A Homological Condition on Equational Unifiability

Mirai Ikebuchi ✉
Massachuseetts Institute of Technology, Cambridge, MA, USA

Abstract

Equational unification is the problem of solving an equation modulo equational axioms. In this paper, we provide a relationship between equational unification and homological algebra for equational theories. We will construct a functor from the category of sets of equational axioms to the category of abelian groups. Then, our main theorem gives a necessary condition of equational unifiability that is described in terms of abelian groups associated with equational axioms and homomorphisms between them. To construct our functor, we use a ringoid (a category enriched over the category of abelian groups) obtained from the equational axioms and a free resolution of a "good" module over the ringoid, which was developed by Malbos and Mimram.

2012 ACM Subject Classification Theory of computation → Equational logic and rewriting

Keywords and phrases Equational unification, Homological algebra, equational theories

Digital Object Identifier 10.4230/LIPIcs.MFCS.2021.61

Acknowledgements I would like to thank Assaf Kfoury and Keisuke Nakano for reading a draft of this paper and for their helpful suggestions.

1 Introduction

Equational unification is the problem of solving a given equation modulo an equational theory. For example, if we consider the axioms of commutative rings with a multiplicative unit, the equational unification problem asks whether given a polynomial equation with integer coefficients has a solution in integers. The decidability of this problem was posed by David Hilbert (Hilbert's tenth problem) and it was shown to be undecidable [12, 5]. There are specific theories such as the theory of abelian groups or the theory of boolean rings such that the equational unification is decidable (see [2, §3.4]). The problem is generally semi-decidable, but not generally decidable. *Narrowing* [6, 7] is a procedure that finds all solutions of the equation, but it may not terminate in general.

Our purpose is to provide a necessary condition of solvability of an equation. The condition is obtained from a homological invariant of equational theories. More precisely, we will define an abelian group $\mathcal{H}(E)$ for a set E of equations (or equational axioms) and an abelian group homomorphism $\mathcal{H}(E \to E') : \mathcal{H}(E) \to \mathcal{H}(E')$ for two sets E, E' of equations satisfying $E^* \subset E'^*$. Here, E^*, E'^* are the equational theories of E, E', i.e., the sets of all equations that can be derived by E, E'. Then, we will prove the following theorem.

▶ **Theorem 1.** *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.*

Although $\mathcal{H}(E)$ and $\mathcal{H}(E \to E')$ are defined using abstract algebra, Theorem 1 is restated in terms of rewriting and matrices if a complete TRS of $E \cup \{t \approx s\}$ is given. In that case, we can compute a matrix associated with E and $E \cup \{t \approx s\}$ and the surjectivity of $\mathcal{H}(E \to E \cup \{t \approx s\})$ can be checked by matrix operations. (Theorem 5). Therefore, we have

a sound procedure for non-E-unifiability; if we compute the matrix and if it does not have full rank, then we can conclude that t, s are not E-unifiable. We will see how this procedure works on some simple examples in Section 3.

Our contribution is not only presenting a new procedure for non-E-unifiability. Our abelian group $\mathcal{H}(E)$ and homomorphism $\mathcal{H}(E \to E')$ can provide an algebraic consideration of equational unification, equational logic, or rewriting. The abelian group $\mathcal{H}(E)$ is invariant under equivalence of E, that is, if two sets E, E' of equations are equivalent, then $\mathcal{H}(E)$ and $\mathcal{H}(E')$ are isomorphic. We define $\mathcal{H}(E)$ using homological algebra of equational theories. The homological algebra of equational theories we use in this paper is based on [10, 11, 8]. Also, we will prove that $\mathcal{H}$ is a functor from the category of sets of equations over a fixed signature to the category of abelian groups.

The paper is organized as follows. In Section 2, we explain basic concepts of unifiability and rewriting. In Section 3, as mentioned earlier, we rephrase Theorem 1 under a certain case so that our condition is checkable by matrix computations. Then, we see some examples and consider equational unification problems on them. In Section 4, we define $\mathcal{H}(E)$ and $\mathcal{H}(E \to E')$ which appear in Theorem 1 and prove Theorem 1 and 5. In Section 5, we see how homological algebra has been applied to rewriting in other contexts and then we conclude in Section 6.

2 Preliminaries

A *signature* Σ is a set associated with a function $\alpha : \Sigma \to \mathbb{Z}_{\geq 0}$. For $f \in \Sigma$, we say that f is of *arity* n if $n = \alpha(f)$. Let V be a countably infinite set distinct from Σ. A *term* over Σ and V is a formal object 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 paper, 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 $V \to \mathrm{Term}(\Sigma, V)$. For a term t and a substitution σ, $t\sigma$ denotes the term obtained by replacing all variables v in t with $\sigma(v)$. 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 $\{v_1 \mapsto t_1, \ldots, v_n \mapsto t_n\}$. 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 satisfying that for any other unifier σ' of t, s, there exists a substitution τ such that $\sigma' = \sigma\tau$.

A *context* is a term in $\mathrm{Term}(\Sigma, V \cup \{\Box\})$ that has just one $\Box$ 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 a 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 $l \approx r$. 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 $t \xrightarrow[l \approx r]{} s$ 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 $\to_E$ is written as $\xleftrightarrow{*}_E$ 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 $t_1 \to_R t_2 \to_R t_3 \to_R \dots$.

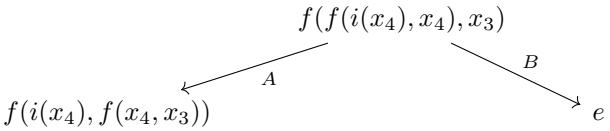
Two terms t_1, t_2 are *joinable* by R if there exists a term s such that $t_1 \xrightarrow{*}_R s \xleftarrow{*}_R t_2$. A TRS R is *confluent* if, for any terms t, t_1, t_2, $t_1 \xleftarrow{*}_R t \xrightarrow{*}_R t_2$ implies that t_1 and t_2 are joinable.

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

Let R be a TRS and $l_1 \approx r_1, l_2 \approx r_2 \in R$ be two rewrite rules. Suppose that the variables of $l_2 \approx r_2$ 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 $C[t] = l_1$, then the pair $(r_1\sigma, C[r_2\sigma])$ is called a *critical pair* of R. For example, suppose that we have two rules

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

The subterm $f(x_1, x_2)$ of the left-hand side of A and $f(i(x_4), x_4)$, the right-hand side of B, can be unified with the mgu $\sigma = \{x_1 \mapsto i(x_4), x_2 \mapsto x_4, x_4 \mapsto x_4\}$. Then, the corresponding critical pair is $(f(i(x_4), f(x_4, x_3)), e)$, as the following diagram shows.



3 A Computable Necessary Condition

Let Σ be a signature. For a set E of equations and two terms t, s, if there exists a complete TRS R of $E \cup \{t \approx s\}$, Theorem 1 can be described more explicitly. To state the explicit version of the theorem, we need some definitions.

▶ **Definition 2.** *Let E be a set of equations. The degree of E, denoted by* $\deg(E)$*, is defined by* $\deg(E) = \gcd\{\#_i l - \#_i r \mid l \approx r \in E, i = 1, 2, \dots\}$ *where $\#_i t$ is the number of occurrences of x_i in t for $t \in T(\Sigma)$ and* $\gcd\{0\}$ *is defined to be 0.*

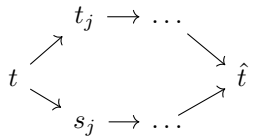
For example, $\deg(\{f(x_1, x_2, x_2) \approx x_1,\ g(x_1, x_1, x_1) \approx e\}) = \gcd\{0, 2, 3\} = 1$.

Let $R = \{l_1 \to r_1, \dots, l_n \to r_n\}$ 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 $j \in \{1, \dots, m\}$, let a_j^R, b_j^R be the numbers in $\{1, \dots, n\}$ such that the critical pair (t_j, s_j) is obtained by $l_{a_j^R} \to r_{a_j^R}$ and $l_{b_j^R} \to r_{b_j^R}$, that is, $t_j = r_{a_j^R}\sigma \leftarrow l_{a_j^R}\sigma = C[l_{b_j^R}\sigma] \to C[r_{b_j^R}\sigma] = s_j$ for some substitution σ and single-hole context C after suitably renaming variables in $l_{a_j^R} \to r_{a_j^R}$ and $l_{b_j^R} \to r_{b_j^R}$. Suppose R is complete. We fix an arbitrary rewriting strategy and for a term t, let $\mathrm{nr}_i^R(t)$ be the number of times $l_i \to r_i$ is used to reduce t into its R-normal form with respect to the strategy.

For a natural number d, we write $\mathbb{Z}_d$ for $\mathbb{Z}/d\mathbb{Z}$, the integers modulo d.

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

In other words, the (i,j)-th entry of $D(R)$ is the difference between (1) the number of $l_i \to r_i$ in the upper path from t to $\hat{t}$ in the diagram below, and (2) that in the lower path.



The degree $\deg(E)$ and the matrix $D(R)$ are introduced in [8] to give a lower bound of number of equational axioms that is needed to present a given equational theory.

▶ **Definition 4.** *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 $d = \deg(R)$.*

For a commutative ring A, two $n \times m$ matrices M, N over A are said to be *equivalent* if $N = PMQ$ for some invertible $n \times n$ matrix P and $m \times m$ matrix Q over R. We write $I_{n,m}$ for the $n \times m$ diagonal matrix whose diagonal elements are all 1.

Here is the explicit version of Theorem 1.

▶ **Theorem 5.** *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 $n \le m$ where m is the number of columns of $(D(R)|U(E,R))$.*

We will prove Theorem 1 and how it implies Theorem 5 in Section 4 after introducing more algebraic tools.

▶ Remark 6. Although the matrices $D(R)$ and $U(E,R)$ depend on the choice of rewriting strategy, the necessary condition stated in Theorem 5 does not depend on the choice. We will prove this fact in Section 4.

▶ Remark 7. It is algorithmically checkable whether a matrix over $\mathbb{Z}_d$ is equivalent to $I_{n,m}$ in polynomial time by computing the Smith normal form [4, Chapter 15]. Note that if the degree d is prime, since $\mathbb{Z}_d$ is a field, it suffices to get a diagonal matrix by elementary row/column operations and see all diagonal elements are nonzero.

We shall see some examples.

▶ **Example 8.** Let E_1 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_1-unification problem $x_1 + x_1 \approx^?_{E_2} s(0)$. By applying Knuth-Bendix completion to $E_1 \cup \{x_1 + x_1 \to s(0)\}$, we obtain a complete TRS R_1:

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

The degree of R_1 is 2 and R_1 has one critical pair $\Pi' : 0 \xleftarrow[B_1]{} 0+0 \xrightarrow[C_1]{} 0$ and the matrix $(D(R_1)|U(E_1, R_1))$ is given as

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

Here, each entry of $D(R_1|U(E_1, R_1))$ 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_1-unifiable.

We can also consider the E_1-unification problem $x_1 + x_1 \approx^?_{E_2} 0$. It has an obvious solution $x_1 \mapsto 0$, so the matrix corresponding to this problem must be equivalent to $I_{n,m}$ for some n, m. We give a complete TRS for $E_1 \cup \{x_1 + x_1\}$, its critical pairs, and the corresponding matrix in the appendix.

More generally, consider the E_1-unification problem $x_1 + x_1 \approx^?_{E_1} s^n(0)$ where $s^n(0) = \underbrace{s(\dots s}_{n}(0)\dots)$. In fact, we can see that if n is odd, $E' = E_1 \cup \{x_1 + x_1 \approx s^n(0)\}$ is equivalent to $E_1 \cup \{x_1 + x_1 \approx s(0)\}$ and if n is even, E' is equivalent to $E_1 \cup \{x_1 + x_1 \approx 0\}$.

▶ **Example 9.** Let $E_2 = \{a(b(b(a(x_1)))) \approx x_1\}$. It is known that E_2 does not have a complete TRS with a finite number of rewrite rules [9]. Consider the E_2-unification problem $a(b(x_1)) \approx^?_{E_2} x_1$. Then, $E_2 \cup \{a(b(x_1)) \approx x_1\}$ has a complete TRS $R_2 = \{a(b(x_1)) \to x_1,\ b(a(x_1)) \to x_1\}$. 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 $(D(R_2)|U(E_2, R_2))$ 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_2-unifiable.

▶ Remark 10. As Example 9 indicates, 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 only when a complete TRS of E is given. So, it is notable that Theorem 5 does not require us to find a complete TRS of E.

4 Homological Algebra on Equational Theories

The aim of this section is to define $\mathcal{H}(E)$ and $\mathcal{H}(E \to E')$, and to prove Theorem 1 and Theorem 5. For that, we will construct some algebraic structures associated with E and applies homological algebra to them. First, let us see the notion of *resolution*, which is often used to define invariants of mathematical objects in many branches of mathematics. See [15] as an introductory text.

Let R be a ring. We say that the sequence

$$\dots \xrightarrow{f_{i+1}} M_{i+1} \xrightarrow{f_i} M_i \xrightarrow{f_{i-1}} M_{i-1} \xrightarrow{f_{i-2}} \dots$$

of left R-modules M_i and R-linear maps f_i is *exact* if $\ker f_i = \operatorname{im} f_{i+1}$ holds. For a left R-module M, a *free resolution* of M is an exact sequence

$$\dots \xrightarrow{\partial_2} F_2 \xrightarrow{\partial_1} F_1 \xrightarrow{\partial_0} F_0 \xrightarrow{\epsilon} M \to 0$$

where each F_i is free. It is known that for any left R-module M, free resolutions of M exist. A *partial free resolution* of M is a exact sequence of finite length

$$F_n \xrightarrow{\partial_n} \dots \xrightarrow{\partial_2} F_2 \xrightarrow{\partial_1} F_1 \xrightarrow{\partial_0} F_0 \xrightarrow{\epsilon} M \to 0$$

with free F_is.

The notion of resolution is defined not only for modules over a ring but also for modules over a *ringoid*. In [11], Malbos and Mimram constructed a ringoid associated with a given equational theory and defined invariants called homology groups using a free resolution over that ringoid. We will also use the free resolution to define $\mathcal{H}(E)$ in Theorem 1. We shall see their construction in the subsections from 4.1 to 4.3, then provide the definitions of $\mathcal{H}(E)$, $\mathcal{H}(E \to E')$ and prove our main theorems.

4.1 Category of Bicontexts

We fix a signature Σ. Let $t = \langle t_1, \dots, t_n \rangle$ be an n-tuple of terms whose variables are in $\{x_1, \dots, x_m\}$ and $s = \langle s_1, \dots, s_m \rangle$ be an m-tuple of terms. We define their composition $t \circ s$ by $\langle t_1[s_1/x_1, \dots, s_m/x_m], \dots, t_n[s_1/x_1, \dots, s_m/x_m] \rangle$ where $t_i[s_1/x_1, \dots, s_m/x_m]$ is the term obtained by substituting s_j for x_j in t_i for each $j = 1, \dots, m$ in parallel.

▶ **Definition 11.** *A* bicontext *is a pair (C, t) of a context C and n-tuple of terms $t = \langle t_1, \dots, t_n \rangle$.*

For two bicontexts (C, t) and (D, s), we define their composition $(C, t) \circ (D, s)$ by $(C[D \circ t], s \circ t)$ where $D \circ t = D[t_1/x_1, \dots, t_n/x_n]$ for $t = \langle t_1, \dots, t_n \rangle$.

▶ **Definition 12.** *The category of bicontexts $\mathbb{K}$ consists of*

- *Objects: natural numbers $0, 1, \dots$,*
- *Morphisms $\mathbb{K}(n_1, n_2)$: bicontexts (C, t) where t is an n_1-tuple of terms such that the elements of t and C have variables in $\{x_1, \dots, x_{n_2}\}$ (except $\Box$ in C),*
- *Identity: $(\Box, \langle x_1, \dots, x_n \rangle)$*

and the composition is defined above.

4.2 Ringods

We consider an algebraic structure called *ringoid*.

▶ **Definition 13.** *A* ringoid $\mathcal{R}$ *is a small* **Ab***-enriched category. That is, each hom-set 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. We can add two morphisms $x : a_1 \to b_1$, $y : a_2 \to b_2$ only if $a_1 = a_2$ and $b_1 = b_2$. Also, we can multiply them as composition $y \circ x$ only if $b_1 = a_2$.

For any small category $\mathcal{C}$, there exists a ringoid $\mathbb{Z}\langle\mathcal{C}\rangle$ called the ringoid *freely generated by* $\mathcal{C}$. The ringoid $\mathbb{Z}\langle\mathcal{C}\rangle$ has the same objects as $\mathcal{C}$ and the hom-set $\mathbb{Z}\langle\mathcal{C}\rangle(a,b)$ between objects a,b is the free abelian group generated by $\mathcal{C}(a,b)$. The composition of $\mathbb{Z}\langle\mathcal{C}\rangle$ is given by linearly extending the composition of $\mathcal{C}$ as $(w+z)\circ(x+y)=w\circ x+w\circ y+z\circ x+z\circ y$.

We can define an ideal of a ringoid and a module over a ringoid.

▶ **Definition 14.** *Let $\mathcal{R}$ be a ringoid. An* ideal *of $\mathcal{R}$ is a subfunctor of the hom-bifunctor $\mathcal{R}(-,-):\mathcal{R}\times\mathcal{R}\to\mathbf{Ab}$. If I is an ideal of $\mathcal{R}$, then we can define the category $\mathcal{R}/I$ whose objects are those of $\mathcal{R}$, morphisms are $(\mathcal{R}/I)(a,b)=\mathcal{R}(a,b)/I(a,b)$, and the composition is induced by that of $\mathcal{R}$. Also, a structure of ringoid of $\mathcal{R}/I$ is induced by that of $\mathcal{R}$.*

▶ **Definition 15.** *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 16.** *Let M_1 be a left $\mathcal{R}$-module. A* submodule *of M_1 is a left $\mathcal{R}$-module M_2 such that there exists a monomorphism $\phi:M_2\to M_1$ and $\phi_a:M_2(a)\to M_1(a)$ is an inclusion of sets for each object a of $\mathcal{R}$.*

We define left free $\mathcal{R}$-modules over ringoids.

▶ **Definition 17.** *Let P be a family of sets P_a ($a\in\mathrm{Obj}(\mathcal{R})$). The* left free $\mathcal{R}$-module generated by P, *denoted by $\mathcal{R}\underline{P}$, is defined as follows. For each $a\in\mathrm{Obj}(\mathcal{R})$, $(\mathcal{R}\underline{P})(a)$ is the abelian group consisting of formal finite sums $\sum_{x\in P_b,b\in\mathrm{Obj}(\mathcal{R})}\lambda_x\underline{x}$, $(\lambda_x\in\mathcal{R}(b,a))$. Here, the underline for x above is added to emphasize the difference between λ_x and x. The scalar multiplication is given as $r\cdot(\sum_x\lambda_x\underline{x})=\sum_x(r\circ\lambda_x)\underline{x}$ $(r\in\mathcal{R}(a,c))$.*

For a ringoid $\mathcal{R}$, let $\mathbf{Mod}_{\mathcal{R}}$ denote the category of left $\mathcal{R}$-modules and $\mathcal{R}$-linear maps. The following proposition tells us that $\mathbf{Mod}_{\mathcal{R}}$ has good properties so that we can apply homological algebra to it.

▶ **Proposition 18** ([13])**.** *$\mathbf{Mod}_{\mathcal{R}}$ is an abelian category and any left $\mathcal{R}$-module has a free resolution.*

We do not give the details of this proposition, but one of the important consequences of being abelian is that we have the notions of kernel and image of an $\mathcal{R}$-linear map in the category.

▶ **Definition 19.** *Let M_1,M_2 be two left $\mathcal{R}$-modules and $f:M_1\to M_2$ be an $\mathcal{R}$-linear map. Then, the kernel and the image of f are defined as $(\ker f)(a)=\ker f_a$, $(\mathrm{im}\,f)(a)=\mathrm{im}\,f_a$ for each object a. Here, f_a is an abelian group homomorphism, so* ker *and* im *in the right-hand sides are the kernel and the image for group homomorphisms.*

Many other notions for modules over a ring can be generalized.

▶ **Definition 20.** *Let M_1 be a left $\mathcal{R}$-module and M_2 be a submodule of M_1. The quotient module M_1/M_2 is the left $\mathcal{R}$-module given as $(M_1/M_2)(a)=M_1(a)/M_2(a)$.*

▶ **Definition 21.** *Let M be a left $\mathcal{R}$-module. For an index set I, for each $i\in I$, let a_i be an object of $\mathcal{R}$ and x_i be an element of $M(a_i)$. The* submodule generated by $\{x_i\}_{i\in I}$ *is the left $\mathcal{R}$-module N such that for each $a\in\mathrm{Obj}(\mathcal{R})$, $N(a)$ is the abelian group consisting of finite sums $\sum_{i\in I}\lambda_i\cdot x_i$ $(\lambda_i\in\mathcal{R}(a,a_i))$.*

▶ **Definition 22.** *Let M_1 be a right $\mathcal{R}$-module and M_2 be a left $\mathcal{R}$-module. The* tensor product *$M_1 \otimes_{\mathcal{R}} M_2$ of M_1 and M_2 is defined as the coend $M_1 \otimes_{\mathcal{R}} M_2 = \int^a M_1(a) \otimes M_2(a)$. That is, 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, $M_1 \otimes_{\mathcal{R}} M_2$ is the abelian group $\left(\bigoplus_{a \in \mathrm{Obj}(\mathcal{R})} M_1(a) \otimes M_2(a)\right)/R$ where R is the abelian group generated by $M_1(f^{\mathrm{op}})(x) \otimes y - x \otimes M_2(f)(y)$ for any $f : a \to a'$, $x \in M_1(a')$, $y \in M_2(a)$, $a, a' \in \mathrm{Obj}(\mathcal{R})$.

Let M_1, M_2 be two left $\mathcal{R}$-modules and N_1, N_2 be two right $\mathcal{R}$-modules. For linear maps $f : M_1 \to M_2$ and $g : N_1 \to N_2$, we define $g \otimes f \colon N_1 \otimes_{\mathcal{R}} M_1 \to N_2 \otimes_{\mathcal{R}} M_2$ to be the abelian group homomorphism $(f \otimes g)(n \otimes m) = g(n) \otimes f(m)$. If $N_1 = N_2$ and g is the identity map, we write $N_1 \otimes f$ instead of $g \otimes f$.

The tensor product of modules over a ringoid satisfies many properties of tensor product of modules over a ring. In particular, we have

▶ **Lemma 23.** *Let N be a right $\mathcal{R}$-module and M_1, M_2, M_3 be left $\mathcal{R}$-modules. If the sequence $M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \to 0$ is exact, then the sequence $N \otimes_{\mathcal{R}} M_1 \xrightarrow{N \otimes f} N \otimes_{\mathcal{R}} M_2 \xrightarrow{N \otimes g} N \otimes_{\mathcal{R}} M_3 \to 0$ is also exact.*

4.3 Partial Free Resolutions

For the category of bicontexts $\mathbb{K}$, consider the ringoid $\mathbb{Z}\langle\mathbb{K}\rangle$. Then, we will define a ringoid $\mathcal{R}^E$ such that any two equivalent sets E, E' of equations give rise to isomorphic ringoids $\mathcal{R}^E \simeq \mathcal{R}^{E'}$.

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

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

Application of linear combination of contexts to a context which 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-uple of terms $u = \langle s_1, \ldots, s_n \rangle$, let $\varphi_{f,u}(t)$ be the linear combination of all contexts C satisfying $C[f(s_1, \ldots, s_n)] = t$.

We define the ideal I_E of $\mathbb{Z}\langle\mathbb{K}\rangle$. Let $I_E(m, n)$ be the subgroup of $\mathbb{Z}\langle\mathbb{K}\rangle(m, n)$ generated by elements of the form

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

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 $\mathcal{R}^E$.

[1] For the original definition of $\mathcal{R}^E$ in [11], the generators $\varphi_{f,vu}(t \circ v) - \varphi_{f,vu}(s \circ v) - \varphi_{f,u}(t) \circ v + \varphi_{f,u}(s) \circ v$ of $I_E(m, n)$ was not given. However, we need these generators to prove $\partial_1(\hat{t}) = \varphi(\hat{t}) - \varphi(t)$ which is used to show $\partial_1 \circ \partial_2 = 0$ in Appendix A of [11]. We do not need to change the other parts of the proof.

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 divided 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 subterm $f(u)$ in t, for any $l \approx r \in E$, $f \in \Sigma$, $t \in T(\Sigma)$, the linear combination $\varphi_{f,u}(r\circ t) - \varphi_{f,u}(l\circ t) - \varphi_{f,u}(r) + \varphi_{f,u}(l)$ 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.

Let X_1 be a singleton set $\{\star\}$, X_i be the empty set for $i = 0$ or $i = 2,3,\dots$, 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 $\mathrm{Var}(u) \subset \{x_1,\dots,x_m\}$ and m-uple $t = \langle t_1,\dots,t_m\rangle$ of terms. Then, we construct a partial free resolution of $\mathcal{Z}^E$

$$\mathcal{R}^E\underline{\mathbf{P}_2^E} \xrightarrow{\partial_1^E} \mathcal{R}^E\underline{\mathbf{P}_1} \xrightarrow{\partial_0^E} \mathcal{R}^E\underline{\mathbf{P}_0} \xrightarrow{\epsilon^E} \mathcal{Z}^E \to 0 \tag{1}$$

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

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

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

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

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

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

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

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

If there is a complete TRS R of E, we can extend the sequence (1) to

$$\mathcal{R}\underline{\mathbf{P}_3^R} \xrightarrow{\partial_2^R} \mathcal{R}\underline{\mathbf{P}_2^R} \xrightarrow{\partial_1^R} \mathcal{R}\underline{\mathbf{P}_1} \xrightarrow{\partial_0^R} \mathcal{R}\underline{\mathbf{P}_0} \xrightarrow{\epsilon^R} \mathcal{Z}^R \to 0. \tag{2}$$

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-uple $(l\to r, t, C, l'\to r', t')$ 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 $k \le j$.

For such a 5-uple $\alpha = (l\to r, t, C, l'\to r', t')$, $\partial_2^R(\underline{\alpha})$ 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 $p_1\to q_1,\dots,p_k\to q_k \in R$ as

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

for some C_is and u_is. Then, $\hat{\hat{s}} = \sum_{i=1}^{k} C_i\underline{p_i\to q_i}u_i$.

▶ **Theorem 24** ([11]). *If R is a complete TRS, the sequence (2) is exact.*

The following lemma is useful for the next subsection.

▶ **Lemma 25.** *Let E be a set of equations with degree d. For any family P of sets $P_0, P_1, \dots$, 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 module generated by $\biguplus P$ over $\mathbb{Z}_d$ as a ring.*

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. ◀

4.4 Invariant $\mathcal{H}(E)$

We are ready to define $\mathcal{H}(E)$.

▶ **Definition 26.** *For a set E of equations, we define the abelian group $\mathcal{H}(E)$ by*

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

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.

$$\begin{array}{ccc} \mathbb{Z}_d \otimes (\ker \partial_0^E(k)) & \xrightarrow{\zeta_k} & \mathbb{Z}_d \otimes_{\mathcal{R}^E} \ker \partial_0^E \\ \downarrow{\scriptstyle f_k} & & \downarrow{\scriptstyle \mathcal{H}(E \to E')} \\ \mathbb{Z}_{d'} \otimes (\ker \partial_0^{E'}(k)) & \xrightarrow{\zeta_k} & \mathbb{Z}_d \otimes_{\mathcal{R}^{E'}} \ker \partial_0^{E'} \end{array} \tag{3}$$

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 1.

Proof of Theorem 1. 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 25), $\mathcal{H}(F') = \mathbb{Z}_d \otimes_{\mathcal{R}^{F'}} \operatorname{im} \partial_1^{F'}$ 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 1 implies Theorem 5. 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 1 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 $\operatorname{coker} \tilde{\partial}_2^R = \mathbb{Z}_d \otimes_{\mathcal{R}^R} \mathcal{R}^R\underline{\mathbf{P}_2^R} / \operatorname{im} \tilde{\partial}_2^R$.

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 $h(1 \otimes \underline{t \approx s}) = 1 \otimes (\hat{t} - \hat{s})$.

▶ **Lemma 27.** *$\check{\partial}_1^R \circ h = \mathcal{H}(E \to R) \circ \check{\partial}_1^E$. 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, $\check{\partial}_1^R(1 \otimes \hat{t}) = 1 \otimes (\varphi(\hat{t}) - \varphi(t)) \in \mathbb{Z}_d \otimes_{\mathcal{R}^R} \operatorname{im} \partial_1^R$ for any term t. If $\hat{t} = 0$, or equivalently, t is normal, then the equality trivially holds. If $\hat{t} = C\underline{l \approx r}u + \hat{t}'$ ($C[l \circ u] = t$, $C[r \circ u] = t'$) and $\check{\partial}_1^R(1 \otimes \hat{t}') = 1 \otimes (\varphi(\hat{t}) - \varphi(t'))$, then $\check{\partial}_1^R(1 \otimes \hat{t}) = 1 \otimes (\varphi(\hat{t}) - \varphi(t') + \varphi(r) - \varphi(l))$. 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 $\check{\partial}_1^{R'}(\hat{t}) = 1 \otimes (\varphi(\hat{t}) - \varphi(t))$.

Now, we have $\check{\partial}_1^R(h(1 \otimes \underline{t \approx s})) = \check{\partial}_1^R(1 \otimes \hat{t}) - \check{\partial}_1^R(1 \otimes \hat{s}) = 1 \otimes (\varphi(s) - \varphi(t))$ 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

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

Theorem 5 follows from Theorem 1 and the lemma below.

▶ **Lemma 28.** *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 5 is independent of the choice of rewriting strategy. (∵ The map $\mathcal{H}(E \to R)$ is defined independently from rewriting strategies.)

4.5 Functoriality

For a signature Σ, consider the category $\mathcal{E}_\Sigma$ such that its objects are sets of equations over Σ and for each pair of objects E, E' with $E^* \subset E'^*$, there exists exactly one morphism $E \to E'$. Then, we shall see that $\mathcal{H} : \mathcal{E}_\Sigma \to \mathbf{Ab}$ is a functor. It is straightforward to show that $\mathcal{H}(E \to E)$ is an identity map, so we show

$$\mathcal{H}(E' \to E'') \circ \mathcal{H}(E \to E') = \mathcal{H}(E \to E'') \tag{4}$$

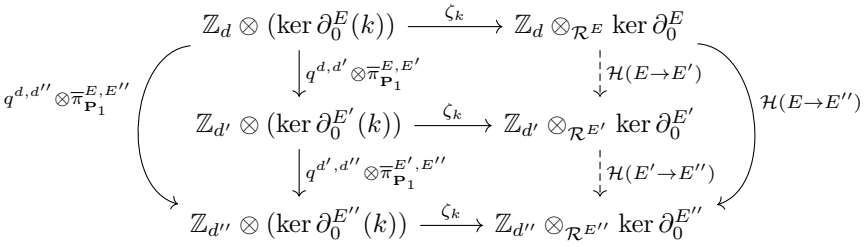
for any E, E', E'' with $E^* \subset E'^* \subset E''^*$. Recall that $\mathcal{H}(E \to E')$ is defined using the functor

$$\pi^{E,E'} : \mathcal{R}^E \to \mathcal{R}^{E'}, \quad [(C_1,u_1) + \cdots + (C_k,u_k)]^E \mapsto [(C_1,u_1) + \cdots + (C_k,u_k)]^{E'}.$$

For a set E'' of equations with $E'^* \subset E''^*$, we can see $\pi^{E',E''} \circ \pi^{E,E'} = \pi^{E,E''}$ and so

$$q^{d',d''} \otimes \overline{\pi}_{\mathbf{P}_1}^{E',E''} \circ q^{d,d'} \otimes \overline{\pi}_{\mathbf{P}_1}^{E,E'} = q^{d,d''} \otimes \overline{\pi}_{\mathbf{P}_1}^{E,E''}. \tag{5}$$

As we saw that the diagram (3) commutes, we have the commutative diagram



where $d = \deg(E)$, $d' = \deg(E')$, and $d'' = \deg(E'')$. By (5) and by the uniqueness of $\mathcal{H}(E \to E'')$, we obtain the equality (4).

5 Related Work

5.1 Free Resolutions in Rewriting

The partial free resolution (2) was given by Malbos and Mimram in [11] to compute invariants called homology groups of an equational theory. For a signature Σ and set E of equational theory over Σ, if we have a free resolution $\dots \xrightarrow{\delta_3} F_3 \xrightarrow{\delta_2} F_2 \xrightarrow{\delta_1} F_1 \xrightarrow{\delta_0} F_0 \xrightarrow{\eta} \mathcal{Z}^E \to 0$ of $\mathcal{Z}^E$, the i-th homology group $H_i(\Sigma, E)$ is defined as the abelian group $\ker(\mathbb{Z}_d \otimes \delta_{i-1})/\operatorname{im}(\mathbb{Z}_d \otimes \delta_i)$. As a general fact of homological algebra, it is shown that the homology groups do not depend on the choice of free resolution. Also, if E' is a set of equations over Σ' and (Σ', E') is Tietze equivalent (see [11] for the definition) to (Σ, E), $H(\Sigma', E')$ is isomorphic to $H(\Sigma, E)$. The partial free resolution (2) is useful to compute the homology groups since each generating set $\mathbf{P}_i$ is finite. Also, it is shown that for any signature Σ' and set E' of equations over Σ', if (Σ', E') is Tietze equivalent to (Σ, E), E' has at least $s(H_2(\Sigma, E))$ elements where $s(A)$ is the minimum number of generators of A. In [8], the author showed that for a set E' of equations over Σ which E is also over, if E' is equivalent to E (in the sense $E^* = E'^*$), E' has at least $s(H_2(\Sigma, E)) + s(\operatorname{im}(\mathbb{Z}_d \otimes \partial_1))$ elements.

Homology groups are defined for many mathematical objects. Homology groups of a group, also called group homologies, have a close relationship with homology groups of an equational theory. For a group G, its homology $H_i(G)$ is defined as follows. Consider the group ring $\mathbb{Z}\langle G\rangle$ and a free resolution of $\mathbb{Z}$ as a left $\mathbb{Z}\langle G\rangle$-module

$$\dots \xrightarrow{\delta_3} F_3 \xrightarrow{\delta_2} F_2 \xrightarrow{\delta_1} F_1 \xrightarrow{\delta_0} F_0 \xrightarrow{\eta} \mathbb{Z} \to 0,$$

then $H_i(G) = \ker(\mathbb{Z} \otimes \delta_{i-1})/\operatorname{im}(\mathbb{Z} \otimes \delta_i)$. If a group G is presented by some generators $S = \{g_1, g_2, \dots\}$ and relations $T = \{r_1 = 1, r_2 = 1, \dots\}$, it is known that there is a partial free resolution

$$\mathbb{Z}\langle G\rangle \underline{T} \to \mathbb{Z}\langle G\rangle \underline{S} \to \mathbb{Z}\langle G\rangle \to \mathbb{Z} \to 0.$$

(See [3, Exercise 3 in §II.5] for example.)

In [14], Squier considered free resolutions of $\mathbb{Z}$ as a module over the monoid ring $\mathbb{Z}\langle M\rangle$ for a monoid M. Also in this case, if M is presented by generators $S = \{g_1, g_1, \dots\}$ and relations $T = \{l_1 = r_1, l_2 = r_2, \dots\}$, we have a partial free resolution

$$\mathbb{Z}\langle M\rangle \underline{T} \to \mathbb{Z}\langle M\rangle \underline{S} \to \mathbb{Z}\langle M\rangle \to \mathbb{Z} \to 0.$$

Moreover, he showed that if the relations form a complete string rewriting system, the partial free resolution is extended to

$$\mathbb{Z}\langle M\rangle\underline{U} \to \mathbb{Z}\langle M\rangle\underline{T} \to \mathbb{Z}\langle M\rangle\underline{S} \to \mathbb{Z}\langle M\rangle \to \mathbb{Z} \to 0.$$

where U is the set of critical pairs. This resolution inspired our free resolution (2) for an equational theory.

5.2 Narrowing

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 non-variable 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 $\mathrm{Var}(l) \cup \mathrm{Var}(s) = \emptyset$.) In that case, we write $s \rightsquigarrow_{\sigma,R} t$. The sequence $t_0 \rightsquigarrow_{\sigma_1,R} t_1 \rightsquigarrow_{\sigma_2,R} \cdots \rightsquigarrow_{\sigma_n,R} t_n$ is abbreviated to $t_0 \rightsquigarrow^*_{\sigma,R} t_n$ for $\sigma = \sigma_0\sigma_1 \dots \sigma_n$. 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 29** ([7]). *Suppose that R is complete and* eq *be a new symbol with arity 2.*

- *If $\mathsf{eq}(s,t) \rightsquigarrow^*_{\sigma,R} \mathsf{eq}(s',t')$ and s', t' are unifiable with the mgu τ, 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 $\mathsf{eq}(s,t) \rightsquigarrow^*_{\sigma,R} \mathsf{eq}(s',t')$ and an mgu τ of s', t' such that $\sigma\tau \leq_R^{\mathrm{Var}(\mathsf{eq}(s,t))} \theta$.*

Consider Example 1 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 by any rules in E_1.

For Example 2, however, we have an infinite narrowing sequence from $\mathsf{eq}(x_1 + x_1, s(0))$:

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

so we can see that narrowing is a semi-decision procedure of the problem of equational unification. It has been studied that what kind of restriction on a TRS ensures termination of narrowing [1].

6 Conclusion

We have obtained a functor $\mathcal{H} : \mathcal{E}_\Sigma \to \mathbf{Ab}$ where $\mathcal{E}_\Sigma$ is the category of sets of equations and proved that E-unifiability of two terms t, s implies the surjectivity of the homomorphism $\mathcal{H}(E \to E \cup \{t \approx s\})$. In case where $E \cup \{t \approx s\}$ has a complete TRS, the surjectivity of $\mathcal{H}(E \to E \cup \{t \approx s\})$ is equivalent to the condition that the matrix $(D(R)|U(E,R))$ has full rank. Therefore, our theorem gives a sound procedure for checking non-E-unifiability.

References

1 María 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, Wayne Snyder, Paliath Narendran, Manfred Schmidt-Schauss, and Klaus Schulz. Unification theory. In *Handbook of Automated Reasoning*, Handbook of Automated Reasoning, pages 445–533. North-Holland, Amsterdam, 2001.

3 K. S. Brown. *Cohomology of Groups*, volume 87 of *Graduate Texts in Mathematics*. Springer-Verlag New York, 1982.

4 W. Brown. *Matrices over commutative rings*. M. Dekker, New York, 1993.

5 Martin Davis. Hilbert's tenth problem is unsolvable. *The American Mathematical Monthly*, 80(3):233–269, 1973. doi:10.1080/00029890.1973.11993265.

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

7 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.

8 Mirai Ikebuchi. A Lower Bound of the Number of Rewrite Rules Obtained by Homological Methods. In Herman Geuvers, editor, *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 für Informatik.

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

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

11 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 für Informatik.

12 Ju V Matijasevic. Enumerable sets are diophantine. In *Soviet Math. Dokl.*, volume 11, pages 354–358, 1970.

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

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

15 Charles A. Weibel. *An Introduction to Homological Algebra*. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 1994.

A The matrix for $E_1 \cup \{x_1 + x_1 \approx 0\}$

The TRS $E_1 \cup \{x_1 + x_1 \approx 0\}$ has the following complete TRS R_3:

$$B_1 : 0 + x_1 \to x_1 \quad B_2 : s(x_1) + x_2 \to s(x_1 + x_2) \quad D_1 : x_1 + x_1 \to 0$$
$$D_2 : s(s(x_1)) \to x_1 \quad D_3 : x_1 + s(x_1) \to s(0) \quad D_4 : s(x_1) + x_1 \to s(0).$$

The critical pairs are listed in Fig. 1 and the matrix $(D(R_3)|U(E_1, R_3))$ is given as follows.

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

It is not too hard to check that it has full rank.

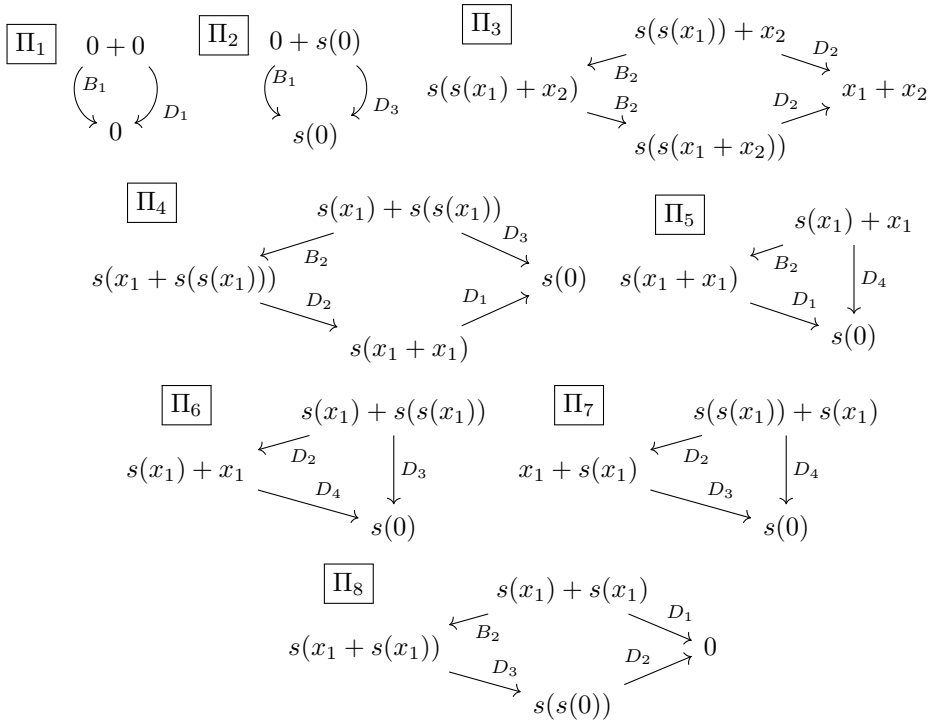


Figure 1 Critical pairs of R_3 in Example 3.