MASTER THESIS

Michael Skotnica

Balanced and almost balanced group presentations from algorithmic viewpoint

I declare that I carried out this master thesis independently, and only with the cited sources, literature and other professional sources.

I understand that my work relates to the rights and obligations under the Act No. 121/2000 Sb., the Copyright Act, as amended, in particular the fact that the Charles University has the right to conclude a license agreement on the use of this work as a school work pursuant to Section 60 subsection 1 of the Copyright Act.

In .... date ....   signature of the author

First, I would like to thank my supervisor Martin Tancer for his guidance, support and advice. Next, I would like to thank my friend and colleague Filip Kliber for helping me with C++. Last but not least, I am also grateful to my parents for supporting me during my studies.

Title: Balanced and almost balanced group presentations from algorithmic viewpoint

Author: Michael Skotnica

Department: Department of Applied Mathematics

Supervisor: doc. RNDr. Martin Tancer, Ph.D, Department of Applied Mathematics

Abstract: In this thesis we study algorithmic aspects of balanced group presentations which are finite presentations with the same number of generators and relations. The main motivation is that the decidability of some problems, such as the triviality problem, is open for balanced presentations.

First, we summarize known results on decision problems for general finite presentations and we show two group properties which are undecidable even for balanced presentations - the property of "being a free group"' and the property of "having a finite presentation with 12 generators".

We also show reductions of some graph problems to the triviality problem for group presentations, such as determining whether a graph is connected, k-connected or connected including an odd cycle. Then we show a reduction of the determining whether a graph with the same number of vertices and edges is a cycle to the triviality problem for balanced presentations. On the other hand, there is also a limitation of reduction to balanced presentations. We prove that there is no balanced presentation with two generators $\langle a, b | a^{p(m)} b^{q(m)}, a^{r(m)} b^{s(m)} \rangle$ for $p(m), q(m), r(m), s(m) \in \mathbb{Z}[m]$ which describes the trivial group if and only if m is odd.

In the last part of this thesis, we describe a relation between group presentations and topology. In addition, this thesis contains a program which constructs a simplicial 2-complex from a group presentation.

Keywords: Group presentation algorithm triviality problem Andrews-Curtis conjecture

Contents

Introduction

Group presentation A group presentation is a tool for describing groups. It was already known in the 19th century when it was studied by Walther von Dyck (see [Dyc82]). Every group may be described by a presentation.

We may informally define it as follows. Note that all terms are precisely defined later. At first, let us consider a set of symbols X and all finite words on the alphabet $X \cup \{x^{-1}; x \in X\}$ which are reduced. That is, they do not contain a pair xx^{-1} or $x^{-1}x$ for every x. Such set we denote W_X. Then we consider a binary operation on the set W_X defined as a concatenation. However, after this concatenation we have to make the result word reduced by deleting forbidden pairs of type xx^{-1} or $x^{-1}x$. The set W_X together with the described binary operation form a group structure. The neutral element is the empty word denoted by 1 and the inverse element for a word $\omega = x_1^{e_1} x_2^{e_2} \ldots x_s^{e_s}$ is $\omega^{-1} = x_s^{-e_s} \ldots x_2^{-e_2} x_1^{-e_1}$ where $e_i \in \{-1, 1\}$. Such group is called *free*.

Now, let us add some relations. For instance, we add $a^3 = 1$ to a free group defined on a set $X = \{a\}$ (which is in fact the group $\mathbb{Z}$). It means the word aaa is equal to the neutral element (the empty word). In this case, we get a group consisting of three elements:

$$a = a^4 = a^{-2} = a^7 = a^{-5} = \cdots,$$
$$a^2 = a^5 = a^{-1} = a^8 = a^{-4} = \cdots, \text{and}$$
$$1 = a^3 = a^6 = a^{-3} = a^9 = a^{-6} = \cdots;$$

hence $X = \{a\}$ together with the relation $a^3 = 1$ describe the group $\mathbb{Z}_3$.

Another example is to use $X = \{a, b\}$ and add a relation $aba^{-1}b^{-1} = 1$. It is equivalent to requiring $ab = ba$ which means the symbols a, b commute. In such case, we may express every element of our group as $a^u b^v$ where $u, v \in \mathbb{Z}$. Therefore we get the group $\mathbb{Z}^2$.

In the former case we described the group $\mathbb{Z}_3$ by two sets $X = \{a\}, R = \{a^3 = 1\}$, in the latter case we described the group $\mathbb{Z}^2$ by sets $X = \{a, b\}, R = \{aba^{-1}b^{-1} = 1\}$. Such a pair of sets is called a *group presentation* which is usually denoted by $\langle X | R \rangle$ where X is a set of symbols which are called generators, and R is a set of relations. Note that we usually write relations as ρ instead of $\rho = 1$. Therefore in the first example, our presentation was $\langle a | a^3 \rangle$ while in the second example, it was $\langle a, b | aba^{-1}b^{-1} \rangle$.

In other words, given a presentation $\langle X | R \rangle$ the presented group is the "most general" group on the set of words on X which fulfils the equations $\rho = 1$ for all $\rho \in R$.

Decision problems for finitely presented groups If the set of generators and the set of relations are both finite, we have a finite description of some group called *finitely presented*. It naturally leads into several decision problems. Such as:

- Determining whether two words are equal (the word problem).
  E.g.: Are the words $a^5 b^7$ and $a^3 b^{14} a^{10} b^3$ equal in $\langle a, b | a^2 b, b^3 a^4 \rangle$?

- Determining whether the presented group is trivial (the triviality problem).
  E.g.: Does $\langle a | a^8, a^{27} \rangle$ describe the trivial group?

- Determining whether two presentation describe the same group (the isomorphism problem).
  E.g.: Does $\langle a, b | a^{10}, a^{15}, b^7, b^3 \rangle$ describe the same group as $\langle a | a^5 \rangle$?

- Determining whether the presented group has a certain property.
  E.g.: Does $\langle a, b | a^{10}, a^{15}, b^4, b^{23} \rangle$ describe a cyclic group?

Unfortunately, most of these problems are algorithmically unsolvable. Novikov and Boone independently proved that the word problem is unsolvable (see [Nov55] and [Boo58]). This led into a proof of the undecidability of the triviality problem and therefore, also to a proof of the undecidability of more general isomorphism problem. Moreover, these problems are reducible to each other. For more detailed description see Section 2.1.

Markov property Adian and Rabin proved undecidability for a large class of group properties called Markov properties (see [Adi55] and [Rab58]). A property $\mathfrak{M}$ is Markov if there exists a finitely presented group H^+ which has the property $\mathfrak{M}$ and a finitely presented group H^- such that H^- being subgroup of a group K implies that K does not have the property $\mathfrak{M}$. For example, determining whether presented group is finite, abelian, free or cyclic is algorithmically unsolvable.

Although many of natural group properties are Markov, there are also interesting properties which are not Markov. They can be both decidable, such as the property of "being a perfect group", and also undecidable as we can see in Section 2.1. An example of such undecidable non-Markov property is the property of "having a finite presentation with k generators" for $k \geq 2$.

Balanced presentation The difference between the set of relation and the set of generators is called the deficiency of a presentation. If the deficiency is zero then the presentation is balanced. It follows from the known theorems that the determining whether a presentation with the deficiency greater then or equal to 12 determines the trivial group is undecidable (see Theorem 2.12). The important problem connected with topology is to determine whether a balanced presentation describes the trivial group. It is still open if there exists an algorithm for this problem.

However, in Section 2.2, we show that the problem of determining whether two presentation, where at least one of them is balanced, are isomorphic is algorithmically unsolvable and also that we cannot determine whether balanced presentation describes a free group. Therefore the property of "being a free group" is a Markov property which is not decidable even for balanced presentations. Using the fact that the triviality problem for presentations with the deficiency 12 is undecidable we also get an example of a property which is neither Markov nor decidable for balanced presentation. It is a property of "having a finite presentation with 12 generators".

In Chapter 3, we describe a method how to determine whether balanced presentation defines a perfect group (see Definition 3.1) using the determinant which is later used in the following chapter.

Reductions to the triviality problem for balanced presentation Since the triviality problem for balanced presentation is still open, it is interesting to find problems which may be reduced to it. In Section 4.1, we show some intuitive reductions of graph problems to the isomorphism problem and the triviality problem. Such as determining whether a graph is connected, connected including an odd cycle or k-connected.

It is easy to determine whether a graph with $|E| = |V| - 1$ is a tree using a balanced presentation and it has a natural topological interpretation (see pages 7-8 in [HAMSS93]). We present a balanced presentation which determines whether a given graph $G = (V, E)$ with $|E| = |V|$ is a cycle. This reduction does not has such an easy interpretation.

Theorem 4.9. *Let $G = (V, E)$ be a graph such that $|V| = |E|$ and $v \in V$. Then the presentation*

$$\langle V \times E | \{(v, e); e \in E\} \cup \bigcup_{e \in E} \{(u, e)(w, e); \{u, w\} \in E \setminus \{e\}\} \rangle$$

is balanced and it is a presentation of the trivial group if and only if G is a cycle.

Given a natural number m the presentation $\langle a | a^m, a^2 \rangle$ describes the trivial group if and only if m is odd (See Theorems 1.20 and 4.11, respectively). However, such presentation is not balanced. In Section 4.2, we conjecture that for $m \in \mathbb{N}$, there is no balanced presentation determining parity with a fixed number of generators and with relations $r_i(m)$ having only integer polynomials of m in their exponents. That is,

$$r_i(m) = a_1^{p_{1,1}^{(i)}(m)} \ldots a_s^{p_{s,1}^{(i)}(m)} a_1^{p_{1,2}^{(i)}(m)} \ldots a_s^{p_{s,j}^{(i)}(m)} a_1^{p_{1,j+1}^{(i)}(m)} \ldots a_s^{p_{1,t}^{(i)}(m)} \ldots a_s^{p_{s,t}^{(i)}(m)}$$

where $p_{j,k}^{(i)}(x) \in \mathbb{Z}[x]$. We at least prove it for a special case:

Theorem 4.14. *There is no balanced presentation*

$$\langle a, b | a^{p(m)} b^{q(m)}, a^{r(m)} b^{s(m)} \rangle$$

for $p(m), q(m), r(m), s(m) \in \mathbb{Z}[m]$ which defines the trivial group if and only if m is odd.

However, if we do not demand the fixed number of generators, we succeed.

Theorem 4.17. *Let $m \in \mathbb{N}$. Then the balanced presentation*

$$\langle a_1, \ldots, a_m | a_1 a_2, a_2 a_3, \ldots, a_{m-1} a_m, a_1 a_m^2 \rangle$$

is a presentation of the trivial group if and only if m is even.

Topology In the last chapter (Chapter 5), we show the connection between group presentations and topology. Then we describe a possible method how to reduce group presentation to a computer representation of simplicial 2-complex. This method is also implemented.

1. Preliminaries

In this chapter, we introduce basic definitions, notation and theorems which are used in the whole thesis.

A note for notation: In this thesis we use both groups and graphs. A graph is denoted by G, while for groups we use the letters H, K, F.

1.1   Group theory

This section is a brief introduction to the three related parts of group theory: free group, presentation of a group and free product.

First of all, we recall a few well-know terms. Let H be a group and $S \subseteq H$. Then $\langle S \rangle$ is the smallest subgroup of H containing S. If $\langle S \rangle = H$ we say that S *generates* H. A group H is *finitely generated* if there exists a finite S such that $\langle S \rangle = H$.

The cardinality of the smallest set which generates H is called the *rank* of H. More precisely, $\mathrm{rank}(H) = \{\min |S|; S \subseteq H, \langle H \rangle = H\}$.

If $\mathrm{rank}(H) = 1$ then H is said to be *cyclic* and such group is either isomorphic to $\mathbb{Z}_n$ for some $n \in \mathbb{N}$ or isomorphic to $\mathbb{Z}$.

Free group

Definition 1.1. A group F is said to be *free* if there exists a subset X of F such that for every group H and for every mapping $f \colon X \to H$, there exists a unique homomorphism $\varphi \colon F \to H$ extending f.

Such subset X is called a *basis* of F and it generates F.

Theorem 1.2 (see Theorem 11.4 in [Rot99]). *"Let F and G be free groups with bases X and Y, respectively. Then $F \cong G$ if and only if $|X| = |Y|$."*

Therefore we may determine free groups only by the cardinality of their bases. In this thesis we consider only free groups with finite bases and we denote them F_n where $n \in \mathbb{N}_0$ is the cardinality of the basis.

Now, we show how to elegantly describe a free group. For a finite set $X = \{x_1, \ldots, x_n\}$ let X^{-1} denote the set $\{x_1^{-1}, \ldots, x_n^{-1}\}$. We also consider that $X \cap X^{-1} = \emptyset$ and for each $x \in X$ there is a unique $x^{-1} \in X$ and vice versa. Thus we can define $(x^{-1})^{-1} = x$.

Definition 1.3. A *word* on X is a finite sequence $(a_1, \ldots, a_s)$ where $a_i \in X \cup X^{-1}$. The sequence may be empty and such empty sequence is called the *empty word* which we denote 1. As an *inverse word* of $\omega = (a_1, \ldots, a_s)$ we consider $(a_s^{-1}, \ldots, a_1^{-1})$ and we denote it ω^{-1}.

The set of words on X we denote W_X. Note that for simplification, we often write $a_1 a_2 \ldots a_s$ instead of $(a_1, a_2, \ldots, a_s)$. If there is a subsequence of the same symbol a or a^{-1} of the length i we shorten it as a^i or a^{-i}, respectively.

Definition 1.4. As a *product* of two words $\omega_1 = a_1 \ldots a_s$ and $\omega_2 = b_1 \ldots b_t$ we consider the sequence $a_1 \ldots a_s b_1 \ldots b_t$ and we denote it $\omega_1 \omega_2$.

Definition 1.5. Let $\omega = x_1^{e_1}, \ldots, x_s^{e_s}$ be a word on X where $x_i \in X$ and $e_i \in \{-1, 1\}$. Then ω is *reduced* if $x_i = x_{i+1}$ implies $e_i = e_{i+1}$ for all $i \in \{1, \ldots s - 1\}$. In other words there is no adjacent pair x, x^{-1} in ω.

We define a relation ϱ on W_X as follows. For two words $\omega_1, \omega_2 \in W_X$, $(\omega_1, \omega_2) \in \varrho$ if and only if there exists words α, β, ν such that $\omega_1 = \alpha\beta$ and $\omega_2 = \alpha\nu\nu^{-1}\beta$.

Let $\sim$ be the smallest equivalence which contains ϱ. That is, $\omega_1 \sim \omega_2$ if and only if there is a sequence $\omega_1 = \gamma_1, \gamma_2, \ldots, \gamma_m = \omega_2$ such that either $(\gamma_i, \gamma_{i+1}) \in \varrho$ or (γ_{i+1}, γ). For $\omega \in W_X$ let $[\omega]_\sim$ denote equivalence class of ω.

If $\omega_1 \sim \omega_2$ and $\nu_1 \sim \nu_2$ then $\omega_1\nu_1 \sim \omega_2\nu_2 \sim \omega_1\nu_2 \sim \omega_2\nu_1$. Thus we may define an operation $[\omega_1]_\sim \cdot [\omega_2]_\sim = [\omega_1\omega_2]_\sim$. Such operation is associative, there exists an identity element $[1]_\sim$ and for each $[\omega]_\sim$ there exists an inverse element $[\omega^{-1}]_\sim$. Therefore it defines a group structure on $W_X / {\sim}$. Moreover such group is free.

Theorem 1.6 (see e.g. Theorem 11.1 in [Rot99]). *The group $W_X / {\sim}$ is free with the basis $\{[x]_\sim; x \in X\}$.*

Moreover, it can be proved that every equivalence class contains exactly one reduced word. Consequently, every equivalence class may be represented by a reduced word and for simplification, we often write $\omega_1\omega_2$ instead of $[\omega_1]_\sim \cdot [\omega_2]_\sim$.

Presentation of a group   Let us define the key term of this thesis.

Definition 1.7. Let X be a set and $R \subseteq W_X$. Let F denote the free group $W_X / {\sim}$ with the basis X described above. Then the ordered pair $\langle X | R \rangle$ is called a *presentation* of group F / N_R where N_R is the normal subgroup of F generated by R. Elements of the set X are called *generators* and elements of the set R are called *relations*.

If X and R are both finite then $\langle X | R \rangle$ is called a *finite presentation*. In fact, every group is a quotient of a free group (see Corollary 11.2 in [Rot99]) and therefore every group has a presentation. But such presentation need not be finite. If a group has a finite presentation then we call it *finitely presented group*.

The elements of presented group are equivalence classes $[[\omega]_\sim]_{N_R}$ for $\omega \in W_R$; however, we often write only ω instead of $[[\omega]_\sim]_{N_R}$. We also write $\omega_1 = \omega_2$ and $\omega_1\omega_2$ which formally means $[[\omega_1]_\sim]_{N_R} = [[\omega_2]_\sim]_{N_R}$ and $[[\omega_1]_\sim \cdot [\omega_2]_\sim]_{N_R} = [[\omega_1\omega_2]_\sim]_{N_R}$, respectively. Note that a relation $\rho \in R$ is sometimes written as $\rho = 1$ since $[1]_\sim \in N_R$.

The group presented by $\langle X | R \rangle$ is generated by X ($\{[[x]_\sim]_{R_N}; x \in X\}$, respectively) and hence its rank is $\leq k$.

As an example, let us consider the presentation $\langle \{x\} | \{x^n\} \rangle$ which is usually written as $\langle x | x^n \rangle$. Such presentation defines the cyclic group $\mathbb{Z}_n$. Indeed, since $x^n = 1$ we get

$$x^{k+in} = x^k x^n \ldots x^n = x^k \, 1 = x^k$$

and also $x^{-k} = x^{n-k}$ since $x^k x^{n-k} = x^n = 1$. Therefore the elements of the presented groups are $\{[[x^i]_\sim]_{N_R}; i \in \{1, \ldots, n\}\}$.

Now, we show some others examples of finite group presentations.

- $\langle X | \emptyset \rangle$ defines the free group $W_X /_\sim$ with the basis $\{[x]_\sim; x \in X\}$ described above since R is the empty set. Note that $F_1 \cong \mathbb{Z}$.

- $\langle x, y | x^2, y^2, x^{-1}y^{-1}xy \rangle$ describes $\mathbb{Z}_2 \times \mathbb{Z}_2$. The relation $x^{-1}y^{-1}xy$ determines that the generators x, y (and hence all elements) commute. Indeed, the relation $x^{-1}y^{-1}xy = 1$ implies $xy = yx$.

The important attribute of a presentation is the difference between the number of generators and the number of relations. We call it the deficiency of a presentation. More precisely:

Definition 1.8. For a presentation $\langle X | R \rangle$ the *deficiency*[1] is $|X| - |R|$. A presentation is *balanced* if its deficiency is zero.

Note that for given group H a difficult part is to find a presentation with the minimum deficiency since the deficiency can be easily increased. Indeed, for instance presentations $\langle X | R \rangle$ and $\langle X \cup \{a\} | R \cup \{a, a^2, \dots, a^s\} \rangle$, where $a \notin X$, define the same group.

Free product

Definition 1.9. Let H be a group with a presentation $\langle X_H | R_H \rangle$ and K a group with a presentation $\langle X_K | R_K \rangle$ such that X_K is disjoint to X_H. Then the *free product* of H and K is the group $H * K$ defined by the presentation $\langle X_H \cup X_K | R_H \cup R_H \rangle$.

There is an alternative definition of the free product which is in fact the co-product in category theory. However, definition using presentations is more illustrative and more suitable for our purpose.

We immediately get that $F_m * F_n$ is F_{m+n} and H, K are embedded as subgroups in $H * K$. Note that if H, K are non-trivial then $H * K$ is infinite.

Lemma 1.10. *Free product of two non-trivial groups is an infinite group.*

Proof. Let H, K be non-trivial groups with presentations $\mathcal{P}_H = \langle X_H | R_H \rangle$ and $\mathcal{P}_K = \langle X_K | R_K \rangle$ such that $X_H \cap X_K = \emptyset$. Then $\mathcal{P}_{H*K} = \langle X_H \cup X_K | R_K \cup R_H \rangle$ is a presentation of $H * K$. Let ω_H be a word from $\mathcal{P}_H$ such that $\omega_H \neq 1$ and ω_K be a word from $\mathcal{P}_K$ such that $\omega_K \neq 1$. Then the word $(\omega_H \omega_K)^i \neq 1 \in \mathcal{P}_{H*K}$ for all $i \in \mathbb{N}$ and also $(\omega_H \omega_K)^i \neq (\omega_H \omega_K)^j$ for $i \neq j$. $\qquad \square$

1.2 Computability theory

In this section we, briefly introduce a theory of algorithmic solvability. At the beginning, we start with basic definitions.

Definition 1.11. As a *partial function* $f \colon X \to Y$ we consider a function $X' \to Y$ where X' is a subset of X. If $X' = X$ then the function is called *total*.

Let Σ be a finite set. Then Σ^* denote the set of all finite sequences on Σ. Such sequence is called *word*. Note that it is very similar to the previous section where the set of words W_X on X was in fact $(X \cup X^{-1})^*$.

---

[1]Some authors define the deficiency as $|R| - |X|$.

Definition 1.12. A *language* is an arbitrary subset of Σ^*. A *decision problem* is to determine whether given word w belongs to the language L. The complement $\Sigma^* \setminus L$ of the language L is denoted by $\overline{L}$.

We interpret words as inputs for a computer program and a language as inputs having certain property. For instance, the words are graphs (some representations of them) and the language is the set of connected graphs. Then the corresponding decision problem is to determine whether a given graph is connected and it is can be decided by the computer program.

Instead of computer programs we consider a different computational model called Turing machine which can simulate any computer program; however, it has a simple formal description.

Consider an infinite memory tape divided into cells. Each cell may contain a symbol from Σ or a symbol b representing a blank cell. There is a reading head operating on the tape and also an information about a current state. In each step, the reading head scans a symbol from the tape, according to the current state and the scanned symbol writes a defined symbol in the cell, moves one cell left or right or stays in the same position and finally changes the state. If there is no defined step for a scanned symbol and the current state then the computation halts.

At the beginning of the computation, given word $w \in \Sigma^*$ is written on the tape and the state is set to q_0. If the computation halts and the current state is one of accepting states then the word w is accepted.

Now we show a formal definition of the described model of computation called a Turing machine.

Definition 1.13. A *Turing machine T* is a 6-tuple

$$T = (Q, \Sigma, b, \delta, q_0, F)$$

where

- Q is a set of *states*,

- Σ is an alphabet,

- $b \notin \Sigma$ is the *blank symbol*,

- δ is a partial function $Q \times \Sigma \cup \{b\} \to Q \times \Sigma \times \{L, N, R\}$ which is called the *transition function* and where L, R represent moving left and right, respectively, and N represents no move,

- $q_0 \in Q$ is the *initial state*,

- $F \subseteq Q$ is the set of *accepting states*.

Turing machine T *recognizes* a language L if each $w \in L$ is accepted by T while each $u \in \overline{L}$ is not accepted. That is, either the computation on u never stops or stops in non-accepting state.

Definition 1.14. A language L is said to be *recursively enumerable* if there exists a Turing machine which recognizes L.

Turing machines which stop for every input word defines a smaller set of languages.

Definition 1.15. A language L is said to be *recursive* if there exists a Turing machine which stops for every $w \in \Sigma^*$ and recognizes L.

The description of each Turing machine may be encoded into a sequence of $0, 1$ (see section 9.1.1 in [HMU07]) which defines a natural number. Hence there is only countable many Turing machines while the number of languages is uncountable. We get that there exist languages which are not recursively enumerable.

Since we have a description of a Turing machine we may consider the *universal Turing machine*. Let $[[T], w]$ be a word encoding the Turing machine T together with the word w. Then the universal machine with the input $[[T], w]$ simulates T on w and accepts $[[T], w]$ if T accepts w.

Therefore the universal Turing machine defines a recursively enumerable language $L_{univ} = \{[[T], w]; T \text{ accepts } w\}$. The language L_{univ} is also an example of a language which is not recursive.

The following theorem gives us a characterization of recursive languages.

Theorem 1.16 (Post, see Theorem 9.4 in [HMU07])**.** *A language L is recursive if and only if both L and $\overline{L}$ are recursively enumerable.*

To sum up, by the Post Theorem we have following types of languages.

1. recursive,

2. recursively enumerable but not a recursive,

3. not a recursively enumerable but the complement is a recursively enumerate,

4. not a recursively enumerable and the complement is not a recursively enumerate, either.

Definition 1.17. Decision problems which are described by languages which are not recursive are called *algorithmically unsolvable* or *undecidable*.

Turing machines can be also used as translators and define partial functions where the image of an input word is a word on the tape when the Turing machine halts. Such function which can be computed by a Turing machine is called *computable*.

Definition 1.18. A language $L \subseteq \Sigma_1^*$ is *reducible* to a language $M \subseteq \Sigma_2^*$ if there exists a total computable function $f \colon \Sigma_1^* \to \Sigma_2^*$ such that $w \in L$ if and only if $f(w) \in M$.

As an example we consider the language L_{univ} and an arbitrary recursively enumerable language L. Hence there exists a Turing machine T which recognizes L. We may map a word $w \in \Sigma$ to $[[T], w]$ which implies that an arbitrary recursively enumerable language is reducible to L_{univ}. Languages which has such property (each recursively enumerable language is reducible to it) are called Turing-complete:

Definition 1.19. A language L is said to be *Turing-complete* if it is recursively enumerable and each recursively enumerable language is reducible to L.

From the definition of reducibility we get the following consequences.

- If a language L is reducible to a language M which is recursively enumerable then L is recursively enumerable as well.

- If a recursively enumerable language M is reducible to a language L then L is not recursive.

- If a Turing-complete language M is reducible to a recursively enumerable language L then L is itself Turing-complete.

In this thesis we usually consider languages which consist of words $[\mathcal{P}]$ encoding group presentations which have a certain property. For instance

$$\{[\mathcal{P}]; \mathcal{P} \text{ defines the trivial group}\}.$$

As an example we also show a simple reduction to this language.

Theorem 1.20. *Let $m, n \in \mathbb{N}$. Then the presentation $\langle a | a^m, a^n \rangle$ is a presentation of the trivial group if and only if m, n are relatively prime.*

Proof. Let $m \geq n$. We define sequences u_i, v_i, r_i. Let $u_1 := m$ and $v_1 := n$. Then

$$r_i = u_i \mod v_i$$

if $v_i \neq 0$,

$$u_{i+1} = v_i,$$
$$v_{i+1} = r_i.$$

From $a^{u_1} = a^m = 1$ and $a^{v_1} = a^n = 1$ we get $a^{u_i} = a^{v_j} = a^{r_k} = 1$ for all i, j, k such that u_i, v_i, r_i is defined. These sequences in fact describe the Euclidean algorithm. Therefore if $v_i = 0$ then $u_i = \gcd(m, n)$ and the given presentation describes $\mathbb{Z}_{\gcd(m,n)}$ where gcd denotes the greatest common divisor. $\qquad \square$

One may interpret this reduction as e.g. a reduction from the language $\{a^m b^n; \gcd(m, n) = 1\}$. Applying this theorem inductively we get the following corollary.

Corollary 1.21. *Let $m_1, \ldots, m_s \in \mathbb{N}$. Then the presentation $\langle a | a^{m_1}, \ldots a^{m_s} \rangle$ defines the trivial group if and only if $m_1, \ldots, m_s$ are relatively prime.*

Reduction of recursive languages Note that we can reduce every recursive language L to the language

$$L_{triv}^B := \{[\mathcal{P}]; \mathcal{P} \text{ is balanced and describes the trivial group}\}$$

using the following function. Let f_L be a function which maps a word w to $\langle a | a \rangle$ if $w \in L$ or to $\langle a | a^2 \rangle$ if $w \notin L$. Such function is total and computable since L is recursive. However, the whole "complexity" belongs to the function f_L.

Therefore we usually require some properties of a reduction in this thesis. Such as intuitive and reasonable description or special properties of a Turing machine which computes a reduction function:

We may consider a three tapes modification of Turing machine which is used as translator and which is equivalent to a single tape Turing machine (see page 346 in [HMU07]). It uses three tapes:

1. Input tape. Read only tape which contains an input word.

2. Output tape. Write only tape which is used for writing an output word.

3. Working tape. Read-write tape which is used for computation.

One of the special properties we often require from a reduction function is that during the computation uses only $\mathcal{O}(\log n)$ cells of the working tape, where n is a length of the input word.

2. Decision problems

In this chapter we summarize known results of decision problems on group presentations and we show some other aspects connected with the computability theory and the deficiency.

2.1   Decision problems for general group presentations

Isomorphism problem   A finitely presented group can be presented by infinitely many presentations. Therefore a natural problem is to determine whether two given presentations define the same group (isomorphic groups). Such problem is called the *Isomorphism problem*.

In 1908 Tietze introduced elementary transformations which transform a given presentation into another which defines the same group.

Definition 2.1 (*Tietze transformations*)**.** Let $\mathcal{P} = \langle X|R \rangle$ be a group presentation. Then the following transformations applied on $\mathcal{P}$ give us a presentation of the same group.

1. *Adding a relation.* If a word $\omega = 1$ in $\mathcal{P}$ then it may be added to the set of relations.

2. *Removing a relation.* If a relation can be derived from the other relations then it may be removed from the set of relations. More precisely, if a relation $\rho \in R$ belongs to the group $N_{R \setminus \{\rho\}}$ (normal group generated by $R \setminus \{\rho\}$) then ρ can be removed from R.

3. *Adding a generator.* Let ω be a word on X and $y \notin X$. Then we can transform $\langle X|R \rangle$ into $\langle X \cup \{y\}|R \cup \{y^{-1}\omega\} \rangle$.

4. *Removing a generator.* If $x = \omega$ for $x \in X$ and for a word $\omega \not\ni x$ then x may be removed from X replacing all instances of x in relations with ω.

Moreover, Tietze also proved that if two presentations define the same group it is possible to transform one into the another using a finite number of this transformations.

Theorem 2.2 (Tietze, see e.g. Proposition 2.1 in [LS01])**.** *Let $\mathcal{P}, \mathcal{T}$ be presentations of the same group. Then $\mathcal{P}$ can be obtained from $\mathcal{T}$ by a finite sequence of Tietze transformations.*

We get the following result.

Corollary 2.3. *The problem of determining whether two presentations define the same group is recursively enumerable.*

Proof. We may generate a finite sequence of Tietze transformation and apply them on the first presentation till we get the second one. If they define the same group then we succeed after a finite number of steps by Theorem 2.2.   □

Word problem Given a presentation $\mathcal{P}$ and words ω_1, ω_2, the *word problem* is to determine whether $\omega_1 = \omega_2$ in $\mathcal{P}$. This is in fact equivalent to $\omega_2^{-1}\omega_1 = 1$ in $\mathcal{P}$ therefore an equivalent definition of the word problem is to determine whether given word equals to the empty word.

Theorem 2.4. *Let $\mathcal{P} = \langle X|R \rangle$ be a presentation. The problem of determining whether a word ω equals empty word in $\mathcal{P}$ is recursively enumerate problem.*

Proof. Note that $\omega = 1$ if and only if ω belongs to the normal group N_R generated by R. We show how to enumerate N_R. We construct a sequence of sets $N_1 \subseteq N_2 \subseteq N_3 \subseteq \ldots \subseteq N_R$ such that $\bigcup_{i=1}^{\infty} = N_R$.

1. $N_1 = \{\rho, \rho^{-1}; \rho \in R\}$.

2. $N_i = \{x\alpha x^{-1}, x^{-1}\alpha x; x \in X, \alpha \in N_{i-1}\} \cup \{\alpha\beta; \alpha, \beta \in N_{i-1}\}$.

It is not difficult to check that if $\omega \in N_R$ then there exists $n \in \mathbb{N}$ such that $\omega \in N_n$. Our determining process is to construct N_i and check whether given $\omega \in N_i$. If $\omega \in N_R$ we stop after a finite number of steps. $\qquad\square$

The most important result for us is the Novikov-Boone Theorem.

Theorem 2.5 (Novikov-Boone, see e.g. [Boo58])**.** *There exists a finite presentation with an unsolvable word problem.*

This was first proved by Novikov in 1955 (see [Nov55]) and a different proof was given by Boone (see [Boo58]). In [Rot99] there is a nice proof which is based on a reduction from a Turing machine. More precisely, for the Turing machine T we can construct a presentation $\mathcal{B}(T)$ and a function f such that a word $w \in L(T)$ if and only if $f(w) = 1$ in $\mathcal{B}(T)$. Therefore the language L_{univ} can be reduced to the word problem. Indeed, the word $[[T], w]$ encoding a Turing machine T and a word w we may map to the word $[[\mathcal{B}(T)], f(w)]$ encoding the presentation $\mathcal{B}(T)$ and the word $f(w)$. This fact together with Theorem 2.4 implies the following.

Corollary 2.6. *The language $L_{word} = \{[[\mathcal{P}], \omega]; \omega = 1 \text{ in } \mathcal{P}\}$ is Turing-complete.*

On the other hand, there are also many presentations which has a solvable word problem. For instance presentations which describe cyclic groups.

Lemma 2.7. *Let $\mathcal{P}$ be a presentation of a cyclic group. Then it has a solvable word problem.*

Proof. Since we know that $\mathcal{P}$ describes a cyclic group there exists n, m and a sequence of Tietze transformations of the length at most n which transforms $\mathcal{P}$ to $\langle a|\emptyset \rangle$ or $\langle a|a^m \rangle$. Note that we also have to change given word according to this transformation. After a finite number of steps we get a presentation of one of described types for which the word problem is easily solvable. Indeed, for $\langle a|\emptyset \rangle$ there is no word equals to the empty word except the 1 itself. In $\langle a|a^m \rangle$ the word $a^s = 1$ if and only if $\gcd(s, m) = 1$. $\qquad\square$

A natural question is what is the simplest presentation with an unsolvable word problem where simplicity may be defined as the least number of generators, the least number of generators or the shortest overall length of presentation.

Note that the presentation with only one generator always defines a cyclic group and has a solvable word problem (see Lemma 2.7). Therefore the lower bound for the number of generators is 2 which is close since Boone showed there is a presentation with 2 generators and 32 relations which has an unslovable word problem (see [Boo58]).

In 1969 Borisov (see [Bor69]) constructed a presentation with an unsolvable word problem with 4 generators and 12 relations which is still the smallest known number of relations.

Theorem 2.8 (Borisov, see [Bor69]). *There exists a presentation with 4 generators and 12 relations which has an unsolvable word problem.*

Triviality problem   The Novikov-Boone Theorem was the crucial result which led to the proving of an undecidability of other group problems. The following lemma gives us a tool for reducing the word problem to some others such as the *triviality problem* which is to determine whether given presentation is a presentation of the trivial group.

Lemma 2.9 (see page 14 in [Mil92]). *Let H be a group and $\mathcal{P} = \langle X|R \rangle$ its presentation where $X = \{x_1, \ldots x_n\}$. Let ω be a fixed word in the generators of H and let S be the following set of relations:*

$$a^{-1}ba = c^{-1}b^{-1}cbc$$
$$a^{-2}b^{-1}aba^2 = c^{-2}b^{-1}cbc^2$$
$$a^{-3}\omega^{-1}b^{-1}\omega ba^3 = c^{-3}bc^3$$
$$a^{-(3+i)}x_iba^{3+i} = c^{-(3+i)}bc^{3+i}, i = 1, 2, \ldots, n.$$

Let K_ω denote the group presented by

$$\mathcal{P}_\omega = \langle \{a, b, c\} \cup X|S \cup R \rangle.$$

Then the following hold:

1. *K_ω is generated by two elements: b and ca^{-1}.*

2. *If $\omega = 1$ in H then K_ω is trivial.*

3. *If $\omega \neq 1$ in H then H is embedded in K_ω via the inclusion of generators.*

This lemma immediately implies that the triviality problem is algorithmically unsolvable. Indeed, let $\mathcal{P}$ be a presentation with an unsolvable word problem. For every word ω in the generators of $\mathcal{P}$ we can construct the presentation $\mathcal{P}_\omega$ such that $\omega = 1$ in $\mathcal{P}$ if and only if $\mathcal{P}_\omega$ describes the trivial group.

Note that given presentation $\mathcal{P}$ describes the trivial group if and only all generators are equal to the empty word in $\mathcal{P}$. Determining whether a generator is equal to the empty word is recursively enumerate problem by Theorem 2.4. Therefore the triviality problem is also recursively enumerate. This together with Corollary 2.6 implies following.

Corollary 2.10. *The language*

$$L_{trivial} = \{\mathcal{P}; \mathcal{P} \text{ defines the trivial group }\}$$

is Turing-complete.

This implies an undecidability of the isomorphism problem since the triviality problem is the special case of the isomorphism problem. Using Corollary 2.3 we also get a Turing completeness.

Theorem 2.11. *The language*

$$L_{isom} = \{[[\mathcal{P}][\mathcal{T}]]; \mathcal{P} \text{ define the same group as } \mathcal{T}\}$$

is Turing-complete.

In this thesis we are interested in the deficiency of presentation. For the presentation $\mathcal{P} = \langle X|R \rangle$ and the word ω we can construct a presentation using Lemma 2.9 adding 3 generators and $3 + |X|$ relations. The number of generators and relations which are added is independent of the choice of ω. If $\mathcal{P} = \langle X|R \rangle$ has an unsolvable word problem we can construct a system of presentations $\{\mathcal{P}_\omega; \omega \in W_X\}$ with the deficiency $(|R| + 3 + |X|) - (|X| + 3) = |R|$ such that $\omega = 1$ if and only if $\mathcal{P}_\omega$ describes the trivial group. As $\mathcal{P}$ we can use the presentation of Borisov with 12 generators (see Theorem 2.8) which gives us the following theorem.

Theorem 2.12. *The triviality problem for finite presentations with the deficiency 12 is algorithmically unsolvable.* □

Markov property

Definition 2.13. We say that $\mathfrak{M}$ is a *Markov property* of a finite presented group if:

1. There exists a finitely presented group H^+ which has the property $\mathfrak{M}$.

2. There exists a finitely presented group H^- which does not have the property $\mathfrak{M}$ and each group K such that H^- is a subgroup of K does not have this property.

Let us show a few examples of a Markov property:

1. Being an abelian group. As H^+ we can choose an arbitrary abelian group, as H^- an arbitrary non-abelian group

2. Being a cyclic group. Similarly, H^+ can be an arbitrary cyclic group and H^- an arbitrary non-cyclic group since every subgroup of a cyclic group is itself cyclic.

3. Being the group H where H is finitely presented. H^+ is H in this case and as H^- we can choose for example $H * \mathbb{Z}$.

Lemma 2.9 is also a tool for proving that the problem of determining whether given presentation defines a group with the Markov property $\mathfrak{M}$ is algorithmically unsolvable.

Theorem 2.14 (Adian-Rabin, see Theorem 12.32 in [Rot99])**.** *"If $\mathfrak{M}$ 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 $\mathfrak{M}$."*

Proof of this theorem is also based on the reduction from the word problem. For the Markov property $\mathfrak{M}$, the presentation $\mathcal{P}$ and the word ω we can construct a presentation $\mathcal{P}_\omega^{\mathfrak{M}}$ such that $\mathcal{P}_\omega^{\mathfrak{M}}$ describes the group with the Markov property $\mathfrak{M}$ if and only if $\omega = 1$ in $\mathcal{P}$ (note that for this construction, it is sufficient to know only presentation of H^+ and H^-). Since the word problem is Turing-complete by Corollary 2.10 all recursively problems can be reduced to determining whether a presentation has the Markov property $\mathfrak{M}$. Moreover, if the determining whether given presentation has the Markov property $\mathfrak{M}$ is recursively enumerable problem then it is also Turing-complete by definition.

We show that it holds for the examples of $\mathfrak{M}$ above.

Theorem 2.15. *The language*

$$L_{\mathfrak{M}} = \{\mathcal{P}; \mathcal{P} \ \text{has property} \ \mathfrak{M}\}$$

where $\mathfrak{M}$ is one of the following Markov properties

1. *Being an abelian group,*

2. *Being a cyclic group,*

3. *Being the group H where H is finite presented,*

is Turing-complete.

Proof. Let $\mathcal{P} = \langle X | R \rangle$ be the given presentation. We have to show that there is a decision process which succeed if $\mathcal{P}$ has the property $\mathfrak{M}$.

1. Being an abelian group. In this case, it is sufficient to check if $xy = yx$ for all $x, y \in X$. This is recursively enumerate problem since the word problem is recursively enumerate.

2. Being a cyclic group. We check if there exists a set $Z \subseteq X$ such that $z = 1$ for each $z \in Z$ and $y_1 = y_2 = \cdots = y_m$ for all $y_i \in X \setminus Z$. If it holds the group presented by the presentation has rank ≤ 1 and therefore it is cyclic. It can be done via the word problem and hence it is recursively enumerable problem.

   Note that in this case we can also determine whether the presented group is trivial, $\mathbb{Z}_k$ or $\mathbb{Z}$. We choose an arbitrary generator $y \in X \setminus Z$ and we substitute the rest of generators from $X \setminus Z$ with y in all relations. Then we delete all generators from X in all relations. This gives us either the presentation $\langle y | \emptyset \rangle$ or

   $$\langle y | y^{e_1}, \ldots y^{e_s} \rangle.$$

   In the former case, the presented group is $\mathbb{Z}$, in the latter case, the presented group is $\mathbb{Z}_{\gcd(e_1, \ldots, e_s)}$ (See Theorem 1.20).

3. Being the finite presented group H. Since H is finite presented this problem is a special case of the Isomorphism problem which is Turing-complete by Theorem 2.11.

$\square$

Now, given a finite presented group H let

$$L_H := \{\mathcal{P}; \mathcal{P} \text{ is a presentation of } H\}.$$

Since it is exactly $L_\mathfrak{M}$ where $\mathfrak{M}$ is being the group H, it follows from the previous theorem it is a Turing-complete language.

Reduction and deficiency Consider following situation. We have a reduction of some problem to a determining whether a presentation with the fixed deficiency d defines the group H. More precisely, for a language L describing our problem, we have a total computable function $\mathcal{P}(x)$ such that $w \in L$ if and only if the presentation $\mathcal{P}(w)$ belongs to the language L_H.

Now, we would like to reduce the language L to the triviality problem. In other words, for a word w we would like to get a presentation $\mathcal{T}(w)$ such that $\mathcal{T}(w) \in L_{trivial}$ (is trivial) if and only if $w \in L$. Since both L_H and $L_{trivial}$ are Turing-complete there exists a reduction from L_H to L_{triv}. Since we have a reduction from L to L_H there exists a reduction from L to $L_{trivial}$.

Unfortunately, we do not know the deficiency of $\mathcal{T}(w)$ in general. It may be much more greater then the deficiency of $\mathcal{P}(w)$ which is d. We show an example of such reduction for which we have tools.

1. Given $\mathcal{P}(w)$ there exists a Turing machine T_H such that $P(w)$ is trivial if and only if T_H stops on $\mathcal{P}(w)$ since L_H is recursive enumerate language.

2. We construct a presentation $\mathcal{B}(T_H)$ and a function f such that T_H stops on $\mathcal{P}(w)$ if and only if $f(\mathcal{P}(w)) = 1$ in $\mathcal{B}(T_H)$. Such construction is described in the proof of Theorem 12.8 in [Rot99].

3. By Lemma 2.9 we can construct a presentation $\mathcal{B}(T_H)_{f(\mathcal{P}(w))}$ which describes the trivial group if and only if $f(\mathcal{P}(w)) = 1$ in $\mathcal{B}(T_H)$. We define $\mathcal{T}(w) := \mathcal{B}(T_H)_{f(\mathcal{P}(w))}$.

Other problems By the Post Theorem (Theorem 1.16) the determining whether a given presentation defines a group which does not have the Markov property $\mathfrak{M}$ (has its complement $\overline{\mathfrak{M}}$) is also algorithmically unsolvable. Moreover, if the determining whether group has the Markov property $\mathfrak{M}$ is recursively enumerate, then the complement is not recursively enumerate problem again by Post Theorem. For instance, if $\mathfrak{M}$ is being an abelian group (see Theorem 2.15).

Observe that the complement $\overline{\mathfrak{M}}$ of a Markov property $\mathfrak{M}$ cannot be itself a Markov property. Indeed, suppose for contradiction that $\overline{\mathfrak{M}}$ is Markov. Then there exists a group $\overline{H^-}$ such that each K which contains $\overline{H^-}$ as a subgroup has the property $\mathfrak{M}$. There exists also a group H^- such that each K which contains H^- as a subgroup has the property $\overline{\mathfrak{M}}$. Hence $\overline{H^-} * H^-$ has both $\mathfrak{M}$ and $\overline{\mathfrak{M}}$. A contradiction.

Therefore the complements of Markov properties are examples of properties which are not Markov and cannot be determined. However, there exists also a property which is not Markov and its complement is not Markov, either and determining whether given presentation defines a group with this property is algorithmically unsolvable.

For instance the property of *having a finite presentation with k generators* for $k \geq 2$. We denote this property by $\mathfrak{P}_k$. Note that for $k = 0$ it is exactly the triviality problem and for $k = 1$ it is determining whether group is cyclic.

First, we show that if $k \geq 2$ then $\mathfrak{P}_k$ is not a Markov property.

Theorem 2.16. *The property $\mathfrak{P}_k$ is not Markov for $k \geq 2$.*

Proof. Suppose, for contradiction, that it is a Markov property. Let H^- be a finite presented group from Definition 2.13(2) which does not have the property $\mathfrak{P}_k$. That is, every finite presentation of H^- has at least $k+1$ generators. Let $\langle X|R \rangle$ be a presentation of H^- such that $|X|$ is minimal. This implies $x \neq 1$ for each $x \in X$.

Now, we use Lemma 2.9 to construct a group K_x from H^- for an arbitrary $x \in X$. The group K_x is finitely presented and generated by two elements by the part (1) of Lemma 2.9. Therefore we can transform a presentation of K_x to a presentation with two generators using Tietze transformations. By the part (2) of Lemma 2.9 the group H^- is embedded in K_x.

Consequently, for an arbitrary finite presented group H^- which does not have a presentation with k generators, for $k \geq 2$, there exists a group which has a presentation with 2 generators and has the subgroup H^-. A contradiction to the definition of Markov property (Definition 2.13(2)). $\square$

Consider a property $\mathfrak{P}$ such that there exists a finitely presented group $H_\mathfrak{P}$ having this property and such that $H_\mathfrak{P} * K$ has the property $\mathfrak{P}$ if and only if K is trivial. The problem of determining such property has to be algorithmically unsolvable since the problem of determine whether K is trivial (the triviality problem) is unsolvable. See page 193 in [LS01].

Now, we show that the property $\mathfrak{P}_k$ is an example of a property of such type $\mathfrak{P}$ described above. Which implies the determining whether a finitely presented group given by a presentation $\mathcal{P}$ has also a finite presentation with k generators is algorithmically unsolvable. For this purpose we need the theorem of Grushko.

Theorem 2.17 (Grushko, see [Gru40]). *Let H, K be finitely generated groups. Then $\mathrm{rank}(K * H) = \mathrm{rank}(H) + \mathrm{rank}(K)$.*

Theorem 2.18. *The property $\mathfrak{P}_k$ is algorithmically undecidable.*

Proof. We have to show that there exists a group $H_{\mathfrak{P}_k}$ having a finite presentation with k generators such that $H_{\mathfrak{P}_k} * K$ has the property $\mathfrak{P}_k$ if and only if K is trivial. Let $H_{\mathfrak{P}_k} := F_k$. If K is not trivial then $\mathrm{rank}(K) \geq 1$. By the Grushko theorem (Theorem 2.17) $\mathrm{rank}(F_k * K) = \mathrm{rank}(K) + \mathrm{rank}(F_k) \geq 1 + k$. Therefore $K * F_k$ cannot have a presentation with k generators. $\square$

Note that the complement of the property of "having a finite presentation with k generators" is not a Markov property, either. Indeed, every group H which has a finite presentation with k generators can be embedded into a group

which cannot be presented by a presentation with k generators. For example $H * F_{k+1}$ has rank $\geq k + 1$ by the Grushko Theorem (Theorem 2.17) and hence cannot be presented by a presentation with k generators.

In the end of this section, we show that the problem of determining whether the group presented by $\mathcal{P}$ has also a presentation with k generators is recursively enumerable and Turing-complete.

Theorem 2.19. *Let $k \geq 2$. Then the language*

$$L_{pre}^{(k)} = \{\mathcal{P}; \mathcal{P} \text{ defines a group with the property } \mathfrak{P}_k\}$$

is Turing-complete.

Proof. Given a presentation $\mathcal{P}$ we can systematically generate presentations with k generators and check whether describe the same group as $\mathcal{P}$ via Tietze transformations. Hence $L_{pre}^{(k)}$ is recursive enumerable.

In the proof of Theorem 2.18 we reduced L_{triv} to $L_{pre}^{(k)}$. Therefore since L_{triv} is Turing-complete and $L_{pre}^{(k)}$ is recursive enumerable it is also Turing-complete. $\square$

2.2 Decision problems for balanced group presentations

In this section we consider a modification of the isomorphism problem for balanced presentations.

Definition 2.20. The *isomorphism problem for balanced presentation* is to determine whether a balanced presentation $\mathcal{P}$ and a finite presentation $\mathcal{T}$ (not necessary balanced) define the same group.

We show that this problem is also unsolvable. First, we introduce the Nielsen-Schreier Theorem.

Theorem 2.21 (Nielsen-Schreier, see Theorem 11.44 in [Rot99]). *"Every subgroup H of free group F is itself free."*

This implies the following corollary.

Corollary 2.22. *Let F be free group and G be non-free group. Then $F * G$ is not free.*

Proof. The group G is subgroup of $F * G$ and it is not free. Therefore by the Nielsen-Schreier Theorem (Theorem 2.21) $F * G$ cannot be free. $\square$

Theorem 2.23. *The isomorphism problem for balanced group presentation is algorithmically unsolvable.*

Proof. By Theorem 2.11 the problem of determining whether general finite presentation describes the trivial group is unsolvable.

Let $\langle X|R \rangle$ be a finite presentation. We may assume that $|X| \leq |R|$. Otherwise, we may add a symbol a to X and relations $a, a^2, \ldots, a^{|X|-|R|+1}$ to R and we get a balanced presentation which defines the same group as $\langle X|R \rangle$.

Let us denote $d := |R| - |X|$ and $C := \{c_1, \ldots, c_d\}$. We assume that C and X are disjoint. Now we define a balanced presentation $\langle X \cup C | R \rangle$ and we claim that $\langle X | R \rangle$ is a presentation of the trivial group if and only if $\langle X \cup C | R \rangle$ is isomorphic to the free group F_d of rank d with the presentation $\langle C | \emptyset \rangle$:

"$\Rightarrow$" If $\langle X | R \rangle$ is a presentation of the trivial group we get $\langle X \cup C | R \rangle \cong \langle X \cup C | X \rangle \cong \langle C | \emptyset \rangle$.

"$\Leftarrow$" Let us assume that $\langle X | R \rangle$ is not a presentation of trivial group. We consider two cases.

   (a) $\langle X | R \rangle$ is a presentation of free group. Then such group is isomorphic to the free group F_n of rank $n \in \mathbb{N}$. Hence $\langle X \cup C | R \rangle$ is a presentation of F_{n+d} and by Theorem 1.2 $F_{n+d} \not\cong F_d$ since they have bases with different cardinality.

   (b) $\langle X | R \rangle$ is a presentation of a non-free group G. Then $\langle X \cup C | R \rangle$ is a presentation of $F_d * G$ which is not isomorphic to F_d by Corollary 2.22.

We get that if the isomorphism problem for balanced presentation were solvable then the triviality problem for general presentation would be also solvable. A contradiction. $\qquad\square$

Note that if we use the balanced presentation $\langle C \cup \{a\} | a, a^2, \ldots, a^{d+1} \rangle$ of F_d in the proof then we get the following theorem.

Theorem 2.24. *The determining whether two balanced groups define the same group is algorithmically unsolvable.* $\qquad\square$

Using the same proof as in Theorem 2.23 we also get following result.

Theorem 2.25. *The problem of determining whether a balanced presentation describes a free group is algorithmically unsolvable.* $\qquad\square$

Therefore being a free group is an example of a Markov property which is undecidable even for balanced presentation.

In the end of this section, we show there exists also a property which is not Markov and which is not decidable for balanced presentation. It is a property of "having a finite presentation with 12 generators" which we denote $\mathfrak{P}_{12}$. Such property is not Markov by Theorem 2.16.

Theorem 2.26. *The property $\mathfrak{P}_{12}$ for balanced presentations is algorithmically undecidable.*

Proof. By Theorem 2.12 the triviality problem is undecidable for presentation with the deficiency 12. Let $\mathcal{P} = \langle X | R \rangle$ be a presentation with the deficiency 12 and let H be a group described by $\mathcal{P}$. We add 12 new generators to it and get $\mathcal{P}' = \langle X \cup \{c_1, \ldots, c_{12}\} | R \rangle$ which is a balanced presentation of $F_{12} * H$. By the Grushko Theorem (Theorem 2.17) $F_{12} * H$ has a presentation with 12 generators if and only if H is trivial. Therefore if we could decide the property $\mathfrak{P}_{12}$ for balanced presentation then the triviality problem for presentations with deficiency 12 would be also decidable. A contradiction with Theorem 2.12. $\qquad\square$

3. Perfect groups

In this chapter we show an easy method to determine whether a balanced presentation is a presentation of a perfect group. We start with basic definitions.

Let H be a group. For $g, h \in H$ we define the *commutator* as the element $[g, h] = g^{-1}h^{-1}gh$. For subgroups A, B of H let $[A, B]$ denote the subgroup $\langle\{[a, b]; a \in A, b \in B\}\rangle$. The group $[H, H]$ is then called the *commutator subgroup*. Note that such group is normal.

Definition 3.1. A group H is said to be *perfect* if the quotient group $H \big/ [H, H]$ is trivial.

Note that the quotient group $H \big/ [H, H]$ is abelian. Indeed, for $abg^{-1}h^{-1} \in ab[H, H]$ we get

$$abg^{-1}h^{-1}gh = baa^{-1}b^{-1}abg^{-1}h^{-1}gh \in ba[H, H].$$

Now we show how we can get the presentation of $R \big/ [R, R]$ from the presentation of R. For this purpose we use the First isomorphism theorem for groups.

Theorem 3.2 (First isomorphism theorem)**.** *Let H, K be groups and $f\colon H \to K$ be a group homomorphism. Then the image of f denoted by $\mathrm{Im}\, f$ is a subgroup of K, $\ker f$ is a normal subgroup of H and $H \big/ \ker f$ is isomorphic to $\mathrm{Im}\, f$.*

Moreover if f is a surjection then we have $H \big/ \ker f \cong K$.

Lemma 3.3. *Let H be a group with presentation $\langle X|R\rangle$. Then the presentation $\langle X|R \cup \{aba^{-1}b^{-1}; a, b \in X\}\rangle$ is a presentation of $H \big/ [H, H]$.*

Proof. Let K denote the group defined by $\langle X|R \cup \{aba^{-1}b^{-1}; a, b \in X\}\rangle$. We show $K \cong H \big/ [H, H]$. Let $f\colon H \to K$ be a mapping defined by

$$f(a_1^{c_{1,1}} \ldots a_m^{c_{1,m}} a_1^{c_{2,1}} \ldots a_m^{c_{i-1,m}} a_1^{c_{i,1}} \ldots a_m^{c_{n,1}} \ldots a_m^{c_{n,m}}) = a_1^{c_{1,1}+\cdots+c_{n,1}} \ldots a_m^{c_{1,m}+\cdots+c_{n,m}}.$$

Such mapping is a group homomorphism which is a surjection. We show that $\ker f = [H, H]$.

1. $[H, H] \subseteq \ker f$
   Let $\omega \in [H, H]$. Then $\omega = [\alpha_1, \beta_2] \ldots [\alpha_p, \beta_p]$ for some words $\alpha_i, \beta_i \in H$. The sum of exponents of each generator from $[\alpha_i, \beta_i]$ is zero by definition of a commutator. Therefore $f([\alpha_i, \beta_i]) = 1$ for all $i \in \{1, \ldots, p\}$ and $f(\omega) = 1$.

2. $\ker f \subseteq [H, H]$
   Let $\chi \in ker f$. Then the sum of exponents of each generator from χ is zero. We show by induction on the length l of χ that $\chi = \gamma_1 \ldots \gamma_p$ where γ_i are the commutators.

   (a) $l = 4$.
       In this case the only possibility is $\chi = a^{-j}b^{-k}a^jb^k$ for $a, b \in X$ and $j, k \in \{-1, 1\}$. Therefore $\chi = [a^j, b^k] \in [H, H]$.

(b) $l > 4$

Since the sum of exponents of each generator in χ is zero each generator must be obtained in χ at least once with positive and at least once with negative exponent. We can express χ as $\chi = \alpha a^j \beta a^k$ for some words α, β, for non-zero k, l with different sign and the last generator a. Consequently, $\chi = \alpha a^{j+k} \beta \beta^{-1} a^{-k} \beta a^k = \alpha a^{j+k} \beta [\beta, a^k]$. Since k has different sign the length of $\alpha a^{j+k} \beta$ is smaller then l. Therefore by induction hypothesis $\alpha a^{j+k} \beta \in [H, H]$ which implies $\alpha a^{j+k} \beta [\beta, a^k] = \chi \in [H, H]$.

Moreover, for every word $\kappa \in K$ we have $f^{-1}(\kappa) = \kappa$ and therefore f is a surjection. Since $\ker f = [H, H]$ and f is a surjection, the First isomorphism theorem (Theorem 3.2) implies $K \cong H \big/ [H, H]$. $\qquad \square$

Definition 3.4. Let H be a group, $\langle X | R \rangle$ its presentation and

$$\langle X | R \cup \{aba^{-1}b^{-1}; a, b \in X\} \rangle$$

be a presentation of $H \big/ [H, H]$. For a word

$$\omega = a_1^{c_{1,1}} \ldots a_m^{c_{1,m}} a_1^{c_{2,1}} \ldots a_m^{c_{i-1,m}} a_1^{c_{i,1}} \ldots a_m^{c_{n,1}} \ldots a_m^{c_{n,m}} \in R$$

we define a vector $v_\omega = (c_{1,1} + \cdots + c_{n,1}, \ldots, c_{1,m} + \cdots + c_{n,m})^T \in \mathbb{Z}^m$.

Since $\langle X | R \cup \{aba^{-1}b^{-1}; a, b \in X\} \rangle$ is a presentation of $H \big/ [H, H]$, all generators from X commute. Therefore for words $\omega, \delta \in H \big/ [H, H]$ we get

$$v_{\omega\delta} = v_\omega + v_\delta,$$
$$v_{\omega^{-1}} = -v_\omega.$$

Let us recall that for a group K with the presentation $\langle a_1, \ldots, a_n | R \rangle$ the generator $a_i = 1$ if and only if $a_i \in N_R$ (normal subgroup generated by R).

Consequently, in the presentation

$$\langle a_1, \ldots, a_m | \{\rho_1, \ldots, \rho_n\} \cup \{a_i^{-1} a_j^{-1} a_i a_j; \forall i, j\} \rangle$$

of $H \big/ [H, H]$, the generator $a_i = 1$ if and only if $a_i \in N_{R \cup \{a_i^{-1} a_j^{-1} a_i a_j; \forall i, j\}}$. Since $H \big/ [H, H]$ is abelian all its subgroups are normal and thus

$$N_{R \cup \{a_i^{-1} a_j^{-1} a_i a_j; \forall i, j\}} = \langle R \cup \{a_i^{-1} a_j^{-1} a_i a_j; \forall i, j\} \rangle.$$

Therefore $a_i \in N_{R \cup \{a_i^{-1} a_j^{-1} a_i a_j; \forall i, j\}}$ if and only if there exist $d_1, \ldots d_n \in \mathbb{Z}$ such that

$$a_i = \rho_1^{d_1} \ldots \rho_n^{d_n}$$

which may be expressed using the vectors $v_{a_i}, v_{\rho_1}, \ldots, v_{\rho_n}$ as

$$\epsilon_i = v_{a_i} = d_1 v_{\rho_1} + \cdots + d_n v_{\rho_n} = \sum_{i=j}^n d_i v_{\rho_i}$$

22

$$\begin{pmatrix} 2 & 2 & 1 \\ 1 & 1 & 9 \\ 0 & 9 & 0 \end{pmatrix}$$

Figure 3.1: An example of matrix $M_{\mathcal{P}_H}$ for the presentation $\mathcal{P}_H = \langle a, b, c | aba, c^2 a^2 bc^7, b^4 ab^5 \rangle$

where ϵ_i denotes a unit vector. In other words, $a_i = 1$ if and only if there exists a vector $d \in \mathbb{Z}^n$ such that

$$\begin{pmatrix} \vdots & & \vdots \\ v_{\rho_1} & \cdots & v_{\rho_n} \\ \vdots & & \vdots \end{pmatrix} d = \epsilon_i\,. \tag{3.1}$$

Definition 3.5. The matrix of the vectors $v_{\rho_1}, \ldots, v_{\rho_n}$ from (3.1) is defined by a presentation $\mathcal{P}_H$ of group H and we denote it by $M_{\mathcal{P}_H}$. See Figure 3.1.

If the presentation $\mathcal{P}_H$ of H is balanced then the matrix M_{P_H} is square and therefore $H \big/ [H, H]$ is trivial if and only if there exists an integer matrix $M_{P_H}^{-1}$ such that $M_{P_H} M_{P_H}^{-1} = I_m$. The following lemma from linear algebra gives us a characterization of integer matrices which have integer inverses.

Lemma 3.6 (See Lemma 2.11 in [Bap10])**.** *Let $M \in \mathbb{Z}^{n \times n}$ be a matrix. Then M has integer inverse if and only if $\det(M) = \pm 1$.*

As a corollary we get following.

Theorem 3.7. *A balanced presentation $\mathcal{P}_H$ defines a perfect group if and only if $\det(M_{P_H}) = \pm 1$.* □

This gives us an easy algorithm which determines whether given presentation defines perfect group which is very simple for presentations with 2 or 3 generators. Note that it is important to determine whether a presentation defines a perfect group. Indeed, if does not then does not define the trivial group, either.

4. Reductions

In this chapter we show some reductions to the triviality and the isomorphism problems.

4.1   Graph problems

Definition 4.1. Let $G = \{V, E\}$ be a graph. We define a set of words $R_G :=$ $\{uv; \{u, v\} \in E\} \subseteq W_V$.

Let us have a look at the presentation $\langle V | R_G \rangle$. First, we assume that the graph G is connected.

Lemma 4.2. *Let $G = (V, E)$ be a connected graph. The presentation $\langle V | R_G \rangle$ for G defines*

1. *$\mathbb{Z}$ if G has no odd cycle (it is bipartite).*

2. *$\mathbb{Z}_2$ if G has an odd cycle (it is not bipartite).*

Proof. We choose an arbitrary vertex $v \in V$. If there is a path v, w, x we have

$$vw = 1,$$
$$wx = xw = 1.$$

Therefore we get

$$vw = xw,$$
$$v = x.$$

Then by induction we get the following.

If there is a path of even length from v to w for $v, w \in V$ then $v = w$.   (4.1)

Now we consider two cases.

1. G has an odd cycle C. We choose an arbitrary vertex v from C and let w be its neighbour in C. Since C is odd there exists an even path from v to w. Thus $v = w$ by (4.1). Since G is connected, for all $x \in V$ there exists an even path from x either to v or w which are equal and thus all generators are equal. See Figure 4.1. Therefore in this case we get $\langle V | R_G \rangle \cong \langle v | v^2 \rangle \cong \mathbb{Z}_2$.

2. G has no odd cycle and therefore it is bipartite. Let X, Y denote its parts. We choose an arbitrary vertex v from the first part X. Since G is connected there is an even path from v to an arbitrary vertex of X. By (4.1), we get that all generators of X are equal. Analogically all generators of the second part Y are equal as well. See Figure 4.2. Therefore $\langle V | R_G \rangle \cong \langle v, w | vw \rangle \cong \mathbb{Z}$.
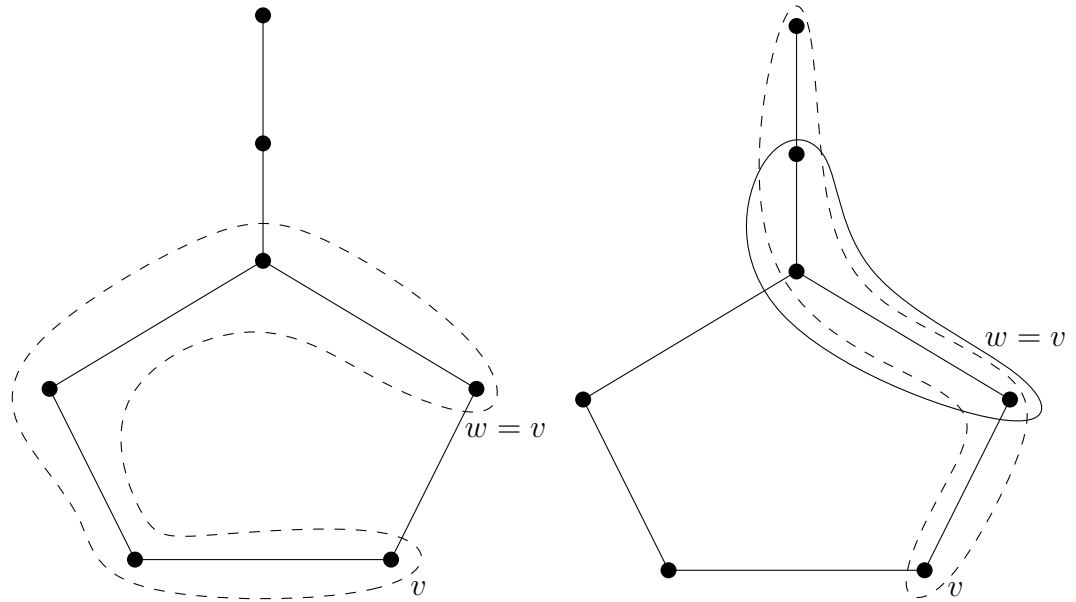
$\square$

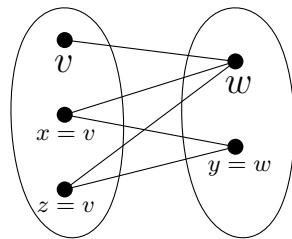Figure 4.1: Path of even length in odd cycle (left) and from the rest of the graph (right).

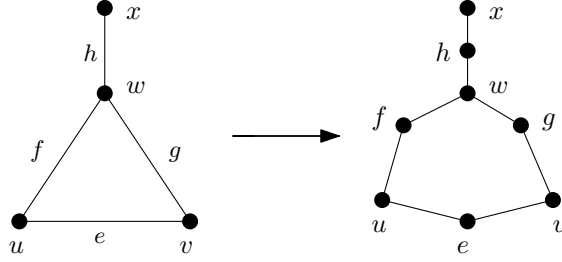Figure 4.2: An example of the bipartite case.

Figure 4.3: Subdivision of each edge of graph.

If the graph G is not connected then $\langle V|R_G \rangle \cong H^{(1)} * \cdots * H^{(k)}$ where $H^{(i)}$ represents i-th component and it is either $\mathbb{Z}$ if i-th component is bipartite or $\mathbb{Z}_2$ if it is not (has an odd cycle).

Now let us have a look at the presentation $\langle V|R_G \cup \{v\} \rangle$ for an arbitrary $v \in V$. Let $H^{(i)}$ be the subgroup of $\langle V|R_G \rangle$ corresponding to the component which contains v. Then the presentation of $H^{(i)}$ with the relation v is either $\langle v|v^2, v \rangle \cong 1$ or $\langle v, w|vw, v \rangle \cong 1$. Consequently, $\langle V|R_G \cup \{v\} \rangle \cong H^{(1)} * \cdots H^{(i-1)} * H^{(i+1)} * \cdots * H^{(k)}$ and we get the following.

Theorem 4.3. *Let $G = (V, E)$ be a graph and $v \in V$. Then $\langle V|R_G \cup \{v\} \rangle$ is a presentation of the trivial group if and only if G is connected.* $\square$

Note that if $|V| - 1 = |E|$ then the corresponding presentation $\langle V|R_G \cup \{v\} \rangle$ is balanced and such graph is connected if and only if it is a tree.

Corollary 4.4. *Let $G = (V, E)$ be a graph such that $|V| - 1 = |E|$ and $v \in V$. Then the balanced presentation $\langle V|R_G \cup \{v\} \rangle$ is a presentation of trivial group if and only if G is a tree.* $\square$

The other relation we can add to the presentation $\langle V|R_G \rangle$ is v^3 for an arbitrary $v \in V$. Again, let $R^{(i)}$ be the subgroup of $\langle V|R_G \rangle$ corresponding to the component which contains v. Then the presentation of $R^{(i)}$ with the relation v^3 is either $\langle v|v^2, v^3 \rangle \cong \langle e \rangle$, if the component of v contains odd cycle, or $\langle v, w|vw, v^3 \rangle$, if the component of v is bipartite. In the latter case we get $w = v^2$ and therefore such group is isomorphic to $\mathbb{Z}_3$ and the following holds.

Theorem 4.5. *Let $G = (V, E)$ be the graph and $v \in V$. Then $\langle V|R_G \cup \{v^3\} \rangle$ is a presentation of trivial group if and only if G is connected and contains an odd cycle.* $\square$

Consequently, G is connected and contains an odd cycle if and only if the presentation $\langle V|R_G \rangle$ defines $\mathbb{Z}_2$ if and only if $\langle V|R_G \cup \{v^3\} \rangle$ defines the trivial group. In this case, we reduced the determining whether a presentation defines $\mathbb{Z}_2$ to the triviality problem by adding one relation v^3 and hence we increased the deficiency by 1. Compare with the paragraph "Reduction and deficiency" on page 17.

Now, we use the fact that $\langle V|R_G \rangle \cong \mathbb{Z} * \cdots * \mathbb{Z} \cong F_k$ for bipartite G where k is a number of its connected components to get the following result.

Corollary 4.6. *Let $G = (V, E)$ be a graph and let k be a number of its connected components. Then the presentation $\langle V \cup E|\{ue, ve; e = \{u, v\} \in E\} \rangle$ defines the free group F_k.*
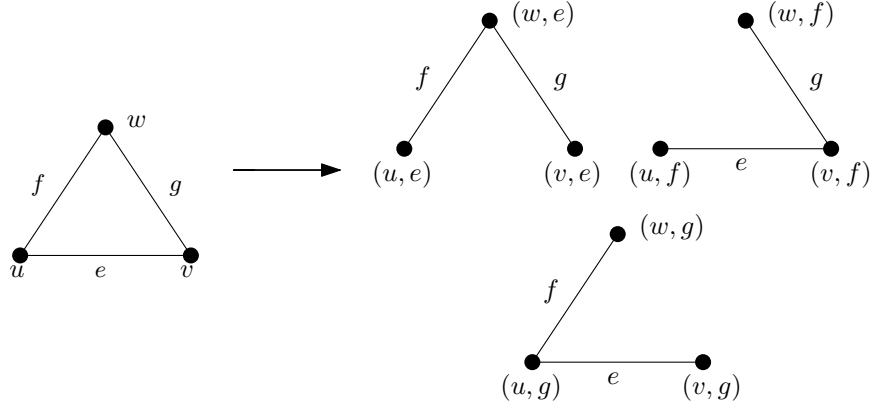
Figure 4.4: An example of graphs G_{e_i} for presentations P_{e_i}.

Proof. Given presentation is in fact the presentation $\langle V'|R_{G'}\rangle$ for the graph G' which is obtained from G by subdivision of each edge when the name of edge is used as the name of new vertex. See Figure 4.3. Consequently, such graph has no odd cycle. $\square$

We already know how to determine by a balanced presentation if the graph $G = (V, E)$, where $|V| - 1 = |E|$, is a tree (see Corollary 4.4). Now we show how to determine by balanced presentation if $G = (V, E)$, where $|V| = |E|$, is a cycle. First we show more general result.

Definition 4.7. Let k be a positive integer. A graph is said to be *k-edge-connected* if it remains connected after removing $k - 1$ arbitrary edges.

Theorem 4.8. *Let $G = (V, E)$ be a graph and $v \in V$. Then the presentation*

$$\langle V \times E | \{(v, e); e \in E\} \cup \bigcup_{e \in E} \{(u, e)(w, e); \{u, w\} \in E \setminus \{e\}\}\rangle$$

is a presentation of the trivial group if and only if G is 2-edge-connected.

Proof. Let $\mathcal{P}$ denote the given presentation and $m := |E|$. We can split P into m parts $P_{e_1}, \ldots, P_{e_m}$ for $e_i \in E$:

$$\mathcal{P}_{e_1} = \langle V \times \{e_1\} | \{(u, e_1)(w, e_1); \{u, w\} \in E \setminus \{e_1\}\} \cup \{(v, e_1)\}\rangle,$$

$$\vdots$$

$$\mathcal{P}_{e_m} = \langle V \times \{e_n\} | \{(u, e_n)(w, e_n); \{u, w\} \in E \setminus \{e_n\}\} \cup \{(v, e_n)\}\rangle.$$

Let H_{e_i} denote the group presented by $\mathcal{P}_{e_i}$. Each $\mathcal{P}_{e_i}$ is in fact the presentation $\langle V \times \{e_i\} | R_{G_{e_i}} \cup \{(v, e_i)\}\rangle$ for graph G_{e_i} with $m-1$ edges which is obtained from G by deleting the edge e_i. See Figure 4.4. Corollary 4.4 implies that H_{e_i} is trivial if and only if G_{e_i} is connected. Therefore $\mathcal{P}$ is a presentation of the trivial group if and only if G is 2-connected since the group presented by $\mathcal{P}$ is $H_{e_1} * \cdots * H_{e_n}$. $\square$

Now we consider $G = (V, E)$ with $|V| = |E|$. Such graph is 2-edge-connected if and only if it is a cycle. Furthermore each presentation $\mathcal{P}_{e_i}$ is balanced and thus the presentation P is balanced as well. We get following corollary.

Corollary 4.9. *Let $G = (V, E)$ be a graph such that $|V| = |E|$ and $v \in V$. Then the presentation*

$$\langle V \times E | \{(v, e); e \in E\} \cup \bigcup_{e \in E} \{(u, e)(w, e); \{u, w\} \in E \setminus \{e\}\}\rangle$$

is balanced and it is a presentation of the trivial group if and only if G is a cycle. $\qquad\square$

Note that the determining whether a graph is a tree using a balanced presentation has a direct topological interpretation. On the other hand, the determining whether a graph is cycle does not have such interpretation. See pages 7–8 in [HAMSS93].

We can also analogically construct a presentation for a graph which determines k-edge-connectivity for $k \geq 3$: Let $\binom{E}{l}$ denote set of all l-element subsets of E. That is, $\binom{E}{l} := \{A \subseteq E; |A| = l\}$.

Theorem 4.10. *Let $G = (V, E)$ and $v \in V$. Then the presentation*

$$\langle V \times \binom{E}{k-1} | \{(v, S); S \in \binom{E}{k-1}\} \cup \bigcup_{S \in \binom{E}{k-1}} \{(u, S)(w, S); \{u, w\} \in E \setminus S\}\rangle$$

is a presentation of the trivial group if and only if G is k-edge-connected.

The deficiency of such presentation is $\binom{|E|}{k-1}((|E| - k + 2) - |V|)$. Therefore it is balanced for graphs with $|V| = n$ vertices and $n + k - 2$ edges. However, such graphs are never k-connected for $k \geq 3$ and thus, despite the previous situation when $k = 2$, corresponding balanced presentation always defines a non-trivial group. Indeed, for a graph with $n+k-2$ we get $\sum_{v \in V} \deg(v) = 2|E| = 2n+2k-4$. Hence there is a vertex which has the degree at most $2 + \lfloor \frac{2k-4}{n} \rfloor < 4$ for all k. Moreover, for $k = 3$ and $n > 2$ it is less then 3. In other words, there is always a vertex with the degree less then k and the graph cannot be k-edge-connected.

Space complexity of reductions Note that all reductions described in this section may be realized using a translator Turing machine whose working tape uses only $\mathcal{O}(\log n)$ cells. The working tape has to load either just one edge of graph or in the case of k-edge-connectivity one edge and a counter of edges. See the paragraph Reduction of recursive languages on page 10.

4.2 Parity

In this chapter we demonstrate that a very simple problem of determining a parity of $m \in \mathbb{N}$ can be easily reduced to the triviality problem for presentations with deficiency 1. However, if we require a balanced presentation we show it is more complicated. Even, if we require some additional properties of a balanced presentation it is impossible.

First, let us recall Theorem 1.20 for a case when $n = 2$.

Theorem 4.11 (See Theorem 1.20)**.** *Let $m \in \mathbb{N}$. Then the presentation $\langle a | a^m, a^2 \rangle$ is a presentation of the trivial group if and only if m is odd.*

This gives us the presentation determining the parity of m. However, such presentation has deficiency 1. Let us try to construct a balanced presentation which determines parity.

First of all, we need to clarify which function can be used in exponents of generators in relations, since one may suggest following presentation

$$\langle a | a^{\lfloor \frac{m+1}{2} \rfloor - \lfloor \frac{m}{2} \rfloor} \rangle.$$

However, the whole "complexity" belongs to the *floor function*. See the paragraph Reduction of recursive languages on page 10. Therefore we consider following problem.

Problem 4.12. Find a balanced presentation $\langle a_1, \ldots a_s | r_1(m), \ldots r_s(m) \rangle$ which determines the parity of m such that

$$r_i(m) = a_1^{p_{1,1}^{(i)}(m)} \ldots a_s^{p_{s,1}^{(i)}(m)} a_1^{p_{1,2}^{(i)}(m)} \ldots a_s^{p_{s,j}^{(i)}(m)} a_1^{p_{1,j+1}^{(i)}(m)} \ldots a_1^{p_{1,t}^{(i)}(m)} \ldots a_s^{p_{s,t}^{(i)}(m)} \quad (4.2)$$

where $p_{j,k}^{(i)} \in \mathbb{Z}[m]$

In other words, we allow only polynomials with integer coefficients in exponents. Note that the presentation $\langle a | a^m, a^2 \rangle$ from Theorem 4.11 fulfils this condition.

Now, assume that such presentation

$$\mathcal{P}(m) := \langle a_1, \ldots a_s | r_1(m), \ldots r_s(m) \rangle,$$

which has the properties described in Problem 4.12, exists and without loss of generality defines the trivial group if and only if m is odd (otherwise we substitute m with $m+1$ in polynomials). Then the presentation $\langle a_1, \ldots a_s | r_1(m), \ldots r_s(m) \cup \{a_i^{-1} a_j^{-1} a_i a_j; \forall i, j\} \rangle$ also describes the trivial group for m odd (since the trivial group is perfect) and therefore the matrix $M_{\mathcal{P}(m)}$ (see Definition 3.5) has determinant either 1 or -1 by Theorem 3.7.

Since we allow only integral polynomials in exponents of generators in relations we may express the matrix $M_{\mathcal{P}(m)}$ as

$$M_{\mathcal{P}(m)} = \begin{pmatrix} p_1^{(1)}(m) & \ldots & p_s^{(1)}(m) \\ \vdots & \ddots & \vdots \\ p_1^{(s)}(m) & \ldots & p_s^{(s)}(m) \end{pmatrix}$$

where $\mathbb{Z}[m] \ni p_j^{(i)}(m) = \sum_{k=1}^t p_{j,k}^{(i)}$. Consequently, the determinant of $M_{\mathcal{P}(m)}$ is also some integral polynomial $p_{det}(m) := \det(M_{\mathcal{P}(m)}) \in \mathbb{Z}[m]$ which is equal to 1 or -1 for all odd m. Therefore $p_{det}(m) = u$ where $u \in \{-1, 1\}$ for infinitely many m and thus the Fundamental theorem of algebra (reference?) implies $p_{det}(m)$ is a constant polynomial equal to u.

Therefore it follows from Theorem 3.7 that $\mathcal{P}(m)$ describes the trivial group if m is odd or a perfect group which is not trivial if m is even.

This property of $\mathcal{P}(m)$ is quite suspicious and therefore I conjecture that such $\mathcal{P}(m)$ cannot exist, but I have not managed to prove this.

Conjecture 4.13. *There is no balanced presentation*

$$\langle a_1, \ldots a_s | r_1(m), \ldots r_s(m) \rangle$$

such that

$$r_i(m) = a_1^{p_{1,1}^{(i)}(m)} \ldots a_s^{p_{s,1}^{(i)}(m)} a_1^{p_{1,2}^{(i)}(m)} \ldots a_s^{p_{s,j}^{(i)}(m)} a_1^{p_{1,j+1}^{(i)}(m)} \ldots a_s^{p_{1,t}^{(i)}(m)} \ldots a_s^{p_{s,t}^{(i)}(m)}$$

where $p_{j,k}^{(i)} \in \mathbb{Z}[m]$, which defines the trivial group if and only if m is odd.

Now, we at least show that if we require $\mathcal{P}(m)$ just with two generators a, b and with relations $a^{p_a^{(1)}(m)} b^{p_b^{(1)}(m)}$, $a^{p_a^{(2)}(m)} b^{p_b^{(2)}(m)}$ with polynomial exponents we get a contradiction.

Theorem 4.14. *There is no balanced presentation*

$$\langle a, b | a^{p(m)} b^{q(m)}, a^{r(m)} b^{s(m)} \rangle$$

for $p(m), q(m), r(m), s(m) \in \mathbb{Z}[m]$ which defines the trivial group if and only if m is odd.

Proof. For contradiction, suppose that such presentation exists. First, observe that from $a^v b^w = 1, a^x b^y = 1$ we get $1 = a^v b^w a^x b^y = a^v \, 1 \, b^w = a^v a^x b^y b^w = a^{v+x} b^{w+y}$ for all $v, w, x, y \in \mathbb{Z}$. Therefore also

$$(a^v b^w)^g (a^x b^y)^h = a^{gv} b^{gw} a^{hx} b^{hy} = 1 \tag{4.3}$$

for all $g, h \in \mathbb{Z}$.

As we can see above, the determinant of the matrix

$$M_{\mathcal{P}(m)} = \begin{pmatrix} p(m) & r(m) \\ q(m) & s(m) \end{pmatrix} \in \mathbb{Z}^{2 \times 2}[m]$$

must be a constant polynomial equal to 1 or -1 for all m. Therefore there exists the inverse matrix matrix

$$M_{\mathcal{P}(m)}^{-1} = \begin{pmatrix} c(m) & e(m) \\ d(m) & f(m) \end{pmatrix} \in \mathbb{Z}^{2 \times 2}[m].$$

Using (4.3) we get

$$1 = (a^{p(m)} b^{q(m)})^{c(m)} (a^{r(m)} b^{s(m)})^{d(m)} =$$
$$a^{c(m)p(m)+d(m)r(m)} b^{c(m)q(m)+d(m)s(m)} = a,$$
$$1 = (a^{p(m)} b^{q(m)})^{e(m)} (a^{r(m)} b^{s(m)})^{f(m)} =$$
$$a^{e(m)p(m)+f(m)r(m)} b^{e(m)q(m)+f(m)s(m)} = b$$

for all m. Therefore if $\mathcal{P}(m)$ describes the trivial group for all odd m then it has to describes the trivial group for all m. A contradiction. $\qquad \square$

In the previous situation we tried to reduce determining parity to the triviality problem. Now, we show that it is quite easy to find a balanced presentation for m meeting the requirements from Theorem 4.14 which describes some finite group H if and only if m is odd. To achieve that, we start with lemma.

Lemma 4.15. *The presentation $\langle a, b | a^2, ab^2 \rangle$ defines the group $\mathbb{Z}_4$.*

Proof. From $a^2 = 1$ and $ab^2 = 1$ we get $a = b^2$. From $a = b^2$ and $a^2 = 1$ we get $b^4 = 1$. Therefore the group consists of words $1, b, b^2 = a, b^3$ and it is generated by b. $\qquad\square$

Now, we are able to introduce a balanced presentation for m which defines $\mathbb{Z}_4$ if and only if m is odd.

Theorem 4.16. *Let $m \in \mathbb{N}$. Then the presentation $\langle a, b | a^m b^2, a^2 \rangle$ is a presentation of $\mathbb{Z}_4$ if and only if m is odd.*

Proof. If m is odd we may transform given presentation into $\langle a, b | a^2, ab^2 \rangle$ which is a presentation of $\mathbb{Z}_4$ by Lemma 4.15. If m is even we may transform the presentation into $\langle a, b | a^2, b^2 \rangle$ which defines an infinite group $\mathbb{Z}_2 * \mathbb{Z}_2$ by Lemma 1.10. $\qquad\square$

At last, we show a different approach to determining parity using balanced presentation. Contrary to the previous situation where we required fixed number of generators, we may change the number of generators according to m. Let us recall that in Theorem 4.5 given presentation for graph defines the trivial group depending on the existence of an even cycle in a graph. We use the technique from this theorem to construct a balanced presentation which determines a parity of m.

Theorem 4.17. *Let $m \in \mathbb{N}$. Then the balanced presentation*

$$\langle a_1, \ldots, a_m | a_1 a_2, a_2 a_3, \ldots, a_{m-1} a_m, a_1 a_m^2 \rangle$$

is a presentation of the trivial group if and only if m is even.

Proof. The generators $a_1, \ldots, a_m$ together with the relations $a_1 a_2 \ldots a_{m-1} a_m$ represent a path $a_1, \ldots a_n$ (see Definition 4.1). As well as in the proof of Lemma 4.2 we get $a_i = a_{i+2}$.

If m is even we get $a_1 = a_{m-1}$. Therefore we have relations $a_1 a_m = 1$ and $a_1 a_m^2 = 1$ which imply $a_m = 1 = a_1 = a_{m-1}$. Since $a_i = a_{i+2}$ the presented group is trivial.

If m is odd we get $a_1 = a_m$. Since $a_i = a_{i+2}$ we may transform the presentation into $\langle a, b | ab, a^3 \rangle$ which is a presentation of $\mathbb{Z}_3$. $\qquad\square$

5. Topology

In the last chapter, we show how group presentations are connected to topology.

5.1 Basic theory

This section is a brief introduction to basic terms which we use in this chapter. We denote the n-dimensional ball by B^n and the n-dimensional sphere by S^n.

Simplicial and CW complexes   In this paragraph we introduce two important types of Hausdorff topological spaces.

Definition 5.1. A *simplicial complex* is a set K of simplices in Euclidean space such that:

1. If a simplex belongs to K then also all its faces belong to K.

2. If simplices σ_1, σ_2 belong to K then their intersection is a face of both σ_1 and σ_2.

Let $k \in \mathbb{N}$. Then *simplicial k-complex* is a simplicial complex which does not contain a simplex of dimension greater than k. See Figure 5.1.

For a computer representation it is convenient to use a combinatorial description of simplicial complex:

Definition 5.2. Let S be a set and let $P(S)$ denote a power set of X. Then $K \subseteq P(S)$ is an *abstract simplicial complex* if $\sigma \in K$ and $\sigma' \subseteq \sigma$ imply $\sigma' \in K$.

Now, we consider a more general construction.

Definition 5.3. A *CW-complex K* is a union of a collection of disjoint subspaces $\{e_i\}_{i \in I}$ called *cells* where each e_i has some dimension $n \in \mathbb{N}_0$ and for each e_i of dimension n there is a continuous mapping $\chi_i \colon B^n \to X$ such that $\partial B^n = S^{n-1}$ is mapped into $X^{\leq n-1} := \{e_j; j \in I, \dim e_i \leq n-1\}$ and $\mathrm{int} B^n$ is mapped homeomorphically onto e_i.

We may informally describe an inductive construction of a CW-complex starting with a discrete 0-dimensional space. In each step we "glue" a cell of dimension k, which is homeomorphic to a ball, by its boundary to the part which was already made from cells of dimension less then k.

Note that simplicial complex is a special type of CW-complex since simplices are homeomorphic to balls. We usually write only complex instead of a CW-complex. If we consider a complex K as a topological space, we in fact consider an union of its "parts" which forms a topological space we denote $|K|$. If K is a simplicial complex then $|K|$ is called *polyhedron of the simplicial complex K*.
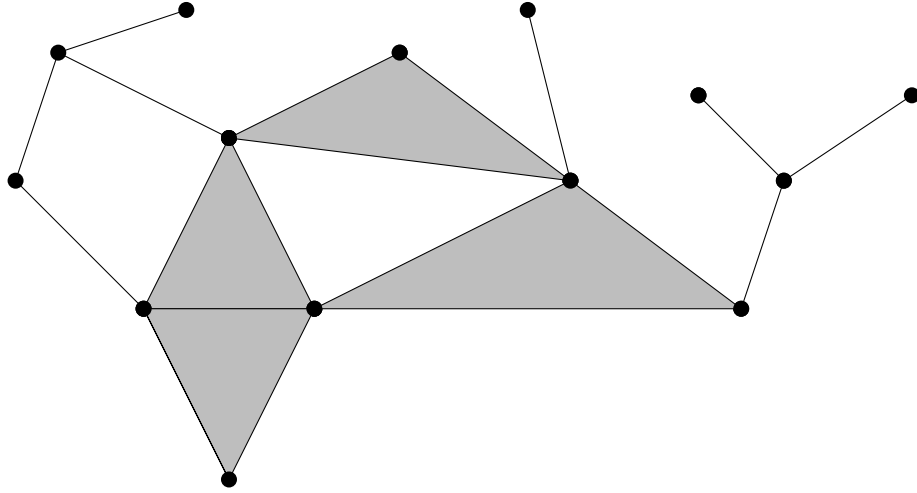
Figure 5.1: An example of a simplicial 2-complex.

Homotopy equivalence Let X, Y be topological spaces and f, g continuous functions from X to Y. A continuous function $H \colon X \times [0,1] \to Y$ is said to be *homotopy* between f and g if $H(x, 0) = f(x)$ and $H(x, 1) = f(x)$. If there is exist such homotopy between f, g then they are *homotopic*. Note that "being homotopic" is an equivalence relation.

Definition 5.4. Topological spaces X, Y are said to be *homotopy equivalent* if there exist continuous functions $f \colon X \to Y$ and $f \colon Y \to X$ such that $f \circ g$ is homotopic to Id_X and $g \circ f$ is homotopic to Id_y. Homotopy equivalence between X and Y is usually denoted by $X \simeq Y$. A topological space is *contractible* if it is homotopy equivalent to a one-point space.

Fundamental group For a topological space X and a point $x \in X_0$ let us consider a continuous function $f \colon [0,1] \to X$ such that $f(0) = f(1) = x_0$. Such mapping is called *loop* with *base point* x_0. For two loops f, g with the same base point x_0 we can define a binary operation $*$ as follows:

$$f * g(t) = \begin{cases} f(2t) & \text{if } 0 \leq t \leq \frac{1}{2} \\ g(2t - 1) & \text{if } \frac{1}{2} \leq t \leq 1. \end{cases}$$

Now, let $\sim$ denote an equivalence relation "being homotopic" on a set of all loops with the base point x_0 and let us define $[f]_\sim *_\sim [g]_\sim = [f * g]_\sim$. The set of equivalence classes of loops with the base point x_0 together with the operation $*_\sim$ define a group which is called a *fundamental group* and denoted by $\pi_1(X, x_0)$. Note that we restrict ourselves to the path-connected topological spaces. In this case, a choice of a different base point gives us the isomorphic fundamental group. That is, $\pi_1(X, x_0) \cong \pi_1(X, y_0)$ for all $x_0, y_0 \in X$. Therefore we write only $\pi_1(X)$.

Note that contractible space must have a trivial fundamental group. However, the opposite implication does not hold. For instance, S^2 has a trivial fundamental group but it is not contractible.

Presentation of fundamental group Given a two dimensional CW-complex we can read off a presentation of its fundamental group. We does not describe
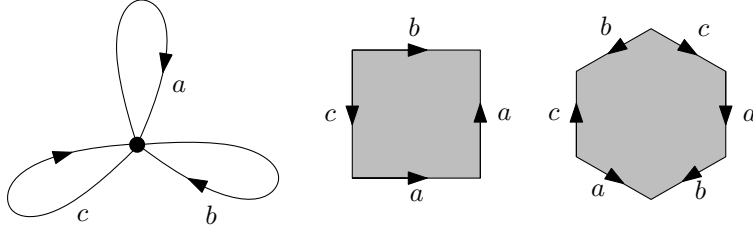
Figure 5.2: An example of the loops and the discs for the presentation $\langle a, b, c | a^2 b^{-1} c, ab^{-1} a^{-1} c^{-1} bc^{-1} \rangle$

this method. It can be found for example on page 7 in [HAMSS93]. However, important fact is, that the presentation read off from two dimensional complex according to the method described in [HAMSS93] is balanced and describes the trivial group if and only if this complex is contractible. This fact is a motivation for the triviality problem for balanced presentation.

Construction a standard complex of presentation   For our purposes the inverse process is more important. That is, a construction of a 2-complex for given presentation.

Let $\langle a_1, \ldots, a_n | \rho_1, \ldots, \rho_m \rangle$ be a finite presentation. First, we construct a vertex with n loops. Each loop corresponds to one generator and has an orientation.

Then we make a disc for each relation $\rho_i = x_1^{e_1} \ldots x_s^{e_s}$ where $e_j \in \{-1, 1\}$. We divide the boundary of the disc into s parts. Each part represents some generator e_j and these parts follow the order of the generators in ρ_i. Each part has also an orientation. We choose an orientation for the first part arbitrary then the orientation of k-th part is changed whenever e_{k-1} has a different sign from the sign of e_k. For an illustration see Figure 5.2.

Finally, we "glue" each disc to the loops such that each part of disc is glued to the corresponding loop with the corresponding orientation.

Collapses   In this paragraph, we show an operation on complex which preserves the homotopy type. That is, we get a homotopy equivalent complex as a result. Such operation is called an elementary collapse.

Definition 5.5. First, we show a definition of elementary collapse for simplicial complex K of dimension d. Let $\sigma \in K$ be a simplex of dimension d and $\tau \subset \sigma$ a simplex of dimension $d-1$ such that no other simplex of dimension d contains τ. Then removing σ and τ from K is called *elementary collapse*. See Figure 5.3.

Now, we informally define a generalization for CW-complexes. Let K be a CW-complex of dimension d. Then the complex L is obtained from K the *elementary collapse* if K can be obtained from L by "gluing" the ball B^d along one of its hemispheres. See definition 11.12 in [Koz07]. For alternative definition see for example page 13 in [HAMSS93].

A complex is *collapsible* if there exists a sequence of collapses which lead into the one-point space. The inverse operation is called *anti-collapse*.

Link   For a simplicial 2-complex and its vertex v we can encode the information of a neighbourhod v to a graph called link.
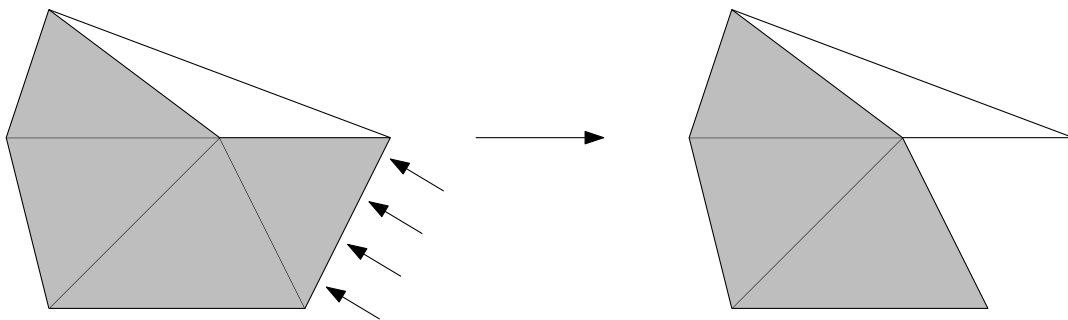
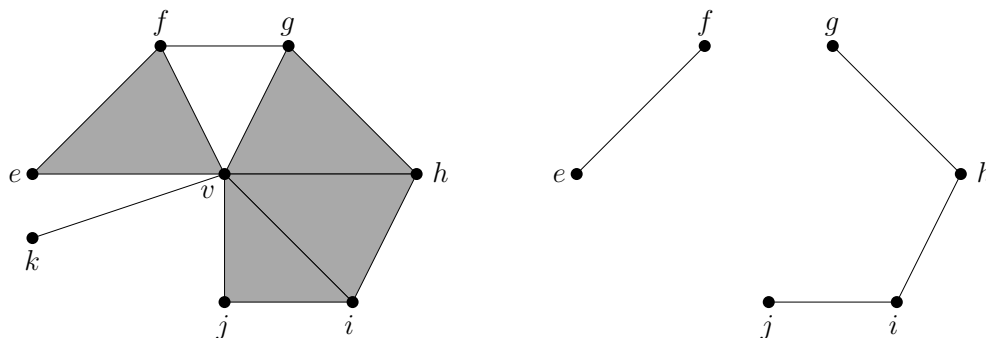Figure 5.3: An example of collapse on a simplicial 2-complex

Figure 5.4: An example of a link of the vertex v.

Definition 5.6. Let v be a vertex of simplicial 2-complex K. Then a *link* of vertex v is a graph given by edges ef such that $\{e, f, v\}$ is a triangle in K. See Figure 5.4

5.2 Andrew-Curtis conjecture

Notice that if a complex is collapsible then it is also contractible, but the converse is not true. However, there is a conjecture that for any contractible 2-complex X there exists a sequence of collapses and anti-collapses which lead to the point and a result of every anti-collapse in this sequence has dimension at most 3. This conjecture is due to Andrews and Curtis in 1965. See [AC65].

As we mentioned above, the contractible 2-complexes correspond to balanced presentations of trivial group. The Andrew-Curtis conjecture may be reformulated to the language of presentations as follows.

Conjecture 5.7 (Andrew and Curtis, see [AC65])**.** *Let* $\langle a_1, \ldots, a_n | \rho_1, \ldots, \rho_n \rangle$ *be a presentation of the trivial group. Than it can be transformed into the empty presentation by a finite sequence of the following* AC*-transformations:*

1. *Replace* ρ_i *by* ρ_i^{-1} *for some* i.

2. *Replace* ρ_i *by* $\rho_i \rho_j$ *for some* $i \neq j$.

3. *Replace* ρ_i *by* $\omega^{-1} \rho_i \omega$ *where* ω *is a word in the generators for some* i.

4. *Add a new generator* b *and a new relation* b *or if there is a generator in a set of relation then remove it from the set of generators and the set of relations.*
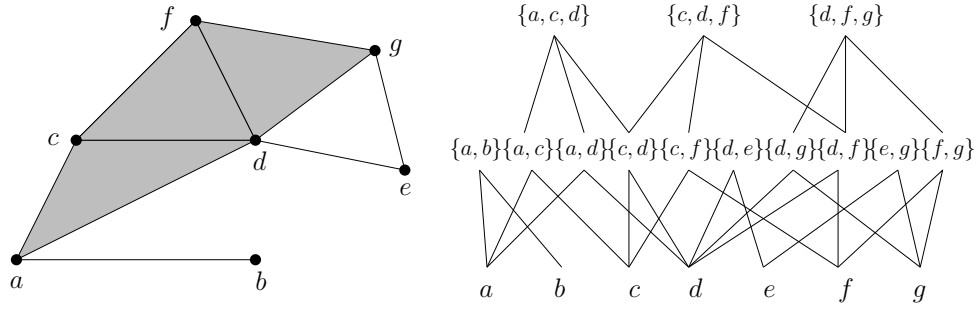
Figure 5.5: An example of a data structure for a simplicial 2-complex
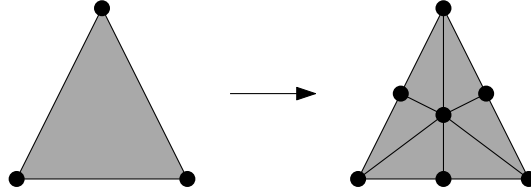

Figure 5.6: An example of a barycentric division on a triangle.

The sequence of such transformations corresponds to the sequence of collapses and anti-collapses.

The conjecture was widely studied in the algebraic formulation. There are also several potential counterexamples. That is, balanced presentations of the trivial group for which we do dot know the sequence of AC-transformations which would lead into the empty presentation. For instance, there is a potential counterexample even with only two generators: $\langle a, b | a^{-1}b^2ab^{-3}, b^{-1}a^2ba^{-3} \rangle$ (See [BM93]).

5.3 Computer representation

In this section we describe an easy method how to transform a group presentation to a computer representation of simplicial 2-complex.

Motivation Andrew-Curtis conjecture was widely studied in the algebraic formulation. It may be interesting to study potential counterexamples as corresponding topological spaces using some topological algorithms. To achieve it, we first need a computer representation for corresponding simplicial 2-complexes.

Data Structure A natural way how to represent a simplicial complex is to use the corresponding abstract simplicial complex. Hence as a data structure we use a list of simplices. Each simplex has a list of pointers on its subsimplices and a list of pointers on simplices which contain it. See Figure 5.5.

Construction of a simplicial complex from a presentation In the previous section, we described how we can get a CW-complex K from a given group presentation. In this section we consider a triangulation of K. That is, a simplicial complex isomorphic to K. For this purpose, we need a definition of a barycentric subdivision.
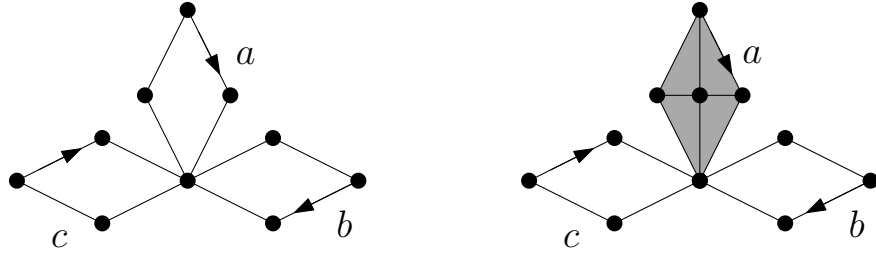
Figure 5.7: An example of loops for simplicial complex (left) and "glued" disc for a relation a of the length 1 (right).
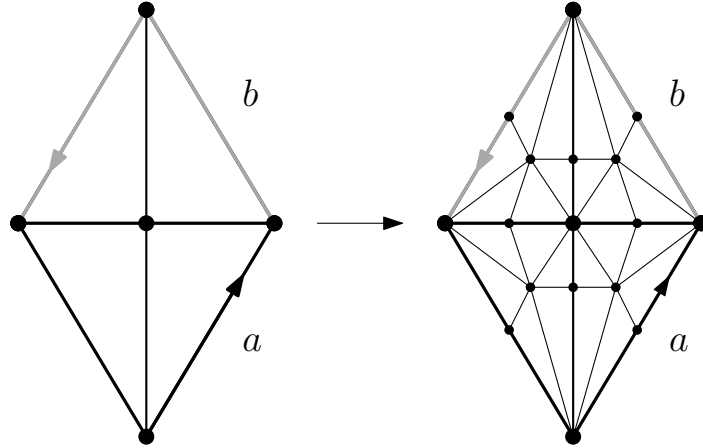

Figure 5.8: A triangulation a of disc created by a barycentric subdivision for a relation ab of the length 2.

Definition 5.8. Let K be a simplicial complex of the dimension k. Then we define a *barycentric subdivision* of K inductively as follows.

1. For $k = 0$ we do nothing.

2. For $k \geq 1$ we first perform a barycentric subdivision on a subcomplex consisting of all simplices of dimension $< k$. Then for all simplices σ of dimension k we add a point c_σ to the "center of gravity" of σ and for all simplices τ lying on the already subdivided boundary of σ we construct a cone with the apex c and the base τ.

See Figure 5.6. Note that for a simplicial complex K and a simplicial complex K', created by a barycentric subdivision of K, we have $|K| = |K'|$.

Now, we use a similar construction as we used for the case of CW-complex. First, make a loops for generators of presentation. However, each loop is represented by a square. See Figure 5.7

Then we create triangulations discs for relations. For a relation of the length 1 we may just add a vertex in the middle of corresponding loop and connect it with the vertices of this loop. See Figure 5.7

For a relation of the length 2 we start with square with one middle vertex such that two incident edges represent corresponding generator in relation. Then we perform a barycentric subdivision on it. See Figure 5.8.
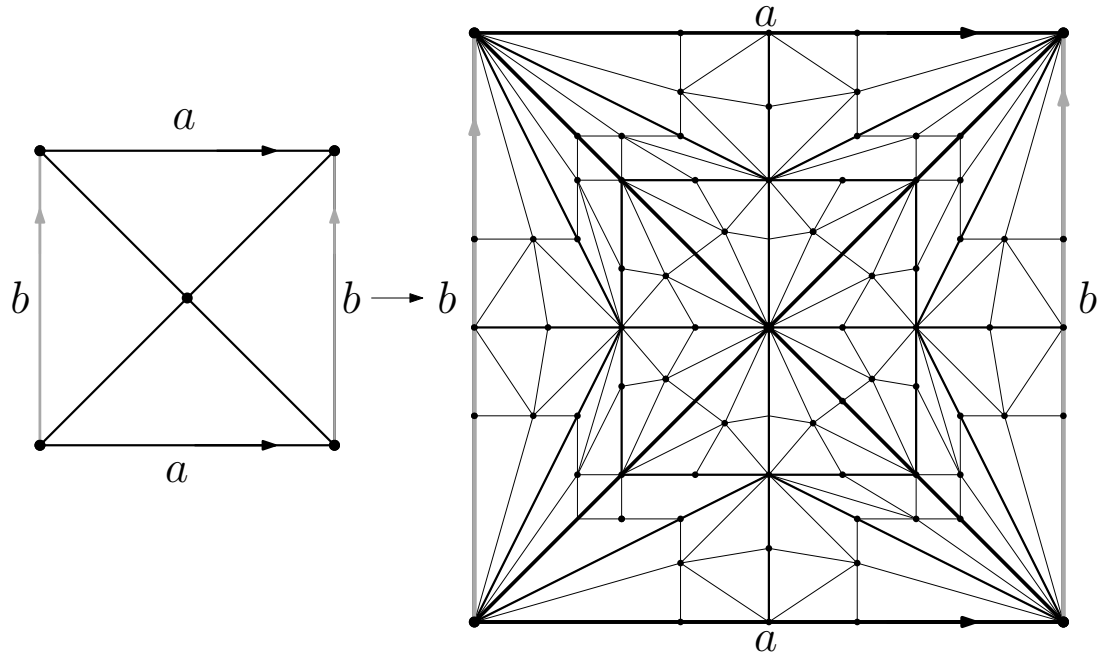
Figure 5.9: A triangulation of a disc created by two barycentric subdivisions for a relation $aba^{-1}b^{-1}$ of the length 4.

For a relation of the length $n \geq 3$ we start with an n-gon with one middle vertex where each side represents corresponding generator in relation. Then we perform a barycentric subdivision two times. See Figure 5.9.

Finally, we "glue" discs to the loops. Note that after this operation, every endpoints of parts of disc representing relations are mapped on the middle point of loops. Hence every two edges incident with different endpoints must be disjoint. This holds for our triangulations.

Note that the link of the common vertex of loops may be non-planar. This is a potential problem for reductions to other special simplicial 2-complex which has certain properties. See page 33 in [HAMSS93].

5.4 Implementation

An additional part of this thesis is also a program which implements the reduction of a group presentation to the corresponding abstract simplicial 2-complex which is described in the previous section (Section 5.3). The program is written in the language C++ using the library *Boost*[1].

Documentation   For a documentation please see the file `doc/html/index.html` in the folder of the program.

Compilation   For a compilation there is a `makefile` or Visual Studio project file.

---

[1]`https://www.boost.org/`

User manual   The input of this program is a group presentation in the following format.

On the first line there is a list of generators. Each generator is represented by one character. There is no delimiter between characters.

The other lines represent relations whereas each line represents one relation. The relation line consists of generators and their exponents separated by space. Each generator is followed by its exponent without any delimiter. As an example, let us consider the presentation $\langle a, b, c | a^{-1} b^2 c^4, abc^2, a^6 \rangle$ Then the input is following.

```
abc
a-1 b2 c4
a1 b1 c2
a6
```

As an output the program prints basic information about corresponding simplicial 2-complex such as the number of edges, vertices and triangles and whether this complex has vertex with non-planar link (for determining whether a graph is planar the library *Boost* is used).

The program may be also run with the following arguments.

- `-f` <u>`filename`</u> Reads the input from the input file. Otherwise the input is read from the standard input.

- `-l` Prints the link of the common vertex of loops in the format of *dot* language[2].

- `-p` Prints the whole simplicial complex. Each simplex is written to one line followed by a list of simplices which contain it.

Future plans   Our future plan is to implement reduction to some special topological spaces "fake surface" and then to a singular 3-manifold. See page 39 in [HAMSS93]. Then to study how a singular 3-manifolds obtained from a potential counterexamples for Andrews-Curtis conjecture differ from a singular 3-manifolds obtained from presentations for which AC conjecture holds.

---

[2]`https://graphviz.gitlab.io/_pages/doc/info/lang.html`

Bibliography

[AC65]   J. J. Andrews and M. L. Curtis. Free groups and handlebodies. *Proceedings of the American Mathematical Society*, 16(2):192—-195, 1965.

[Adi55]   S. I. Adian. Algorithmic unsolvability of problems of recognition of certain properties of groups. *Doklady Akademii Nauk SSSR*, 103:533—535, 1955.

[Bap10]   R.B. Bapat. *Graphs and Matrices*. Universitext. Springer London, 2010.

[BM93]   R. Burns and O. Macedonska. Balanced presentations of the trivial group. 25, 11 1993.

[Boo58]   W. W. Boone. The word problem. *Proceedings of the National Academy of Sciences of the United States of America*, 44(10):1061–1065, 1958.

[Bor69]   V. V. Borisov. Simple examples of groups with unsolvable word problem. *Mathematical Notes*, 6:768–775, 1969.

[Dyc82]   W. Dyck. Gruppentheoretische studien. *Mathematische Annalen*, 20(1):1–44, Mar 1882.

[Gru40]   I. A. Grushko. On the bases of a free product of groups. *Matematicheskii Sbornik*, 8(50):169–182, 1940.

[HAMSS93]   C. Hog-Angeloni, W. Metzler, A.J. Sieradski, and London Mathematical Society. *Two-Dimensional Homotopy and Combinatorial Group Theory*. Lecture note series. Cambridge University Press, 1993.

[HMU07]   J.E. Hopcroft, R. Motwani, and J.D. Ullman. *Introduction to Automata Theory, Languages, and Computation*. Pearson/Addison Wesley, 2007.

[Koz07]   D. Kozlov. *Combinatorial Algebraic Topology*. Algorithms and Computation in Mathematics. Springer Berlin Heidelberg, 2007.

[LS01]   R.C. Lyndon and P.E. Schupp. *Combinatorial Group Theory*. Classics in Mathematics. Springer Berlin Heidelberg, 2001.

[Mil92]   C. F. Miller. Decision problems for groups: Survey and reflections. In *Algorithms and Classification in Combinatorial Group Theory*, MSRI publications No. 23, pages 1–59. Springer New York, 1992.

[Nov55]   P. S. Novikov. On the algorithmic unsolvability of the word problem in group theory. *Proceedings of the Steklov Institute of Mathematics*, 44:1–143, 1955.

[Rab58] M. O. Rabin. Recursive unsolvability of group theoretic problems. *Annals of Mathematics*, 67(2):172—-194, 1958.

[Rot99] J. Rotman. *An Introduction to the Theory of Groups.* Graduate Texts in Mathematics. Springer New York, 1999.