

# Presentations and various algorithmic results: Lecture 1

Gilbert Baumslag

© Draft date September 1, 2008

September 1, 2008

## 1 Cayley's description of a group

It was Cayley, who in 1865, defined a group as *a combination of its symbols*. However it was not until 1882, that Walther von Dyck explicitly defined a presentation and in particular what is meant by a finitely presented group. This opened up a new way of describing groups that had not been thought of before.

A presentation of a group  $G$  is simply a piece of notation which takes the following form:

$$G = \langle x_1, \dots, x_m; r_1 = 1, \dots, r_n = 1 \rangle. \quad (1)$$

This simply carries with it two pieces of information:

- each of the  $x_j$  represent elements of  $G$ ;
- every element of  $G$  can be expressed as the value of a *word*

$$w = a_1 \dots a_\ell,$$

where each  $a_j$  is either an  $x_j$  or the inverse of an  $x_j$ , i.e., the result of multiplying the elements listed in the group itself;

- each of the equations  $r_i = 1$  hold in  $G$ ;
- everything about  $G$  can be deduced from this information together with the group laws.

The elements  $x_j$  are termed *generators* of  $G$ , the equations  $r_k = 1$  *defining relations* and the  $r_i$  *defining relators* or simply *relators*. The right-hand-side of (1) is termed a *presentation*; if both  $m$  and  $n$  are finite, then it is termed a *finite presentation*. A group  $G$  is said to be *finitely generated* if it has a presentation with  $m$  finite and it is *finitely presented* or *finitely presentable* if it has a finite presentation. Sometimes the equations  $r_i = 1$  are re-expressed in the form  $r = s$  if  $r_i = rs^{-1}$ . Despite the suggestive notation, we allow both the number of generators and defining relations to be infinite.

Here are three examples of finitely presented groups:

### Example 1.1

$$T = \langle a, b; a^1ba = b^2, b^{-1}ab = a^2 \rangle,$$

**Example 1.2**

$$S = \langle a, b, c, d, e; a^{-1}b^{-1}abc^{-1}d^{-1}cd = 1 \rangle$$

and

**Example 1.3** *a group which we call  $L$  with generators*

$$u, s, t_0, t_1, t_2, t_3$$

and defining relations

$$s^{-1}t_i s = t_{i+1} \quad \text{for } i = 0, 1, 2$$

$$u^{-1}s^3u = s^4$$

$$u^{-1}t_i u = t_i \quad \text{for } i = 1, 2, 3$$

$$t_0^2 = 1$$

$$(t_i t_j)^3 = 1 \quad \text{for } i, j = 0, 1, 2, 3 \text{ with } i \neq j$$

$$(t_i t_j t_k)^2 = 1 \quad \text{for } i, j, k = 0, 1, 2, 3 \text{ all different.}$$

The amazing thing about  $L$  is that it is so large that contains a copy of every finite group!

**More information 1.4** *The study of finitely presented groups became particularly important with the introduction of the fundamental group by Poincaré in 1895, the discovery of knot groups by Wirtinger in 1905 and the proof by Tietze in 1908 that the fundamental group of a finite dimensional, compact, connected manifold is finitely presented.*

**1.1 The group  $T$** 

Notice that in  $T$  we have

$$a = a^{-1}a^2 = a^{-1}b^{-1}ab = b^{-2}b = b^{-1}$$

which implies that

$$a^2 = b^{-1}ab = aaa^{-1} = a$$

and so  $a = 1 = b$  and  $T = \{1\}$  is the trivial group.

**1.2 The group  $S$** 

This is the fundamental group of an orientable surface of genus 2.

**1.3 The group  $L$** 

This group contains the group of finitary permutations of a countably infinite set.

## 2 How a presentation defines a group

Let  $I$  be a non-empty set and let

$$\Sigma = \{x_i, X_i \mid i \in I\}$$

be a set indexed by the elements of  $i \in I$ , sometimes referred to as an *alphabet* and the elements in  $\Sigma$  as *letters*. We denote the free monoid on  $\Sigma$  by  $\Sigma^*$ . So  $\Sigma^*$  consists of all of the words or strings of letters

$$a_1 \dots a_n, (a_i \in \Sigma)$$

including the empty word, denoted here by 1. Two such words are equal if they are identical. The binary operation in  $\Sigma^*$  is concatenation. For each  $i \in I$ , define  $x'_i = X_i$  and  $X'_i = x_i$  and if  $w = x_1 \dots x_n$ , then we define  $w' = x'_n \dots x'_1$ . Now let  $R$  be any subset of  $\Sigma^*$  and let  $R^+$  be obtained from  $R$  by adjoining to  $R$  all of the words  $w'$  with  $w$  ranging over  $R$ , all of the words

$$\{x_i X_i, X_i x_i \mid i \in I\}$$

and the empty word. Now consider the following transformations of the words  $w \in \Sigma^*$ :

1. Expansion: insertion of any word  $r \in R^+$  into  $w$ , either at the beginning of  $w$  or at the end of  $w$  or between two consecutive letters appearing in  $w$ .
2. Contraction: deletion of any subword of  $w$  which is contained in  $R^+$ .

We define an equivalence relation  $\sim_R$  on  $\Sigma^*$ , which depends on  $R$ , by  $u \sim_R v$  if  $u$  can be transformed into  $v$  by a finite number of the expansions and contractions described above by 1 and 2. For each  $w \in \Sigma^*$ , denote the equivalence class of  $w$  by  $[w]_R$  or more simply by  $[w]$  if  $R$  is understood. Finally, let  $G$  denote the set of all such equivalence classes

$$G = \{[w] \mid w \in \Sigma^*\}$$

and define

$$[v][w] = [vw] \mid v, w \in \Sigma^*.$$

This turns  $G$  into a group with  $[x_i]^{-1} = [X_i]$ . If we now identify  $[w]$  with  $w$  and  $x_i^{-1}$  with  $X_i$  then we find that

$$G = \langle X; R \rangle.$$

In other words, we claim that every element of  $G$  can be expressed as a product of the elements  $x_i$  and their inverses, that if  $r \in R$ , then  $r = 1$  in  $G$  and everything about  $G$  can be deduced from this data.

## 3 Exercises

**Exercise 3.1** Prove that

$$G = \langle a, b; a^2 = 1, (ab)^2 = 1, b^3 = 1 \rangle$$

is finite. Can you find its order?

**Exercise 3.2** Let  $S_n$  denote the group permutations of the set  $\{1, 2, \dots, n\}$ . Recall that  $S_n$  has order  $n!$ . Find a presentation of  $S_4$ . Can you find one for  $S_n$  in general?

**Exercise 3.3** A group  $F$  is called free on  $X$  if

$$F = \langle X; \rangle,$$

i.e.,  $F$  has a presentation with an empty set of relators. Prove or find out how to prove the following

**Proposition 3.4** A group  $F$  is free on  $X$  if and only if

1.  $X$  generates  $F$ , i.e., every element of  $F$  can be expressed as a product of the elements of  $X$  and their inverses;
2. if  $x \in X$ , then  $x \neq 1$ ;
3. every reduced  $X$ -product, i.e., every product is not equal to 1 in  $F$  if it takes the form

$$x_1^{\epsilon_1} \dots x_n^{\epsilon_n},$$

where  $x_i \in X$ ,  $\epsilon_i = \pm 1$  and  $x_i \neq x_{i+1} \neq 1$  whenever  $\epsilon_i + \epsilon_{i+1} = 0$ .

**Exercise 3.5** Prove that if  $F$  is free on  $X$  and  $Y$ , then  $X$  and  $Y$  have the same cardinality. This cardinality is called the rank of the free group  $F$ .

**Exercise 3.6** A group  $F$  is free if and only if it contains a subset  $X$  such that for every group  $G$  and every mapping  $\phi : X \rightarrow G$  can be extended to a unique homomorphism of  $F$  into  $G$ .

## 4 Expacon

This procedure has been codified as a game, called Expacon. You can find it on the website [www.expacon.com](http://www.expacon.com).

## 5 Dehn's algorithmic problems

In 1912 Dehn raised three problems about finitely presented groups.

### 5.1 The word problem

Suppose that  $G$  is a group given by a finite presentation

$$G = \langle X; R \rangle.$$

The word problem for  $G$  is the problem as to whether there is an algorithm which decides whether or not any word evaluates to the identity in  $G$ .

## 5.2 The conjugacy problem

Suppose that  $G$  is a group given by a finite presentation

$$G = \langle X; R \rangle.$$

The conjugacy problem for  $G$  is the problem as to whether there is an algorithm which decides whether or not any pair of words  $v, w$  evaluate conjugate elements in  $G$  i.e. if there exists an  $X$ -word  $z$  such that

$$w = z^{-1}vz \text{ in } G$$

## 5.3 The isomorphism problem

If we recursively list all possible finite presentations in the countably infinite set  $a_1, a_2, \dots$ , is there an algorithm which determines whether or not any pair of these presentations define isomorphic groups? given by finite presentations are isomorphic?

## 5.4 The word problem is solvable for one-relator groups

In 1930 W. Magnus proved his famous Freiheitssatz:

**Theorem 5.1** *Let  $G$  be a group with a single definition relation, i.e.,*

$$G = \langle x_1, \dots, x_q; r \rangle.$$

*Suppose that  $r$  is cyclically reduced i.e., the first and last letters in  $r$  are not inverses of each other. If each of  $x_1, \dots, x_q$  actually appears in  $r$ , then any proper subset of  $\{x_1, \dots, x_q\}$  freely generates a free group.*

This made it possible for Magnus to solve the word problem for groups defined by a single relation in 1932:

**Theorem 5.2** *The word problem for groups defined by a single relation is solvable.*

# 6 Novikov, Adian, Rabin, Neumann, Boone, Baumslag

## 6.1 The word problem is undecidable

Novikov proved that there exists a group with an unsolvable word problem in 1954:

**Theorem 6.1** *There exists a finitely presented group with an insoluble word problem.*

New and simpler proofs were obtained by Boone in 1959 and Britton in 1961.

## 6.2 The conjugacy problem

**Theorem 6.2** *There exists a finitely presented group such that there is no algorithm which determines whether or not any pair of words represent conjugate elements.*

## 6.3 The isomorphism problem

Novikov also proved at the same time that

**Theorem 6.3** *The isomorphism problem is recursively undecidable.*

## 6.4 Most properties of finitely presented groups are algorithmically undecidable

The very existence of a finitely presented group with an insoluble word problem led Adyan in 1957 to prove a most striking negative theorem about finitely presented groups. In order to explain we need the notion of a Markov property.

**Definition 6.4** *An algebraic property (i.e., one preserved under isomorphism) of finitely presented groups is termed a Markov property if*

1. *there exists a finitely presented group with the property,*
2. *there exists a finitely presented group which is not isomorphic to a subgroup of a group with the property.*

Here is Rabin's formulation, in 1958, of Adyan's theorem:

**Theorem 6.5** *(Adyan 1957, Rabin 1958) Let  $\mathcal{M}$  be a Markov property. Then there is no algorithm which decides whether or not any finitely presented group has  $\mathcal{M}$ .*

It follows almost immediately from this theorem that almost all properties of finitely presented groups are algorithmically undecidable. Here is a sample list of properties of finitely presented groups that are algorithmically undecidable:

- triviality;
- finiteness;
- commutativity;
- having solvable word problem;
- simplicity;
- freeness.

It is obvious that being trivial i.e., being of order 1, is a Markov property, as are finiteness, commutativity, having solvable word problem as well as freeness. Now a finitely presented simple group has a solvable word problem. Hence a finitely presented group with an insoluble word problem cannot be embedded in a finitely presented simple group. This means that being simple is also a Markov property.

Notice that the seemingly haphazard proof that the group in Example 1 is trivial was no accident or lack of skill – the insolubility of the triviality problem makes such proofs ad hoc by necessity!

## 6.5 Other unrecognizable properties of finitely presented groups

Adyan's theorem was followed in 1959 by similar, much easier, theorems about elements and subgroups of a group in work of Baumslag, Boone, B.H. Neumann.

**Theorem 6.6** *There is a finitely presented group  $G_0$  such that no effective procedure exists to determine whether or not a word in the generators of  $G_0$  represents*

1. *an element in the center of  $G_0$ ;*
2. *an element permutable with a given element of  $G_0$ ;*
3. *an  $n$ -th power with  $n > 1$ ;*
4. *an element whose conjugacy class is finite;*
5. *an element of a given subgroup of  $G_0$ ;*
6. *a commutator i.e. of the form  $x^{-1}y^{-1}xy$ ;*
7. *an element of finite order.*

## 7 Why finitely presented groups are so complicated

In an amazing paper, Graham Higman proved the following theorem in 1961.

**Theorem 7.1** *Let  $G$  be a finitely generated group. Then  $G$  is a subgroup of a finitely presented group if and only if  $G$  can be presented in the following form*

$$G = \langle x_1, \dots, x_q ; r_1, r_2, \dots \rangle \quad (q < \infty)$$

*where  $r_1, r_2, \dots$  is a recursively enumerable set of defining relators.*

I will discuss this in more detail later. It is important to observe that Higman's theorem establishes a bond between recursive function theory and the subgroup structure of finitely presented groups.

To get a hint as to the power of this theorem, let  $f$  be a function with domain and range the positive integers and suppose that

- given any positive integer  $n$  we can effectively compute  $f(n)$ ;

- given any positive integer  $m$  there is no effective method which decides whether or not there is a positive integer  $n$  such that  $f(n) = m$ . noindent So  $f$  is a recursive (or computable) function whose range is not a recursive subset of the positive integers.

Now form

$$G = \langle a, b, c, d ; b^{-f(n)}ab^{f(n)} = c^{-f(n)}dc^{f(n)} \quad (n \geq 1) \rangle.$$

$G$  then is a finitely generated, recursively presented group. Moreover it can be shown that

$$b^{-m}ab^m = c^{-m}dc^m \text{ if and only if } m = f(n).$$

Thus

$$b^{-m}ab^m c^{-m}d^{-1}c^m = 1 \text{ if and only if } m = f(n).$$

This means that in order to solve the word problem in  $G$  we need to know the range of  $f$ . But this, by assumption, is not a recursive set. So  $G$  has an insoluble word problem. By Higman's theorem

$$G \leq H$$

with  $H$  finitely presented. So  $H$  has an insoluble word problem.

An intriguing open problem is to find a characterisation of the subgroups of finitely presented groups which are not finitely generated.

## 8 Exercises

**Exercise 8.1** Let  $S_n$  denote the group of permutations of the set  $\{1, 2, \dots, n\}$ . Find a presentation of  $S_3$  and  $S_4$ .

**Exercise 8.2** Find a presentation of  $S_n$ .

**Exercise 8.3** Prove that the group

$$G = \langle a, b ; a^{-1}b^2a = b^3, b^{-1}a^2b = a^3 \rangle$$

is trivial.

**Exercise 8.4** Prove that the group

$$G = \langle a^{-1}ba = b^2, b^{-1}cb = c^2, c^{-1}ac = a^2 \rangle$$

is trivial.

**Exercise 8.5** By way if contrast, Bernhard Neumann has proved that

$$G_{a,b,c} = \langle a^{-1}b^2a = b^3, b^{-1}c^2b = c^3, c^{-1}a^2c = a^3 \rangle$$

is infinite. Find his paper and see if you can figure out something about this group. For instance, is it torsion-free, i.e., have no elements of finite order except for the identity element?

**Exercise 8.6** *The rigid motions of a regular  $n$ -gon forms a group under composition called the dihedral group of order  $2n$ . Find presentations of the dihedral groups.*

**Exercise 8.7** *Find a presentation of the direct product of two finitely presented groups.*

**Exercise 8.8** *Given a decomposition of a finitely generated abelian group  $A$  into a direct product of cyclic groups write down a presentation for  $A$ .*

**Exercise 8.9** *Prove that a finite group is finitely presentable.*

**Exercise 8.10** *Prove that a finitely generated subgroup of a finitely presented group is recursively presentable.*

**More information 8.11** *Have a look at the book by Magnus et. al. for some additional examples and further information about the contents of this lecture.*