that if $\omega \neq 1$ in $G$, then $G \leq C \leq R(\omega)$.

If $\omega = 1$ in $G$, the presentation $\mathcal{P}(\omega)$ is still defined (though it need not be an amalgam). The presentations $\mathcal{P}(\omega)$ are uniform in $\omega$:

$$\mathcal{P}(\omega) = (a_1, a_2, b_1, b_2, c, r, s, t | \Delta, b_i^{-1}a_ia_i = a_i^2, c^{-1}b_ic = b_i^2, i = 1, 2, s^{-1}rs = r^2, t^{-1}st = s^2, r = c, t = [\omega, x]).$$

We claim that $\mathcal{P}(\omega)$ is a presentation of the trivial group if $\omega = 1$ in $G$. Watch the dominoes fall: $\omega = 1 \Rightarrow [\omega, x] = 1 \Rightarrow t = 1 \Rightarrow s = 1 \Rightarrow r = 1 \Rightarrow c = 1 \Rightarrow b_1 = 1 = b_2 \Rightarrow a_1 = 1 = a_2$. ■

**Definition.** A property $\mathcal{M}$ of finitely presented groups is called a **Markov property** if:

(i) every group isomorphic to a group with property $\mathcal{M}$ also has property $\mathcal{M}$;

(ii) there exists a finitely presented group $G_1$ with property $\mathcal{M}$; and

(iii) there exists a finitely presented group $G_2$ which cannot be imbedded in a finitely presented group having property $\mathcal{M}$.

Here are some examples of Markov properties: order 1; finite; finite exponent; $p$-group; abelian; solvable; nilpotent; torsion; torsion-free; free; having a
solvable word problem. Being simple is also a Markov property, for the Boone–Higman theorem shows that finitely presented simple groups must have a solvable word problem (and hence so do all their finitely presented subgroups). Having a solvable conjugacy problem is also a Markov property: a finitely presented group $G_2$ with an unsolvable word problem cannot be imbedded in a finitely presented group $H$ having a solvable conjugacy problem, for $H$ and all its finitely presented subgroups have a solvable word problem. It is fair to say that most interesting group-theoretic properties are Markov properties.

The following result was proved for semigroups by Markov (1950).

**Theorem 12.32 (Adian–Rabin, 1958).** If $\mathcal{M}$ is a Markov property, then there does not exist a decision process which will determine, for an arbitrary finite presentation, whether the group presented has property $\mathcal{M}$.

**Proof.** Let $G_1$ and $G_2$ be finitely presented groups as in the definition of Markov property, and let $\mathcal{B}$ be a finitely presented group with an unsolvable word problem. Define $G = G_2 \ast \mathcal{B}$, construct groups $R(\omega)$ as in Rabin's lemma, and define (finitely presented) groups $\mathcal{D}(\omega) = G_1 \ast R(\omega)$.

Restrict attention to words $\omega$ on the generators of $\mathcal{B}$. If such a word $\omega \neq 1$ in $\mathcal{B}$, then $G_2 \leq G \leq R(\omega) \leq \mathcal{D}(\omega)$. But the defining property of $G_2$ implies that $\mathcal{D}(\omega)$ does not have property $\mathcal{M}$. If, on the other hand, $\omega = 1$ in $\mathcal{B}$, then $R(\omega) = 1$ and $\mathcal{D}(\omega) \cong G_1$ which does have property $\mathcal{M}$. Therefore, any decision process determining whether $\mathcal{D}(\omega)$ has property $\mathcal{M}$ can also determine whether $\omega = 1$ in $\mathcal{B}$; that is, any such decision process would solve the word problem in $\mathcal{B}$. ■

**Corollary 12.33.** There is no decision process to determine, for an arbitrary finite presentation, whether the presented group has any of the following properties: order 1; finite; finite exponent; $p$-group; abelian; solvable; nilpotent; simple; torsion; torsion-free; free; solvable word problem; solvable conjugacy problem.

**Proof.** Each of the listed properties is Markov. ■

**Corollary 12.34.** There is no decision process to determine, for an arbitrary pair of finite presentations, whether the two presented groups are isomorphic.

**Proof.** Enumerate the presentations $\mathcal{P}_1, \mathcal{P}_2, \ldots$ and the groups $G_1, G_2, \ldots$ they present. If there were a decision process to determine whether $G_i \cong G_j$ for all $i$ and $j$, then, in particular, there would be a decision process to determine whether $\mathcal{P}_n$ presents the trivial group. ■

While a property of finitely presented groups being Markov is sufficient for the nonexistence of a decision process as in the Adian–Rabin theorem, it is
not necessary. For example, the property of being infinite is not a Markov property. However, a decision process that could determine whether the group given by an arbitrary finite presentation is infinite would obviously determine whether the group is finite, contradicting Corollary 12.33. Indeed, this example generalizes to show that the Adian–Rabin theorem also holds for the "complement" of a Markov property.

Does every finitely presented group have some Markov property?

**Theorem 12.35.** A finitely presented group $H$ satisfies no Markov property if and only if it is a universal finitely presented group (i.e., $H$ contains an isomorphic copy of every finitely presented group as a subgroup).

**Proof.** Recall that the existence of universal finitely presented groups was proved in Theorem 12.29.

Let $H$ be a universal finitely presented group, and assume that $H$ has some Markov property $\mathcal{M}$. There is some finitely presented group $G_2$ that cannot be imbedded in a finitely presented group with property $\mathcal{M}$. But $G_2$ can be imbedded in $H$, and this is a contradiction. The converse follows from the observation that "not universal" is a Markov property. 