A Lower Bound of the Number of Rewrite Rules Obtained by Homological Methods

Mirai Ikebuchi
Massachusetts Institute of Technology, Computer Science and Artificial Intelligence Laboratory, Cambridge, USA
ikebuchi@mit.edu

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 systems), using homological algebra. Their method is an analog of Squier's homology theory on string rewriting systems. In this paper, we develop the homology theory for term rewriting systems more and provide a better lower bound under a stronger notion of equivalence than their equivalence. The author also implemented a program to compute the lower bounds.

2012 ACM Subject Classification Theory of computation → Rewrite systems

Keywords and phrases Term rewriting systems, Equational logic, Homological algebra

Digital Object Identifier 10.4230/LIPIcs.FSCD.2019.24

1 Introduction

The purpose of this paper is to find a lower bound of the number of axioms that are equivalent to a given equational theory. For example, the theory of groups is given by the following axioms:

$$\begin{array}{lll} G_1.\ m(m(x_1,x_2),x_3)=m(x_1,m(x_2,x_3)), & G_2.\ m(x_1,e)=x_1, & G_3\ m(e,x_1)=x_1, \\ G_4.\ m(i(x_1),x_1)=e, & G_5.\ m(x_1,i(x_1))=e. & \end{array} \tag{1}$$

It is well-known that G_2 and G_5 can be derived from only $\{G_1, G_3, G_4\}$. Moreover, the theory of groups can be given by two axioms: the axiom

$$m(x_1, i(m(m(i(m(i(x_2), m(i(x_1), x_3))), x_4), i(m(x_2, x_4))))) = x_3$$

together with G_4 is equivalent to the group axioms [4]. If we use the new symbol n which corresponds to the "multiplication of inverses" $m(i(x_1), i(x_2))$, a single axiom,

$$n(x_1, n(n(n(e, x_2), n(n(n(e, x_3), x_3), x_4)), n(n(e, x_1), x_2))) = x_4,$$

is equivalent to the group axioms [5]. However, no single axiom written in symbols m, i, e is equivalent to the group axioms. This is stated without proof by Tarski [9] and published proofs are given by Neumann [4] and Kunen [2]. Malbos and Mimram developed a general method to calculate a lower bound of the number of axioms that are "Tietze-equivalent" to a given complete term rewriting system (TRS) [3, Proposition 23]. We omit the definition of Tietze equivalence here, but roughly speaking, it is an equivalence between equational theories (or TRSs) (Σ_1, R_1), (Σ_2, R_2) where signatures Σ_1 and Σ_2 are not necessarily equal to each other, while the usual equivalence between TRSs is defined for two TRSs (Σ, R_1), (Σ, R_2) over the same signature (specifically, by $\overset{*}{\leftrightarrow}_{R_1} = \overset{*}{\leftrightarrow}_{R_2}$).

In this paper, we will develop Malbos and Mimram's theory more, and show an inequality which gives a better lower bound of the number of axioms with respect to the usual equivalence between TRSs over the same signature. For the theory of groups, our inequality gives that the number of axioms equivalent to the group axioms is greater than or equal to 2, so we have another proof of Tarski's theorem above as a special case. Our lower bound is algorithmically computable if a complete TRS is given.

We will first give the statement of our main theorem and some examples in Section 2. Then, we will see Malbos-Mimram's work briefly. The idea of their work is to provide an algebraic structure to TRSs and extract information of the TRSs, called homology groups, which are invariant under Tietze equivalence. The basics of such algebraic tools are given in Section 3, and we will see the idea of the construction of the homology groups of TRSs in Section 4. Finally, in Section 5, we will prove our main theorem.

2 Main Theorem

In this section, we will see our main theorem and some examples. Throughout this paper, we assume that any terms are over the set of variables $\{x_1, x_2, \dots\}$ and all signatures we consider are unsorted. For a signature Σ, let $T(\Sigma)$ denote the set of terms over the signature Σ and the set of variables $\{x_1, x_2, \dots\}$.

▶ **Definition 1.** *Let (Σ, R) be a TRS. 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 $t \in T(\Sigma)$ and we define $\gcd\{0\} = 0$ for convenience. For example, $\deg(\{f(x_1, x_2, x_2) \to x_1,\ g(x_1, x_1, x_1) \to e\}) = \gcd\{0, 2, 3\} = 1$.

Let $(\Sigma, R = \{l_1 \to r_1, \dots, l_n \to r_n\})$ be a TRS and $\mathrm{CP}(R) = \{(t_1, s_1), \dots, (t_m, s_m)\}$ be the set of the critical pairs of R. For any $i \in \{1, \dots, m\}$, let a_i, b_i be the numbers in $\{1, \dots, n\}$ such that the critical pair (t_i, s_i) is obtained by $l_{a_i} \to r_{a_i}$ and $l_{b_i} \to r_{b_i}$, that is, $t_i = r_{a_i}\sigma \leftarrow l_{a_i}\sigma = C[l_{b_i}\sigma] \to C[r_{b_i}\sigma] = s_i$ for some substitution σ and single-hole context C. Suppose R is complete. We fix an arbitrary rewriting strategy and 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. To state our main theorem, we introduce a matrix $D(R)$ and a number $e(R)$:

▶ **Definition 2.** *Suppose $d = \deg(R)$ is prime or 0. If $d = 0$, let $\mathfrak{R}$ be $\mathbb{Z}$, and if d is prime, let $\mathfrak{R}$ be $\mathbb{Z}/d\mathbb{Z}$ (integers modulo d). For $1 \le i \le m$, $1 \le j \le n$, let $D(R)_{ij}$ be the integer $\mathrm{nr}_j(s_i) - \mathrm{nr}_j(t_i) + \delta(b_i, j) - \delta(a_i, j)$ where $\delta(x, y)$ is the Kronecker delta. The matrix $D(R)$ is defined by $D(R) = (D(R)_{ij})_{i=1,\dots,m, j=1,\dots,n}$.*

▶ **Definition 3.** *Let $\mathfrak{R}$ be $\mathbb{Z}$ or $\mathbb{Z}/p\mathbb{Z}$ for any prime p. 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. *We call e_is 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 [7, 9.4]. (If $d = 0$, the invertible elements in $\mathfrak{R} \cong \mathbb{Z}$ are 1 and -1, and if d is prime, any nonzero elements in $\mathfrak{R} = \mathbb{Z}/d\mathbb{Z}$ are invertible.) In general, the same fact holds for any principal ideal domain $\mathfrak{R}$.

▶ **Definition 4.** *We define $e(R)$ as the number of invertible elements in the Smith normal form of the matrix $D(R)$ over $\mathfrak{R}$.*

Note that if $\mathfrak{R} = \mathbb{Z}/d\mathbb{Z}$ for a prime d, $e(R)$ is equal to the rank of $D(R)$ since every nonzero elements in $\mathbb{Z}/d\mathbb{Z}$ is invertible.

We state the main theorem.

▶ **Theorem 5.** *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*

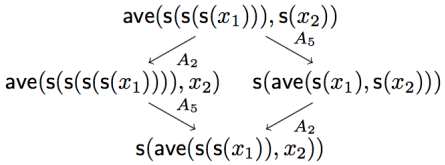
$$\#R' \geq \#R - e(R). \tag{2}$$

We shall see some examples.

▶ **Example 6.** Consider the signature $\Sigma = \{\mathsf{0}^{(0)}, \mathsf{s}^{(1)}, \mathsf{ave}^{(2)}\}$ and the set R of rules

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

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



We can see the matrix $D(R)$ is the 5×1 zero matrix. 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, denoted by $s(H_2(\Sigma, R))$, is equal to 3, though we do not explain how to compute it in this paper. (We will briefly see the meaning of $s(H_2(\Sigma, R))$ in Section 4.)

▶ **Example 7.** We compute the lower bound for the theory of groups, (1). A complete TRS R for the theory of groups is given by

$$G_1.\ m(m(x_1,x_2),x_3) \to m(x_1,m(x_2,x_3)) \quad G_2.\ m(e,x_1) \to x_1$$
$$G_3.\ m(x_1,e) \to x_1 \quad G_4.\ m(x_1,i(x_1)) \to e$$
$$G_5.\ m(i(x_1),x_1) \to e \quad G_6.\ m(i(x_1),m(x_1,x_2)) \to x_2$$
$$G_7.\ i(e) \to e \quad G_8.\ i(i(x_1)) \to x_1$$
$$G_9.\ m(x_1,m(i(x_1),x_2)) \to x_2 \quad G_{10}.\ i(m(x_1,x_2)) \to m(i(x_2),i(x_1)).$$

Since $\deg(R) = 2$, we set $\mathfrak{R} = \mathbb{Z}/2\mathbb{Z}$. R has 48 critical pairs and we get the 10×48 matrix $D(R)$ given in the appendix. The author implemented a program which 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`. The author checked $e(R) = \mathrm{rank}(D(R)) = 8$ by 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 is given by $s(H_2(\Sigma, R)) = 0$.

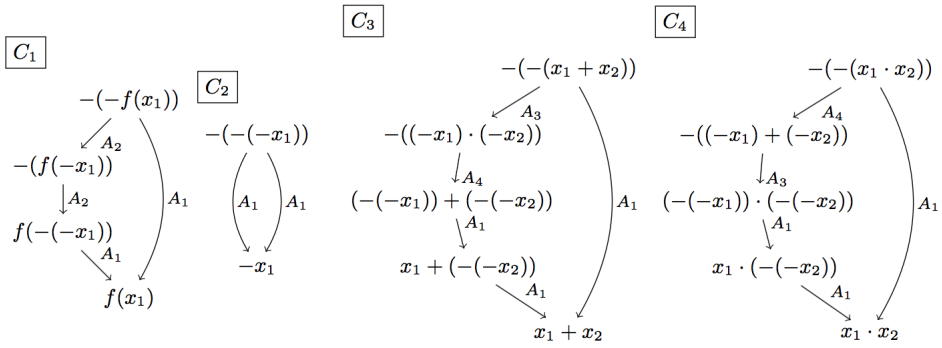


Figure 1 The critical pairs of R.

▶ **Example 8.** Let $\Sigma = \{-^{(1)}, f^{(1)}, +^{(2)}, \cdot^{(2)}\}$ and R be

$$A_1.\ -(-x_1) \to x_1, \qquad A_2.\ -f(x_1) \to f(-x_1),$$
$$A_3.\ -(x_1+x_2) \to (-x_1)\cdot(-x_2), \qquad A_4.\ -(x_1\cdot x_2) \to (-x_1)+(-x_2).$$

We have $\deg(R) = 0$ and R has four critical pairs (Figure 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 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, $\{A_1, A_2, A_3\}$.

Malbos-Mimram's lower bound for this TRS is given by $s(H_2(\Sigma, R)) = 1$.

Although the equality of (2) is attained for the above three examples, it is not guaranteed the equality is attained by some TRS R' in general.

3 Preliminaries on Algebra

In this section, we give a brief introduction to module theory, homological algebra, and Squier's theory of homological algebra for string rewriting systems (SRSs) [8]. Even though Squier's theory is not directly needed to prove our theorem, it is helpful to understand the homology theory for TRSs, which is more complicated than SRSs' case.

3.1 Modules and Homological Algebra

We give basic definitions and theorems on module theory and homological algebra without proofs. For more details, readers are referred to [7, 6] for example.

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

▶ **Definition 9.** *Let $\mathfrak{R}$ be a ring and $(M, +)$ be an abelian group. For a map $\cdot : R \times M \to M$, $(M, +, \cdot)$ is a* left $\mathfrak{R}$-module *if for all $r, s \in R$ 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.

For a map $\cdot : M \times R \to M$, $(M, +, \cdot)$ 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 10.** *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 11.** Any abelian group $(M, +)$ is a $\mathbb{Z}$-module under the scalar multiplication $n \cdot x = \underbrace{x + \cdots + x}_{n}$.

▶ **Example 12.** 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 13.** 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 said *free* if M is isomorphic to $\mathfrak{R}\underline{X}$ for some X. Free modules have some similar properties to vector spaces. If a left $\mathfrak{R}$-module F if 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. 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.

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

▶ **Definition 14.** *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 15** (First isomorphism theorem). *[7, Theorem 7.8] 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 16** (Third isomorphism theorem). *[7, 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 17.** *[7, 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 $\mathfrak{R}$.)*

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 18.** Let M be the $\mathbb{Z}$-module defined by

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

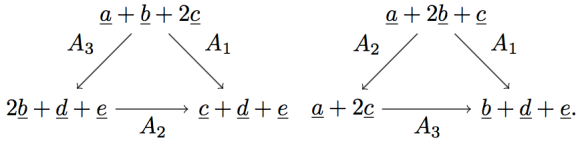
We consider the $\mathbb{Z}$-linear map between free $\mathbb{Z}$-modules $f_0 : \mathbb{Z}^3 \to \mathbb{Z}\underline{\{a, b, c, d, e\}}$ defined by

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

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 systems. 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 rewriting system 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:

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

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 19.** *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 (3) 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 (3) 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 some information of M from a (partial) free resolution which does not depend on the choice of the free resolution. The information is called *homology groups*. To define the homology groups, we introduce the tensor product of modules.

▶ **Definition 20.** *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 $N \times M$. 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 $x \otimes y$.

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.

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

$$\cdots \xrightarrow{N \otimes f_1} N \otimes_{\mathfrak{R}} F_1 \xrightarrow{N \otimes f_0} N \otimes_{\mathfrak{R}} F_0. \tag{4}$$

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 21.** *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 groups *of the chain complex $(C_\bullet, f_\bullet)$.*

The homology groups of the chain complex (4) depend only on M, N, and $\mathfrak{R}$:

▶ **Theorem 22.** *[6, 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 subsection by giving some basic facts on exact sequences.

▶ **Proposition 23.** *[7, Proposition 7.20 and 7.21]*

1. *$M_1 \xrightarrow{f} M_2 \to 0$ is exact if and only if $\ker f = 0$.*
2. *$0 \to M_1 \xrightarrow{f} M_2$ is exact if and only if $\mathrm{im}\, f = M_2$.*
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 24.** *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 [7, Proposition 7.22].

3.2 String Rewriting Systems and Homology Groups of Monoids

For an alphabet Σ, Σ^* denotes the set of all strings of symbols over Σ. Σ^* forms a monoid under the operation of concatenation with the empty string serving as the identity, and we call Σ^* the free monoid generated by Σ. For a string rewriting system (SRS) (Σ, R), we write $\mathcal{M}_{(\Sigma,R)}$ for the set defined by $\mathcal{M}_{(\Sigma,R)} = \Sigma^*/\overset{*}{\leftrightarrow}_R$. We can see $\mathcal{M}_{(\Sigma,R)}$ is a monoid under the operations $[u] \cdot [v] = [uv]$ where $[w]$ denotes the equivalence class of $w \in \Sigma^*$ with respect to $\overset{*}{\leftrightarrow}_R$.

We say that two SRSs $(\Sigma_1, R_1), (\Sigma_2, R_2)$ are *isomorphic* if the monoids $\mathcal{M}_{(\Sigma_1,R_1)}, \mathcal{M}_{(\Sigma_2,R_2)}$ are isomorphic. It is not difficult to show that for any two SRSs $(\Sigma, R_1), (\Sigma, R_2)$ with the same signature, if R_1 and R_2 are equivalent (i.e., $\overset{*}{\leftrightarrow}_{R_1} = \overset{*}{\leftrightarrow}_{R_2}$), then (Σ, R_1) and (Σ, R_2) are isomorphic. Roughly speaking, the notion that two SRSs are isomorphic means that the SRSs are equivalent but their alphabets can be different. For example, let Σ_1 be $\{a, b, c\}$ and R_1 be $\{abb \to ab,\ ba \to c\}$. Then, (Σ_1, R_1) is isomorphic to (Σ_2, R_2) where $\Sigma_2 = \{a, b\}$ and $R_2 = \{abb \to ab\}$. Intuitively, since c is equivalent to ba with respect to the congruence $\overset{*}{\leftrightarrow}_{R_1}$, c is redundant as long as we consider strings modulo $\overset{*}{\leftrightarrow}_{R_1}$ and (Σ_2, R_2) is the SRS made by removing c from (Σ_1, R_1).

If a monoid S is isomorphic to $\mathcal{M}_{(\Sigma,R)}$ for an SRS (Σ, R), we call (Σ, R) a *presentation* of the monoid S.

Let S be a monoid and consider the free $\mathbb{Z}$-module $\mathbb{Z}\underline{S}$. $\mathbb{Z}\underline{S}$ can be equipped with a ring structure under the multiplication $\left(\sum_{w\in S} n_w\underline{w}\right)\left(\sum_{w\in S} m_w\underline{w}\right) = \sum_{w,v\in S} n_w m_v \underline{wv}$ where $n_w m_v$ is the usual multiplication of integers and wv is the multiplication of the monoid S. $\mathbb{Z}\underline{S}$ as a ring is called the *integral monoid ring* of S. When we think of $\mathbb{Z}\underline{S}$ as a ring, we write $\mathbb{Z}\langle S\rangle$ instead of $\mathbb{Z}\underline{S}$.

We consider $\mathbb{Z}\langle S\rangle$-modules. The group of integers $\mathbb{Z}$ forms a left (resp. right) $\mathbb{Z}\langle S\rangle$-module under the scalar multiplication $\left(\sum_{w\in S} n_w\underline{w}\right)\cdot m = \sum_{w\in S} n_w m\underline{w}$ (resp. $m\cdot\left(\sum_{w\in S} n_w\underline{w}\right) = \sum_{w\in S} n_w m\underline{w}$). Let $\cdots \xrightarrow{\partial_1} F_1 \xrightarrow{\partial_0} F_0 \xrightarrow{\epsilon} \mathbb{Z}$ be a free resolution of $\mathbb{Z}$ over the ring $\mathbb{Z}\langle S\rangle$. The *$i$-th monoid homology* $H_i(S)$ is defined as the i-th homology group of the chain complex $(\mathbb{Z}\otimes_{\mathbb{Z}\langle S\rangle} F_\bullet, \mathbb{Z}\otimes\partial_\bullet)$, i.e.,

$$H_i(S) = H_i(\mathbb{Z}\otimes_{\mathbb{Z}\langle S\rangle} F_\bullet, \mathbb{Z}\otimes\partial_\bullet) = \ker \mathbb{Z}\otimes\partial_{i-1}/\operatorname{im}\mathbb{Z}\otimes\partial_i.$$

If S is isomorphic to $\mathcal{M}_{(\Sigma,R)}$ for some SRS (Σ, R), it is known that there is a free resolution in the form of

$$\cdots \to (\mathbb{Z}\langle S\rangle)\underline{P} \xrightarrow{\partial_2} (\mathbb{Z}\langle S\rangle)\underline{R} \xrightarrow{\partial_1} (\mathbb{Z}\langle S\rangle)\underline{\Sigma} \xrightarrow{\partial_0} (\mathbb{Z}\langle S\rangle)\underline{\{\star\}} \xrightarrow{\epsilon} \mathbb{Z}$$

for some set P. Squier [8] showed that if the SRS (Σ, R) is complete and reduced[1], there is $\partial_2 : (\mathbb{Z}\langle S\rangle)\underline{P} \to (\mathbb{Z}\langle S\rangle)\underline{R}$ for $P =$ (the critical pairs of R) so that we can compute $H_2(S) = \ker\partial_1/\operatorname{im}\partial_2$ explicitly. This is an analog of Example 18, but we omit the details here. For an abelian group G, let $s(G)$ denote the minimum number of generators of G (i.e., the minimum cardinality of the subset $A \subset G$ such that any element $x \in G$ can be written by $x = a_1 + \cdots + a_k - a_{k+1} - \cdots - a_m$ for $a_1, \ldots, a_m \in A$). Then, we have the following theorem:

▶ **Theorem 25.** *Let (Σ, R) be an SRS and $S = \mathcal{M}_{(\Sigma,R)}$. Then $\#\Sigma \geq s(H_1(S))$, $\#R \geq s(H_2(S))$.*

To prove this theorem, we use the following lemma:

▶ **Lemma 26.** *Let X be a set. The group homomorphism $\mathbb{Z}\otimes_{\mathbb{Z}\langle S\rangle}(\mathbb{Z}\langle S\rangle)\underline{X} \to \mathbb{Z}\underline{X}$, $n\langle w\rangle\underline{x} \mapsto n\underline{x}$ is an isomorphism.*

This lemma is proved in a straightforward way.

Proof of Theorem 25. Since $\mathbb{Z}\otimes_{\mathbb{Z}\langle S\rangle}(\mathbb{Z}\langle S\rangle)\underline{X} \cong \mathbb{Z}\underline{X}$ by the above lemma, $s(\mathbb{Z}\otimes_{\mathbb{Z}\langle S\rangle}(\mathbb{Z}\langle S\rangle)\underline{X}) = s(\mathbb{Z}\underline{X}) = \#X$. For any set Y and group homomorphism $f : \mathbb{Z}\underline{X} \to \mathbb{Z}\underline{Y}$, since $\ker f$ is a subgroup of $\mathbb{Z}\underline{X}$, we have $\#X \geq s(\ker f)$. For any subgroup H of $\ker f$, $\ker f/H$ is generated by $[x_1], \ldots, [x_k]$ if $\ker f$ is generated by $x_1, \ldots, x_k$. Thus $\#\Sigma \geq s(\ker\partial_0/\operatorname{im}\partial_1) = s(H_1(S))$, $\#R \geq s(\ker\partial_1/\operatorname{im}\partial_2) = s(H_2(S))$. ◀

Note that $H_i(S)$ does not depend on the choice of presentation (Σ, R) by Theorem 22. Therefore, Theorem 25 can be restated as follows: Let (Σ, R) be an SRS. For any SRS (Σ', R') isomorphic to (Σ, R), the number of symbols $\#\Sigma'$ is bounded below by $s(H_1(\mathcal{M}_{(\Sigma,R)}))$ and the number of rules $\#R'$ is bounded below by $s(H_2(\mathcal{M}_{(\Sigma,R)}))$.

[1] An SRS (Σ, R) is reduced if for each $l \to r \in R$, r is normal w.r.t. $\to_R$ and there does not exist $l' \to r' \in R$ such that $l' = ulv \neq l$ for some $u, v \in \Sigma^*$

4 An Overview of the Homology Theory of TRSs

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

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

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

where $t_i[s_1/x_1, \dots, s_m/x_m]$ denotes the term obtained by substituting s_j for x_j in t_i for each $j = 1, \dots, m$ 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-uple $\langle s_1, \dots, s_m \rangle$ of terms as a (parallel) substitution $\{x_1 \mapsto s_1, \dots, x_m \mapsto s_m\}$. 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-uple s of terms, and rewrite rule $l \to r \in R$ whose variables are included in $\{x_1, \dots, x_m\}$. This definition suggests that the pair of a context C and an m-uple of terms (or equivalently, substitution) s is useful to think about rewrite relations. Malbos and Mimram [3] called the pair of a context and an m-uple 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 $l_1 \to r_1$, $l_2 \to r_2$.

The composition of two bicontexts $(C, t), (D, s)$ $(t = \langle t_1, \dots, t_n \rangle,\ s = \langle s_1, \dots, s_m \rangle)$ is defined by

$$(C, t) \circ (D, s) = (C[D \circ t], s \circ t)$$

where $D \circ t = D[t_1/x_1, \dots, t_n/x_n]$ and note that the order of composition is reversed in the second component. With this composition, we can define the small category of bicontexts $\mathbb{K}$ as

- Objects : natural numbers,
- Morphisms $\mathbb{K}(n, m)$ $(n, m \in \mathbb{N})$: bicontexts (C, t) where $t = \langle t_1, \dots, t_n \rangle$ and each t_i and C have variables in $\{x_1, \dots, x_m\}$ (except $\Box$ in C),
- Identity $\mathrm{id}_n = (\Box, \langle x_1, \dots, x_n \rangle)$,
- Composition $\circ : \mathbb{K}(n, m) \times \mathbb{K}(k, n) \to \mathbb{K}(k, m)$: defined above.

To apply homological algebra to TRSs, we construct an algebraic structure from $\mathbb{K}$. We write $\mathbb{Z}\langle\mathbb{K}\rangle$ for the (small) category whose objects are natural numbers, set of morphisms $(\mathbb{Z}\langle\mathbb{K}\rangle)(n, m)$ is 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 in the form of 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). The composition on $\mathbb{Z}\langle\mathbb{K}\rangle$ is defined by

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

By this definition, we can see that this composition $\circ$ is bilinear, that is,

$$a \circ (b_1 + b_2) = a \circ b_1 + a \circ b_2, \tag{5}$$

$$(a_1 + a_1) \circ b = a_1 \circ b + a_2 \circ b \tag{6}$$

for any $a, a_1, a_2 \in (\mathbb{Z}\langle\mathbb{K}\rangle)(n, m)$, $b, b_1, b_2 \in (\mathbb{Z}\langle\mathbb{K}\rangle)(k, n)$. Also, we have

$$a \circ 0 = 0 \circ b = 0. \tag{7}$$

One may notice that this looks something similar to the ring structure. Indeed, $\mathbb{Z}\langle\mathbb{K}\rangle$ forms the structure called *ringoid*, which is defined as follows:

▶ **Definition 27.** *A ringoid $\mathcal{R}$ is a small category in which each hom-set $\mathcal{R}(X, Y)$ is equipped with a structure of abelian group $(\mathcal{R}(X, Y), +)$ and satisfies (5, 6, 7).*

Intuitively, a ringoid $\mathcal{R}$ is a "multi-sorted" ring where sorts are the hom-sets $\mathcal{R}(X, Y)$ for any objects X, Y of $\mathcal{R}$ and it has an addition $+ : \mathcal{R}(X, Y) \times \mathcal{R}(X, Y) \to \mathcal{R}(X, Y)$ for each pair (X, Y) of objects, and a multiplication $\circ : \mathcal{R}(Y, Z) \times \mathcal{R}(X, Y) \to \mathcal{R}(X, Z)$ for each triple (X, Y, Z) of objects. If $\mathcal{R}$ has exactly one object $\star$, the ringoid $\mathcal{R}$ can be identified with the ring $(\mathcal{R}(\star, \star), +, \circ)$. (Note that the morphisms correspond to the elements of the ring, not objects.) We can also define modules over a ringoid. For a ringoid $\mathcal{R}$, a left $\mathcal{R}$-module M associates each object X of $\mathcal{R}$ with an abelian group $M(X)$ and has a "multi-sorted" scalar multiplication $\cdot : \mathcal{R}(X, Y) \times M(X) \to M(Y)$ for each pair of objects X, Y of $\mathcal{R}$. This notion is interpreted as a functor from the category $\mathcal{R}$ to the category of abelian groups:

▶ **Definition 28.** *Let $\mathcal{R}$ be a ringoid. A left $\mathcal{R}$-module is a functor $M : \mathcal{R} \to \mathbf{Ab}$ satisfying*

$$M(a + b) = M(a) + M(b),\ M(0) = 0 \quad (a, b \in \mathcal{R}(X, Y), X, Y \in \mathrm{Obj}(\mathcal{R}))$$

where $\mathbf{Ab}$ is the category of abelian groups. We define the scalar multiplication $\cdot : \mathcal{R}(X, Y) \times M(X) \to M(Y)$ by $a \cdot m = M(a)(m)$.

A right $\mathcal{R}$-module is defined as 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 such that each component $f_X : M_1(X) \to M_2(X)$ is a group homomorphism.

If $\mathcal{R}$ has exactly one object $\star$, M can be identified with the left $\mathcal{R}(\star, \star)$-module $(M(\star), +, \cdot)$. A free $\mathcal{R}$-module is defined as follows.

▶ **Definition 29.** *Let $\mathcal{R}$ be a ringoid and P be a family of sets P_X $(X \in \mathrm{Obj}(\mathcal{R}))$. The free left $\mathcal{R}$-module generated by P, denoted by $\mathcal{R}\underline{P}$ is defined as follows. For each object $X \in \mathrm{Obj}(\mathcal{R})$, $(\mathcal{R}\underline{P})(X)$ is the abelian group of formal finite sums*

$$\sum_{x_Y \in P_Y,\ Y \in \mathrm{Obj}(\mathcal{R})} a_{x_Y} \underline{x_Y}, \quad (a_{x_Y} \in \mathcal{R}(Y, X))$$

and for each morphism $r \in \mathcal{R}(X, Z)$,

$$r \cdot \left(\sum_{x_Y \in P_Y,\ Y \in \mathrm{Obj}(\mathcal{R})} a_{x_Y} \underline{x_Y} \right) = \sum_{x_Y \in P_Y,\ Y \in \mathrm{Obj}(\mathcal{R})} (r \circ a_{x_Y}) \underline{x}_Y.$$

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 $D\underline{x}t + C\underline{x}t$.

The tensor product of two modules over a ringoid is also defined.

▶ **Definition 30.** *Let $\mathcal{R}$ be a ringoid, M_1 be a right $\mathcal{R}$-module, and M_2 be a left $\mathcal{R}$-module. For a family of 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 $\{(g_X)_{X \in P} \in \prod_{X \in P} G_X \mid g_X = 0$ except for finite Xs$\}$. The direct sum of groups also forms a group.*

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

Now, we outline Malbos-Mimram's construction of the homology groups of TRSs.

1. We begin by defining the quotient ringoid $\overline{\mathbb{Z}\langle\mathbb{K}\rangle}^{(\Sigma,R)}$ of $\mathbb{Z}\langle\mathbb{K}\rangle$ by some relations so that $\overline{\mathbb{Z}\langle\mathbb{K}\rangle}^{(\Sigma,R)}$ depends only on the Tietze equivalence class of (Σ, R). $\overline{\mathbb{Z}\langle\mathbb{K}\rangle}^{(\Sigma,R)}$ corresponds to $\mathcal{M}_{(\Sigma,R)}$ in the case (Σ, R) is an SRS.
2. From this step, we write $\mathcal{R}$ for $\overline{\mathbb{Z}\langle\mathbb{K}\rangle}^{(\Sigma,R)}$. It can be shown that we have a partial free resolution

$$\mathcal{R}\underline{\mathbf{P}_3} \xrightarrow{\partial_2} \mathcal{R}\underline{\mathbf{P}_2} \xrightarrow{\partial_1} \mathcal{R}\underline{\mathbf{P}_1} \xrightarrow{\partial_0} \mathcal{R}\underline{\mathbf{P}_0} \xrightarrow{\epsilon} \mathcal{Z}$$

   where every $\mathbf{P}_i$ is a family of sets $(\mathbf{P}_i)_j$ given by $(\mathbf{P}_0)_1 = \{1\}$, $(\mathbf{P}_0)_j = \emptyset$ $(j \neq 1)$, $(\mathbf{P}_1)_j = \Sigma^{(j)} = \{f \in \Sigma \mid f \text{ is of arity } j\}$, $(\mathbf{P}_2)_j = \{l \to r \in R \mid l \to r \text{ is of arity } j\}$, $(\mathbf{P}_3)_j = \{((\Box, A, s), (C, B, t)) : \text{critical pair} \mid A, B \in (\mathbf{P}_2)_j\}$. $\mathcal{Z}$ is a left $\mathcal{R}$-module defined as the quotient of $\mathcal{R}\underline{P}$ by all relations of the form $\sum_i (\kappa_i(u) \circ t)\underline{\star}\langle t_i\rangle - \Box\underline{\star}\langle u \circ t\rangle$ for every term $u \circ t$ where $P_1 = \{\star\}$, $P_j = \emptyset$ $(j \neq 1)$ and κ_i is defined later.
3. By taking the tensor product $\mathbb{Z}\otimes_{\mathcal{R}}$, we have the chain complex

$$\mathbb{Z} \otimes_{\mathcal{R}} \mathcal{R}\underline{\mathbf{P}_3} \xrightarrow{\mathbb{Z}\otimes\partial_2} \mathbb{Z} \otimes_{\mathcal{R}} \mathcal{R}\underline{\mathbf{P}_2} \xrightarrow{\mathbb{Z}\otimes\partial_1} \mathbb{Z} \otimes_{\mathcal{R}} \mathcal{R}\underline{\mathbf{P}_1} \xrightarrow{\mathbb{Z}\otimes\partial_0} \mathbb{Z} \otimes_{\mathcal{R}} \mathcal{R}\underline{\mathbf{P}_0} \tag{8}$$

   where $\mathbb{Z}$ above is the $\mathcal{R}$-module defined by $\mathbb{Z}(i) = \mathbb{Z}$ (the abelian group of integers) for each object i, and the scalar multiplication is given by $(C, t) \cdot k = k$.
4. The homology groups can be defined by

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

   It is shown that the homology groups of TRS depend only on the "Tietze equivalence" class of (Σ, R). Tietze equivalence is an analog of isomorphism between SRSs; it is an equivalence between two TRSs (Σ_1, R_1), (Σ_2, R_2) where the signatures Σ_1 and Σ_2 can be different, while the usual equivalence is defined for TRSs with the same signature by $\overset{*}{\leftrightarrow}_{R_1} = \overset{*}{\leftrightarrow}_{R_2}$. Especially, any two TRSs (Σ, R_1),(Σ, R_2) are Tietze equivalent if they are equivalent in the usual sense, $\overset{*}{\leftrightarrow}_{R_1} = \overset{*}{\leftrightarrow}_{R_2}$. Thus, we have the following:

$$\overset{*}{\leftrightarrow}_{R_1} = \overset{*}{\leftrightarrow}_{R_2} \implies H_i(\Sigma, R_1) \cong H_i(\Sigma, R_2).$$

For the step 1, we define the relations of $\overline{\mathbb{Z}\langle\mathbb{K}\rangle}^{(\Sigma,R)}$. We identify elements in $\mathbb{Z}\langle\mathbb{K}\rangle$ as follows. (a) For two m-uples $t = \langle t_1, \ldots, t_m\rangle, s = \langle s_1, \ldots, s_m\rangle$ of terms, we identify t and s if $t \overset{*}{\leftrightarrow}_R s$. (b) Similarly, for two single-hole contexts C, D, we identify C and D if $C \overset{*}{\leftrightarrow}_R D$. For the last identification, we introduce operator κ_i which takes a term t and returns the formal sum of single-hole contexts $C_1 + \cdots + C_m$ where C_j $(j = 1, \ldots, m)$ is obtained by replacing the j-th occurrence of x_i with $\Box$ in t, and m is the number of the occurrences of x_i in t. For example, we have

$$\begin{aligned}
\kappa_1(f(g(x_1, x_2), x_1)) &= f(g(\Box, x_2), x_1) + f(g(x_1, x_2), \Box),\\
\kappa_2(f(g(x_1, x_2), x_1)) &= f(g(x_1, \Box), x_1),\\
\kappa_2(h(x_1)) &= 0.
\end{aligned}$$

The definition of κ_i can be stated inductively as follows:

$$\begin{aligned}
\kappa_i(x_i) = \Box,\ \kappa_i(x_j) = 0 \quad (j \neq i),\\
\kappa_i(f(t_1, \ldots, t_n)) = \sum_{k=1}^{n} f(t_1, \ldots, t_{k-1}, \kappa_i(t_k), t_{k+1}, \ldots, t_n).
\end{aligned}$$

Then, (c) we identify formal sums of bicontexts $(C_1,t)+\cdots+(C_k,t)$ and $(D_1,t)+\cdots+(D_l,t)$ if $\kappa_i(u)=C_1+\cdots+C_k$, $\kappa_i(v)=D_1+\cdots+D_l$ for some positive integer i and terms u,v such that $u \overset{*}{\leftrightarrow}_R v$. $\overline{\mathbb{Z}\langle\mathbb{K}\rangle}^{(\Sigma,R)}$ is defined as the quotient of $\mathbb{Z}\langle\mathbb{K}\rangle$ by the equivalence class generated by the identifications (a), (b), and (c).

We omit the definitions of the $\mathcal{R}$-linear maps ϵ,∂_i $(i=0,1,2)$ in the step 2, but we describe the group homomorphisms $\mathbb{Z}\otimes\partial_i : \mathbb{Z}\otimes_{\mathcal{R}}\mathcal{R}\underline{\mathbf{P}_{i+1}} \to \mathbb{Z}\otimes_{\mathcal{R}}\mathcal{R}\underline{\mathbf{P}_i}$. Let $\tilde{\partial}_i$ denote $\mathbb{Z}\otimes\partial_i$ for simplicity. For the step 2, we define the $\mathcal{R}$-linear maps ϵ,∂_i $(i=0,1,2)$. For $f^{(n)}\in\Sigma$, the homomorphism $\tilde{\partial}_0 : \mathbb{Z}\otimes_{\mathcal{R}}\mathcal{R}\underline{\mathbf{P}_1} \to \mathbb{Z}\otimes_{\mathcal{R}}\mathcal{R}\underline{\mathbf{P}_0}$ is given by

$$\tilde{\partial}_0(\underline{f}) = (n-1)\underline{1}.$$

For a term t, we define $\varphi(t)$ as the linear combinaton of symbols $\sum_{f\in\Sigma} n_f \underline{f}$ where n_f is the number of occurrences of f in t. Using this, for $l\to r\in R$, the homomorphism $\tilde{\partial}_1 : \mathbb{Z}\otimes_{\mathcal{R}}\mathcal{R}\underline{\mathbf{P}_2} \to \mathbb{Z}\otimes_{\mathcal{R}}\mathcal{R}\underline{\mathbf{P}_1}$ is given by

$$\tilde{\partial}_1(\underline{l\to r}) = \varphi(r)-\varphi(l).$$

For a critical pair $((\Box,l\to r,s),(C,u\to v,t))$, let $(D_i,l_i\to r_i,s_i)$, $(C_j,u_j\to v_j,t_j)$ $(i=1,\dots,k,j=1,\dots,l)$ be rewriting steps such that $r\circ s = D_1[l_1\circ s_1],D_1[r_1\circ s_1] = D_2[l_2\circ s_2],\dots,D_{k-1}[r_{k-1}\circ s_{k-1}] = D_k[l_k\circ s_k]$, $C[v\circ t]=C_1[u_1\circ t_1],C_1[v_1\circ t_1]=C_2[u_2\circ t_2],\dots,C_{l-1}[v_{l-1}\circ t_{l-1}]=C_l[u_l\circ t_l]$, $D_k[r_k\circ s_k]=C_l[v_l\circ t_l]$. Then the map $\tilde{\partial}_2((\Box,l\to r,s),(C,u\to v,t))$ is defined by

$$\underline{u\to v}-\underline{l\to v}-\sum_{i=1}^{k}\underline{u_i\to v_i}-\sum_{j=1}^{l}\underline{l_j\to r_j}.$$

Malbos-Mimram's lower bound for the number of rewrite rules is given by $s(H_2(\Sigma,R))$. (Recall that $s(G)$ denotes the minimum number of generators of an abelian group G.) More precisely, $\#\Sigma'\geq s(H_1(\Sigma,R))$ and $\#R'\geq s(H_2(\Sigma,R))$ hold for any TRS (Σ',R') that is Tietze equivalent to (Σ,R). These inequalities are shown in a similar way to the proof of Theorem 25.

5 Proof of Main Theorem

Let (Σ,R) be a complete TRS. We first simplify the tensor product $\mathbb{Z}\otimes_{\mathcal{R}}\mathbb{Z}\underline{\mathbf{P}_i}$ in (8).

▶ **Lemma 31.** *Let $d=\deg(R)$ and P be a family of sets $P_0,P_1,\dots$. Then, we have $\mathbb{Z}\otimes_{\mathcal{R}}\mathcal{R}\underline{P}\cong(\mathbb{Z}/d\mathbb{Z})\underline{\biguplus_i P_i}$. Especially, if $d=0$, $\mathbb{Z}\otimes_{\mathcal{R}}\mathcal{R}\underline{P}\cong\mathbb{Z}\underline{\biguplus_i P_i}$.*

Proof. We define a group homomorphism $f:\mathbb{Z}\otimes_{\mathcal{R}}\mathcal{R}\underline{P}\to(\mathbb{Z}/d\mathbb{Z})\underline{\biguplus_i P_i}$ by $f((w_n)_{n\geq 0})=\sum_{n\geq 0}f_n(w_n)$ where $f_n:\mathbb{Z}\otimes_{\mathcal{R}(n,n)}\mathcal{R}\underline{P}(n)\to(\mathbb{Z}/d\mathbb{Z})\underline{P_n}$ is defined by $f_n(k\otimes C\underline{a}t)=[k]\underline{a}$ for $a\in P_n$. It is enough to show each f_n is an isomorphism. If $\#_i l-\#_i r=m$ for $l\to r\in R$, we have a relation of $\mathcal{R}$

$$0=1\otimes(\kappa_i(l)\underline{a}t-\kappa_i(r)\underline{a}t)=1\otimes\kappa_i(l)\underline{a}t-1\otimes\kappa_i(r)\underline{a}t=\#_i l\otimes\underline{a}-\#_i r\otimes\underline{a}=m\otimes\underline{a}.$$

Since d divides m, $f_n(m\otimes\underline{a})=[m]\underline{a}=0$. Therefore f_n is well-defined. To prove f_n is injective, it suffices to show $qd\otimes\underline{a}=0$ for any $q\in\mathbb{Z}$. Since $d=\gcd\{\#_i l-\#_i r\mid l\to r\in R,i=1,2,\dots\}$, there exist integers $c_{i,l\to r}$ such that $d=\sum_{l\to r\in R,\ i=1,2,\dots}c_{i,l\to r}(\#_i l-\#_i r)$. Since $(\#_i l-\#_i r)\otimes\underline{a}=1\otimes(\kappa_i(l)-\kappa_i(r))\underline{a}\langle x_1,\dots,x_n\rangle=0$ for each $i\in\{0,1,\dots\}$, $l\to r\in R$, we have $qd\otimes\underline{a}=q\sum_{l\to r\in R,\ i=1,2,\dots}c_{i,l\to r}(\#_i l-\#_i r)\otimes\underline{a}=0$. The surjectivity of f_n is trivial. ◀

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

To prove Theorem 5, we show the following lemma.

▶ **Lemma 32.** *Let $d = \deg(R)$. If $d = 0$ or d is prime, $\#R - e(R) = s(H_2(\Sigma, R)) + s(\operatorname{im} \tilde{\partial}_1)$.*

Proof. By definition, $D(R)$ defined in Section 2 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 $\mathbb{Z}/d\mathbb{Z}$-vector space. By the rank-nullity theorem, we have

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

Suppose $d = 0$. We show $H_2(\Sigma, R) \cong \mathbb{Z}^{\#R-r-k} \times \mathbb{Z}/e_1\mathbb{Z} \times \cdots \times \mathbb{Z}/e_r\mathbb{Z}$ 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 $\mathbb{Z} \otimes_{\mathcal{R}} \mathcal{R}\underline{\mathbf{P}_1}/\operatorname{im} \tilde{\partial}_2 \cong \mathbb{Z}^{\#R-r} \times \mathbb{Z}/e_1\mathbb{Z} \times \cdots \times \mathbb{Z}/e_k\mathbb{Z}$. 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, $\ker \overline{\partial}_1 \cong \mathbb{Z}^{\#R-r-k} \times \mathbb{Z}/e_1\mathbb{Z} \times \cdots \times \mathbb{Z}/e_r\mathbb{Z}$.

Since $\mathbb{Z}/e\mathbb{Z} \cong 0$ if e is invertible, $\mathbb{Z}^{\#R-r-k} \times \mathbb{Z}/e_1\mathbb{Z} \times \cdots \times \mathbb{Z}/e_k\mathbb{Z} \cong \mathbb{Z}^{\#R-r-k} \times \mathbb{Z}/e_{e(R)+1}\mathbb{Z} \times \cdots \mathbb{Z}/e_r\mathbb{Z} =: G$. G is generated by $(\underbrace{1, 0, \ldots, 0}_{\#R-r-k}, \underbrace{[0], \ldots, [0]}_{r-e(R)})$, $(0, \ldots, 0, 1, [0], \ldots, [0])$, $(0, \ldots, 0, [1], [0], \ldots, [0])$, $(0, \ldots, 0, [0], \ldots, [0], [1])$, 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 $G/pG \cong (\mathbb{Z}/p\mathbb{Z})^{\#R-k-e(R)}$. It is not hard to see $s(G) \geq s(G/pG)$, and since G/pG is a $\mathbb{Z}/p\mathbb{Z}$-vector space, $s(G/pG) = \dim(G/pG) = \#R - k - e(R)$. Thus, $s(H_2(\Sigma, R)) = s(G) = \#R - s(\operatorname{im} \tilde{\partial}_1) - e(R)$. ◀

By Lemma 32, Theorem 5 is implied by the following theorem:

▶ **Theorem 33.** *Let (Σ, R) be a complete TRS and $d = \deg(R)$. If $d = 0$ or d is prime,*

$$\#R \geq s(H_2(\Sigma, R)) + s(\operatorname{im} \tilde{\partial}_1). \tag{9}$$

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

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

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

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

Thus, we obtain the following exact sequence by Proposition 23:

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

By Theorem 17, since $\operatorname{im}\tilde{\partial}_1 \subset \mathbb{Z} \otimes_{\mathcal{R}} \mathcal{R}\underline{\mathbb{P}_1} \cong (\mathbb{Z}/d\mathbb{Z})\underline{R}$ and $(\mathbb{Z}/d\mathbb{Z})\underline{R}$ is a free $\mathbb{Z}/d\mathbb{Z}$-module, $\operatorname{im}\tilde{\partial}_1$ is also free and by Proposition 24, we have $\mathbb{Z} \otimes_{\mathcal{R}} \mathcal{R}\underline{\mathbb{P}_2}/\operatorname{im}\tilde{\partial}_2 \cong H_2(\Sigma, R) \times \operatorname{im}\tilde{\partial}_1$. Therefore, $s(\mathbb{Z} \otimes_{\mathcal{R}} \mathcal{R}\underline{\mathbb{P}_2}/\operatorname{im}\tilde{\partial}_2) = s(H_2(\Sigma, R)) + s(\operatorname{im}\tilde{\partial}_1)$. Since $\mathbb{Z} \otimes_{\mathcal{R}} \mathcal{R}\underline{\mathbb{P}_2}/\operatorname{im}\tilde{\partial}_2$ 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

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

Thus, we get (9). ◀

Proof of Theorem 5. As we stated, $H_2(\Sigma, R)$ depends only on the Tietze equivalence class of (Σ, R). Let us show $s(\operatorname{im}\tilde{\partial}_1)$ also depends only on the Tietze equivalence class of (Σ, 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 any element $s_1, \ldots, s_k \in \Gamma$, and $r_1 s_1 + \cdots + r_k s_k = 0 \implies r_1 = \cdots = r_k = 0$ 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 [7, 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 equivalence class of (Σ, R), so does $\operatorname{rank}(\operatorname{im}\tilde{\partial}_1)$.

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

We consider the case where every symbol in Σ is of arity 1. Notice that any TRS (Σ, R) can be seen as an SRS and $\deg(R) = 0$ in this case. We have $\operatorname{rank}(\ker\tilde{\partial}_0) = \#\Sigma$ since $\tilde{\partial}_0(\underline{f}) = 0$ for any $f \in \Sigma$. Therefore, (9) can be rewritten to

$$\#R - \#\Sigma \geq s(H_2(\Sigma, R)) - \operatorname{rank}(H_1(\Sigma, R)).$$

So, for SRSs, we have a lower bound of the number of the rewrite rules minus the number of the symbols. For groups, in fact, this inequality is proved in terms of group homology [1].

References

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

2 K. Kunen. Single axioms for groups. *Journal of Automated Reasoning*, 9(3):291–308, December 1992. doi:10.1007/BF00245293.

3 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.

4 B. H. Neumann. Another single law for groups. *Bulletin of the Australian Mathematical Society*, 23(1):81–102, 1981. doi:10.1017/S0004972700006912.

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

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

7 J. J. Rotman. *Advanced Modern Algebra*, volume 114. American Mathematical Soc., 2010.

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

9 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.

A The matrix $D(R)$ for The Theory of Groups

For the TRS R defined in Example 7, $D(R)$ is given by the transpose of

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

where the i-th column corresponds to the rule G_i, and the j-th row corresponds to the critical pair C_j shown in the next pages.

$C_1 : m(m(x_1,x_2),x_3) \to m(x_1,m(x_2,x_3)),\quad m(m(x_4,x_5),x_6) \to m(x_4,m(x_5,x_6)),\quad m(\Box,x_3),$
$\{x_6 \mapsto x_2, x_1 \mapsto m(x_4,x_5)\}$
$C_2 : i(m(x_1,x_2)) \to m(i(x_2),i(x_1)),\quad m(m(x_3,x_4),x_5) \to m(x_3,m(x_4,x_5)),\quad i(\Box),$
$\{x_5 \mapsto x_2, x_1 \mapsto m(x_3,x_4)\}$
$C_3 : m(m(x_1,x_2),x_3) \to m(x_1,m(x_2,x_3)),\quad m(x_4,m(i(x_4),x_5)) \to x_5,\quad m(\Box,x_3),$
$\{x_2 \mapsto m(i(x_1),x_5), x_4 \mapsto x_1\}$
$C_4 : m(x_1,m(i(x_1),x_2)) \to x_2,\quad m(m(x_3,x_4),x_5) \to m(x_3,m(x_4,x_5)),\quad \Box,$
$\{x_5 \mapsto m(i(m(x_3,x_4)),x_2), x_1 \mapsto m(x_3,x_4)\}$
$C_5 : m(m(x_1,x_2),x_3) \to m(x_1,m(x_2,x_3)),\quad m(i(x_4),m(x_4,x_5)) \to x_5,\quad m(\Box,x_3),$
$\{x_2 \mapsto m(x_4,x_5), x_1 \mapsto i(x_4)\}$
$C_6 : m(i(x_1),m(x_1,x_2)) \to x_2,\quad m(m(x_3,x_4),x_5) \to m(x_3,m(x_4,x_5)),\quad m(i(x_1),\Box),$
$\{x_5 \mapsto x_2, x_1 \mapsto m(x_3,x_4)\}$
$C_7 : m(m(x_1,x_2),x_3) \to m(x_1,m(x_2,x_3)),\quad m(i(x_4),x_4) \to e,\quad m(\Box,x_3),$
$\{x_4 \mapsto x_2, x_1 \mapsto i(x_2)\}$
$C_8 : m(m(x_1,x_2),x_3) \to m(x_1,m(x_2,x_3)),\quad m(x_4,i(x_4)) \to e,\quad m(\Box,x_3),$
$\{x_2 \mapsto i(x_1), x_4 \mapsto x_1\}$
$C_9 : m(x_1,i(x_1)) \to e,\quad m(m(x_2,x_3),x_4) \to m(x_2,m(x_3,x_4)),\quad \Box,$
$\{x_4 \mapsto i(m(x_2,x_3)), x_1 \mapsto m(x_2,x_3)\}$
$C_{10} : m(m(x_1,x_2),x_3) \to m(x_1,m(x_2,x_3)),\quad m(x_4,e) \to x_4,\quad m(\Box,x_3),\quad \{x_2 \mapsto e, x_4 \mapsto x_1\}$
$C_{11} : m(x_1,e) \to x_1,\quad m(m(x_2,x_3),x_4) \to m(x_2,m(x_3,x_4)),\quad \Box,\quad \{x_4 \mapsto e, x_1 \mapsto m(x_2,x_3)\}$
$C_{12} : m(m(x_1,x_2),x_3) \to m(x_1,m(x_2,x_3)),\quad m(e,x_4) \to x_4,\quad m(\Box,x_3),\quad \{x_4 \mapsto x_2, x_1 \mapsto e\}$
$C_{13} : i(m(x_1,x_2)) \to m(i(x_2),i(x_1)),\quad m(e,x_3) \to x_3,\quad i(\Box),\quad \{x_3 \mapsto x_2, x_1 \mapsto e\}$
$C_{14} : m(x_1,m(i(x_1),x_2)) \to x_2,\quad m(e,x_3) \to x_3,\quad \Box,\quad \{x_3 \mapsto m(i(e),x_2), x_1 \mapsto e\}$
$C_{15} : m(i(x_1),m(x_1,x_2)) \to x_2,\quad m(e,x_3) \to x_3,\quad m(i(x_1),\Box),\quad \{x_3 \mapsto x_2, x_1 \mapsto e\}$
$C_{16} : m(x_1,i(x_1)) \to e,\quad m(e,x_2) \to x_2,\quad \Box,\quad \{x_2 \mapsto i(e), x_1 \mapsto e\}$
$C_{17} : m(x_1,e) \to x_1,\quad m(e,x_2) \to x_2,\quad \Box,\quad \{x_2 \mapsto e, x_1 \mapsto e\}$
$C_{18} : i(m(x_1,x_2)) \to m(i(x_2),i(x_1)),\quad m(x_3,e) \to x_3,\quad i(\Box),\quad \{x_2 \mapsto e, x_3 \mapsto x_1\}$
$C_{19} : m(x_1,m(i(x_1),x_2)) \to x_2,\quad m(x_3,e) \to x_3,\quad m(x_1,\Box),\quad \{x_2 \mapsto e, x_3 \mapsto i(x_1)\}$
$C_{20} : m(i(x_1),m(x_1,x_2)) \to x_2,\quad m(x_3,e) \to x_3,\quad m(i(x_1),\Box),\quad \{x_2 \mapsto e, x_3 \mapsto x_1\}$
$C_{21} : m(i(x_1),x_1) \to e,\quad m(x_2,e) \to x_2,\quad \Box,\quad \{x_1 \mapsto e, x_2 \mapsto i(e)\}$
$C_{22} : m(x_1,i(x_1)) \to e,\quad i(m(x_2,x_3)) \to m(i(x_3),i(x_2)),\quad m(x_1,\Box),\quad \{x_1 \mapsto m(x_2,x_3)\}$
$C_{23} : i(m(x_1,x_2)) \to m(i(x_2),i(x_1)),\quad m(x_3,i(x_3)) \to e,\quad i(\Box),\quad \{x_2 \mapsto i(x_1), x_3 \mapsto x_1\}$
$C_{24} : m(x_1,m(i(x_1),x_2)) \to x_2,\quad m(x_3,i(x_3)) \to e,\quad m(x_1,\Box),\quad \{x_2 \mapsto i(i(x_1)), x_3 \mapsto i(x_1)\}$

Figure 2 The critical pairs of the complete TRS R
($C_j : l \to r,\ l' \to r',\ C,\ \sigma$ means C_j is the critical pair $(r\sigma, C[r'\sigma])$.) – Part 1.

$C_{25} : m(x_1, i(x_1)) \to e, \quad i(i(x_2)) \to x_2, \quad m(x_1, \Box), \quad \{x_1 \mapsto i(x_2)\}$
$C_{26} : m(x_1, i(x_1)) \to e, \quad i(e) \to e, \quad m(x_1, \Box), \quad \{x_1 \mapsto e\}$
$C_{27} : m(i(x_1), m(x_1, x_2)) \to x_2, \quad m(x_3, i(x_3)) \to e, \quad m(i(x_1), \Box), \quad \{x_2 \mapsto i(x_1), x_3 \mapsto x_1\}$
$C_{28} : m(i(x_1), x_1) \to e, \quad i(m(x_2, x_3)) \to m(i(x_3), i(x_2)), \quad m(\Box, x_1), \quad \{x_1 \mapsto m(x_2, x_3)\}$
$C_{29} : i(m(x_1, x_2)) \to m(i(x_2), i(x_1)), \quad m(i(x_3), x_3) \to e, \quad i(\Box), \quad \{x_3 \mapsto x_2, x_1 \mapsto i(x_2)\}$
$C_{30} : m(x_1, m(i(x_1), x_2)) \to x_2, \quad m(i(x_3), x_3) \to e, \quad m(x_1, \Box), \quad \{x_1 \mapsto x_2, x_3 \mapsto x_2\}$
$C_{31} : m(i(x_1), x_1) \to e, \quad i(i(x_2)) \to x_2, \quad m(\Box, x_1), \quad \{x_1 \mapsto i(x_2)\}$
$C_{32} : m(i(x_1), x_1) \to e, \quad i(e) \to e, \quad m(\Box, x_1), \quad \{x_1 \mapsto e\}$
$C_{33} : m(i(x_1), m(x_1, x_2)) \to x_2, \quad m(i(x_3), x_3) \to e, \quad m(i(x_1), \Box), \quad \{x_3 \mapsto x_2, x_1 \mapsto i(x_2)\}$
$C_{34} : m(i(x_1), m(x_1, x_2)) \to x_2, \quad m(i(x_3), m(x_3, x_4)) \to x_4, \quad m(i(x_1), \Box), \quad \{x_2 \mapsto m(x_3, x_4), x_1 \mapsto i(x_3)\}$
$C_{35} : m(i(x_1), m(x_1, x_2)) \to x_2, \quad i(m(x_3, x_4)) \to m(i(x_4), i(x_3)), \quad m(\Box, m(x_1, x_2)), \quad \{x_1 \mapsto m(x_3, x_4)\}$
$C_{36} : i(m(x_1, x_2)) \to m(i(x_2), i(x_1)), \quad m(i(x_3), m(x_3, x_4)) \to x_4, \quad i(\Box), \quad \{x_2 \mapsto m(x_3, x_4), x_1 \mapsto i(x_3)\}$
$C_{37} : m(i(x_1), m(x_1, x_2)) \to x_2, \quad m(x_3, m(i(x_3), x_4)) \to x_4, \quad m(i(x_1), \Box), \quad \{x_2 \mapsto m(i(x_1), x_4), x_3 \mapsto x_1\}$
$C_{38} : m(x_1, m(i(x_1), x_2)) \to x_2, \quad m(i(x_3), m(x_3, x_4)) \to x_4, \quad m(x_1, \Box), \quad \{x_2 \mapsto m(x_1, x_4), x_3 \mapsto x_1\}$
$C_{39} : m(i(x_1), m(x_1, x_2)) \to x_2, \quad i(i(x_3)) \to x_3, \quad m(\Box, m(x_1, x_2)), \quad \{x_1 \mapsto i(x_3)\}$
$C_{40} : m(i(x_1), m(x_1, x_2)) \to x_2, \quad i(e) \to e, \quad m(\Box, m(x_1, x_2)), \quad \{x_1 \mapsto e\}$
$C_{41} : m(x_1, m(i(x_1), x_2)) \to x_2, \quad i(e) \to e, \quad m(x_1, m(\Box, x_2)), \quad \{x_1 \mapsto e\}$
$C_{42} : i(i(x_1)) \to x_1, \quad i(e) \to e, \quad i(\Box), \quad \{x_1 \mapsto e\}$
$C_{43} : i(i(x_1)) \to x_1, \quad i(i(x_2)) \to x_2, \quad i(\Box), \quad \{x_1 \mapsto i(x_2)\}$
$C_{44} : i(i(x_1)) \to x_1, \quad i(m(x_2, x_3)) \to m(i(x_3), i(x_2)), \quad i(\Box), \quad \{x_1 \mapsto m(x_2, x_3)\}$
$C_{45} : m(x_1, m(i(x_1), x_2)) \to x_2, \quad i(i(x_3)) \to x_3, \quad m(x_1, m(\Box, x_2)), \quad \{x_1 \mapsto i(x_3)\}$
$C_{46} : m(x_1, m(i(x_1), x_2)) \to x_2, \quad m(x_3, m(i(x_3), x_4)) \to x_4, \quad m(x_1, \Box),$
$\{x_2 \mapsto m(i(i(x_1)), x_4), x_3 \mapsto i(x_1)\}$
$C_{47} : m(x_1, m(i(x_1), x_2)) \to x_2, \quad i(m(x_3, x_4)) \to m(i(x_4), i(x_3)), \quad m(x_1, m(\Box, x_2)), \quad \{x_1 \mapsto m(x_3, x_4)\}$
$C_{48} : i(m(x_1, x_2)) \to m(i(x_2), i(x_1)), \quad m(x_3, m(i(x_3), x_4)) \to x_4, \quad i(\Box), \quad \{x_2 \mapsto m(i(x_1), x_4), x_3 \mapsto x_1\}$

Figure 3 The critical pairs of the complete TRS R
($C_j : \ l \to r, \ l' \to r', \ C, \ \sigma$ means C_j is the critical pair $(r\sigma, C[r'\sigma])$.) – Part 2.