Applications of Homological Algebra to Equational Theories

by

Mirai Ikebuchi

B.S., University of Tsukuba (2015)
M.S., Nagoya University (2017)

Submitted to the Department of Electrical Engineering and Computer Science
in partial fulfillment of the requirements for the degree of

Doctor of Philosophy in Electrical Engineering and Computer Science

at the

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

February 2022

Author .....
Department of Electrical Engineering and Computer Science
October 14, 2021

Certified by .....
Adam Chlipala
Associate Professor of Electrical Engineering and Computer Science
Thesis Supervisor

Accepted by .....
Leslie A. Kolodziejski
Professor of Electrical Engineering and Computer Science
Chair, Department Committee on Graduate Students

Applications of Homological Algebra to Equational Theories

by

Mirai Ikebuchi

Submitted to the Department of Electrical Engineering and Computer Science
on October 14, 2021, in partial fulfillment of the
requirements for the degree of
Doctor of Philosophy in Electrical Engineering and Computer Science

Abstract

It is well-known that some equational theories such as groups or Boolean algebras can be defined by fewer equational axioms than the original axioms. However, it is not easy to determine if a given set of axioms is the smallest or not. Malbos and Mimram investigated a general method to find a lower bound of the cardinality of the set of equational axioms (or rewrite rules) that is equivalent to a given equational theory (or term rewriting system), using homological algebra. Their method is an analog of Squier's homology theory on string rewriting systems. In this dissertation, I develop the homology theory for term rewriting systems more and provide a better lower bound under a stronger notion of equivalence than their equivalence.

Also, the same methodology applies to equational unification, the problem of solving an equation modulo equational axioms. I provide a relationship between equational unification and homological algebra for equational theories. I will construct abelian groups associated with equational theories. Then, the main theorem gives a necessary condition of equational unifiability that is described in terms of the abelian groups and homomorphisms between them.

Thesis Supervisor: Adam Chlipala
Title: Associate Professor of Electrical Engineering and Computer Science

Acknowledgments

I would like to thank my advisor, Adam Chlipala, who admitted me as an intern and then a PhD student of his group, and has supported me through my time at MIT. If I did not contact him to ask for an internship, my life would be much different. I would also like to thank the other thesis committee members, Assaf Kfoury, Erik Demaine, and Haynes Miller. I did not have many people to discuss my thesis topics with, but Assaf nicely proposed to have weekly meetings. Haynes gave me invaluable technical comments and advices from a mathematician's view. I took 6.892, Erik's class on computational complexity of puzzles and video games, and that was a lot of fun and relaxing.

I am grateful to my past advisors in Japan, who helped in learning advanced mathematics, including homological algebra. I remember that Shinichi Tajima, one of my past advisors, said "Math is wonderful. If you learn some mathematical topics deeply, you will often find that two apparently distinct notions are in fact connected." Yes, that is true, and this dissertation is about an example of such surprising connections.

Finally, I thank my friends and family for supporting my life.

This dissertation is based on two papers [8, 9]. The former was presented at FSCD 2019, and an extended version is currently under revision for publication in the FSCD 2019 Special Issue of Logical Methods in Computer Science. The latter was presented at MFCS 2021.

Contents

Chapter 1

Introduction

In this dissertation, I will provide partial answers to the following two questions: Given an equational theory E,

1. How many axioms are needed to present E?
2. For two terms t, s with variables, is the equation $t = s$ modulo E solvable? (E-unifiability)

The first problem has been well-studied for some specific theories such as groups or Boolean algebras, but not for general theories. Malbos and Mimram proved an inequality to give lower bounds [13], but they did not give any nontrivial examples. (They gave one example, but the computation for it was incorrect.) I extended their methodology and developed a better inequality. Also, I found that my inequality provides a nontrivial lower bound for a number of theories.

In more detail, in [13], Malbos and Mimram showed that for any equational theory E, the cardinality of a set E' of equational axioms presenting E is bounded

below by the integer $s(H_2(E))$, that is,

$$s(H_2(E)) \leq \#E'. \tag{1.1}$$

Here, $H_2(E)$ is the abelian group called the *second homology* of E, and $s(H_2(E))$ denotes the minimum number of generators of $H_2(E)$. The number $s(H_2(E))$ bounds below the cardinality of a set of equational axioms Also, $s(H_2(E))$ is computable if a complete (i.e., terminating and confluent) term-rewriting system for E is given. This work is surprising because (i) it is the first result that gives a lower bound on the number of axioms for a general equational theory, and (ii) it connects two different fields, equational logic and homological algebra. However, not many theories are known to have $s(H_2(E)) > 1$, that is, it does not often give a nontrivial lower bound. For example, if E is the theory of groups, $s(H_2(E)) = 0$.

The inequality (1.1) holds for E' with possibly different constant/function symbols than E. In [8], expanding Malbos and Mimram's work, I found that there is a better lower bound if we allow only E' that has the same constant/function symbols with E. I showed that there is a lower bound that is greater than or equal to $s(H_2(E))$ and, for various theories including the theory of groups, it is the tight lower bound.

I also found that the same methodology can be used for the E-unifiability problem. The E-unifiability problem has been studied for many specific Es, such as the theory of non-unital monoids, the theory of non-unital commutative monoids, and so on. If we include E in the problem input and if E satisfies confluence and some good conditions (like termination), *narrowing* is known as a semidecidable procedure for the problem [5, 6]. Narrowing attempts to find solutions of a given equation, but

if the equation does not have any solutions, it may not terminate. The method I propose gives a sound procedure for non-E-unifiability under some conditions on E. It does not require E to be confluent, but it requires a condition different from narrowing. I found some pairs of Es and equations without solutions on which narrowing does not terminate but my procedure does and detects that they indeed have no solutions.

In the next chapter, a quick introduction to equations, rewriting, and unification is given. Then, in Chapter 3, my main theorems are described without using the language of homology. In Chapter 4, the proof idea is explained through *simplicial homology*, a homology theory that is more famous and simpler than the homology of equational theories. Chapter 5 provides an introduction to module theory, which we need for the proofs. The construction of the homology of equational theories is given in Chapter 6. Then, we prove the results on questions 1 and 2 in Chapter 7.

Chapter 2

Preliminaries

A *signature* Σ is a set together with a function $\alpha : \Sigma \to \mathbb{Z}_{\geq 0}$. For $f \in \Sigma$, we say that f is of *arity* n if $n = \alpha(f)$, and we write $f^{(n)}$ for f to indicate that f is of arity n. Let V be a countably infinite set distinct from Σ. A *term* over Σ and V is a formal expression defined inductively as follows:

1. Any element in V, called a *variable*, is a term.

2. For $f \in \Sigma$ of arity n, if $t_1, \ldots, t_n$ are terms, then $f(t_1, \ldots, t_n)$ is also a term.

Here, $f(t_1, \ldots, t_n)$ is a formal expression and not a function application, though its semantics is often treated as a function application. If $c \in \Sigma$ is of arity 0, we write just c for $c()$. For a signature Σ, let $\mathrm{Term}(\Sigma, V)$ denote the set of terms over Σ and V. Also, in this dissertation, the variables we use are $x_1, x_2, \ldots$, so we just write $\mathrm{Term}(\Sigma)$ for $\mathrm{Term}(\Sigma, \{x_1, x_2, \ldots\})$. If f is a symbol of arity 2 that is usually written in infix notation (e.g., $+$, $\times$), we write $t_1 f t_2$ instead of $f(t_1, t_2)$. We write $\mathrm{Var}(t)$ for the set of variables that occur in t.

A *substitution* is a function $V \to \mathrm{Term}(\Sigma, V)$. If a substitution σ satisfies $\sigma(v_1) = t_1, \ldots, \sigma(v_n) = t_n$ and $\sigma(v) = v$ for any $v \neq v_1, \ldots, v_n$, σ is written as $\{v_1 \mapsto t_1, \ldots, v_n \mapsto t_n\}$. For a substitution $\sigma \colon V \to \mathrm{Term}(\Sigma, V)$, we can extend it to a map $\hat{\sigma} \colon \mathrm{Term}(\Sigma, V) \to \mathrm{Term}(\Sigma, V)$ as

$$\begin{aligned} \hat{\sigma}(v) &= \sigma(v) \quad \text{for } v \in V, \\ \hat{\sigma}(f(t_1, \ldots, t_n)) &= f(\hat{\sigma}(t_1), \ldots, \hat{\sigma}(t_n)) \quad \text{for } f \in \Sigma \text{ and } t_1, \ldots, t_n \in \mathrm{Term}(\Sigma, V). \end{aligned}$$

We write $t\sigma$ for $\hat{\sigma}(t)$. For two substitutions $\sigma, \tau \colon V \to \mathrm{Term}(\Sigma, V)$, their composition $\sigma\tau$ is defined as $\sigma\tau(v) = \hat{\tau}(\sigma(v))$. We can check $t(\sigma\tau) = (t\sigma)\tau$ for any term t.

Two terms t, s are *unifiable* if there exists a substitution σ such that $t\sigma = s\sigma$. Such σ is called a *unifier*. A *most general unifier (mgu)* of unifiable terms t, s is a unifier σ of t, s such that for any other unifier σ' of t, s, there exists a substitution τ such that $\sigma' = \sigma\tau$. An mgu is unique up to renaming of variables.

A *context* is a term in $\mathrm{Term}(\Sigma, V \cup \{\Box\})$ that has just one $\Box$, called a *hole*, in it. For a context $C \in \mathrm{Term}(\Sigma, V \cup \{\Box\})$ and a term $t \in \mathrm{Term}(\Sigma, V)$, $C[t]$ denotes the term $C\{\Box \mapsto t\}$.

An *equation* is an ordered pair of terms. Equations are written as $l \approx r$. A *rewrite rule* is an equation $l \approx r$ satisfying $\mathrm{Var}(l) \supset \mathrm{Var}(r)$. For rewrite rules, we write $l \to r$ instead of $l \approx r$ when we want to emphasize the order of l and r. A *term-rewriting system (TRS)* is a set of rewrite rules. For an equation $l \approx r$ and a term t, we say that t is rewritten to s by $l \approx r$, denoted $t \underset{l \approx r}{\longrightarrow} s$, if there is a context C and a substitution σ such that $t = C[l\sigma]$ and $s = C[r\sigma]$. For a set of equations E and two terms t, s, we say that t is rewritten to s by E, denoted $t \to_E s$, if $t \underset{l \approx r}{\longrightarrow} s$ holds for some $l \approx r \in E$. The reflexive transitive closure of the relation $\to_E$ is

written as $\xrightarrow{*}_E$, and the reflexive symmetric transitive closure of $\rightarrow_E$ is written as $\overset{*}{\leftrightarrow}_E$ or $\approx_E$. Two sets E, E' of equations are *equivalent* if $\approx_E = \approx_{E'}$. Two terms t, s are said to be *E-unifiable* if there exists a substitution σ such that $t\sigma \approx_E s\sigma$. Such a σ is called an *E-unifier*. If we consider the problem of finding an E-unifier of two terms t, s, we write $t \approx_E^? s$ for the problem.

A TRS R is *terminating* if there is no infinite path $t_1 \rightarrow_R t_2 \rightarrow_R t_3 \rightarrow_R \ldots$.

Two terms t_1, t_2 are *joinable* by R if there exists a term s such that $t_1 \xrightarrow{*}_R s \xleftarrow{*}_R t_2$. A TRS R is *confluent* if, for any terms t, t_1, t_2, $t_1 \xleftarrow{*}_R t \xrightarrow{*}_R t_2$ implies that t_1 and t_2 are joinable.

A TRS R is *complete* if R is terminating and confluent.

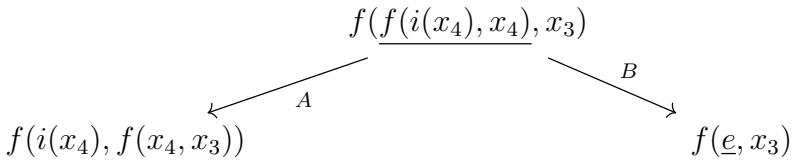
For a TRS R, a term t is *R-normal* if t cannot be rewritten by R. If R is terminating, for any term t, there exists an R-normal term s such that $t \xrightarrow{*}_R s$, and if R is complete, such an s is unique.

Let R be a TRS and $l_1 \rightarrow r_1, l_2 \rightarrow r_2 \in R$ be two rewrite rules. Suppose that the variables of $l_2 \rightarrow r_2$ are renamed so that $\mathrm{Var}(l_1) \cap \mathrm{Var}(l_2) = \emptyset$. For some context C and nonvariable term t, if t and l_2 are unifiable with mgu σ and if $C[t] = l_1$, the pair $(r_1\sigma, C[r_2\sigma])$ is called a *critical pair* of R. The diagram $r_1\sigma \leftarrow l_1\sigma = C[l_2\sigma] \rightarrow C[r_2\sigma]$ is called a *critical peak*. For example, suppose that we have two rules

$$A : f(f(x_1, x_2), x_3) \rightarrow f(x_1, f(x_2, x_3))$$
$$B : f(i(x_4), x_4) \rightarrow e.$$

The subterm $f(x_1, x_2)$ of the left-hand side of A and $f(i(x_4), x_4)$, the left-hand side of B, can be unified with the mgu $\sigma = \{x_1 \mapsto i(x_4), x_2 \mapsto x_4\}$. Then, the corresponding

critical pair is $(f(i(x_4), f(x_4, x_3)), f(e, x_3))$, as the following diagram shows.



Here, the underlined subterms are the terms matched with the LHS and RHS of the rule B. Note that if a TRS R finite, then the critical pairs and peaks are also finite up to renaming of variables. Also, we do not distinguish critical pairs/peaks that are transformed into each other by renaming variables.

A famous application of critical pairs is checking confluence of a terminating TRS:

Proposition 1. [2] A terminating TRS is confluent if and only if its critical pairs are joinable.

The *equational theory* of a set E of equations is the set $E^* = \{(t, s) \mid t \approx_E s\}$. Two sets E, E' of equations are said to be *equivalent* if $E^* = E'^*$. For a set E of equations and a TRS R, we say that R is a TRS of E if R is equivalent to E.

Chapter 3

Results

3.1 Lower Bounds on Numbers of Rules

We introduce some notions to describe our lower bounds. Let (Σ, R) be a TRS.

Definition 2. The degree of R, denoted by $\deg(R)$, is defined by

$$\deg(R) = \gcd\{\#_i l - \#_i r \mid l \to r \in R, i = 1, 2, \dots\}$$

where $\#_i t$ is the number of occurrences of x_i in t for $t \in T(\Sigma)$. Here, recall that $\gcd\{0, a, b, \dots\} = \gcd\{a, b, \dots\}$ and $\gcd\{0\} = 0$. For example, $\deg(\{f(x_1, x_2, x_2) \to x_1,\ g(x_1, x_1, x_1) \to e\}) = \gcd\{0, 2, 3\} = 1$.

Suppose that R is complete and consists of n rules, $l_1 \to r_1, \dots, l_n \to r_n$. Note that any TRS with finitely many rules has finitely many critical peaks. So, suppose that R has m critical peaks and that the set of them is written as $\{r_{a_i}\sigma \leftarrow l_{a_i}\sigma = C[l_{b_i}\sigma] \to C[r_{b_i}\sigma] \mid i = 1, \dots, m\}$ for some $a_i, b_i \in \{1, \dots, n\}$. For each term t, if it

can be rewritten in several ways, we fix one of them. Such a correspondence between a term and a way of rewriting is called a *rewriting strategy*. For a term t, let $\mathrm{nr}_j(t)$ be the number of times $l_j \to r_j$ is used to reduce t into its R-normal form with respect to the strategy.

Definition 3. Let $d = \deg(R)$. The matrix $D(R)$ is the $n \times m$ matrix over $\mathbb{Z}_d$ whose (i,j)-th entry $D(R)_{ij}$ $(1 \le i \le n,\ 1 \le j \le m)$ is $[\mathrm{nr}_i^R(C[r_{b_j}\sigma]) - \mathrm{nr}_i^R(r_{a_j}\sigma) + \delta(b_j^R, i) - \delta(a_j^R, i)] \in \mathbb{Z}_d$ where $\delta(x,y)$ is the Kronecker delta. (That is, $\delta(x,y) = 1$ if $x = y$ and 0 if $x \neq y$.)

Definition 4. Let $\mathfrak{R}$ be $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ for any p that is prime or 0. If an $m \times n$ matrix M over $\mathfrak{R}$ is of the form

$$\begin{pmatrix} e_1 & 0 & \dots & \dots & \dots & \dots & \dots & 0 \\ 0 & e_2 & 0 & \dots & \dots & \dots & \dots & 0 \\ \vdots & 0 & \ddots & 0 & \dots & \dots & \dots & \vdots \\ \vdots & \vdots & 0 & e_r & 0 & \dots & \dots & \vdots \\ \vdots & \vdots & \vdots & 0 & 0 & \dots & \dots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \dots & \vdots \\ 0 & 0 & \dots & \dots & \dots & \dots & \dots & 0 \end{pmatrix}$$

and e_i divides e_{i+1} for every $1 \le i < r$, we say M is in *Smith normal form*. The e_is are unique up to multiplication by an invertible element, and we call them the *elementary divisors*.

It is known that every matrix over $\mathfrak{R}$ can be transformed into Smith normal form by elementary row/column operations, that is, (1) switching a row/column with another row/column, (2) multiplying each entry in a row/column by an invertible

element in $\mathfrak{R}$, and (3) adding a multiple of a row/column to another row/column [18, 9.4]. (If $p = 0$, the invertible elements in $\mathfrak{R} \cong \mathbb{Z}$ are 1 and -1, and if p is prime, any nonzero elements in $\mathfrak{R} = \mathbb{Z}_p$ are invertible.) In general, the same fact holds for any principal ideal domain $\mathfrak{R}$.

Definition 5. Let (Σ, R) be a complete TRS, and suppose $d = \deg(R)$ is 0 or prime. We define $e(R)$ as the number of invertible elements in the Smith normal form of the matrix $D(R)$ over $\mathfrak{R} = \mathbb{Z}_d$. (Note that if $\mathfrak{R}$ is a field, $e(R)$ is the rank of $D(R)$.)

Although we fixed a rewriting strategy to define the matrix $D(R)$, in fact, $e(R)$ is independent from the choice:

Lemma 6. The integer $e(R)$ does not depend on the rewriting strategy used to define $D(R)$.

Here is our theorem for lower bounds.

Theorem 7. Let (Σ, R) be a complete TRS, and suppose $d = \deg(R)$ is 0 or prime. For any set of rules R' equivalent to R, i.e., $\overset{*}{\leftrightarrow}_{R'} = \overset{*}{\leftrightarrow}_{R}$, we have

$$\#R' \geq \#R - e(R). \tag{3.1}$$

Remark 8. The condition that $d = \deg(R)$ is 0 or prime is to make $\mathbb{Z}_d$ a PID. Most TRSs of interest have degree 0, 1, or 2, but it is difficult to simply extend this theorem to the case $d = 1$ since $\mathbb{Z}_1 = \{0\}$.

Example 9. Consider the signature $\Sigma = \{\mathsf{0}^{(0)}, \mathsf{s}^{(1)}, \mathsf{ave}^{(2)}\}$ and the set R of rules

$$A_1.\mathsf{ave}(\mathsf{0},\mathsf{0}) \to \mathsf{0}, \quad A_2.\mathsf{ave}(x_1,\mathsf{s}(x_2)) \to \mathsf{ave}(\mathsf{s}(x_1),x_2), \quad A_3.\mathsf{ave}(\mathsf{s}(\mathsf{0}),\mathsf{0}) \to \mathsf{0},$$
$$A_4.\mathsf{ave}(\mathsf{s}(\mathsf{s}(\mathsf{0})),\mathsf{0}) \to s(\mathsf{0}), \quad A_5.\mathsf{ave}(\mathsf{s}(\mathsf{s}(\mathsf{s}(x_1))),x_2) \to \mathsf{s}(\mathsf{ave}(\mathsf{s}(x_1),x_2)).$$

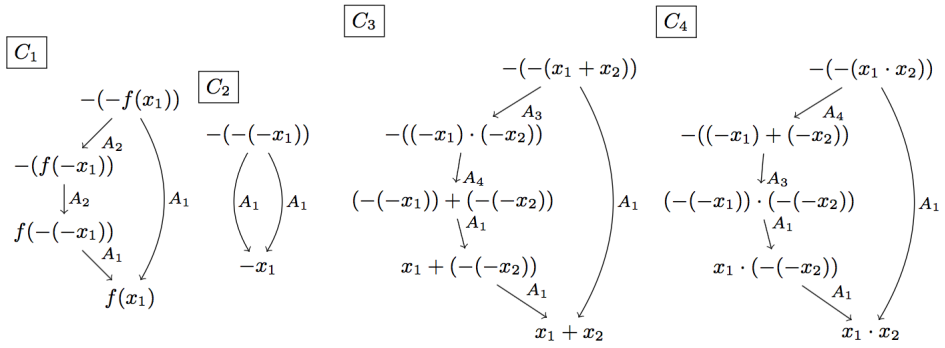
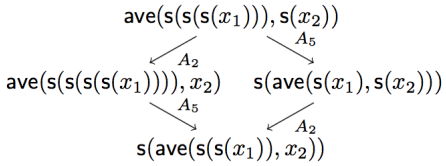


Figure 3-1: The critical peaks of R extended to the normal forms.

R satisfies $\deg(R) = 0$ and has one critical peak:



We can see the matrix $D(R)$ is the 5×1 zero matrix since the two normalizing paths have the same multiset $\{A_2, A_5\}$ of rewrite rules. The zero matrix is already in Smith normal form, and $e(R) = 0$. Thus, for any R' equivalent to R, $\#R' \geq \#R = 5$. This means there is no smaller TRS equivalent to R. Also, Malbos-Mimram's lower bound is equal to 3, though I do not explain how to compute it in this dissertation.

As a generalization of this example, we have an interesting corollary of our main theorem:

Corollary 10. Let (Σ, R) be a complete TRS. If for any critical pair $u \leftarrow t \rightarrow v$, any two rewriting paths $t \rightarrow u \rightarrow \cdots \rightarrow \hat{t}$ and $t \rightarrow v \rightarrow \cdots \rightarrow \hat{t}$ contain the same number of $l \rightarrow r$ for each $l \rightarrow r \in R$, then there is no R' equivalent to R which satisfies $\#R' < \#R$.

Example 11. Let $\Sigma = \{-^{(1)}, f^{(1)}, +^{(2)}, \cdot^{(2)}\}$ and R be

$$\begin{aligned} &A_1.\ -(-x_1) \to x_1, && A_2.\ -f(x_1) \to f(-x_1), \\ &A_3.\ -(x_1 + x_2) \to (-x_1) \cdot (-x_2), && A_4.\ -(x_1 \cdot x_2) \to (-x_1) + (-x_2). \end{aligned}$$

We have $\deg(R) = 0$, and R has four critical pairs (Fig. 3-1). The corresponding matrix $D(R)$ and its Smith normal form are computed as

$$D(R) = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 2 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 0 & 0 & 1 & 1 \\ 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 0 & 0 & 1 & 0 \\ 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Thus, $\#R - e(R) = 3$. This tells us R does not have any equivalent TRS with 2 or fewer rules, and it is not difficult to see R has an equivalent TRS with 3 rules, $\{A_1, A_2, A_3\}$. (Note that the equivalence here is with respect to unordered rules, so we can use A_1 and A_3 backwards to derive A_4.) Malbos-Mimram's lower bound of this example is 1.

Example 12. Over the signature $\Sigma = \{e^{(0),-1^{(1)}}, \cdot^{(2)}\}$, the theory of groups is given as

$$\begin{aligned} &(x_1 \cdot x_2) \cdot x_3 = x_1 \cdot (x_2 \cdot x_3), \quad x_1 \cdot e = x_1, \quad e \cdot x_1 = x_1, \\ &x_1^{-1} \cdot x_1 = e, \qquad\qquad x_1 \cdot x_1^{-1} = e. \end{aligned} \tag{3.2}$$

A complete TRS R for the theory of groups is given by

$$
\begin{array}{ll}
G_1.\ (x_1 \cdot x_2) \cdot x_3 \to x_1 \cdot (x_2 \cdot x_3) & G_2.\ e \cdot x_1 \to x_1 \\
G_3.\ x_1 \cdot e \to x_1 & G_4.\ x_1 \cdot x_1^{-1} \to e \\
G_5.\ x_1^{-1} \cdot x_1 \to e & G_6.\ x_1^{-1} \cdot (x_1 \cdot x_2) \to x_2 \\
G_7.\ e^{-1} \to e & G_8.\ (x_1^{-1})^{-1} \to x_1 \\
G_9.\ x_1 \cdot (x_1^{-1} \cdot x_2) \to x_2 & G_{10}.\ (x_1 \cdot x_2)^{-1} \to x_2^{-1} \cdot x_1^{-1}.
\end{array}
$$

Since $\deg(R) = 2$, we set $\mathfrak{R} = \mathbb{Z}_2$. R has 48 critical pairs, and we get the 10×48 matrix $D(R)$ given in Appendix A. I implemented a program that takes a complete TRS as input and computes its critical pairs, the matrix $D(R)$, and $e(R)$. The program is available at `https://github.com/mir-ikbch/homtrs`. I checked $e(R) = \mathrm{rank}(D(R)) = 8$ with the program and also by MATLAB's `gfrank` function (`https://www.mathworks.com/help/comm/ref/gfrank.html`). Therefore we have $\#R - e(R) = 2$. This provides a new proof that there is no single axiom equivalent to the theory of groups.

Malbos-Mimram's lower bound of this example is 0.

Although the equality of (3.1) is attained for the above three examples, it is not guaranteed the equality is attained by some TRS R' in general. For example, the TRS with only the associative rule $\{f(f(x_1, x_2), x_3) \to f(x_1, f(x_2, x_3))\}$ satisfies $\#R - e(R) = 0$, and it is obvious that no TRS with zero rules is equivalent.

Many other examples are given in the appendix and:

`https://mir-ikbch.github.io/homtrs/experiment/result.html`

3.2 E-unifiability

To describe our theorem for E-unifiability, we need matrix $U(E, R)$.

Definition 13. Let $E = \{l'_1 \approx r'_1, \ldots, l'_{n'} \approx r'_{n'}\}$ be a set of equations and $R = \{l_1 \to r_1, \ldots, l_n \to r_n\}$ be a complete TRS. Suppose $E^* \subset R^*$. Then, $U(E, R)$ is the $n \times n'$ matrix over $\mathbb{Z}_d$ whose (i, j)-th entry is $[\mathrm{nr}_i^R(l'_j) - \mathrm{nr}_i^R(r'_j)] \in \mathbb{Z}_d$ where $d = \deg(R)$.

Then, our theorem is as follows.

Theorem 14. Let $E = \{u_1 \approx v_1, \ldots, u_k \approx v_k\}$ be a set of equations and t, s be two terms. Suppose that there is a complete TRS $R = \{l_1 \to r_1, \ldots, l_n \to r_n\}$ of $E \cup \{t \approx s\}$ and $\deg(R) \neq 1$. If t, s are E-unifiable, then the augmented matrix $(D(R)|U(E, R))$ is equivalent to $I_{n,m}$ and $n \leq m$, where m is the number of columns of $(D(R)|U(E, R))$.

Example 15. Let E_1 be the set of equations

$$A_1 : f(x_1 + x_2) \approx f(x_1) + f(x_2),$$
$$A_2 : f(a) \approx a, \quad A_3 : f(b) \approx b$$

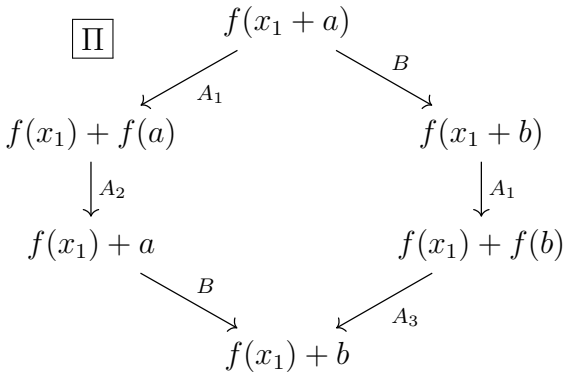
and consider the E_1-unification problem

$$f(x_1) + a \approx^?_{E_1} f(x_1) + b.$$

The set $E_1 \cup \{f(x) + a \approx f(x) + b\}$ has a complete TRS R_1:

$$A_1 : f(x_1 + x_2) \to f(x_1) + f(x_2),$$
$$A_2 : f(a) \to a, \quad A_3 : f(b) \to b,$$
$$B : x_1 + a \to x_1 + b.$$

The degree of R_1 is 0, and R_1 has one critical pair Π



The matrix $(D(R_1)|U(E_1, R_1))$ is computed as

$$\begin{array}{c|c|ccc} & \Pi & A_1 & A_2 & A_3 \\ \hline A_1 & 0 & 1 & 0 & 0 \\ A_2 & 1 & 0 & 1 & 0 \\ A_3 & -1 & 0 & 0 & 1 \\ B & 0 & 0 & 0 & 0 \end{array}.$$

It does not have full rank, so it is not equivalent to the identity matrix $I_{4,4}$. (Recall that the *rank* of M is the number of linearly independent rows of M, and an $n \times m$ matrix M has *full rank* if the rank of M is $\min(n, m)$. The rank is invariant under elementary row and column operations.) By the contrapositive of Theorem 14, $x_1 + a$

and $x_1 + b$ are not E_1-unifiable.

Example 16. Let E_2 be the set of equations

$$B_1 : 0 + x_1 \approx x_1, \quad B_2 : s(x_1) + x_2 \approx s(x_1 + x_2).$$

Consider the E_2-unification problem

$$x_1 + x_1 \approx^?_{E_2} s(0).$$

The TRS $E_2 \cup \{x_1 + x_1 \to s(0)\}$ has a complete TRS R_2:

$$B_1 : 0 + x_1 \to x_1, \quad C_1 : x_1 + x_1 \to 0,$$
$$C_2 : s(x_1) \to x_1.$$

The degree of R_2 is 2, and R_2 has one critical pair Π'

$$\boxed{\Pi'} \quad \begin{array}{c} 0+0 \\ {\scriptstyle B_1}\big(\searrow \quad \swarrow\big){\scriptstyle C_1} \\ 0 \end{array}$$

and the matrix $(D(R_2)|U(E_2, R_2))$ is given as

$$\begin{array}{c|ccc} & \Pi' & B_1 & B_2 \\ \hline B_1 & 1 & 1 & 0 \\ C_1 & 1 & 0 & 0 \\ C_2 & 0 & 0 & 0 \end{array}.$$

Here, each entry of $D(R_2|U(E_2, R_2))$ is thought of as an element in $\mathbb{Z}_2$. Since it does not have full rank, $x_1 + x_1$ and $s(0)$ are not E_2-unifiable.

Example 17. We use the same E_2 as the previous example and consider the E_2-unification problem

$$x_1 + x_1 \approx^?_{E_2} 0.$$

The TRS $E_2 \cup \{x_1 + x_1 \approx 0\}$ has the following complete TRS R_3:

$$\begin{array}{ll} B_1 : 0 + x_1 \to x_1 & B_2 : s(x_1) + x_2 \to s(x_1 + x_2) \\ D_1 : x_1 + x_1 \to 0 & D_2 : s(s(x_1)) \to x_1 \\ D_3 : x_1 + s(x_1) \to s(0) & D_4 : s(x_1) + x_1 \to s(0). \end{array}$$

The critical pairs are listed in Fig. 3-2, and the matrix $(D(R_3)|U(E_2, R_3))$ is given in Fig. 3-3. It has full rank, and $x_1 + x_1 \approx^?_E 0$ has the solution $x_1 \mapsto 0$.

More generally, consider the E_2-unification problem

$$x_1 + x_1 \approx^?_{E_2} s^n(0)$$

where $s^n(0) = \underbrace{s(\ldots s}_{n}(0)\ldots)$. In fact, we can see that if n is odd, $E' = E_2 \cup \{x_1 + x_1 \approx s^n(0)\}$ is equivalent to $E_2 \cup \{x_1 + x_1 \approx s(0)\}$, and if n is even, E' is equivalent to $E_2 \cup \{x_1 + x_1 \approx 0\}$.

Example 18. Let $E_4 = \{a(b(b(a(x_1)))) \approx x_1\}$. It is known that E_4 does not have a complete TRS with a finite number of rewrite rules [10]. Consider the E_4-unification problem

$$a(b(x_1)) \approx^?_{E_4} x_1.$$

Then, $E_4 \cup \{a(b(x_1)) \approx x_1\}$ has a complete TRS R_4:

$$a(b(x_1)) \to x_1, \quad b(a(x_1)) \to x_1.$$

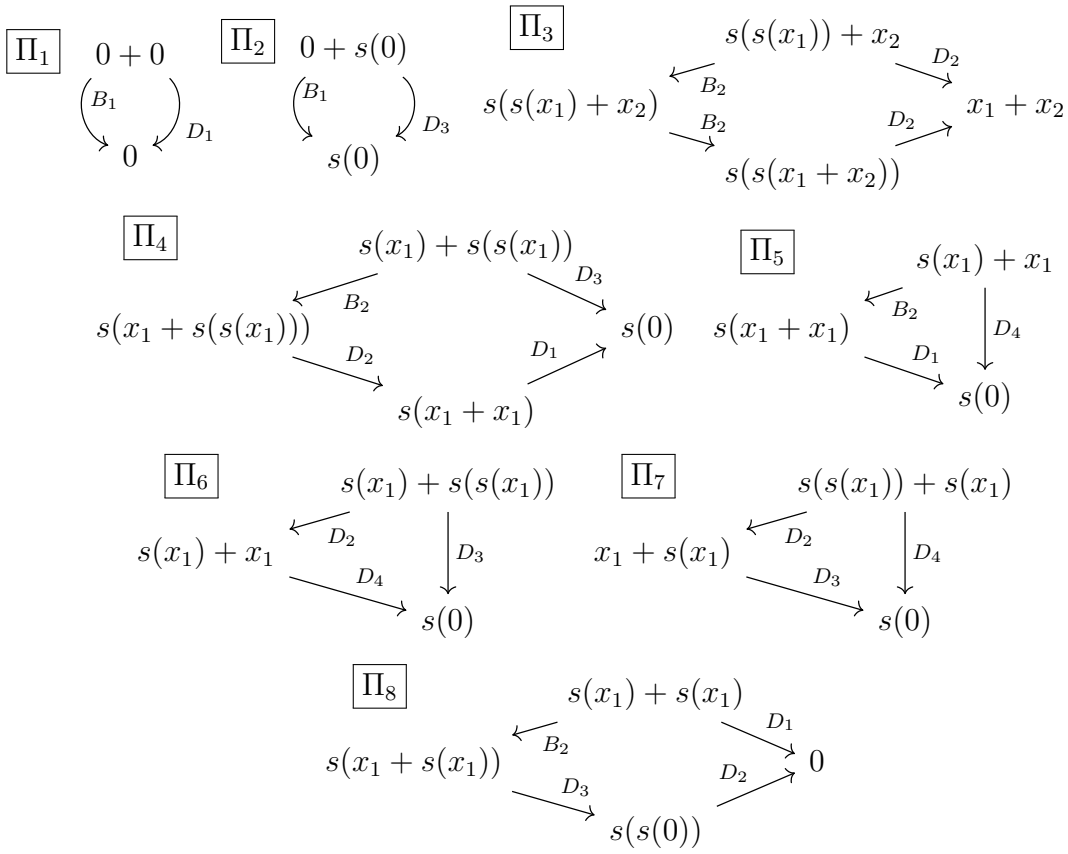


Figure 3-2: Critical pairs of R_3 in Example 17

$$
\begin{array}{c}
 \\
B_1 \\
B_2 \\
D_1 \\
D_2 \\
D_3 \\
D_4
\end{array}
\begin{array}{c}
\begin{array}{ccccccccc|cc}
\Pi_1 & \Pi_2 & \Pi_3 & \Pi_4 & \Pi_5 & \Pi_6 & \Pi_7 & \Pi_8 & \Pi_9 & B_1 & B_2
\end{array} \\
\left(\begin{array}{ccccccccc|cc}
1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\
1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\
0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0
\end{array}\right)
\end{array}
$$

Figure 3-3: The matrix $(D(R_3)|U(E_2, R_3))$. Each element is considered to be in $\mathbb{Z}_2$.

Then, there are two critical pairs

$$a(x_1) \xleftarrow{a(b(x_1))\to x_1} a(b(a(x_1))) \xrightarrow{b(a(x_1))\to x_1} a(x_1),$$
$$b(x_1) \xleftarrow{a(b(x_1))\to x_1} b(a(b(x_1))) \xrightarrow{b(a(x_1))\to x_1} b(x_1).$$

It is easy to check that $(D(R_4)|U(E_4, R_4))$ is the 2×3 matrix whose entries are all 1, and so it is not equivalent to $I_{2,3}$. Therefore, $a(b(x_1))$ and x_1 are not E_4-unifiable.

Remark 19. As in Example 18, it can be the case that it is difficult or impossible to find a complete TRS of the given set E of equations, but a complete TRS of $E \cup \{t \approx s\}$ is easy to find. The basic version of narrowing, the main existing tool for E-unification for unspecified E, is applicable when a complete TRS of E is given. So, it is notable that Theorem 14 does not require us to find a complete TRS of E.

Example 20. Recall that the Ackermann function $A : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ is defined as

$$A(0, n) = n + 1,$$
$$A(m + 1, 0) = A(m, 1),$$
$$A(m + 1, n + 1) = A(m, A(m + 1, n)).$$

Here is a question: Is there a pair of natural numbers m, n such that $A(m+1, n+1) = A(m, n)$? To try to answer this question, let us apply Theorem 14. If we directly interpret the definition of the Ackermann function into a set of equations between terms, the set has degree 1 because of the third equation. We can avoid it by

expanding the third equation into

$$\begin{aligned} A(1,1) &= 3, \\ A(m+2,1) &= A(m+1, A(m, A(m,1))), \\ A(m+1,n+2) &= A(m, A(m, A(m+1,n))). \end{aligned}$$

Let E_5 be the set of equations representing the Ackermann function:

$$\begin{aligned} &F_1 : a(0,x_1) \approx s(x_1), \\ &F_2 : a(s(x_1),0) \approx a(x_1,s(0)), \\ &F_3 : a(s(0),s(0)) \approx s(s(s(0))), \\ &F_4 : a(s(s(x_1)),s(0)) \approx a(s(x_1),a(x_1,a(x_1,s(0)))), \\ &F_5 : a(s(x_1),s(s(x_2))) \approx a(x_1,a(x_1,a(s(x_1),x_2))). \end{aligned}$$

Consider the E_5-unification problem

$$a(s(x_1),s(x_2)) \approx^{?}_{E_5} a(x_1,x_2).$$

Then, $E_5 \cup \{a(s(x_1),s(x_2)) \approx a(x_1,x_2)\}$ has the following complete TRS R_5:

$$\begin{aligned} &F_1 : a(0,x_1) \to s(x_1), \\ &G_1 : s(s(x_1)) \to s(x_1), \\ &G_2 : a(s(x_1),x_2) \to a(x_1,x_2), \\ &G_3 : a(x_1,a(x_1,a(x_1,x_2))) \to a(x_1,x_2) \\ &G_4 : a(x_1,s(x_2)) \to a(x_1,x_2). \end{aligned}$$

We can see $\deg(R_5) = 2$. The critical pairs are listed in Fig. 3-4. For the matrix $D(R_5)$, we only need to consider the labeled critical pairs Ξ_1, Ξ_2, and Ξ_3 since the other critical pairs produce columns consisting of 0s or columns matching those produced by Ξ_1, Ξ_2, and Ξ_3. Reducing such columns from $(D(R_5)|U(E_5, R_5))$, we get the matrix (over $\mathbb{Z}_2$)

$$\begin{array}{c|ccc|ccccc} & \Xi_1 & \Xi_2 & \Xi_3 & F_1 & F_2 & F_3 & F_4 & F_5 \\ \hline F_1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ G_1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ G_2 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ G_3 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ G_4 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{array}$$

and we can check it does not have full rank, so it is not equivalent to $I_{5,8}$. Therefore, $a(s(x_1), s(x_2))$ and $a(x_1, x_2)$ are not E_5-unifiable. This means that there is no pair of natural numbers m, n such that $A(m + 1, n + 1) = A(m, n)$.

3.3 Comparison with Narrowing

Narrowing is another syntactic method of solving E-unification problems. For a TRS R, a term s is said to be *narrowable* into a term t if there exist a rule $l \to r \in R$, a context C, and nonvariable term s' such that $s = C[s']$, s' and l are unifiable with the mgu σ, and $t = C[r]\sigma$. (We rename variables in l so that $\mathrm{Var}(l) \cap \mathrm{Var}(s) = \emptyset$.) In that case, we write $s \rightsquigarrow_{\sigma,R} t$. The sequence

$$t_0 \rightsquigarrow_{\sigma_1,R} t_1 \rightsquigarrow_{\sigma_2,R} \cdots \rightsquigarrow_{\sigma_n,R} t_n$$

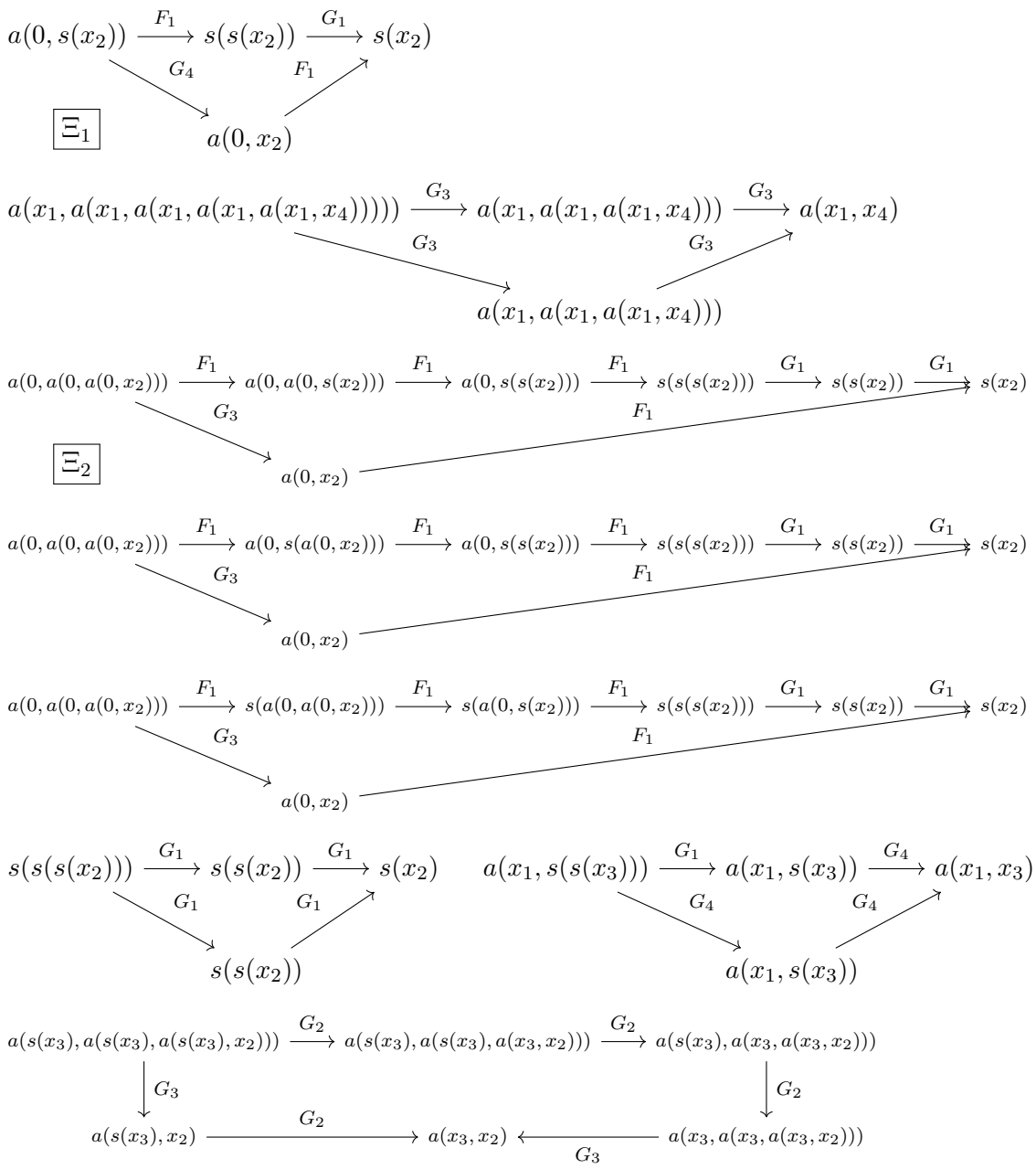


Figure 3-4: Critical pairs of R_5

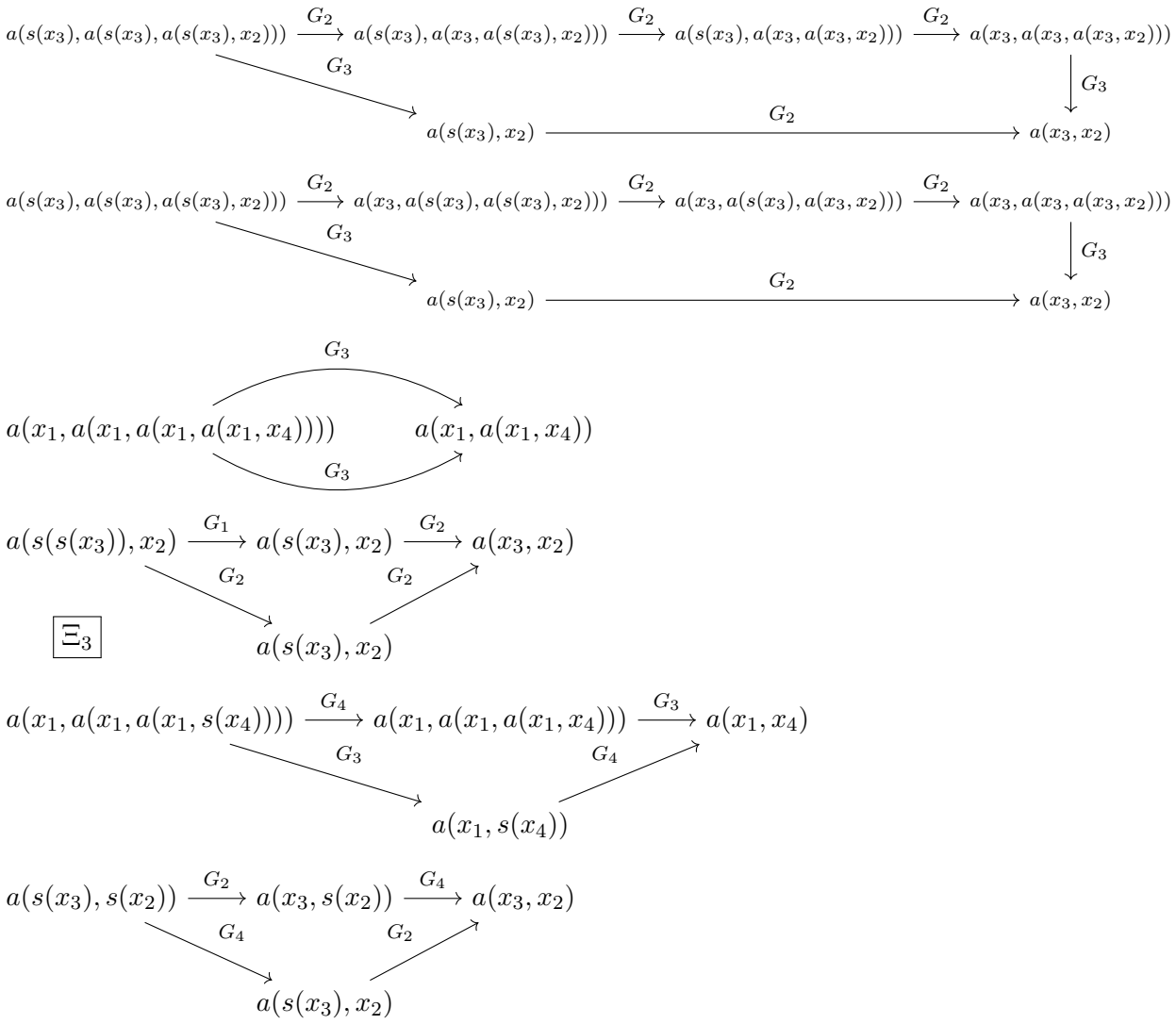


Figure 3-4: Critical pairs of R_5 (cont.)

is abbreviated to $t_0 \leadsto^*_{\sigma,R} t_n$ for $\sigma = \sigma_0\sigma_1 \ldots \sigma_n$. For two substitutions σ, θ and a set X of variables, σ is *more general modulo* R *on* X than θ, denoted $\sigma \leq^X_R \theta$, if there exists a substitution τ such that $x\theta \approx_R x\sigma\tau$ for any $x \in X$. Then, it is known that narrowing is a complete procedure for R-unification:

Theorem 21. [6] Suppose that R is complete and let eq be a new symbol with arity 2.

- If $\mathsf{eq}(s,t) \leadsto^*_{\sigma,R} \mathsf{eq}(s',t')$, and s', t' are unifiable with the mgu τ, then s, t are R-unifiable with the unifier $\sigma\tau$.
- If s,t are R-unifiable with a unifier θ, then there exist a narrowing sequence $\mathsf{eq}(s,t) \leadsto^*_{\sigma,R} \mathsf{eq}(s',t')$ and an mgu τ of s', t' such that $\sigma\tau \leq_R^{\mathrm{Var}(\mathsf{eq}(s,t))} \theta$.

Consider Example 15 again. We can say $x_1 + a$ and $x_1 + b$ are not E_1-unifiable since $\mathsf{eq}(x_1 + a, x_1 + b)$ is not narrowable into any term by any rules in E_1.

For Example 16, however, we have an infinite narrowing sequence from $\mathsf{eq}(x_1 + x_1, s(0))$:

$$\begin{aligned}
&\mathsf{eq}(x_1 + x_1, s(0)) \\
&\leadsto_{x_1 \mapsto s(x_1), E_2} \mathsf{eq}(s(x_1 + s(x_1)), s(0)) \\
&\leadsto_{x_1 \mapsto s(x_1), E_2} \mathsf{eq}(s(s(x_1 + s(s(x_1)))), s(0)) \\
&\leadsto_{x_1 \mapsto s(x_1), E_2} \cdots
\end{aligned}$$

so we can see that narrowing is a semi-decision procedure for the problem of equational unification. We can also check narrowing does not terminate for the problem in Example 20. Past work has studied what kind of restriction on a TRS ensures termination of narrowing [1].

Also, Theorem 21 requires R to be complete. Therefore this method cannot be applied to Example 18 since $E_4 = \{a(b(b(a(x_1)))) \approx x_1\}$ does not have any complete TRS.

Chapter 4

Simplicial Homology

As mentioned in the introduction, the proofs of my theorems use the notion of homology. A homology theory is a sequence of algebraic objects associated to another mathematical object. Homology was originally defined for geometric objects, but it was generalized for a variety of structures such as groups or rings. First, we look at the notion of homology for *simplicial complexes*.

The 1-dimensional homology group of a surface consists of equivalence classes loops on the surface. Here, two loops are identified if they can be transformed into each other by stretching, shortening, and wiggling. In this section, we see how such a structure is defined algebraically.

Consider a polygon (possibly with holes) X built from triangles by attaching edges to edges or vertices to vertices (e.g., Fig. 4-1). We call component triangles (gray small triangles in Fig. 4-1) *2-simplices*, edges *1-simplices*, and vertices *0-simplices*. The composed polygons are called *simplicial complexes*. (Simplicial complexes are defined more generally; we can attach line segments, tetrahedra, and their higher-

dimensional counterparts, but we omit the details here.) For two vertices v_0, v_1, we write $[v_0, v_1]$ for the 1-simplex from v_0 to v_1. We think of $[v_1, v_0]$ as the same 1-simplex as $[v_0, v_1]$ but with the opposite orientation. Also, $[v_0, v_1, v_2]$ denotes the 2-simplex with the vertices v_0, v_1, v_2. For an odd permutation $\sigma\colon \{0,1,2\} \to \{0,1,2\}$ (σ is *odd* (resp. *even*) if it is a permutation obtainable from an odd (resp. even) number of two-element swaps), $[v_{\sigma(0)}, v_{\sigma(1)}, v_{\sigma(2)}]$ is considered to have the opposite orientation from $[v_0, v_1, v_2]$. If the permutation σ is even, $[v_0, v_1, v_2]$ and $[v_{\sigma(0)}, v_{\sigma(1)}, v_{\sigma(2)}]$ are identified. For convenience, we write $[v]$ for the 0-simplex v. (Generally, $[v_0, \ldots, v_n]$ is defined for $n > 2$, but we only consider $n \leq 2$ here.) Both X_1 and X_2 in Fig. 4-1 share the same set of 0- and 1-simplices. The complex X_1 has three 2-simplices, and X_2 has one more 2-simplex $[v_1, v_4, v_2]$.

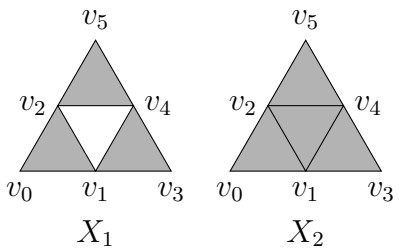


Figure 4-1: examples (X_1) with hole (X_2) without hole

For $n \geq 0$, let $\Delta'_n(X)$ be the set consisting of formal finite sums $\sum r_{\alpha_0,\ldots,\alpha_n}[v_{\alpha_0}, \ldots, v_{\alpha_n}]$ with coefficients $r_{\alpha_0,\ldots,\alpha_n} \in \mathbb{Q}$ where the summation takes all possible $[v_{\alpha_0}, \ldots, v_{\alpha_n}]$ in X, and let $\Delta_n(X)$ be the quotient of $\Delta'_n(X)$ by the relation

$$[v_{\alpha_0}, \ldots, v_{\alpha_n}] = -[v_{\sigma(\alpha_0)}, \ldots, v_{\sigma(\alpha_n)}]$$

for odd permutations σ.[1] For example, $\Delta_2(X_1)$ contains

$$2[v_0, v_1, v_2] + [v_1, v_3, v_4],$$
$$[v_1, v_3, v_4] - \frac{3}{4}[v_2, v_4, v_5],$$
$$\ldots.$$

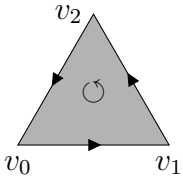
and we have $[v_0, v_1, v_2] = [v_1, v_2, v_0] = [v_2, v_0, v_1] = -[v_1, v_0, v_2] = -[v_2, v_1, v_0] = -[v_0, v_2, v_1]$. The set $\Delta_n(X)$ forms a vector space over $\mathbb{Q}$. For example, $\Delta_2(X_1)$ is a vector space with basis $S = \{[v_0, v_1, v_2], [v_1, v_3, v_4], [v_2, v_4, v_5]\}$, and $\Delta_2(X_2)$ is a vector space with basis $S \cup \{[v_1, v_2, v_4]\}$. Also, $\Delta_{-1}(X)$ is defined as $\{0\}$.

Then, for $n > 0$, we define linear maps $\partial_n^X \colon \Delta_n(X) \to \Delta_{n-1}(X)$, called *boundary maps*, as

$$\partial_n^X([v_0, \ldots, v_n]) = \sum_{i=0}^{n} (-1)^i [v_0, \ldots, \hat{v}_i, \ldots, v_n]$$

where $[v_0, \ldots, \hat{v}_i, \ldots, v_n]$ is shorthand for $[v_0, \ldots, v_{i-1}, v_{i+1}, \ldots, v_n]$. Also, ∂_0 is defined as $\partial_0(c) = 0$ for any $c \in \Delta_0(X)$.

For $n = 2$, the following figure indicates that the map returns the boundary coherently oriented.



$$\partial_2^X([v_0, v_1, v_2]) = [v_1, v_2] - [v_0, v_2] + [v_0, v_1] = [v_1, v_2] + [v_2, v_0] + [v_0, v_1]$$

We can check that $\partial_n^X(\partial_{n+1}^X(c)) = 0$ for any n and $c \in \Delta_{n+1}(X)$ by simple computation. In other words, the vector space $\operatorname{im} \partial_{n+1}^X := \{\partial_{n+1}^X(c) \mid c \in \Delta_{n+1}(X)\}$

[1] Usually, we consider integer coefficients $r_{\alpha_0,\ldots,\alpha_n} \in \mathbb{Z}$, but here we consider rationals because then we can use notions from linear algebra, rather than group or module theory.

is a subspace of $\ker \partial_n := \{c' \in \Delta_n \mid \partial_n^X(c') = 0\}$. The elements of $\ker \partial_n^X$ are called *n-cycles*, and the elements of $\operatorname{im} \partial_{n+1}^X$ are called *n-boundaries*. We can see that any 1-cycles are loops consisting of edges and 1-boundaries are loops that are the boundaries of some regions.

For Fig. 4-1 X_2, $c = [v_1, v_4] + [v_4, v_2] + [v_2, v_1]$ is a 1-cycle and 1-boundary at the same time since $\partial_2([v_1, v_4, v_2]) = c$, but for X_1, c is a 1-cycle but not a 1-boundary. (Note that $[v_2, v_1, v_4]$ is not in $\Delta_2(X_1)$.)

The n-th *(simplicial) homology group* of a simplicial complex X is the quotient $H_n(X) = \ker \partial_n^X / \operatorname{im} \partial_{n+1}^X$. That is, two n-cycles $c_1, c_2 \in \ker \partial_n^X$ are identified in $H_n(X)$ if $c_1 - c_2 \in \operatorname{im} \partial_{n+1}^X$, i.e., $c_1 - c_2$ is a boundary of some region.

Consider $H_1(X)$ for $X = X_1, X_2$. In $H_1(X_2)$, any 1-cycle c is identified with 0. Intuitively, this is because X_2 does not have any hole and so the cycle $c - 0 = c$ is a boundary of some region. So, $H_1(X_2) = \{0\}$. In $H_1(X_1)$, on the other hand, the 1-cycle $c = [v_1, v_4] + [v_4, v_2] + [v_2, v_1]$ is not identified with 0 since c is not a boundary in X_1. Also, c is identified with $c' = [v_1, v_4] + [v_4, v_5] + [v_5, v_2] + [v_2, v_1]$ in $H_1(X_1)$ since $c' - c = [v_4, v_5] + [v_5, v_2] - [v_4, v_2] = \partial_2^{X_1}([v_4, v_5, v_2])$. In fact, any element of $H_1(X_1)$ is represented by rc for some rational r, so $H_1(X_1)$ is isomorphic to $\mathbb{Q}$.

One important fact about simplicial homology groups is invariance: For any two simplicial complexes X, X', if the topological spaces realized by X, X' are homotopy equqivalent, i.e., they can be transformed into each other by stretching, squishing (a line to a point, an area to a line, etc.), and its converse (expanding a point to a line, a line to an area, etc.), then $H_n(X)$ and $H_n(X')$ are isomorphic as groups for any n. For example, the simplicial complex X_3 in Fig. 4-2 realizes the same surface (a triangle) as X_2 in Fig. 4-1 does, so they are trivially homotopic. We can easily see that $\ker \partial_1^{X_3} = \operatorname{im} \partial_2^{X_3} = \{r([v_0, v_1] + [v_1, v_2] + [v_2, v_0]) \mid r \in \mathbb{Q}\}$, so

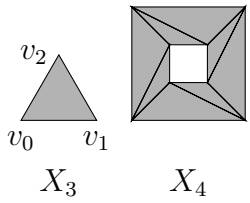


Figure 4-2: More simplicial complexes

Figure 4-3: X_1 and X_4 are homotopic.

$H_1(X_3) = \{0\}$, which is equal to $H_1(X_2)$. Also, X_1 in Fig. 4-1 and X_4 in Fig. 4-2 realize two homotopy equivalent spaces as shown in Fig. 4-3, and we can check that $H_1(X_4) \simeq H_1(X_1) \simeq \mathbb{Q}$.

We write $|X|$ for the topological space realized by the simplicial complex X. Here, we can consider the following questions: (a) Given a simplicial complex X, how many 1-simplices are needed to present a simplicial complex X' such that $|X|$ and $|X'|$ are homotopic? (b) Given a simplicial complex X, how many 1-simplices are needed to present a simplicial complex X' such that $|X|$ and $|X'|$ are homotopic, and X and X' have the same set of 0-simplices? These questions are related to our question about the number of equational axioms/rewrite rules. 0-simplices correspond to symbols, and 1-simplices correspond to axioms/rules. So, question (b) corresponds to our setting since Theorem 7 is about the number of rules over a fixed signature. For simplicial complexes, we can also give inequalities. First, for question (a), the number of 1-simplices is bounded below by $\dim(H_1(X))$. This can be proved as follows: Since a basis of the vector space $\Delta_1(X)$ consists of 1-simplices, and since $\ker \partial_1^X$ is a subspace of $\Delta_1(X)$, we have $\dim \ker \partial_1^X \leq \dim \Delta_1(X)$. Also, since $H_1(X)$ is defined as the quotient $\ker \partial_1^X / \operatorname{im} \partial_2^X$, $\dim H_1(X) \leq \dim \ker \partial_1^X$. Using the invariance of $H_n(X)$, we can see that for any simplicial complex X' such that $|X|$ and $|X'|$ are homotopic, the number of 1-simplices, which equals $\dim \Delta_1(X')$, is bounded below

by $\dim H_1(X) = \dim H_1(X')$. We can improve the inequality for question (b). We use two lemmas from linear algebra.

Lemma 22. For two vector spaces V, W, $\dim V/W = \dim V - \dim W$.

Lemma 23 (Rank-Nullity Theorem)**.** For a linear map $f\colon V \to W$ between vector spaces V, W, $\dim \ker f + \dim \operatorname{im} f = \dim V$.

By these lemmas, we have $\dim H_1(X) - \dim H_0(X) = \dim \ker \partial_1 - \dim \operatorname{im} \partial_2 - \dim \ker \partial_0 + \dim \operatorname{im} \partial_1 = \dim \Delta_1(X) - \dim \operatorname{im} \partial_2 - \dim \ker \partial_0$. Also, since ∂_0 is defined as $\partial_0(c) = 0$ for any c, $\ker \partial_0 = \Delta_0(X)$. Therefore, we have

$$\#(\text{1-simplices}) \geq \dim H_1(X) - \dim H_0(X) + \#(\text{0-simplices}). \tag{4.1}$$

In fact, Theorem 7 is an analog of this inequality. For equational theories/TRSs, it is more technical to define the homology groups, but the proof works in a similar way. As stated earlier, there are correspondences between 0-simplices and symbols, and 1-simplices and axioms/rules. We will later see that 2-simplices correspond to critical peaks.

simplicial homology	rewriting
0-simplices (points)	symbols
1-simplices (lines)	axioms/rules
2-simplices (triangles)	critical peaks

Chapter 5

Modules over a Ring

To introduce homology in general setting, we consider the notion of *modules*. Two of the important notions here are *free resolutions* (Definition 35) and *tensor products* (Definition 29), from which we can derive homology groups. For the homology of equational theories, we will generalize them for modules over *ringoids* in the next chapter. Fig. 5-1 shows a dependency graph of mathematical notions towards homology groups of an equational theory.

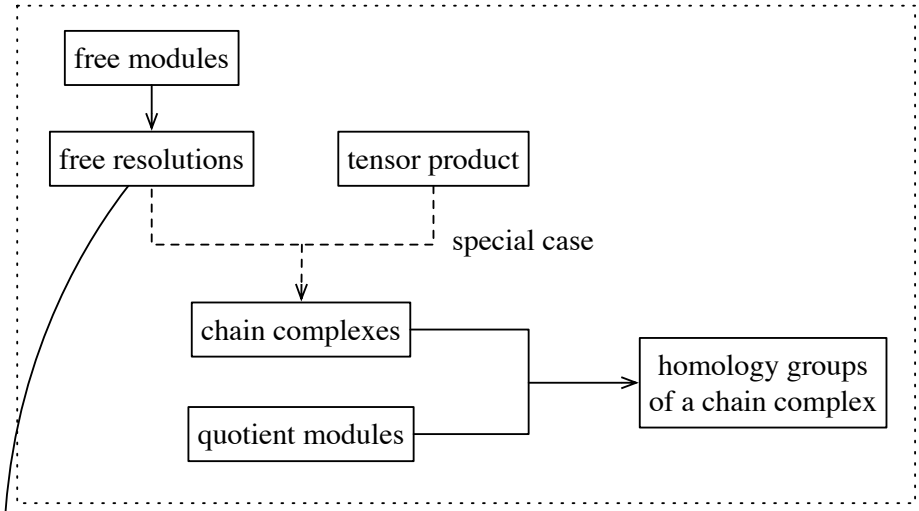
Modules are the generalization of vector spaces in which the set of scalars form a ring, not necessarily a field.

Definition 24. Let $\mathfrak{R}$ be a ring and $(M, +)$ be an abelian group. For a map $\cdot : \mathfrak{R} \times M \to M$, $(M, +, \cdot)$ is a *left* $\mathfrak{R}$*-module* if for all $r, s \in \mathfrak{R}$ and $x, y \in M$, we have

$$r \cdot (x + y) = r \cdot x + r \cdot y,\ (r + s) \cdot x = r \cdot x + s \cdot x,\ (rs) \cdot x = r \cdot (s \cdot x)$$

where rs denotes the multiplication of r and s in $\mathfrak{R}$. We call the map $\cdot$ *scalar multiplication*.

Chapter 5 for rings and Chapter 6 for ringoids



Chapter 6

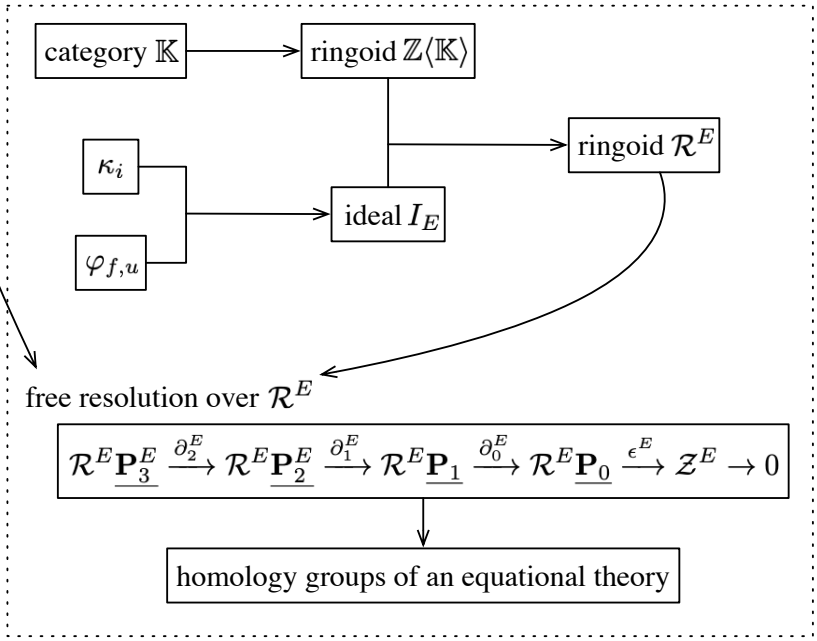


Figure 5-1: Dependency graph

For a map $\cdot : M \times \mathfrak{R} \to M$, $(M, +, \cdot)$ is a *right* $\mathfrak{R}$-*module* if for any $r, s \in \mathfrak{R}$ and $x, y \in M$,

$$(x + y) \cdot r = x \cdot r + y \cdot r,\ x \cdot (r + s) = x \cdot r + x \cdot s,\ x \cdot (sr) = (x \cdot s) \cdot r.$$

If ring $\mathfrak{R}$ is commutative, we do not distinguish between left $\mathfrak{R}$-modules and right $\mathfrak{R}$-modules and simply call them $\mathfrak{R}$-modules.

Linear maps and isomorphisms of modules are also defined in the same way as for vector spaces.

Definition 25. For two left $\mathfrak{R}$-modules $(M_1, +_1, \cdot_1), (M_2, +_2, \cdot_2)$, a group homomorphism $f : (M_1, +_1) \to (M_2, +_2)$ is an $\mathfrak{R}$-*linear map* if it satisfies $f(r \cdot_1 x) = r \cdot_2 f(x)$ for any $r \in \mathfrak{R}$ and $x \in M_1$. An $\mathfrak{R}$-linear map f is an *isomorphism* if it is bijective, and two modules are called *isomorphic* if there exists an isomorphism between them.

Example 26. Any abelian group $(M, +)$ is a $\mathbb{Z}$-module under the scalar multiplication $n \cdot x = \underbrace{x + \cdots + x}_{n}$ for $n \geq 0$.

Example 27. For any ring $\mathfrak{R}$, the direct product $\mathfrak{R}^n = \underbrace{\mathfrak{R} \times \cdots \times \mathfrak{R}}_{n}$ forms a left $\mathfrak{R}$-module under the scalar multiplication $r \cdot (r_1, \ldots, r_n) = (rr_1, \ldots, rr_n)$.

Example 28. Let $\mathfrak{R}$ be a ring and X be a set. $\mathfrak{R}\underline{X}$ denotes the set of formal linear combinations

$$\sum_{x \in X} r_x \underline{x} \quad (r_x \in \mathfrak{R})$$

where $r_x = 0$ except for finitely many xs. The underline is added to emphasize a distinction between $r \in \mathfrak{R}$ and $x \in X$. $\mathfrak{R}\underline{X}$ forms a left $\mathfrak{R}$-module under the addition

and the scalar multiplication defined by

$$\left(\sum_{x\in X} r_x\underline{x}\right)+\left(\sum_{x\in X} s_x\underline{x}\right)=\sum_{x\in X}(r_x+s_x)\underline{x},\quad s\cdot\left(\sum_{x\in X} r_x\underline{x}\right)=\sum_{x\in X}(sr_x)\underline{x}.$$

If X is the empty set, $\mathfrak{R}\underline{X}$ is the left $\mathfrak{R}$-module $\{0\}$ consisting of only the identity element. We simply write 0 for $\{0\}$. $\mathfrak{R}\underline{X}$ is called the *free left $\mathfrak{R}$-module generated by X*. If $\#X = n \in \mathbb{N}$, $\mathfrak{R}\underline{X}$ can be identified with $\mathfrak{R}^n$.

A left $\mathfrak{R}$-module M is called *free* if M is isomorphic to $\mathfrak{R}\underline{X}$ for some X. Free modules share some properties with vector spaces. If a left $\mathfrak{R}$-module F is free, there exists a basis (i.e., a subset that is linearly independent and generating) of F. If a free left $\mathfrak{R}$-module F has a basis $(v_1,\ldots,v_n)$, any $\mathfrak{R}$-linear map $f : F \to M$ is uniquely determined if the values $f(v_1),\ldots,f(v_n)$ are specified arbitrarily. Suppose F_1, F_2 are free left $\mathfrak{R}$-modules and $f : F_1 \to F_2$ is an $\mathfrak{R}$-linear map. If F_1 has a basis $(v_1,\ldots,v_n)$ and F_2 has a basis $(w_1,\ldots,w_m)$, the matrix $(a_{ij})_{i=1,\ldots,n,j=1,\ldots,m}$ where a_{ij}s satisfy $f(v_i) = a_{i1}w_1 + \cdots + a_{im}w_m$ for any $i = 1,\ldots,n$ is called a *matrix representation* of f.

If we have a left and a right module, we can construct a group called the *tensor product* of the two modules.

Definition 29. Let N be a right $\mathfrak{R}$-module and M be a left $\mathfrak{R}$-module. Let $F(N\times M)$ be the free abelian group generated by the direct product $N\times M$. The *tensor product* of N and M, denoted by $N\otimes_{\mathfrak{R}} M$, is the quotient group of $F(N\times M)$ by the subgroup generated by the elements of the form

$$(x,y)+(x,y')-(x,y+y'),\ (x,y)+(x',y)-(x+x',y),\ (x\cdot r,y)-(x,r\cdot y)$$

where $x, x' \in N$, $y, y' \in M$, $r \in R$. The equivalence class of (x, y) in $N \otimes_{\mathfrak{R}} M$ is written as $x \otimes y$. (That is, $x \otimes y + x \otimes y' - x \otimes (y + y') = x \otimes y + x' \otimes y - (x + x') \otimes y = (x \cdot r) \otimes y - x \otimes (r \cdot y) = 0$ holds.)

For a right $\mathfrak{R}$-module N and a $\mathfrak{R}$-linear map $f : M \to M'$ between left $\mathfrak{R}$-modules M, M', we write $N \otimes f : N \otimes_{\mathfrak{R}} M \to N \otimes_{\mathfrak{R}} M'$ for the map $(N \otimes f)(a \otimes x) = a \otimes f(x)$. $N \otimes f$ is known to be well-defined and be a group homomorphism.

We define submodules and quotient modules, as in linear algebra.

Definition 30. Let $(M, +, \cdot)$ be a left (resp. right) $\mathfrak{R}$-module. A subgroup N of $(M, +)$ is a *submodule* if for any $x \in N$ and $r \in \mathfrak{R}$, the scalar multiplication $r \cdot x$ (resp. $x \cdot r$) is in N.

For any submodule N, the quotient group M/N is also an $\mathfrak{R}$-module. M/N is called the *quotient module* of M by N.

For submodules and quotient modules, the following basic theorems are known:

Theorem 31 (First isomorphism theorem)**.** [18, Theorem 8.8] Let $(M, +, \cdot), (M', +', \cdot')$ be left (or right) $\mathfrak{R}$-modules, and $f : M \to M'$ be an $\mathfrak{R}$-linear map.

1. The inverse image of 0 by f, $\ker f = \{x \in M \mid f(x) = 0\}$, is a submodule of M.
2. The image of M by f, $\operatorname{im} f = \{f(x) \mid x \in M\}$, is a submodule of M'.
3. The image $\operatorname{im} f$ is isomorphic to $M/\ker f$.

Theorem 32 (Third isomorphism theorem)**.** [18, Theorem 7.10] Let M be a left (or right) $\mathfrak{R}$-module, N be a submodule of M, and L be a submodule of N. Then $(M/L)/(N/L)$ is isomorphic to M/N.

Theorem 33. [18, Theorem 9.8] Let $\mathfrak{R}$ be $\mathbb{Z}$ or $\mathbb{Z}/p\mathbb{Z}$ for some prime p. Every submodule of a free $\mathfrak{R}$-module is free. Moreover, if an $\mathfrak{R}$-module M is isomorphic to $\mathfrak{R}^n$, then every submodule N of M is isomorphic to $\mathfrak{R}^m$ for some $m \leq n$. (In general, this holds for any principal ideal domain $\mathfrak{R}$.)

If p is not prime, a counterexample is given as follows. Consider $\mathbb{Z}/4\mathbb{Z} = \{[0], [1], [2], [3]\}$ as a $\mathbb{Z}/4\mathbb{Z}$-module and let N be its submodule $\{[0], [2]\}$. If there were an isomorphism $f : N \to (\mathbb{Z}/4\mathbb{Z})\underline{X}$ for some set X, the cardinality of $(\mathbb{Z}/4\mathbb{Z})\underline{X}$ must be equal to the cardinality of N, 2. However, it can be seen that $\#(\mathbb{Z}/4\mathbb{Z})\underline{X} = 1 + 3 \cdot \#X$. (For example, if $X = \emptyset$, $(\mathbb{Z}/4\mathbb{Z})\underline{X} = \{0\}$, and if $X = \{\star\}$, $(\mathbb{Z}/4\mathbb{Z})\underline{X} = \{0, [1]\underline{\star}, [2]\underline{\star}, [3]\underline{\star}\}$.)

Let M be a left $\mathfrak{R}$-module. For $S \subset M$, the set $\mathfrak{R}S$ of all elements in M of the form $\sum_{i=1}^{k} r_i s_i$ $(k \in \mathbb{Z}_{\geq 0}, r_i \in \mathfrak{R}, s_i \in S)$ is a submodule of M. If $\mathfrak{R}S = M$, S is called a *generating set* of S and the elements of S are called *generators* of M. Let $S = \{s_i\}_{i \in I}$ be a generating set of M for some indexing set I. For a set $X = \{x_i\}_{i \in I}$, the linear map $\epsilon : \mathfrak{R}\underline{X} \ni x_i \mapsto s_i \in M$ is a surjection from the free module $\mathfrak{R}\underline{X}$. The elements of $\ker \epsilon$, that is, elements $\sum_{x_i \in X} r_i \underline{x_i}$ satisfying $\epsilon(\sum_{x_i \in X} r_i \underline{x_i}) = \sum_{x_i \in X} r_i s_i = 0$, are called *relations* of M.

Now, we introduce one of the most important notions to develop the homology theory of rewriting systems, *free resolutions*. We first start from the following example.

Example 34. Let M be the $\mathbb{Z}$-module defined by

$$\mathbb{Z}\{\underline{a, b, c, d, e}\}/\mathbb{Z}\{\underline{a} + \underline{b} + \underline{c} - \underline{d} - \underline{e},\ 2\underline{b} - \underline{c},\ \underline{a} + 2\underline{c} - \underline{b} - \underline{d} - \underline{e}\}.$$

That is, M is the module of sums $n_1\underline{a} + n_2\underline{b} + n_3\underline{+}n_4\underline{d} + n_5\underline{e}$ with relations

$$\underline{a} + \underline{b} + \underline{c} - \underline{d} - \underline{e} = 0,\ 2\underline{b} - \underline{c} = 0,\ \underline{a} + 2\underline{c} - \underline{b} - \underline{d} - \underline{e} = 0.$$

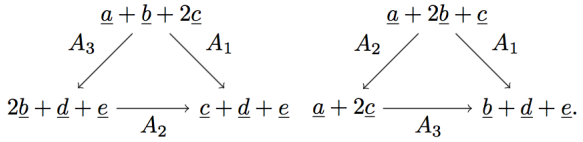
We consider the $\mathbb{Z}$-linear map between free $\mathbb{Z}$-modules $f_0 : \mathbb{Z}^3 \to \mathbb{Z}\underline{\{a, b, c, d, e\}}$ defined by

$$f_0(1,0,0) = \underline{a} + \underline{b} + \underline{c} - \underline{d} - \underline{e},\ f_0(0,1,0) = 2\underline{b} - \underline{c},\ f_0(0,0,1) = \underline{a} + 2\underline{c} - \underline{b} - \underline{d} - \underline{e}.$$

We can see that the image of f_0 is the set of relations of M. In other words, $\operatorname{im} f_0 = \ker \epsilon$ for the linear map $\epsilon : \mathbb{Z}\underline{\{a, b, c, d, e\}} \to M$ which maps each element to its equivalence class. Then, we consider the "relations between relations", that is, triples (n_1, n_2, n_3) which satisfy $f_0(n_1, n_2, n_3) = n_1(\underline{a}+\underline{b}+\underline{c}-\underline{d}-\underline{e})+n_2(2\underline{b}-\underline{c})+n_3(\underline{a}+2\underline{c}-\underline{b}-\underline{d}-\underline{e}) = 0$, or equivalently, elements of $\ker f_0$. We can check $\ker f_0 = \{m(-1,1,1) \mid m \in \mathbb{Z}\}$. This fact can be explained in terms of rewriting modulo AC (associativity and commutativity). Let $\mathrm{AC} = \{(x_1 + x_2) + x_3 \approx x_1 + (x_2 + x_3),\ x_1 + x_2 \approx x_2 + x_1\}$. A rewrite rule $l \to r$ *AC-rewrites* a term t into s if there exists t' such that $t \approx_{\mathrm{AC}} t'$ and $l \to r$ rewrites t' into s. If we write relations in the form of rewrite rules

$$A_1.\ \underline{a} + \underline{b} + \underline{c} \to \underline{d} + \underline{e},\ A_2.\ 2\underline{b} \to \underline{c},\ A_3.\ \underline{a} + 2\underline{c} \to \underline{b} + \underline{d} + \underline{e},$$

we see $\{A_1, A_2, A_3\}$ is a complete AC-rewriting system (over the signature $\{\underline{a}, \underline{b}, \underline{c}, \underline{d}, \underline{e}, +\}$) with two joinable critical pairs



We associate these critical pairs with an equality between formal sums $A_2 + A_3 = A_1$,

and it corresponds to

$$f_0(-1,1,1) = \underbrace{-(\underline{a}+\underline{b}+\underline{c}-\underline{d}-\underline{e})}_{-A_1} + \underbrace{(2\underline{b}-\underline{c})}_{A_2} + \underbrace{(\underline{a}+2\underline{c}-\underline{b}-\underline{d}-\underline{e})}_{A_3} = 0.$$

In fact, this correspondence between critical pairs and "relations between relations" is a key to the homology theory of TRSs.

We define a linear map $f_1 : \mathbb{Z} \to \mathbb{Z}^3$ by $f_1(1) = (-1,1,1)$ and then f_1 satisfies $\operatorname{im} f_1 = \ker f_0$. We can go further, that is, we can consider $\ker f_1$, but it clearly turns out that $\ker f_1 = 0$.

We encode the above information in the following diagram:

$$\mathbb{Z} \xrightarrow{f_1} \mathbb{Z}^3 \xrightarrow{f_0} \mathbb{Z}\underline{\{a,b,c,d,e\}} \xrightarrow{\epsilon} M \tag{5.1}$$

where $\operatorname{im} f_1 = \ker f_0, \operatorname{im} f_0 = \ker \epsilon$ and ϵ is surjective. Sequences of modules and linear maps with these conditions are called free resolutions:

Definition 35. A sequence of left $\mathfrak{R}$-modules and $\mathfrak{R}$-linear maps

$$\cdots \xrightarrow{f_{i+1}} M_{i+1} \xrightarrow{f_i} M_i \xrightarrow{f_{i-1}} \cdots$$

is called an *exact sequence* if $\operatorname{im} f_i = \ker f_{i-1}$ holds for any i.

Let M be a left $\mathfrak{R}$-module. For infinite sequence of free modules F_i and linear maps $f_i : F_{i+1} \to F_i$, $\epsilon : F_0 \to M$, if the sequence

$$\cdots \xrightarrow{f_1} F_1 \xrightarrow{f_0} F_0 \xrightarrow{\epsilon} M$$

is exact and ϵ is surjective, the sequence above is called a *free resolution* of M. If

the sequence is finite, it is called a *partial free resolution*.

(Exact sequences and free resolutions are defined for right $\mathfrak{R}$-modules in the same way.)

Notice that the exact sequence (5.1) can be extended to the infinite exact sequence

$$\cdots \to 0 \to \cdots \to 0 \to \mathbb{Z} \xrightarrow{f_1} \mathbb{Z}^3 \xrightarrow{f_0} \mathbb{Z}\underline{\{a,b,c,d,e\}} \xrightarrow{\epsilon} M$$

since $\ker f_1 = 0$. Thus, the sequence (5.1) is a free resolution of M.

As there are generally several rewriting systems equivalent to a given equational theory, free resolutions of M are not unique. However, we can construct a type of homology constructed from a (partial) free resolution of M which does not depend on the choice of the free resolution.

Let $\cdots \xrightarrow{f_1} F_1 \xrightarrow{f_0} F_0 \xrightarrow{\epsilon} M$ be a free resolution of a left $\mathfrak{R}$-module M. For a right $\mathfrak{R}$-module N, we consider the sequence

$$\cdots \xrightarrow{N\otimes f_1} N \otimes_{\mathfrak{R}} F_1 \xrightarrow{N\otimes f_0} N \otimes_{\mathfrak{R}} F_0. \tag{5.2}$$

Then, it can be shown that $\mathrm{im}(N \otimes f_i) \subset \ker(N \otimes f_{i-1})$ for any $i = 1, 2, \ldots$. In general, a sequence $\cdots \xrightarrow{f_{i+1}} M_{i+1} \xrightarrow{f_i} M_i \xrightarrow{f_{i-1}} \cdots$ of left/right $\mathfrak{R}$-modules satisfying $\mathrm{im}\, f_i \subset \ker f_{i-1}$ for any i is called a *chain complex*. The homology groups of a chain complex are defined to be the quotient group of $\ker f_{i-1}$ by $\mathrm{im}\, f_i$:

Definition 36. Let $(C_\bullet, f_\bullet)$ denote the pair $(\{C_i\}_{i=0,1,\ldots}, \{f_i : C_{i+1} \to C_i\}_{i=0,1,\ldots})$. For a chain complex $\cdots \xrightarrow{f_{i+1}} C_{i+1} \xrightarrow{f_i} C_i \xrightarrow{f_{i-1}} \cdots$, the abelian group $H_j(C_\bullet, f_\bullet)$ defined by

$$H_j(C_\bullet, f_\bullet) = \ker f_{j-1} / \mathrm{im}\, f_j$$

is called the *j-th homology group* of the chain complex $(C_\bullet, f_\bullet)$.

Note that the simplicial homology group is the homology group of the chain complex $(\Delta_n(X), \partial_n)$.

The theorem below shows that the homology groups of the chain complex of the form (5.2) depend only on M, N, and $\mathfrak{R}$:

Theorem 37. [17, Corollary 6.21] Let M be a left $\mathfrak{R}$-module and N be a right $\mathfrak{R}$-module. For any two resolutions $\cdots \xrightarrow{f_1} F_1 \xrightarrow{f_0} F_0 \xrightarrow{\epsilon} M$, $\cdots \xrightarrow{f_1'} F_1' \xrightarrow{f_0'} F_0' \xrightarrow{\epsilon} M$, we have a group isomorphism

$$H_j(N \otimes_{\mathfrak{R}} F_\bullet, N \otimes f_\bullet) \cong H_j(N \otimes_{\mathfrak{R}} F_\bullet', N \otimes f_\bullet').$$

We end this section by giving some basic facts on exact sequences.

Proposition 38. [18, Proposition 7.20 and 7.21]

1. $M_2 \xrightarrow{f} M_1 \to 0$ is exact if and only if $\ker f = 0$.

2. $0 \to M_2 \xrightarrow{f} M_1$ is exact if and only if $\operatorname{im} f = M_1$.

3. If M_1 is a submodule of M_2, the sequence $0 \to M_2 \xrightarrow{\iota} M_1 \xrightarrow{\pi} M_1/M_2 \to 0$ is exact where ι is the inclusion map $\iota(x) = x$ and π is the projection $\pi(x) = [x]$.

Proposition 39. Suppose we have an exact sequence of $\mathfrak{R}$-modules $0 \to M_1 \to M_2 \to M_3 \to 0$. If M_3 is free, then M_2 is isomorphic to $M_1 \times M_3$.

The proof is given by using [18, Proposition 7.22].

5.1 Homology of Equational Theories

In this section, we will briefly see the homology theory of algebraic theories, which is the main tool to obtain our lower bounds.

We fix a signature Σ. Let $t = \langle t_1, \ldots, t_n \rangle$ be a n-tuple of terms and suppose that for each t_i, the set of variables in t_i is included in $\{x_1, \ldots, x_m\}$. For an m-tuple of term $s = \langle s_1, \ldots, s_m \rangle$, we define the composition of t and s by

$$t \circ s = \langle t_1[s_1/x_1, \ldots, s_m/x_m], \ldots, t_n[s_1/x_1, \ldots, s_m/x_m] \rangle$$

where $t_i[s_1/x_1, \ldots, s_m/x_m]$ denotes the term obtained by substituting s_j for x_j in t_i for each $j = 1, \ldots, m$ in parallel. (For example, $f(x_1, x_2)[g(x_2)/x_1, g(x_1)/x_2] = f(g(x_2), g(x_1))$.) By this definition, we can think of any m-tuple $\langle s_1, \ldots, s_m \rangle$ of terms as a (parallel) substitution $\{x_1 \mapsto s_1, \ldots, x_m \mapsto s_m\}$. Recall that, for a TRS R, the reduction relation $\to_R$ between terms is defined as $t_1 \to_R t_2 \iff t_1 = C[l \circ s],\ t_2 = C[r \circ s]$ for some single-hole context C, m-tuple s of terms, and rewrite rule $l \to r \in R$ whose variables are included in $\{x_1, \ldots, x_m\}$. This definition suggests that the pair of a context C and an m-tuple of terms (or equivalently, substitution) s is useful to think about rewrite relations. Malbos and Mimram [13] called the pair of a context and an m-tuple of terms a *bicontext*. For a bicontext (C, t) and a rewrite rule A, we call the triple (C, A, t) a *rewriting step*. The pair of two rewriting steps $(\Box, l_1 \to r_1, s), (C, l_2 \to r_2, t)$ is called a *critical pair* if the pair $(r_1 \circ s, C[r_2 \circ t])$ of terms is a critical pair in the usual sense given by $l_1 \to r_1$, $l_2 \to r_2$.

We write $\mathbb{K}(n, m)$ $(n, m \in \mathbb{N})$ for the set of bicontexts (C, t) where $t = \langle t_1, \ldots, t_n \rangle$ and each t_i and C have variables in $\{x_1, \ldots, x_m\}$ (except $\Box$ in C). The composition of two bicontexts $(C, t) \in \mathbb{K}(n, k)$, $(D, s) \in \mathbb{K}(m, n)$ $(t = \langle t_1, \ldots, t_n \rangle,\ s = \langle s_1, \ldots, s_m \rangle)$

is defined by

$$(C,t) \circ (D,s) = (C[D \circ t], s \circ t) \in \mathbb{K}(m,k)$$

where $D \circ t = D[t_1/x_1, \ldots, t_n/x_n]$, and note that the order of composition is reversed in the second component. We can check that this composition is associative, that is, for any $(C,t) \in \mathbb{K}(n,k)$, $(D,s) \in \mathbb{K}(m,n)$, $(E,r) \in \mathbb{K}(l,m)$, $(C,t) \circ ((D,s) \circ (E,r)) = ((C,t) \circ (D,s)) \circ (E,r)$. Also, the bicontext $(\Box, \langle x_1, \ldots, x_m \rangle)$ is a unit in the sense that $(C,t) \circ (\Box, \langle x_1, \ldots, x_m \rangle) = (C,t)$, $(\Box, \langle x_1, \ldots, x_m \rangle) \circ (D,s) = (D,s)$ for any $(C,t) \in \mathbb{K}(n,k)$, $(D,s) \in \mathbb{K}(l,m)$. From these facts, we can see that there is a category whose objects are natural numbers and morphisms from n to k are bicontexts in $\mathbb{K}(n,k)$.

To apply homological algebra to TRSs, we construct an algebraic structure from bicontexts. For two natural numbers n, m, we define $\mathbb{Z}\langle\mathbb{K}\rangle(n,m)$ to be the free abelian group generated by $\mathbb{K}(n,m)$ (i.e., any element in $\mathbb{Z}\langle\mathbb{K}\rangle(n,m)$ is written as a formal sum $\sum_{(C,t)\in\mathbb{K}(n,m)} \lambda_{(C,t)}(C,t)$ where each $\lambda_{(C,t)}$ is in $\mathbb{Z}$ and is equal to 0 except for finitely many (C,t)s.) Then, the composition $\circ : \mathbb{K}(n,m) \times \mathbb{K}(k,n) \to \mathbb{K}(k,m)$ can be extended to $\circ : \mathbb{Z}\langle\mathbb{K}\rangle(n,m) \times \mathbb{Z}\langle\mathbb{K}\rangle(k,n) \to \mathbb{Z}\langle\mathbb{K}\rangle(k,m)$ by

$$\left(\sum_{(C,t)} \lambda_{(C,t)}(C,t)\right) \circ \left(\sum_{(D,s)} \mu_{(D,s)}(D,s)\right) = \sum_{(C,t)} \sum_{(D,s)} \lambda_{(C,t)}\mu_{(D,s)}((C,t) \circ (D,s)).$$

This family of free abelian groups forms a structure called *ringoid*.

Definition 40. A *ringoid* $\mathcal{R}$ is a small **Ab**-enriched category. That is, the set $\hom_{\mathcal{R}}(a,b)$ of morphisms from a to b for each pair of objects a, b is equipped with abelian group structure $(\hom_{\mathcal{R}}(a,b), +, 0)$ and satisfies the following rules.

$$0 \circ x = 0, \quad x \circ 0 = 0, \quad z \circ (x+y) = z \circ x + z \circ y, \quad (z+w) \circ x = z \circ x + w \circ x$$

where $x, y \in \hom_{\mathcal{R}}(a, b), z, w \in \hom_{\mathcal{R}}(b, c)$.

A ringoid can be thought of as a "many-sorted" ring. If a ringoid has just a single object, its morphisms form a ring with addition $+$ and multiplication $\circ$. If a ringoid has multiple objects, each object can be thought of as a sort. The addition of two morphisms $x : a_1 \to b_1$, $y : a_2 \to b_2$ is defined only if $a_1 = a_2$ and $b_1 = b_2$. Also, we can multiply them as composition $y \circ x$ only if $b_1 = a_2$. The notion of modules over a ring is extended to modules over a ringoid.

Definition 41. Let $\mathcal{R}$ be a ringoid.

- A left $\mathcal{R}$-module is a functor $M : \mathcal{R} \to \mathbf{Ab}$ satisfying $M(x + y) = M(x) + M(y)$, $M(0) = 0$ for any $x, y \in \mathcal{R}(a, b)$, $a, b \in \mathrm{Obj}\,(\mathcal{R})$). We define the scalar multiplication $\cdot : \mathcal{R}(a, b) \times M(a) \to M(b)$ as $a \cdot m = M(a)(m)$.

- A right $\mathcal{R}$-module is a left $\mathcal{R}^{\mathrm{op}}$-module.

- For two left $\mathcal{R}$-modules M_1, M_2, an $\mathcal{R}$-linear map $f : M_1 \to M_2$ is a natural transformation. (We can define an $\mathcal{R}$-linear map between right $\mathcal{R}$-modules in the same manner.)

Definition 42. Let $\mathcal{R}$ be a ringoid whose objects are natural numbers, and P be a family of sets P_i $(i \in \mathbb{N})$. The free left $\mathcal{R}$-module generated by P, denoted by $\mathcal{R}\underline{P}$, is defined as follows. For each $i \in \mathbb{N}$, $(\mathcal{R}\underline{P})(i)$ is the abelian group of formal finite sums

$$\sum_{p_j \in P_j,\ j \in \mathbb{N}} a_{p_j} \underline{p_j}, \quad (a_{p_j} \in \mathcal{R}(j, i))$$

and for each $r \in \mathcal{R}(i,k)$,

$$r \cdot \left(\sum_{p_j \in P_j,\ j \in \mathbb{N}} a_{p_j} \underline{p_j} \right) = \sum_{p_j \in P_j,\ j \in \mathbb{N}} (r \circ a_{p_j}) \underline{p_j}.$$

If a left $\mathcal{R}$-module M is isomorphic to $\mathcal{R}\underline{P}$ for some P, we say that M is free.

For $\mathbb{Z}\langle\mathbb{K}\rangle$, we write $C\underline{x}t$ for elements of $((\mathbb{Z}\langle\mathbb{K}\rangle)\underline{P})(X)$ instead of $(C,t)\underline{x}$, and $(D+C)\underline{x}t$ for $D\underline{x}t + C\underline{x}t$.

To define the tensor product of two modules over a ringoid, we introduce some notions.

Definition 43. For a family of abelian groups $\{G_X \mid X \in P\}$ for some indexing set P, its direct sum, denoted by $\bigoplus_{X \in P} G_X$, is the subset of the direct product defined by $\{(g_X)_{X \in P} \in \prod_{X \in P} G_X \mid g_X = 0 \text{ except for finite } X\text{s}\}$. The direct sum of groups also forms a group.

Definition 44. For categories A, B, C, let $F\colon A^{\mathrm{op}} \times A \to C$ be a functor, and c be an object of C. A family of morphisms $\eta(a)\colon F(a,a) \to c$ is a *extranatural transformation* if for any morphism $g\colon a \to a'$ in A, the following diagram commutes:

$$\begin{array}{ccc} F(a',a) & \xrightarrow{F(\mathrm{id},f)} & F(a',a') \\ \Big\downarrow{\scriptstyle F(g,\mathrm{id})} & & \Big\downarrow{\scriptstyle \eta(a')} \\ F(a,a) & \xrightarrow{\eta(a)} & c. \end{array}$$

Definition 45. Let $\mathcal{R}$ be a ringoid, M_1 be a right $\mathcal{R}$-module, and M_2 be a left $\mathcal{R}$-module. An abelian group $M_1 \otimes_{\mathcal{R}} M_2$ is the *tensor product* of M_1, M_2 if there is an extranatural transformation $\zeta : M_1(-) \otimes M_2(-) \to M_1 \otimes_{\mathcal{R}} M_2$ such that for any abelian group A and any extranatural transformation $\gamma : M_1(-) \otimes M_2(-) \to A$, there

exists a unique abelian group homomorphism $\phi : M_1 \otimes_{\mathcal{R}} M_2 \to A$ with $\gamma_a = \phi \circ \zeta_a$ for any $a \in \mathrm{Obj}\,(\mathcal{R})$.

Explicitly, the tensor product $M_1 \otimes_{\mathcal{R}} M_2$ is the quotient abelian group of $\bigoplus_{X \in \mathcal{R}} M_1(X) \otimes_{\mathbb{Z}} M_2(X)$ by relations $(x \cdot a) \otimes y - x \otimes (a \cdot y)$ for all $a \in \mathcal{R}(Y, X)$, $x \in M(X), y \in M(Y)$.

We define an equivalence between two TRSs (Σ, R), (Σ', R'), called *Tietze equivalence*.

Definition 46. Two TRSs are *Tietze equivalent* if one is obtained from the other by applying a series of *Tietze transformations* defined as follows:

1. If $f^{(n)}$ is a symbol not in Σ and $t \in T(\Sigma)$ has variables in $\{x_1, \ldots, x_n\}$, then (Σ, R) can be transformed into $(\Sigma \cup \{f\}, R \cup \{t \to f(x_1, \ldots, x_n)\})$.

2. If $t \to f(x_1, \ldots, x_n) \in R$, $t \in T(\Sigma \setminus \{f\})$, and f does not occur in any rule in $R' = R \setminus \{t \to f(x_1, \ldots, x_n)\}$, then (Σ, R) can be transformed into $(\Sigma \setminus \{f\}, R')$.

3. If $t \overset{*}{\leftrightarrow}_R s$, then (Σ, R) can be transformed into $(\Sigma, R \cup \{t \to s\})$.

4. If $t \to s \in R$ and $t \overset{*}{\leftrightarrow}_{R'} s$ for $R' = R \setminus \{t \to s\}$, then (Σ, R) can be transformed into (Σ, R').

With rule 1, we can add a new symbol, and with rule 2, we can remove a redundant symbol. Rules 3 and 4 can be used to add/remove a redundant rule.

We can see that any two TRSs (Σ, R_1),(Σ, R_2) with finite number of rewrite rules are Tietze equivalent if they are equivalent in the usual sense, $\overset{*}{\leftrightarrow}_{R_1} = \overset{*}{\leftrightarrow}_{R_2}$. Tietze equivalence was originally introduced in group theory [23, §11] and is also defined for monoids [3, 7.2].

Example 47. Consider the signature $\Sigma = \{+^{(2)}, S^{(1)}, 0^{(0)}\}$ and the set R of four rules

$$0 + x \to x,\ x + 0 \to x,\ S(x) + y \to S(x + y),\ (x + y) + z \to x + (y + z).$$

We can see (Σ, R) is Tietze equivalent to (Σ', R') where

$$\Sigma' = \{+^{(2)}, 0^{(0)}, 1^{(0)}\},\ R' = \{0 + x \to x,\ x + 0 \to x,\ (x + y) + z \to x + (y + z)\}$$

as follows:

$$\begin{aligned}
(\Sigma, R) &\xrightarrow{(1)} (\Sigma \uplus \{1^{(0)}\}, R \uplus \{S(0) \to 1\}) \\
&\xrightarrow{(3)} (\Sigma \uplus \{1^{(0)}\}, R \uplus \{S(0) \to 1,\ 1 + x \to S(x)\}) \\
&\xrightarrow{(4)} (\Sigma \uplus \{1^{(0)}\}, R \uplus \{1 + x \to S(x)\}) \\
&\xrightarrow{(4)} (\Sigma \uplus \{1^{(0)}\}, R \uplus \{1 + x \to S(x)\} \setminus \{S(x) + y \to S(x + y)\}) \\
&\xrightarrow{(2)} (\Sigma \uplus \{1^{(0)}\} \setminus \{S^{(1)}\}, R \setminus \{S(x) + y \to S(x + y)\}) = (\Sigma', R').
\end{aligned}$$

We will define a ringoid $\mathcal{R}^E$ such that any two equivalent sets E, E' of equations give rise to isomorphic ringoids $\mathcal{R}^E \simeq \mathcal{R}^{E'}$ and $\mathcal{R}^E$, and that we can have a "good" partial free resolution over $\mathcal{R}^E$ introduced by Malbos and Mimram.

For a term t and a positive integer i, let $\kappa_i(t)$ be the formal sum of contexts given inductively by

$$\kappa_i(x_i) = \Box, \quad \kappa_i(x_j) = 0 \quad (i \neq j), \quad \kappa_i(f(t_1, \ldots, t_k)) = \sum_{j=1}^{k} f(t_1, \ldots, \underbrace{\Box}_{j\text{th}}, \ldots, t_k)[\kappa_i(t_j)].$$

Application of a formal sum of contexts to a context as appears in the last rule is defined by $C[D_1 + \cdots + D_n] = C[D_1] + \cdots + C[D_n]$. Also, for a term t, symbol $f \in \Sigma^{(n)}$, and n-tuple of terms $u = \langle s_1, \ldots, s_n \rangle$, let $\varphi_{f,u}(t)$ be the formal sum of all contexts C satisfying $C[f(s_1, \ldots, s_n)] = t$.

We define I_E as the ideal of of $\mathbb{Z}\langle\mathbb{K}\rangle$ generated by elements of the form

$$(\kappa_i(s) - \kappa_i(t), w), \quad (\varphi_{f,uv}(t \circ v) - \varphi_{f,uv}(s \circ v) - \varphi_{f,u}(t) \circ v + \varphi_{f,u}(s) \circ v, w), \quad (\Box, w_1) - (\Box, w_2)$$

for any $s \approx_E t, w_1 \approx_E w_2$. Then, define $\mathcal{R}^E$ to be $\mathbb{Z}\langle\mathbb{K}\rangle / I_E$. [1] For a morphism x of $\mathbb{Z}\langle\mathbb{K}\rangle$, we write $[x]^E$ or just $[x]$ for the equivalence class of x in $\mathcal{R}^E$. If we consider the free module $\mathcal{R}^E \underline{P}$ for a family P of sets $P_0, P_1, \ldots$, we write $C_1 \underline{p} u_1 + \cdots + C_k \underline{p} u_k$ for $[(C_1, u_1) + \cdots + (C_k, u_k)]\underline{p} \in \mathcal{R}^E \underline{P}(i)$. By definition, for any E' equivalent to E, $\mathcal{R}^{E'}$ is isomorphic to $\mathcal{R}^E$.

Let $d = \deg(E)$. Consider the right $\mathcal{R}^E$-module that maps any object n to $\mathbb{Z}_d$ and whose scalar multiplication $\cdot : \mathbb{Z}_d \times \mathcal{R}^E(m, n) \to \mathbb{Z}_d$ is given by $[1] \cdot [(C_1, t_1) + \cdots + (C_k, t_k)] = [k]$. We write $\mathbb{Z}_d$ also for this right $\mathcal{R}^E$-module. We show that the scalar multiplication is well-defined. If $C_1 + \cdots + C_k = \kappa_i(s)$ and $D_1 + \cdots + D_{k'} = \kappa_i(t)$ for some $s \approx t$, then $k - k' = \#_i s - \#_i t$ is divisible by d by the definition of $\deg(E)$. Thus, $[1] \cdot [\sum_{i=1}^{k} (C_i, t) - \sum_{i=1}^{k'} (D_i, t)] = [0]$. Also, since the number of bicontexts in $\varphi_{f,u}(t)$ is the number of subterms $f(u)$ in t, for any $l \approx r \in E$, $f \in \Sigma$, $t \in T(\Sigma)$, the linear combination $\varphi_{f,tu}(r \circ t) - \varphi_{f,tu}(l \circ t) - \varphi_{f,u}(r) + \varphi_{f,u}(l)$ consists of da contexts for some nonnegative integer a. Therefore, $[1] \cdot [\varphi_{f,u}(r \circ t) - \varphi_f(l \circ t) - \varphi_{f,u}(r) + \varphi_{f,u}(l)] = [0]$, so the scalar multiplication for $\mathbb{Z}_d$ is well-defined.

[1] For the original definition of $\mathcal{R}^E$ in [13], the generators $\varphi_{f,uv}(t \circ v) - \varphi_{f,uv}(s \circ v) - \varphi_{f,u}(t) \circ v + \varphi_{f,u}(s) \circ v$ was not given. However, we need these generators to prove $\partial_1(\hat{\hat{t}}) = \varphi(\hat{t}) - \varphi(t)$ which is used to show $\partial_1 \circ \partial_2 = 0$ in Appendix A of [13]. We do not need to change the other parts of the proof.

Let X_1 be a singleton set $\{\star\}$, X_i be the empty set for $i = 0$ or $i = 2, 3, \ldots$, and X be the family consisting of X_is. We define a left $\mathcal{R}^E$-module $\mathcal{Z}^E$ to be the quotient $\mathcal{R}^E\underline{X}/N$ where N is the submodule of $\mathcal{R}^E\underline{X}$ generated by $\sum_{i=1}^{m} \kappa_i(u) \circ t \underline{\star} t_i - \Box \underline{\star} \langle u \circ t \rangle$ for every term u with $\mathrm{Var}(u) \subset \{x_1, \ldots, x_m\}$ and m-tuple $t = \langle t_1, \ldots, t_m \rangle$ of terms. The homology groups of equational theories are defined as follows: 1. Take a free resolution of $\mathcal{Z}^E$

$$\cdots \to F_2 \xrightarrow{\partial_1} F_1 \xrightarrow{\partial_0} F_0 \xrightarrow{\epsilon} \mathcal{Z}^E \to 0,$$

2. obtain the chain complex

$$\cdots \to \mathbb{Z}_d \otimes F_2 \xrightarrow{\mathbb{Z}_d \otimes \partial_1} \mathbb{Z}_d \otimes F_1 \xrightarrow{\mathbb{Z}_d \otimes \partial_0} \mathbb{Z}_d \otimes F_0,$$

3. then the homology group $H_i(\Sigma, E)$ is defined as

$$H_i(\Sigma, E) = \ker \partial_{i-1} / \operatorname{im} \partial_i.$$

Theorem 37 can be generalized to modules over ringoids [15], so the homology group $H_i(\Sigma, E)$ only depends on the Tietze-equivalence class of (Σ, E).

We construct a partial free resolution of $\mathcal{Z}^E$

$$\mathcal{R}^E\underline{\mathbf{P}_2^E} \xrightarrow{\partial_1^E} \mathcal{R}^E\underline{\mathbf{P}_1} \xrightarrow{\partial_0^E} \mathcal{R}^E\underline{\mathbf{P}_0} \xrightarrow{\epsilon^E} \mathcal{Z}^E \to 0 \tag{5.3}$$

as follows. First, $\mathbf{P}_0, \mathbf{P}_1$, $\mathbf{P}_2^E$ are families of sets $(\mathbf{P}_0)_j$, $(\mathbf{P}_1)_j$, $(\mathbf{P}_2^E)_j$ given as

$$(\mathbf{P}_0)_j = \begin{cases} \{1\} & (j=1) \\ \emptyset & (j \neq 1) \end{cases}, \quad (\mathbf{P}_1)_j = \Sigma^{(j)} = \{f \in \Sigma \mid f \text{ has arity } j\}$$

$$(\mathbf{P}_2^E)_j = \{l \approx r \in E \mid \mathrm{Var}(l) \cup \mathrm{Var}(r) \subset \{x_1, \ldots, x_j\}\}.$$

Then, we define $\mathcal{R}^E$-linear maps ϵ^E, ∂_0^E, ∂_1^E as

$$\epsilon^E(\underline{1}) = \underline{\star}, \qquad \partial_0^E(\underline{f}) = \sum_{i=1}^{n} f(x_1, \ldots, \underbrace{\square}_{i\text{th}}, \ldots, x_n)\underline{1}\langle x_i \rangle - \underline{1}\langle f(x_1, \ldots, x_n)\rangle,$$

$$\partial_1^E(\underline{l \approx r}) = \varphi(r) - \varphi(l)$$

where $\varphi : \mathrm{Term}(\Sigma) \to \mathcal{R}^E\underline{\mathbf{P}_1}$ is defined inductively as

$$\varphi(x_i) = 0, \quad \varphi(f(t_1, \ldots, t_n)) = \underline{f}\langle t_1, \ldots, t_n\rangle + \sum_{i=1}^{n} f(t_1, \ldots, \underbrace{\square}_{i\text{th}}, \ldots, t_n)\varphi(t_i).$$

For any term t, $\varphi(t)$ can be written as

$$\varphi(t) = \sum_{f,u} \varphi_{f,u}(t)\underline{f}u \tag{5.4}$$

where the sum takes all $f \in \Sigma$ and $\mathrm{ar}(f)$-tuples u of terms.

Lemma 48. For any terms t, s with $t \approx_E s$, context C, and n-tuple v of terms,

$$\varphi(C[t \circ v]) - \varphi(C[s \circ v]) = C\varphi(t)v - C\varphi(s)v. \tag{5.5}$$

Proof.

$$\begin{aligned} C\varphi(t)v - C\varphi(s)v &= C\left(\sum_{f,u} \varphi_{f,u}(t)\underline{f}u - \varphi_{f,u}(s)\underline{f}u\right)v \\ &= C\left(\sum_{f,u} \varphi_{f,u}(t)v\underline{f}uv - \varphi_{f,u}(s)v\underline{f}uv\right) \\ &= C\left(\sum_{f,uv} \varphi_{f,u}(tv)\underline{f}uv - \varphi_{f,uv}(sv)\underline{f}uv\right) \\ &= C\left(\varphi(tv) - \varphi(sv)\right) \end{aligned}$$

□

If there is a complete TRS R of E, we can extend the sequence (5.3) to

$$\mathcal{R}\underline{\mathbf{P}_3^R} \xrightarrow{\partial_2^R} \mathcal{R}\underline{\mathbf{P}_2^R} \xrightarrow{\partial_1^R} \mathcal{R}\underline{\mathbf{P}_1} \xrightarrow{\partial_0^R} \mathcal{R}\underline{\mathbf{P}_0} \xrightarrow{\epsilon^R} \mathcal{Z}^R \to 0. \tag{5.6}$$

Here, $\mathbf{P}_3^R$ is the family of sets $(\mathbf{P}_3^R)_j$ where each $(\mathbf{P}_3^R)_j$ consists of 5-tuples $(l \to r, t, C, l' \to r', t')$ such that

- $l \circ t = C[l' \circ t']$ and $r \circ t \leftarrow l \circ t = C[l' \circ t'] \to C[r' \circ t']$ is a critical peak, and
- either $l \to r$ or $l' \to r'$ is in $(\mathbf{P}_2^R)_j$ and the other is in $(\mathbf{P}_2^R)_k$ for some $k \leq j$.

For such a 5-tuple $\alpha = (l \to r, t, C, l' \to r', t')$, $\partial_2^R(\underline{\alpha})$ is defined as

$$\partial_2^R(\underline{\alpha}) = \underline{l' \to r'}t' - C\underline{l \to r}t + \widehat{\widehat{r' \circ t'}} - \widehat{\widehat{C[r \circ t]}}$$

where $\hat{\hat{s}}$ is defined for any term s as follows. Suppose s is rewritten to its normal

form $\hat{s}$ by rewrite rules $p_1 \to q_1, \ldots, p_k \to q_k \in R$ as

$$s = C_1[p_1 \circ u_1],\ C_1[q_1 \circ u_1] = C_2[p_2 \circ u_2], \ldots, C_{k-1}[q_{k-1} \circ u_{k-1}] = C_k[p_k \circ u_k],\ C_k[q_k \circ u_k] = \hat{s}$$

for some C_is and u_is. Then, $\hat{\hat{s}} = \sum_{i=1}^{k} C_i \underline{p_i \to q_i} u_i$. We will omit the superscript R of $\mathbf{P}_i^R$ and ∂_i^R if there is no confusion.

Theorem 49. [13] If R is a complete TRS, the sequence (5.6) is exact.

The following lemma is useful for the next section.

Lemma 50. Let E be a set of equations with degree d. For any family P of sets $P_0, P_1, \ldots$, we have an abelian group isomorphism $\mathbb{Z}_d \otimes_{\mathcal{R}^E} \mathcal{R}^E \underline{P} \simeq \mathbb{Z}_d \underline{\biguplus P}$ where $\biguplus P$ is the disjoint union of P_is and the right-hand side is the free $\mathbb{Z}_d$-module generated by $\biguplus P$.

Proof. Consider the abelian group homomorphism $\psi : \mathbb{Z}_d \underline{\biguplus P} \to \mathbb{Z}_d \otimes_{\mathcal{R}^E} \mathcal{R}^E \underline{P}, \quad \underline{p} \mapsto 1 \otimes \underline{p}$. Then, ψ is surjective since $1 \otimes C\underline{p}u = 1 \cdot [(C, u)] \otimes \underline{p} = 1 \otimes \underline{p}$ for any $1 \otimes C\underline{p}u \in \mathbb{Z}_d \otimes_{\mathcal{R}^E} \mathcal{R}^E \underline{P}$. Let $\gamma_i : \mathbb{Z}_d \otimes (\mathcal{R}^E \underline{P}(i)) \to \mathbb{Z}_d \underline{\bigcup P}$ be the abelian group homomorphism $1 \otimes C\underline{p}u \mapsto \underline{p}$. We can check that γ_is form an extranatural transformation γ, so we have $\phi : \mathbb{Z}_d \otimes_{\mathcal{R}^E} \mathcal{R}^E \underline{P} \to \mathbb{Z}_d \underline{\biguplus P}$ with $\gamma_i = \phi \circ \zeta_i$ for $\zeta_i : \mathbb{Z}_d \otimes (\mathcal{R}^E \underline{P}(i)) \to \mathbb{Z}_d \otimes_{\otimes} \mathcal{R}^E \underline{P}$. Then, $\phi(\psi(\underline{p})) = \phi(\zeta_i(1 \otimes \underline{p})) = \gamma_i(1 \otimes \underline{p}) = \underline{p}$. Thus, ψ is an isomorphism. □

As special cases of this lemma, we have $\mathbb{Z}_d \otimes_{\mathcal{R}} \mathcal{R}\underline{\mathbf{P}_0} \cong (\mathbb{Z}_d)\underline{\Sigma}$, $\mathbb{Z}_d \otimes_{\mathcal{R}} \mathcal{R}\underline{\mathbf{P}_1} \cong (\mathbb{Z}_d)\underline{R}$, and $\mathbb{Z}_d \otimes_{\mathcal{R}} \mathcal{R}\underline{\mathbf{P}_2} \cong (\mathbb{Z}_d)\underline{\biguplus \mathbf{P}_3^R}$. Additionally, we can see each group homomorphism $\tilde{\partial}_i$ $(i = 0, 1, 2)$ is a $\mathbb{Z}_d$-linear map.

5.2 Lower Bounds

Let (Σ, R) be a complete TRS. In this section, we prove Theorem 7. We first show the following lemma.

Lemma 51. Let $d = \deg(R)$. If $d = 0$ or d is prime, $\#R - e(R) = s(H_2(\Sigma, R)) + s(\operatorname{im} \tilde{\partial}_1)$. (Recall that $s(G)$ is the minimum number of generators of a group G.)

Proof. By definition, $D(R)$ is a matrix representation of $\tilde{\partial}_2$. Suppose d is prime. In this case, $s(H_2(\Sigma, R))$ is equal to the dimension of $H_2(\Sigma, R)$ as a $\mathbb{Z}_d$-vector space. By the rank-nullity theorem, we have

$$\begin{aligned}
\dim(H_2(\Sigma, R)) &= \dim(\ker \tilde{\partial}_1) - \dim(\operatorname{im} \tilde{\partial}_2) \\
&= \dim(\mathbb{Z}_d \otimes_{\mathcal{R}} \mathcal{R}\underline{\mathbf{P}_1}) - \dim(\operatorname{im} \tilde{\partial}_1) - \dim(\operatorname{im} \tilde{\partial}_2) \\
&= \dim((\mathbb{Z}_d)\underline{R}) - \dim(\operatorname{im} \tilde{\partial}_1) - \operatorname{rank}(D(R)) \\
&= \#R - \dim(\operatorname{im} \tilde{\partial}_1) - e(R).
\end{aligned}$$

Suppose $d = 0$. We show $H_2(\Sigma, R) \cong \mathbb{Z}^{\#R-r-k} \times \mathbb{Z}_{e_1} \times \cdots \times \mathbb{Z}_{e_r}$ where $r = \operatorname{rank}(D(R))$, $k = s(\operatorname{im} \tilde{\partial}_1)$, and $e_1, \ldots, e_r$ are the elementary divisors of $D(R)$. Let

$$\overline{\partial}_1 : \mathbb{Z} \otimes_{\mathcal{R}} \mathcal{R}\underline{\mathbf{P}_1} / \operatorname{im} \tilde{\partial}_2 \to \mathbb{Z} \otimes_{\mathcal{R}} \mathcal{R}\underline{\mathbf{P}_0}$$

be the group homomorphism defined by $[x] \mapsto \tilde{\partial}_1(x)$. $\overline{\partial}_1$ is well-defined since $\operatorname{im} \tilde{\partial}_2 \subset \ker \tilde{\partial}_1$, and $\ker \overline{\partial}_1$ is isomorphic to $\ker \tilde{\partial}_1 / \operatorname{im} \tilde{\partial}_2 = H_2(\Sigma, R)$. By taking the basis $v_1, \ldots, v_{\#R}$ of $\mathbb{Z} \otimes_{\mathcal{R}} \mathcal{R}\underline{\mathbf{P}_1} \cong \mathbb{Z}\underline{R}$ such that $D(R)$ is the matrix representation of $\tilde{\partial}_2$ under the basis $v_1, \ldots, v_{\#R}$ and some basis of $\mathbb{Z} \otimes_{\mathcal{R}} \mathcal{R}\underline{\mathbf{P}_2}$, we can see $\mathbb{Z} \otimes_{\mathcal{R}} \mathcal{R}\underline{\mathbf{P}_1} / \operatorname{im} \tilde{\partial}_2 \cong \mathbb{Z}^{\#R-r} \times \mathbb{Z}_{e_1} \times \cdots \times \mathbb{Z}_{e_k}$. Suppose $\overline{\partial}_1(e_i[x]) = 0$ for some x and

$i = 1, \ldots, r$. Since $\overline{\partial}_1$ is a homomorphism, $\overline{\partial}_1(e_i[x]) = e_i\overline{\partial}_1([x]) \in \mathbb{Z} \otimes_{\mathcal{R}} \mathcal{R}\underline{\mathbf{P}_0} \cong \mathbb{Z}\underline{\Sigma}$ holds. Since $\mathbb{Z}\underline{\Sigma}$ is free, we have $[x] = 0$. Therefore, $\ker \overline{\partial}_1$ is included in the subset of $\mathbb{Z} \otimes_{\mathcal{R}} \mathcal{R}\underline{\mathbf{P}_1}/\operatorname{im} \tilde{\partial}_2$ isomorphic to $\mathbb{Z}^{\#R-r} \times \{0\} \times \cdots \times \{0\}$. Thus, $\ker \overline{\partial}_1 \cong \mathbb{Z}^{\#R-r-k} \times \mathbb{Z}_{e_1} \times \cdots \times \mathbb{Z}_{e_r}$.

Let G be $\mathbb{Z}^{\#R-r-k} \times \mathbb{Z}_{e_{e(R)+1}} \times \cdots \mathbb{Z}_{e_r}$. Since $\mathbb{Z}_e$ is a trivial group if e is invertible, $\mathbb{Z}^{\#R-r-k} \times \mathbb{Z}_{e_1} \times \cdots \times \mathbb{Z}_{e_k} \cong G$. The group G is generated by $(\underbrace{1, 0, \ldots, 0}_{\#R-r-k}, \underbrace{[0], \ldots, [0]}_{r-e(R)})$, $\ldots, (0, \ldots, 0, 1, [0], \ldots, [0]), \ldots, (0, \ldots, 0, [1], [0], \ldots, [0]), \ldots, (0, \ldots, 0, [0], \ldots, [0], [1])$, so we have $s(G) \leq \#R - r - k + r - e(R) = \#R - k - e(R)$. Let p be a prime number which divides $e_{e(R)+1}$. We can see $G/pG \cong (\mathbb{Z}_p)^{\#R-k-e(R)}$. It is not hard to see $s(G) \geq s(G/pG)$, and since G/pG is a $\mathbb{Z}_p$-vector space, $s(G/pG) = \dim(G/pG) = \#R - k - e(R)$. Thus, $s(H_2(\Sigma, R)) = s(G) = \#R - s(\operatorname{im} \tilde{\partial}_1) - e(R)$. □

This lemma proves Lemma 6 since $e(R) = \#R - s(H_2(\Sigma, R)) - s(\operatorname{im} \tilde{\partial}_1)$ and the RHS does not depend on the rewriting strategy. Also, Theorem 7 is implied by the following theorem:

Theorem 52. Let (Σ, R) be a TRS and $d = \deg(R)$. If $d = 0$ or d is prime,

$$\#R \geq s(H_2(\Sigma, R)) + s(\operatorname{im} \tilde{\partial}_1). \tag{5.7}$$

Proof. By the first isomorphism theorem, we have an isomorphism between $\mathbb{Z}_d$-modules

$$\operatorname{im} \tilde{\partial}_1 \simeq \mathbb{Z}_d \otimes_{\mathcal{R}} \mathcal{R}\underline{\mathbf{P}_2}/\ker \tilde{\partial}_1$$

and by the third isomorphism theorem, the right hand side is isomorphic to

$$\begin{aligned}\mathbb{Z}_d \otimes_{\mathcal{R}} \mathcal{R}\underline{\mathbf{P}_2}/\ker\tilde{\partial}_1 &\simeq \left(\mathbb{Z}_d \otimes_{\mathcal{R}} \mathcal{R}\underline{\mathbf{P}_2}/\operatorname{im}\tilde{\partial}_2\right) / \left(\ker\tilde{\partial}_1/\operatorname{im}\tilde{\partial}_2\right) \\ &\simeq \left(\mathbb{Z}_d \otimes_{\mathcal{R}} \mathcal{R}\underline{\mathbf{P}_2}/\operatorname{im}\tilde{\partial}_2\right) / H_2(\Sigma, R).\end{aligned}$$

Thus, we obtain the following exact sequence by Proposition 38:

$$0 \to H_2(\Sigma, R) \to \mathbb{Z}_d \otimes_{\mathcal{R}} \mathcal{R}\underline{\mathbf{P}_2}/\operatorname{im}\tilde{\partial}_2 \to \operatorname{im}\tilde{\partial}_1 \to 0.$$

By Theorem 33, since $\operatorname{im}\tilde{\partial}_1 \subset \mathbb{Z}_d \otimes_{\mathcal{R}} \mathcal{R}\underline{\mathbf{P}_1} \cong (\mathbb{Z}_d)\underline{R}$ and $(\mathbb{Z}_d)\underline{R}$ is a free $\mathbb{Z}_d$-module, $\operatorname{im}\tilde{\partial}_1$ is also free and by Proposition 39, we have $\mathbb{Z}_d \otimes_{\mathcal{R}} \mathcal{R}\underline{\mathbf{P}_2}/\operatorname{im}\tilde{\partial}_2 \cong H_2(\Sigma, R) \times \operatorname{im}\tilde{\partial}_1$. Therefore, $s(\mathbb{Z}_d \otimes_{\mathcal{R}} \mathcal{R}\underline{\mathbf{P}_2}/\operatorname{im}\tilde{\partial}_2) = s(H_2(\Sigma, R)) + s(\operatorname{im}\tilde{\partial}_1)$. Since $\mathbb{Z}_d \otimes_{\mathcal{R}} \mathcal{R}\underline{\mathbf{P}_2}/\operatorname{im}\tilde{\partial}_2$ is generated by $[l_1 \to r_1], \ldots, [l_k \to r_k]$ if $R = \{l_1 \to r_1, \ldots, l_k \to r_k\}$, we obtain

$$k = \#R \geq s(\mathbb{Z}_d \otimes_{\mathcal{R}} \mathcal{R}\underline{\mathbf{P}_2}/\operatorname{im}\tilde{\partial}_2) = s(H_2(\Sigma, R)) + s(\operatorname{im}\tilde{\partial}_1).$$

Thus, we get (5.7). □

Now, we prove our main theorem, Theorem 7.

Proof of Theorem 7. As we stated, $H_2(\Sigma, R)$ depends only on the Tietze equivalence class of (Σ, R) and particularly, $H_2(\Sigma, R')$ is isomorphic to $H_2(\Sigma, R)$ if R' is equivalent to R (in the sense $\overset{*}{\leftrightarrow}_R = \overset{*}{\leftrightarrow}_{R'}$). Let us show $s(\operatorname{im}\tilde{\partial}_1)$ depends only on the equivalence class of R. For a left $\mathfrak{R}$-module M, $\operatorname{rank}(M)$ denotes the cardinality of a minimal linearly independent generating set of M, that is, a minimal generating set S of G such that $r_1 s_1 + \cdots + r_k s_k = 0 \implies r_1 = \cdots = r_k = 0$ for any $r_1, \ldots, r_k \in \mathfrak{R}$, $s_1, \ldots, s_k \in S$. It can be shown that $\operatorname{rank}(M) = s(M)$

if M is free. Especially, $s(\operatorname{im}\tilde{\partial}_1) = \operatorname{rank}(\operatorname{im}\tilde{\partial}_1)$ since $\operatorname{im}\tilde{\partial}_1 \subset \mathbb{Z}\underline{R}$ if $\deg(R) = 0$. Also, $\operatorname{rank}(\operatorname{im}\tilde{\partial}_1) = \operatorname{rank}(\ker\tilde{\partial}_0) - \operatorname{rank}(\ker\tilde{\partial}_0/\operatorname{im}\tilde{\partial}_1)$ is obtained by a general theorem [18, Ch 10, Lemma 10.1]. By definition, $\tilde{\partial}_0$ does not depend on R. Since $\ker\tilde{\partial}_0/\operatorname{im}\tilde{\partial}_1 = H_1(\Sigma, R)$ depends only on the Tietze quivalence class of R, two sets of rules R, R' with $\overset{*}{\leftrightarrow}_R = \overset{*}{\leftrightarrow}_{R'}$ give the same $\operatorname{rank}(\operatorname{im}\tilde{\partial}_1)$.

In conclusion, for any TRS R' equivalent to R, we obtain $\#R' \geq s(H_2(\Sigma, R)) + s(\operatorname{im}\tilde{\partial}_1) = \#R - e(R)$. □

Chapter 6

Unifiability

In this section, we show the result about E-unifiability, Theorem 14. For that, we first define the abelian group $\mathcal{H}(E)$ and the homomorphism $\mathcal{H}(E \to E')$ for sets E, E' of equations, and then prove the abstract version of Theorem 14 stated as follows:

Theorem 53. Let Σ be a signature, E be a set of equations of $\mathrm{Term}(\Sigma)$ and $t, s \in \mathrm{Term}(\Sigma)$ be two terms. If t, s are E-unifiable, then $\mathcal{H}(E \to E \cup \{t \approx s\})$ is surjective.

We will later show how Theorem 53 implies Theorem 14.

The abelian group $\mathcal{H}(E)$ is defined using the maps ∂_i^E introduced in Secion 5.1.

Definition 54. For a set E of equations, we define the abelian group $\mathcal{H}(E)$ by

$$\mathcal{H}(E) = \mathbb{Z}_d \otimes_{\mathcal{R}^E} \ker \partial_0^E = \mathbb{Z}_d \otimes_{\mathcal{R}^E} \mathrm{im}\, \partial_1^E \quad (d = \deg(E)).$$

If two sets E, E' of equations are equivalent, since $\mathcal{R}^E$ and $\mathcal{R}^{E'}$ are isomorphic

and $\partial_0^E = \partial_0^{E'}$, we have $\mathcal{H}(E) \simeq \mathcal{H}(E')$. That is, we can see that $\mathcal{H}(E)$ is invariant under the equivalence of E. (This holds especially since we are fixing a signature Σ.)

Let E, E' be sets of equations with $E^* \subset E'^*$. Then, the functor $\pi^{E,E'} : \mathcal{R}^E \to \mathcal{R}^{E'}$ given as $[(C_1, u_1) + \cdots + (C_k, u_k)]^E \mapsto [(C_1, u_1) + \cdots + (C_k, u_k)]^{E'}$ is well-defined. For a family of sets P, $\pi^{E,E'}$ extends to $\overline{\pi}_P^{E,E'} : \mathcal{R}^E\underline{P} \to \mathcal{R}^{E'}\underline{P}$. Then, we can see that the diagram

$$\begin{array}{ccc} \mathcal{R}^E\underline{\mathbf{P}_1} & \xrightarrow{\partial_0^E} & \mathcal{R}^E\underline{\mathbf{P}_0} \\ \downarrow{\scriptstyle \overline{\pi}_{\mathbf{P}_1}^{E,E'}} & & \downarrow{\scriptstyle \overline{\pi}_{\mathbf{P}_0}^{E,E'}} \\ \mathcal{R}^{E'}\underline{\mathbf{P}_1} & \xrightarrow{\partial_0^{E'}} & \mathcal{R}^{E'}\underline{\mathbf{P}_0} \end{array}$$

commutes. Therefore, if we restrict $\overline{\pi}_{\mathbf{P}_1}^{E,E'}$ to $\ker \partial_0^E$, we get $\overline{\pi}_{\mathbf{P}_1}^{E,E'}|_{\ker \partial_0^E} : \ker \partial_0^E \to \ker \partial_0^{E'}$. Let $d = \deg(E)$ and $d' = \deg(E')$. Since $E^* \subset E'^*$, d' divides d and we can define a group homomorphism $q^{d,d'} : \mathbb{Z}_d \to \mathbb{Z}_{d'}$ as $q^{d,d'}(n + d\mathbb{Z}) = n + d'\mathbb{Z}$. Consider the composition of abelian group homomorphisms

$$\mathbb{Z}_d \otimes (\ker \partial_0^E(k)) \xrightarrow{f_k} \mathbb{Z}_{d'} \otimes (\ker \partial_0^{E'}(k)) \xrightarrow{\zeta_k} \mathbb{Z}_{d'} \otimes_{\mathcal{R}^{E'}} \ker \partial_0^{E'}$$

where $f_k = q^{d,d'} \otimes (\overline{\pi}_{\mathbf{P}_1}^{E,E'}|_{\ker \partial_0^E}(k))$ and ζ_k is the extranatural transformation given in the definition of tensor product. Since $\zeta_k \circ f_k$ $(k = 0, 1, \dots)$ form an extranatural transformation, we get an abelian group homomorphism $\mathbb{Z}_d \otimes_{\mathcal{R}^E} \ker \partial_0^E \to \mathbb{Z}_{d'} \otimes_{\mathcal{R}^{E'}} \ker \partial_0^{E'}$ by naturality and let $\mathcal{H}(E \to E')$ denote it. That is, $\mathcal{H}(E \to E')$ makes the following diagram commute.

$$\begin{array}{ccc} \mathbb{Z}_d \otimes (\ker \partial_0^E(k)) & \xrightarrow{\zeta_k} & \mathbb{Z}_d \otimes_{\mathcal{R}^E} \ker \partial_0^E \\ \downarrow{\scriptstyle f_k} & & \downarrow{\scriptstyle \mathcal{H}(E \to E')} \\ \mathbb{Z}_{d'} \otimes (\ker \partial_0^{E'}(k)) & \xrightarrow{\zeta_k} & \mathbb{Z}_d \otimes_{\mathcal{R}^{E'}} \ker \partial_0^{E'} \end{array} \tag{6.1}$$

Thus, we have obtained an abelian group homomorphism $\mathcal{H}(E \to E') : \mathcal{H}(E) \to \mathcal{H}(E')$.

Now, we can prove Theorem 53.

Proof of Theorem 53. Let $F = E \cup \{t \approx s\}$. If $t\sigma \approx_E s\sigma$ for some σ, then E is equivalent to $E' = E \cup \{t\sigma \approx s\sigma\}$ and F is equivalent to $F' = F \cup \{t\sigma \approx s\sigma\}$. Since $\mathbb{Z}_d \otimes_{\mathcal{R}^{F'}} \mathcal{R}^{F'}\underline{\mathbf{P}_2^{F'}}$ is freely generated by $1 \otimes \underline{l \approx r}$ for $l \approx r \in F'$ (Lemma 50), $\mathcal{H}(F') = \mathbb{Z}_d \otimes_{\mathcal{R}^{F'}} \operatorname{im} \partial_1^{F'}$ is generated by $1 \otimes \partial_1^{F'}(\underline{l \approx r})$ for $l \approx r \in F'$. For $l \approx r \in E'$, since $\mathcal{H}(E' \to F')(1 \otimes \partial_1^{E'}(\underline{l \approx r})) = 1 \otimes \partial_1^{F'}(\underline{l \approx r})$, to show the surjectivity of $\mathcal{H}(E' \to F')$, it suffices to check that $1 \otimes \partial_1^{F'}(\underline{t \approx s})$ is in $\operatorname{im} \mathcal{H}(E' \to F')$. We have $1 \otimes \partial_1^{F'}(\underline{t \approx s} - \underline{t\sigma \approx s\sigma}) = 0 \in \mathbb{Z}_d \otimes \operatorname{im} \partial_1^{F'}$ since

$$\begin{aligned} 1 \otimes \partial_1^{F'}(\underline{t \approx s} - \underline{t\sigma \approx s\sigma}) &= 1 \otimes (\varphi(s) - \varphi(t) - \varphi(s\sigma) + \varphi(t\sigma)) \\ &= 1 \otimes (\varphi(s) - \varphi(t)) - 1 \otimes (\varphi(s\sigma) - \varphi(t\sigma)) \\ &= 1 \otimes (\varphi(s)\sigma - \varphi(t)\sigma) - 1 \otimes (\varphi(s\sigma) - \varphi(t\sigma)) = 0. \end{aligned}$$

Therefore, $1 \otimes \partial_1^{F'}(\underline{t \approx s}) = 1 \otimes \partial_1^{F'}(\underline{t\sigma \approx s\sigma})$ in $\mathbb{Z}_d \otimes_{\mathcal{R}^F} \operatorname{im} \partial_1^{F'}$. Also, since $t\sigma \approx s\sigma \in E'$, we have $1 \otimes \partial_1^{F'}(\underline{t\sigma \approx s\sigma}) = \mathcal{H}(E' \to F')(1 \otimes \partial_1^{E'}(\underline{t\sigma \approx s\sigma}))$. Thus, $1 \otimes \partial_1^{F'}(\underline{t \approx s}) \in \operatorname{im} \mathcal{H}(E' \to F')$. □

We show that Theorem 53 implies Theorem 14. Suppose R is a complete TRS with degree d. First, notice that if $d = 1$, then $\mathbb{Z}_d$ is a trivial group and so is $\mathcal{H}(R)$. Hence Theorem 52 is not interesting in that case. We write $\tilde{\partial}_2^R$ for the map $\mathbb{Z}_d \otimes \partial_2^R : \mathbb{Z}_d \otimes_{\mathcal{R}^R} \mathcal{R}^R\underline{\mathbf{P}_3^R} \to \mathbb{Z}_d \otimes_{\mathcal{R}^R} \mathcal{R}^R\underline{\mathbf{P}_2^R}$ and write $\check{\partial}_1^R$ for the map $\mathbb{Z}_d \otimes (\partial_1^R :$

$\mathcal{R}^R\underline{\mathbf{P}_2^R} \to \operatorname{im}\partial_1^R$). Since the sequence

$$\mathbb{Z}_d \otimes_{\mathcal{R}^R} \mathcal{R}^R\underline{\mathbf{P}_3^R} \xrightarrow{\tilde{\partial}_2^R} \mathbb{Z}_d \otimes_{\mathcal{R}^R} \mathcal{R}^R\underline{\mathbf{P}_2^R} \xrightarrow{\check{\partial}_1^R} \mathbb{Z}_d \otimes_{\mathcal{R}^R} \operatorname{im}\partial_1^R \to 0$$

is exact, $\mathcal{H}(E) = \mathbb{Z}_d \otimes_{\mathcal{R}^R} \operatorname{im}\partial_1^R$ is isomorphic to $\mathbb{Z}_d \otimes_{\mathcal{R}^R} \mathcal{R}^R\underline{\mathbf{P}_2^R}/\operatorname{im}\tilde{\partial}_2^R$.

Let E be a set of equations with degree d' and R be a complete TRS with degree d such that $E^* \subset R^*$. We define $h : \mathbb{Z}_{d'} \otimes_{\mathcal{R}^E} \mathcal{R}^E\underline{\mathbf{P}_2^E} \to \mathbb{Z}_d \otimes_{\mathcal{R}^R} \mathcal{R}^R\underline{\mathbf{P}_2^R}$ by $h(1 \otimes \underline{t \approx s}) = 1 \otimes (\hat{\hat{t}} - \hat{\hat{s}})$.

Lemma 55. $\check{\partial}_1^R \circ h = \mathcal{H}(E \to R) \circ \check{\partial}_1^E$. That is, the following diagram commutes:

$$\begin{array}{ccc} \mathbb{Z}_{d'} \otimes_{\mathcal{R}^E} \mathcal{R}^E\underline{\mathbf{P}_2^E} & \xrightarrow{\check{\partial}_1^E} & \mathbb{Z}_{d'} \otimes_{\mathcal{R}^E} \operatorname{im}\partial_1^E \\ \downarrow h & & \downarrow \mathcal{H}(E\to R) \\ \mathbb{Z}_d \otimes_{\mathcal{R}^R} \mathcal{R}^R\underline{\mathbf{P}_2^R} & \xrightarrow{\check{\partial}_1^R} & \mathbb{Z}_d \otimes_{\mathcal{R}^R} \operatorname{im}\partial_1^R. \end{array}$$

Proof. First, we show, by induction, $\check{\partial}_1^R(1 \otimes \hat{\hat{t}}) = 1 \otimes (\varphi(\hat{t}) - \varphi(t)) \in \mathbb{Z}_d \otimes_{\mathcal{R}^R} \operatorname{im}\partial_1^R$ for any term t. If $\hat{\hat{t}} = 0$, or equivalently, t is normal, then the equality trivially holds. If $\hat{\hat{t}} = C\underline{l \approx r}u + \hat{\hat{t}}'$ ($C[l \circ u] = t$, $C[r \circ u] = t'$) and $\check{\partial}_1^R(1 \otimes \hat{\hat{t}}') = 1 \otimes (\varphi(\hat{t}) - \varphi(t'))$, then $\check{\partial}_1^R(1 \otimes \hat{\hat{t}}) = 1 \otimes (\varphi(\hat{t}) - \varphi(t') + \varphi(r) - \varphi(l))$. Since $1 \otimes (\varphi(r) - \varphi(l)) = 1 \otimes (C\varphi(r)u - C\varphi(l)u) = 1 \otimes (\varphi(t') - \varphi(t))$, we have $\check{\partial}_1^{R'}(\hat{\hat{t}}) = 1 \otimes (\varphi(\hat{t}) - \varphi(t))$.

Now, we have $\check{\partial}_1^R(h(1 \otimes \underline{t \approx s})) = \check{\partial}_1^R(1 \otimes \hat{\hat{t}}) - \check{\partial}_1^R(1 \otimes \hat{\hat{s}}) = 1 \otimes (\varphi(s) - \varphi(t))$ and thus $\mathcal{H}(E \to R)(\check{\partial}_1^E(1 \otimes \underline{t \approx s})) = 1 \otimes (\varphi(s) - \varphi(t))$. □

The above lemma implies that the map

$$\overline{h} : \mathbb{Z}_{d'} \otimes_{\mathcal{R}^E} \mathcal{R}^E\underline{\mathbf{P}_2^E}/\ker\check{\partial}_1^E \to \mathbb{Z}_d \otimes_{\mathcal{R}^R} \mathcal{R}^R\underline{\mathbf{P}_2^R}/\ker\check{\partial}_1^R, \quad [x] \mapsto [h(x)]$$

is well-defined since if $x \in \ker \check{\partial}_1^E$, then $\check{\partial}_1^R(h(x)) = \mathcal{H}(E \to R)(\check{\partial}_1^E(x)) = 0$. Also, $\mathcal{H}(E \to R)$ is surjective iff $\overline{h}$ is surjective since we have the diagram

$$\begin{array}{ccc} \mathbb{Z}_{d'} \otimes_{\mathcal{R}^E} \mathcal{R}^E \underline{\mathbf{P}_2^E} / \ker \check{\partial}_1^E & \xrightarrow{\simeq} & \mathbb{Z}_{d'} \otimes_{\mathcal{R}^E} \operatorname{im} \partial_1^E \\ \downarrow \overline{h} & & \downarrow \mathcal{H}(E \to R) \\ \mathbb{Z}_d \otimes_{\mathcal{R}^R} \mathcal{R}^R \underline{\mathbf{P}_2^R} / \ker \check{\partial}_1^R & \xrightarrow{\simeq} & \mathbb{Z}_d \otimes_{\mathcal{R}^R} \operatorname{im} \partial_1^R. \end{array}$$

Theorem 14 follows from Theorem 53 and the lemma below.

Lemma 56. The map $\mathcal{H}(E \to R)$ is surjective iff the matrix $(D(E)|U(E,R))$ is equivalent to $I_{n,m}$ and $n \leq m$ where n (resp. m) is the number of rows (resp. columns) in $(D(R)|U(E,R))$.

Proof. We can see that $U(E,R)$ is a matrix representation of h and $D(R)$ is a matrix representation of $\tilde{\partial}_2^R$. So, $(D(E)|U(E,R))$ is equivalent to $I_{n,m}$ and $n \leq m$ iff the map

$$(\mathbb{Z}_d \otimes_{\mathcal{R}^R} \mathcal{R}^R \underline{\mathbf{P}_3^R}) \times (\mathbb{Z}_d \otimes_{\mathcal{R}^E} \mathcal{R}^E \underline{\mathbf{P}_2^E}) \to \mathbb{Z}_d \otimes_{\mathcal{R}^R} \mathcal{R}^R \underline{\mathbf{P}_2^R}, \quad (x,y) \mapsto \tilde{\partial}_2^R(x) + h(y)$$

is surjective.

Suppose $\mathcal{H}(E \to R)$ is surjective. Then, $\overline{h}$ is surjective and so for any $z \in \mathbb{Z}_d \otimes_{\mathcal{R}^R} \mathcal{R}^R \underline{\mathbf{P}_2^R}$, we have $y \in \mathbb{Z}_{d'} \otimes_{\mathcal{R}^E} \mathcal{R}^E \underline{\mathbf{P}_2^E}$ and $z' \in \ker \check{\partial}_1^R$ satisfying $z = h(y) + z'$. Since $\ker \check{\partial}_1^R = \operatorname{im} \tilde{\partial}_2^R$, there exists x such that $\tilde{\partial}_2^R(x) = z'$. Therefore, the map $(x,y) \mapsto \tilde{\partial}_2(x) + h(y)$ is surjective. The converse can be shown in a similar way. □

The above lemma implies that the necessary condition stated in Theorem 14 is independent of the choice of rewriting strategy. (∵ The map $\mathcal{H}(E \to R)$ is defined independently from rewriting strategies.)

Chapter 7

Related Work

The fact that the theory of groups over the signature $\{\cdot, \ ^{-1}, e\}$ cannot be presented by a single axiom was stated by Tarski [22], and published proofs were given by Neumann [16] and Kunen [12].

The homology of equational theories is first developed by Jibladze and Pirashvili [11]. Malbos-Mimram's partial free resolution is a generalization of Squier's partial free resolution for string rewriting systems (SRS) [20]. Squire showed that, using his resolution, there exists an SRS that does not have any equivalent complete SRS with a finite number of rewrite rules. Inequalities like (5.7) appear in other homology theories. Inequality (4.1) for simplicial complexes is an example, and there are similar inequalities for homology *of* groups [4] and Morse theory [14].

Chapter 8

Future Work and Conclusion

8.1 Conclusion

We have proved an inequality about the number of equational axioms/rewrite rules (Theorem 7), and a necessary condition for E-unification (Theorem 14). Both theorems are obtained using homological algebra of equational theories. Theorem 7 is the first result providing a nontrivial lower bounds of the number of axioms/rules for various equational theories/TRSs. Theorem 14 may ensure that E-unification problems $t \approx^{?}_{E} s$ does not have any solutions if $E \cup \{t \approx s\}$ has a complete TRS.

8.2 Future Work

There are several directions for future work. My main theorems require complete TRSs, which are not easy to obtain in general. For example, an equational theory with a commutative law does not have any equivalent terminating TRS. To extend

my methodology to such theories, it should be useful to generalize Malbos-Mimram's construction to rewriting modulo commutativity.

Also, I would like to use my methodology to show that a given TRS does not have any equivalent complete TRSs with finite rewrite rules. Since existing completion procedures generally do not terminate in that case, such a method is helpful to have.

Bibliography

[1] Maria Alpuente, Santiago Escobar, and José Iborra. Termination of narrowing revisited. *Theoretical Computer Science*, 410(46):4608 – 4625, 2009. Abstract Interpretation and Logic Programming: In honor of professor Giorgio Levi.

[2] Franz Baader and Tobias Nipkow. *Term Rewriting and All That*. Cambridge University Press, 1998.

[3] Ronald V. Book and Friedrich Otto. *String-rewriting Systems*. Springer-Verlag, Berlin, Heidelberg, 1993.

[4] D. Epstein. Finite presentations of groups and 3-manifolds. *The Quarterly Journal of Mathematics*, 12(1):205–212, 1961.

[5] M. Fay. First-order unification in an equational theory. In *4th Workshop on Automated Deduction*, Austin, Texas, 1978.

[6] Jean-Marie Hullot. Canonical forms and unification. In Wolfgang Bibel and Robert Kowalski, editors, *5th Conference on Automated Deduction Les Arcs, France, July 8–11, 1980*, pages 318–334, Berlin, Heidelberg, 1980. Springer Berlin Heidelberg.

[7] E. Westbrook I. Wehrman, A. Stump. Slothrop: Knuth-Bendix completion with a modern termination checker. *Term Rewriting and Applications. RTA*, 4098, 2006.

[8] Mirai Ikebuchi. A Lower Bound of the Number of Rewrite Rules Obtained by Homological Methods. In *4th International Conference on Formal Structures for Computation and Deduction (FSCD 2019)*, volume 131 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 24:1–24:17, Dagstuhl, Germany, 2019. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik.

[9] Mirai Ikebuchi. A Homological Condition on Equational Unifiability. In Filippo Bonchi and Simon J. Puglisi, editors, *46th International Symposium on Mathematical Foundations of Computer Science (MFCS 2021)*, volume 202 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 61:1–61:16, Dagstuhl, Germany, 2021. Schloss Dagstuhl – Leibniz-Zentrum für Informatik.

[10] M. Jantzen. A note on a special one-rule semi-thue system. *Information Processing Letters*, 21(3):135 – 140, 1985.

[11] Mamuka Jibladze and Teimuraz Pirashvili. Cohomology of algebraic theories. *Journal of Algebra*, 137(2):253–296, 1991.

[12] K. Kunen. Single axioms for groups. *Journal of Automated Reasoning*, 9(3):291–308, Dec 1992.

[13] P. Malbos and S. Mimram. Homological computations for term rewriting systems. In *1st International Conference on Formal Structures for Computation and Deduction (FSCD 2016)*, volume 52 of *Leibniz International Proceedings*

in Informatics (LIPIcs), pages 27:1–27:17, Dagstuhl, Germany, 2016. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik.

[14] J. Milnor. *Morse Theory.* Annals of Mathematics Studies 51. Princeton University Press, 1963.

[15] B. Mitchell. Rings with several objects. *Advances in Mathematics*, 8(1):1 – 161, 1972.

[16] B. H. Neumann. Yet another single law for groups. *Illinois J. Math.*, 30(2):295–300, 06 1986.

[17] J. J. Rotman. *An Introduction to Homological Algebra.* Springer-Verlag New York, 2009.

[18] J. J. Rotman. *Advanced Modern Algebra*, volume 114. American Mathematical Soc., 2010.

[19] H. Sato, S. Winkler, M. Kurihara, and A. Middeldorp. Multi-completion with termination tools (system description). In *Proc. 4th IJCAR*, volume 5195 of *LNAI*, pages 306–312, 2008.

[20] C. C. Squier. Word problems and a homological finiteness condition for monoids. *Journal of Pure and Applied Algebra*, 49(1-2):201–217, 1987.

[21] J. Steinbach and U. Kühler. Check your ordering - termination proofs and problems. Technical Report Technical Report R-90-25, Universität Kaiserslautern, 1990.

[22] A. Tarski. Equational logic and equational theories of algebras. In *Contributions to Mathematical Logic*, volume 50 of *Studies in Logic and the Foundations of Mathematics*, pages 275 – 288. Elsevier, 1968.

[23] Heinrich Tietze. Über die topologischen invarianten mehrdimensionaler mannigfaltigkeiten. *Monatshefte für Mathematik und Physik*, 19(1):1–118, Dec 1908.

[24] Ian Wehrman and Aaron Stump. Mining propositional simplification proofs for small validating clauses. *Electronic Notes in Theoretical Computer Science*, 144(2):79 – 91, 2006. Proceedings of the Third Workshop on Pragmatics of Decision Procedures in Automated Reasoning (PDPAR 2005).

Appendix A

Experimental Results

We present our experimental data in Table 1 and Table 2. The data set of complete TRSs is taken from experimental results of MKBtt [19], which include benchmark problems [21],[24],[7]. The column headed "degree" shows the degree of the TRS, the column $\#R_{before}$ the number of rules, the column $\#R_{after}$ the number of rules after completion, the column $s(H_2)$ Malbos-Mimram's lower bound, and the column $\#R_{after} - e(R)$ our lower bound. The table is also available at `https://mir-ikbch.github.io/homtrs/experiment/result.html` which has links to TRS files.

ASK93_1

```
w(a(x)) -> a(b(x))
a(c(x)) -> a(b(c(x)))
```

ASK93_6

```
x(w(e(f(z)))) -> x(w(e(g(z))))
e(g(c(z))) -> d(g(c(z)))
```

```
x(w(d(z))) -> x(w(i(z)))
u(b(c(z))) -> o(z)
x(w(i(g(c(z))))) -> o(z)
x(w(a(z))) -> u(z)
a(b(c(z))) -> e(f(c(z)))
j(f(z)) -> z
h(j(z)) -> w(e(z))
y(b(z)) -> g(z)
i(y(z)) -> a(z)
```

BD94_collapse

```
c -> a
g(x) -> x
f(x, b) -> x
f(x, g(y)) -> f(g(x), y)
f(b, z) -> c
```

BD94_peano

```
+(x, 0) -> x
+(x, s(y)) -> s(+(x, y))
*(x, 0) -> 0
*(x, s(y)) -> +(*(x, y), x)
```

BD94_sqrt

```
i(0) -> 0
```

```
sqrt(+(i(x), x)) -> 0
+(i(0), 0) -> 0
```

BGK94_D08

```
f(x,f(y,z)) ->  f(f(x,y),z)
f(x,i(x)) -> e
f(x,e) ->  x
f(a, f(a, f(a, a))) -> e
f(b, b) -> e
f(a, b) -> f(b, i(a))
```

BGK94_D10

```
f(x,f(y,z)) ->  f(f(x,y),z)
f(x,i(x)) -> e
f(x,e) ->  x
f(a, f(a, f(a, f(a, a)))) -> e
f(b, b) -> e
f(a, b) -> f(b, i(a))
```

BGK94_D12

```
f(x,f(y,z)) ->  f(f(x,y),z)
f(x,i(x)) -> e
f(x,e) ->  x
f(a, f(a, f(a, f(a, f(a, a))))) -> e
f(b, b) -> e
f(a, b) -> f(b, i(a))
```

BGK94_D16

```
f(x,f(y,z)) ->  f(f(x,y),z)
f(x,i(x)) -> e
f(x,e) ->  x
f(a, f(a, f(a, f(a, f(a, f(a, f(a, a)))))))  -> e
f(b, b) -> e
f(a, b) -> f(b, i(a))
```

BH96_fac8_theory

```
+(x,0) -> x
+(x,s(y)) -> s(+(x,y))
*(x,0) -> 0
*(x,s(y)) -> +(*(x,y),x)
fac(0) -> s(0)
fac(s(x)) -> *(s(x),fac(x))
```

Chr89_A2

```
f(f(x, y), z) -> f(x, f(y, z))
f(a1, y) -> y
f(a2, y) -> y
f(x, i1(x)) -> a1
f(x, i2(x)) -> a2
```

Chr89_A3

```
f(f(x, y), z) -> f(x, f(y, z))
f(a1, y) -> y
f(a2, y) -> y
f(a3, y) -> y
f(x, i1(x)) -> a1
f(x, i2(x)) -> a2
f(x, i3(x)) -> a3
```

KK99_linear_assoc

```
+(+(x, y), z) -> +(x, +(y, z))
f(+(x, y)) -> +(f(x), f(y))
```

LS94_G0

```
f(x, f(y,z)) ->  f(f(x,y), z)
f(x, i(x)) -> e
f(i(x), x) -> e
f(x, e) ->  x
f(e, x) -> x
a(a(x)) -> x
b(b(x)) -> x
a(b(a(b(a(b(x)))))) -> x
```

Les83_fib

```
+(0, x) -> x
+(s(x), y) -> s(+(x, y))
```

```
+(+(x, y), z) -> +(x, +(y, z))
fib(0) -> 0
fib(s(0)) -> s(0)
fib(s(s(x))) -> +(fib(x), fib(s(x)))
dfib(0, y) -> y
dfib(s(0), y) -> s(y)
dfib(s(s(x)), y) -> dfib(s(x), dfib(x, y))
```

Les83_subset

```
if(tt, x, y) -> x
if(ff, x, y) -> y
if(x, y, y) -> y
if(x, tt, ff) -> x
eq(0, 0) -> tt
eq(0, s(x)) -> ff
eq(s(x), 0) -> ff
eq(s(x), s(y)) -> eq(x, y)
has(empty, x) -> ff
has(+(u, x), y) -> if(eq(x, y), tt, has(u, y))
subset(empty, v) -> tt
subset(+(u, x), v) -> if(has(v, x), subset(u, v), ff)
```

OKW95_dt1_theory

```
fib(0) -> s(0)
fib(s(0)) -> s(0)
```

```
fib(s(s(x))) -> +(fib(s(x)),fib(x))
dfib(0) -> s(0)
dfib(s(0)) -> s(0)
dfib(s(s(x))) -> +(dfib(s(x)),+(dfib(x),dfib(x)))
+(x,s(y)) -> s(+(x,y))
+(x,0) -> x
-(s(x),s(y)) -> -(x,y)
-(x,0) -> x
p(x) -> -(x, s(0))
```

SK90_3.01

```
*(one, y) -> y
*(i(x), x) -> one
*(*(x, y), z) -> *(x, *(y, z))
div(x, y) -> *(x, i(y))
```

SK90_3.02

```
f(f(x)) -> x
+(f(x), f(y)) -> f(+(x, y))
+(+(x, y), z) -> +(x, +(y, z))
```

SK90_3.03

```
d(d(x, x), d(d(y, y), y)) -> y
d(d(x, y), d(z, y)) -> d(x, z)
d(x, x) -> one
```

```
d(one, y) -> i(y)
d(x, i(y)) -> *(x, y)
```

SK90_3.04

```
*(*(x, y), z) -> *(x, *(y, z))
*(one, y) -> y
g(x) -> *(f(x), x)
*(g(x), y) -> y
```

SK90_3.05

```
*(*(x, y), *(y, z)) -> y
*(*(x, x), x) -> f(x)
*(x, *(x, x)) -> g(x)
*(g(x), y) -> *(x, y)
```

SK90_3.06

```
*(x, *(y, z)) -> *(*(x, y), z)
*(1, 1) -> 1
*(x, i(x)) -> 1
g(*(x, y), y) -> f(*(x, y), x)
f(1, y) -> y
```

SK90_3.07

```
+(+(x, y), z) -> +(x, +(y, z))
+(0, 0) -> 0
```

```
+(x, -(x)) -> 0
f(0, y, z) -> y
g(+(x, y), y) -> f(+(x, y), x, y)
```

SK90_3.08

```
*(x, \(x, y)) -> y
\(x, *(x, y)) -> y
/(*(x, y), y) -> x
*(/(x, y), y) -> x
*(x, *(y, x)) -> y
```

SK90_3.10

```
f(x, *(x, y)) -> y
g(*(x, y), y) -> x
*(x, one) -> x
*(one, y) -> y
```

SK90_3.11

```
p(0) -> 0
p(s(x)) -> x
+(x, 0) -> x
s(+(x, p(y))) -> +(x, y)
```

SK90_3.12

```
/(x, x) -> 1
```

```
/(x, 1) -> x
i(/(x, y)) -> /(y, x)
/(/(x, y), z) -> /(x, /(z, i(y)))
```

SK90_3.13

```
+(+(x, y), z) -> +(x, +(y, z))
+(x, 0) -> x
*(*(x, y), z) -> *(x, *(y, z))
*(x, 1) -> x
exp(0) -> 1
exp(+(x, y)) -> *(exp(x), exp(y))
```

SK90_3.14

```
s(s(x)) -> x
f(0,y) -> y
f(s(x),y) -> s(f(x,y))
f(f(g(x,y), 0), 0) -> g(x,y)
g(0,y) -> y
g(s(x),y) -> f(g(x,y),0)
h(0) -> s(0)
```

SK90_3.15

```
p(s(x)) -> x
eq(x, x) -> true
eq(s(x),x) -> false
```

```
eq(x, s(x)) -> false
eq(s(x), s(y)) -> eq(x, y)
eq(x, p(x)) -> false
eq(p(x), x) -> false
eq(p(x), p(y)) -> eq(x, y)
```

SK90_3.16

```
car(.(x, y)) -> x
cdr(.(x, y)) -> y
.(car(x), cdr(x)) -> x
atom(.(x, y)) -> false
```

SK90_3.17

```
or(&(x, y), &(z, y)) -> &(or(x, z), y)
&(x, x) -> x
or(x, x) -> x
```

SK90_3.18

```
@(nil, y) -> y
@(.(x,y), z) -> .(x, @(y,z))
rev(nil) -> nil
rev(.(x,y)) -> @(rev(y), .(x, nil))
rev(rev(x)) -> x
```

SK90_3.19

```
@(nil, y) -> y
@(.(x,y), z) -> .(x, @(y,z))
@(@(x,y), z) -> @(x, @(y,z))
reviter(nil, y) -> y
reviter(.(x,y), z) -> reviter(y, .(x,z))
rev(nil) -> nil
rev(.(x,y)) -> @(rev(y), .(x, nil))
@(rev(x), y) -> reviter(x, y)
rev(x) -> reviter(x, nil)
```

SK90_3.20

```
eq(x,x) -> true
eq(nil, end(y,z)) -> false
eq(end(x,y), nil) -> false
eq(end(x,y), end(u,v)) -> and(eq(y, v), eq(x, u))
f(x, nil) -> end(nil, x)
f(x, end(y,z)) -> end(f(x,y), z)
.(nil, y) -> y
.(end(x,y), z) -> .(x, f(y, z))
null(nil) -> true
null(end(x,y)) -> false
```

SK90_3.21

```
f(x, nil) -> g(nil,x)
f(x, g(y, z)) -> g(f(x, y), z)
```

```
g(g(x,y),y) -> g(x,y)
g(cdr(g(x,y)),y) -> cdr(g(x,y))
cons(x,nil) -> x
cons(x,g(y,z)) -> g(cons(x, y), z)
cdr(nil) -> nil
cdr(g(nil,y)) -> nil
cdr(g(g(x, y), z)) -> g(cdr(g(x, y)), z)
```

SK90_3.23

```
b(d(x)) -> x
d(a(x)) -> e(x)
e(c(x)) -> a(x)
c(e(x)) -> a(x)
```

SK90_3.24

```
a(b(a(x))) -> b(a(x))
c(x) -> a(x)
c(x) -> b(x)
```

SK90_3.25

```
a(b(a(a(b(x))))) -> a(x)
```

SK90_3.27

```
a(x) -> c(c(c(b(c(c(x))))))
b(c(b(x))) -> c(c(b(c(x))))
```

```
b(c(c(b(x))))-> c(c(c(c(c(c(b(c(c(c(c(c(x)))))))))))
b(c(c(c(b(x))))) -> c(b(c(c(c(c(x))))))
b(b(c(c(c(b(x)))))) -> c(c(c(c(b(c(c(x)))))))
b(c(c(c(c(c(b(x))))))) -> c(c(x))
b(c(c(c(c(c(c(b(x)))))))) -> c(c(c(c(c(b(c(c(c(x)))))))))
c(c(c(c(c(c(c(x))))))) -> x
```

SK90_3.28

```
b(u(x)) -> a(b(x))
a(u(x)) -> x
a(w(x)) -> c(a(x))
c(v(x)) -> b(c(x))
b(v(x)) -> x
c(w(x)) -> x
u(a(x)) -> x
v(b(x)) -> x
w(c(x)) -> x
```

SK90_3.29

```
a(c(x)) -> e(a(x))
a(d(x)) -> v(a(x))
b(c(x)) -> e(b(x))
b(d(x)) -> v(b(x))
a(u(x)) -> b(u(x))
u(x) -> c(w(x))
d(w(x)) -> u(x)
```

SK90_3.30

```
f(g(x), x) -> a
f(g(x), y) -> h(y)
f(g(x), f(y,z)) -> k(f(g(x),y), f(g(x),z))
```

SK90_3.31

```
f(x, h(y)) -> j(x)
f(h(x),y) -> j(h(x))
g(f(x,x)) -> i(x)
```

SK90_3.32

```
f(x,x) -> x
f(g(x),y) -> g(x)
g(g(x)) -> x
```

SK90_3.33

```
f(g(x)) -> g(x)
g(a) -> a
g(g(x)) -> x
```

TPTP-BOO027-1_theory

```
multiply(X,add(Y,Z)) -> add(multiply(Y,X),multiply(Z,X))
add(X,inverse(X)) -> one
add(multiply(X,inverse(X)),add(multiply(X,Y),multiply(inverse(X),Y))) -> Y
```

```
add(multiply(X,inverse(Y)),add(multiply(X,Y),multiply(inverse(Y),Y))) -> X
add(multiply(X,inverse(Y)),add(multiply(X,X),multiply(inverse(Y),X))) -> X
```

TPTP-COL053-1_theory

```
response(compose(X,Y),W) -> response(X,response(Y,W))
```

TPTP-COL056-1_theory

```
 response(compose(X,Y),W) -> response(X,response(Y,W))
response(a,b) -> c
esponse(a,c) -> b
```

TPTP-COL060-1_theory

```
apply(apply(apply(b,X),Y),Z) -> apply(X,apply(Y,Z))
apply(apply(t,X),Y) -> apply(Y,X)
```

TPTP-COL085-1_theory

```
response(a,b) -> b
```

TPTP-GRP010-4_theory

```
multiply(multiply(X,Y),Z) -> multiply(X,multiply(Y,Z))
multiply(identity,X) -> X
multiply(inverse(X),X) -> identity
multiply(c,b) -> identity
```

TPTP-GRP011-4_theory

```
multiply(multiply(X,Y),Z) -> multiply(X,multiply(Y,Z))
multiply(identity,X) -> X
multiply(inverse(X),X) -> identity
multiply(b,c) -> multiply(d,c)
```

TPTP-GRP012-4_theory

```
multiply(X,identity) -> X.
multiply(X,inverse(X)) -> identity
```

slothrop_ackermann

```
a(z,x) ->  s(x)
a(s(x),z) ->  a(x,s(z))
a(s(x),s(y)) ->  a(x,a(s(x),y))
```

slothrop_cge

```
trans(trans(x,y), z) ->  trans(x,trans(y,z))
trans(symm(x), x) ->   refl
trans(refl,x) ->  x
trans(f(x), f(y)) ->  f(trans(x,y))
trans(f(x), g(y)) ->  trans(g(y), f(x))
trans(g(x), g(y)) ->  g(trans(x,y))
```

slothrop_cge3

```
trans(trans(x,y), z) ->  trans(x,trans(y,z))
trans(symm(x), x) ->   refl
```

```
trans(refl,x) ->  x
trans(f(x), f(y)) ->  f(trans(x,y))
trans(f(x), g(y)) ->  trans(g(y), f(x))
trans(h(x), f(y)) ->  trans(f(y), h(x))
trans(g(x), g(y)) ->  g(trans(x,y))
trans(g(x), h(y)) ->  trans(h(y), g(x))
trans(h(x), h(y)) ->  h(trans(x,y))
```

slothrop_endo

```
f(x,f(y,z)) ->  f(f(x,y),z)
f(x,i(x)) -> e
f(x,e) ->  x
h(f(x,y)) ->  f(h(x), h(y))
```

slothrop_equiv_proofs

```
trans(trans(x1,x2),x3)  ->  trans(x1,trans(x2,x3))
trans(refl,x1)  ->  x1
trans(x1,refl)  ->  x1
congror1(refl)  ->  refl
congror2(refl)  ->  refl
trans(congror1(x1),ortrue2)  ->  ortrue2
trans(congror2(x1),ortrue1)  ->  ortrue1
trans(orfalse1,x1)  ->  trans(congror2(x1),orfalse1)
trans(orfalse2,x1)  ->  trans(congror1(x1),orfalse2)
trans(trans(congror1(x1),congror2(x2)), trans(congror1(x3),congror2(x4)))
```

```
  ->  trans(congror1(trans(x1,x3)), congror2(trans(x2,x4)))
trans(ortrue1,x1)  ->  ortrue1
trans(ortrue2,x1)  ->  ortrue2
```

slothrop_fgh

```
h(x,y) ->  f(x)
h(x,y) ->  f(y)
g(x,y) ->  h(x,y)
g(x,y) ->  a
```

slothrop_groups

```
f(x,f(y,z)) ->  f(f(x,y),z)
f(x,i(x)) -> e
f(x,e) ->  x
```

slothrop_groups_conj

```
f(x,f(y,z)) ->  f(f(x,y),z)
f(x,i(x)) -> e
f(x,e) ->  x
f(e,x) ->  x
i(f(y,x)) ->  f(i(x),i(y))
```

slothrop_hard

```
plus(x,z) ->  x
s(plus(x,y)) ->  plus(x,s(y))
```

Table A.1: Malbos-Mimram's and our lower bounds (1)

name	degree	$\#R_{before}$	$\#R_{after}$	$s(H_2)$	$\#R_{after} - e(R)$
ASK93_1	0	2	2	0	2
ASK93_6	0	11	11	0	9
BD94_collapse	1	5	5	–	–
BD94_peano	1	4	4	–	–
BD94_sqrt	2	3	4	0	3
BGK94_D08	2	6	21	2	5
BGK94_D10	2	6	21	1	4
BGK94_D12	2	6	20	2	5
BGK94_D16	2	6	20	2	5
BH96_fac8_theory	1	6	6	–	–
Chr89_A2	2	5	18	0	4
Chr89_A3	2	7	16	0	6
KK99_linear_assoc	0	2	2	0	1
LS94_G0	2	8	13	1	4
Les83_fib	1	9	9	–	–
Les83_subset	1	12	12	–	–
OKW95_dt1_theory	1	11	11	–	–
SK90_3.01	2	4	11	0	3
SK90_3.02	0	3	3	1	2
SK90_3.03	2	5	11	0	3
SK90_3.04	1	4	8	–	–
SK90_3.05	1	4	13	–	–
SK90_3.06	1	5	12	–	–
SK90_3.07	1	5	15	–	–
SK90_3.08	2	5	4	0	2
SK90_3.10	2	4	8	0	3
SK90_3.11	0	4	3	0	3
SK90_3.12	2	4	9	0	2
SK90_3.13	0	6	6	0	3
SK90_3.14	0	7	8	1	5
SK90_3.15	2	8	7	1	4
SK90_3.16	1	4	4	–	–
SK90_3.17	1	3	5	–	–

Table A.2: Malbos-Mimram's and our lower bounds (2)

name	degree	$\#R_{before}$	$\#R_{after}$	$s(H_2)$	$\#R_{after} - e(R)$
SK90_3.18	0	5	6	2	4
SK90_3.19	0	9	7	1	4
SK90_3.20	1	10	11	–	–
SK90_3.21	1	9	4	–	–
SK90_3.23	0	4	8	1	4
SK90_3.24	0	3	2	0	2
SK90_3.25	0	1	2	0	1
SK90_3.27	0	8	3	0	3
SK90_3.28	0	9	18	0	6
SK90_3.29	0	7	8	2	7
SK90_3.30	1	3	3	–	–
SK90_3.31	1	3	3	–	–
SK90_3.32	1	3	2	–	–
SK90_3.33	0	3	3	0	2
TPTP-BOO027-1_theory	1	5	5	–	–
TPTP-COL053-1_theory	0	1	1	0	1
TPTP-COL056-1_theory	0	3	3	0	3
TPTP-COL060-1_theory	0	2	2	0	2
TPTP-COL085-1_theory	0	1	1	0	1
TPTP-GRP010-4_theory	2	4	11	1	3
TPTP-GRP011-4_theory	2	4	11	1	3
TPTP-GRP012-4_theory	2	4	10	0	2
slothrop_ackermann	1	3	3	–	–
slothrop_cge	2	6	20	0	4
slothrop_cge3	2	9	28	0	5
slothrop_endo	2	4	14	0	3
slothrop_equiv_proofs	1	12	23	–	–
slothrop_fgh	1	4	3	–	–
slothrop_groups	2	3	10	0	2
slothrop_groups_conj	2	5	10	0	2
slothrop_hard	0	2	2	1	2