

Rigidity is undecidable

Mikołaj Bojanczyk, Stanisław Szawiel,
Marek Zawadowski

April 28, 2012

Abstract

We show that the problem ‘whether a finite set of regular-linear axioms defines a rigid theory’ is undecidable.

2010 Mathematical Subject Classification 03D35, 03C05, 03G30, 18C10, 18C15

Keywords: Equational theory, interpretation, undecidable problem, word problem for monoid

1 Introduction

In [SZ] it was shown that the category of polynomial monads is equivalent to the category of rigid equational theories, solving a problem stated in [CJ2]. A linear-regular theory is an equational theory that has as a set of axioms equations of terms $s = t$ such that the variables occurring in s and t are the same and each of them occurs once. For example the theory of monoids, commutative monoids, and monoids with anti-involution are linear-regular. Recall that the theory of monoids with anti-involution has three function symbols e , i , m of arity 0, 1, 2, respectively, contains the usual axioms for monoids, and additionally the equations $i(i(x_1)) = x_1$ and $i(m(x_1, x_2)) = m(i(x_2), i(x_1))$. A linear-regular theory is rigid if and only if for any term $t(x_1, \dots, x_n)$ and permutation $\sigma \in S_n$, if $T \vdash t(x_1, \dots, x_n) = t(x_{\sigma(1)}, \dots, x_{\sigma(n)})$ then σ is an identity permutation. In other words, T is rigid if any (proper) permutation of variables changes the meanings of terms in T . For example, the theories of monoids and monoids with anti-involution are rigid but the theory of commutative monoids is not as it contains the axiom $m(x_1, x_2) = m(x_2, x_1)$. Rigidity refers to provability in T and hence it is a global property concerning a linear-regular theories. In this paper we show that the problem whether an equational theory T with finite set of linear-regular axioms is rigid, is undecidable.

2 Preliminaries

When dealing with equational theories we follow mostly the terminology of [BN]. However, we want to specify what variables might occur in a term, and for this reason we deal with terms in context. We call an ‘equation’ what in [BN] is called an ‘identity’.

By an *equational theory* we mean a pair of sets $T = (L, A)$, $L = \bigcup_{n \in \omega} L_n$ and L_n is the set of n -ary operations. The sets of operations of different arities are disjoint. The set $Tr(L, \vec{x}^n)$ of terms of L in context $\vec{x}^n = \langle x_1, \dots, x_n \rangle$ is the usual set of terms over L built with the help of variables from \vec{x}^n . We write $t : \vec{x}^n$ for the term t in context \vec{x}^n . Thus all the variables occurring in t are among those in \vec{x}^n . The set A is a set of equations in context $t = s : \vec{x}^n$, i.e. both $t : \vec{x}^n$ and $s : \vec{x}^n$ are terms in context, $n \in \omega$.

If we do not specify explicitly the context of a term then we mean that the context consists of variables explicitly occurring in the term. As in [BN] we often think of a term as a tree labeled by functions symbols and variables. A derivation consists of a finite number of rewrite steps. One rewrite step replaces a part of a term tree that matches a substitution of one side of an equation in T by the same substitution of the other side of that equation. For details see [BN] definition 3.1.8. When possible, a simple derivation will be presented as a sequence of equations.

A morphism of equational theories, an *interpretation*, $I : T \rightarrow T' = (L', A')$, is a set of functions $I_n : L_n \rightarrow \mathcal{T}r(L', \vec{x}^n)$ for $n \in \omega$. Moreover, we require that I preserves the equations, i.e. for any $t = s : \vec{x}^n$ in A we have

$$A' \vdash \bar{I}(t) = \bar{I}(s) : \vec{x}^n$$

where $A' \vdash$ (or $T' \vdash$) is the provability in the equational logic from axioms in the set of axioms A' (or theory T'). \bar{I} is the extension of I_n 's to functions $\bar{I}_n : \mathcal{T}r(L, \vec{x}^n) \rightarrow \mathcal{T}r(L', \vec{x}^n)$ for $n \in \omega$ as follows. We usually drop index n in \bar{I}_n .

$$\bar{I}(x_i : \vec{x}^n) = x_i : \vec{x}^n$$

for $i = 1, \dots, n$, $n \in \omega$ and

$$\bar{I}(f(t_1, \dots, t_k) : \vec{x}^n) = I(f)(x_1 \setminus \bar{I}(t_1), \dots, x_k \setminus \bar{I}(t_k)) : \vec{x}^n$$

for $f \in L_k$ and $t_i \in \mathcal{T}r(L, \vec{x}^n)$ for $i = 1, \dots, k$. On the right-hand side, we have a simultaneous substitution of terms t_i 's for variables x_i 's. We identify two such interpretations I and $I' : (L, A) \rightarrow (L', A')$ iff they interpret all function symbols as provably equivalent terms, i.e.

$$A' \vdash I(f) = I'(f) : \vec{x}^n$$

for any $n \in \omega$ and $f \in L_n$. An interpretation $I : T \rightarrow T'$ is *conservative* iff for any equation in context $s = t : \vec{x}^n$ in T if $T' \vdash \bar{I}(s) = \bar{I}(t) : \vec{x}^n$ then $T \vdash s = t : \vec{x}^n$.

A term in context $t : \vec{x}^n$ is *linear-regular* if every variable in \vec{x}^n occurs in t exactly once. An equation $s = t : \vec{x}^n$ is *linear-regular* iff both $s : \vec{x}^n$ and $t : \vec{x}^n$ are linear-regular terms in contexts.

A *simple ϕ -substitution of a term in context $t : \vec{x}^n$* along a function $\phi : (n) \rightarrow (k)$ is a term in context denoted $\phi \cdot t : \vec{x}^k$ such that every occurrence of the variable x_i is replaced by the occurrence of $x_{\phi(i)}$.

An equational theory $T = (L, A)$ is a *linear-regular theory* iff all the consequences of T are consequences of linear-regular consequences of T . An interpretation is a *linear-regular interpretation* iff it interprets function symbols as linear-regular terms.

A theory $T = (L, A)$ is a *rigid theory* iff it is linear-regular and for any linear-regular term in context $t : \vec{x}^n$ whenever $A \vdash t = \sigma \cdot t : \vec{x}^n$ then σ is the identity permutation. $\tau \cdot t$ is the simple σ -substitution of a term in context $t : \vec{x}^n$ along a permutation $\sigma \in S_n$.

The definitions of both linear-regular and rigid theories are such to make sure that if a theory is isomorphic to a linear-regular (rigid) theory then it is also linear-regular (rigid).

3 Main result

If we find a linear-regular set of axioms of an equational theory T we can be sure that T is linear-regular, (cf. [SZ]). However, it is not so easy to decide whether a given theory is rigid. The main result of this paper says that even if we restrict ourselves to finitely

axiomatizable linear-regular theories it is still undecidable whether such theories are rigid or not.

A term $t(x_1, \dots, x_n)$ is *flabby* in T if it is linear-regular in variables x_1, \dots, x_n such that

$$T \vdash t(x_1, \dots, x_n) = t(x_{\sigma(1)}, \dots, x_{\sigma(n)}) \quad (1)$$

for a non-identity permutation $\sigma \in S_n$. A theory is rigid iff it does not contain flabby terms.

Theorem 3.1. *The problem whether an equational theory $T = (L, A)$ in finite language L with a finite set of linear-regular axioms A is rigid is undecidable.*

Proof. The word problem for monoids is undecidable; (cf. [M], [P]). We shall show that it reduces to our problem. Below we sketch the construction of the reduction and an argument showing that it is indeed a reduction. Then in a series of Lemmas proved in the remaining part of the paper we shall make the sketched construction and argument more precise.

First we define a simple theory T_0 that is rigid, (cf. Lemma 3.2). For an arbitrary instance of the word problem for monoids,

$$\bigwedge_{i \in n} u_i = v_i \vdash u = v \quad (2)$$

where u_i, v_i, u, v are words over a finite alphabet, we will define a theory T such that T is rigid iff (2) does not hold.

An easy argument shows that if (2) holds then there is an obvious flabby term in T and hence T is not rigid, (cf. Lemma 3.4).

Next we define a linear-regular interpretation $I : T_0 \rightarrow T$ which is conservative iff (2) does not hold, (cf. Lemma 3.5). The terms in the image of $\bar{I} : Tr(T_0) \rightarrow Tr(T)$ are called special and the set of special terms is denoted by $Sp(T)$. We construct a function

$$\widehat{(-)} : Tr(T) \longrightarrow Sp(T)$$

sending all terms of T to the special terms such that

1. $\widehat{(-)}$ is onto;
2. $\widehat{\bar{I}(s)} = \bar{I}(s)$, for any $s \in Tr(T_0)$;
3. for $t \in Tr(T)$, the variables occurring in both terms t and \hat{t} are the same and they occur in the same order;
4. for $t, t' \in Tr(T)$, if $T \vdash t = t'$ then $T \vdash \hat{t} = \hat{t}'$;

(cf. Lemma 3.6).

Having established the above, to get a contradiction, we shall assume that (2) does not hold but T is still not rigid. Let $t(x_1, \dots, x_n)$ be a flabby term in T and $\sigma \in S_n$ such that (1) holds. Then, by Lemma 3.6,

$$T \vdash \hat{t}(x_1, \dots, x_n) = \hat{t}(x_{\sigma(1)}, \dots, x_{\sigma(n)}) \quad (3)$$

holds. As \bar{I} is onto there is a term $s(x_1, \dots, x_n)$ in T_0 such that $\bar{I}(s)(x_1, \dots, x_n) = \hat{t}(x_1, \dots, x_n)$. Thus

$$T \vdash \bar{I}(s)(x_1, \dots, x_n) = \bar{I}(s)(x_{\sigma(1)}, \dots, x_{\sigma(n)})$$

and since I is conservative

$$T_0 \vdash s(x_1, \dots, x_n) = s(x_{\sigma(1)}, \dots, x_{\sigma(n)}).$$

But this means that s is a flabby term in T_0 , contradicting rigidity of T_0 . This ends the proof of the theorem. \square

Now, we fix for the rest of the paper the theory T constructed as in the (sketch of) proof of Theorem 3.1 and we fill the details of the above argument.

The theory T_0 contains three binary symbols l, r, m and one equation

$$l(x_1, x_2) = r(x_2, x_1) \tag{4}$$

We have

Lemma 3.2. *T_0 is a rigid theory.*

Proof.

The theory T_0 is equivalent (in fact isomorphic) to a theory that has two binary function symbols and no equations. Thus it contains no non-trivial equations. In particular it is rigid. \square

Let us fix an instance of the word problem for monoids. Let u_i, v_i, u, v words over the alphabet $G = \{g_1, \dots, g_n\}$, for $i \in m$. The problem is to decide whether (2) holds true. We define an equational theory T corresponding to this problem. The alphabet of T consists of unary symbols from G and additionally one unary symbol α and one binary symbol m . If $w = g_{k_1} \dots g_{k_m}$ is a word over G then $w(x)$ denotes the corresponding term $g_{k_1} \dots g_{k_m}(x)$ of T . The axioms of T are

$$u_i(x_1) = v_i(x_1) \quad \text{for } i \in m \tag{5}$$

and moreover

$$m(u\alpha(x_1), x_2) = m(v\alpha(x_2), x_1) \tag{6}$$

The following Lemma makes simple but useful observations concerning the derivations in theory T .

Lemma 3.3. *1. For any two words w_1, w_2 over G we have*

$$\bigwedge_{i \in m} u_i = v_i \vdash w_1 = w_2 \quad \text{iff } T \vdash w_1(x_1) = w_2(x_1) \tag{7}$$

where \vdash on the left is the consequence relation in the theory of monoids.

- 2. The symbol α does not take part in any rewrite step over T concerning unary symbols.*
- 3. Each rewrite step over T concerns only unary symbols or it is performed on a subterm with the root labeled m . In particular, no derivation changes the number of symbols m . \square*

Remark. Last property says that in the derivations in T we can trace the identity of each symbol m . We are going to use it when arguing about derivations.

Lemma 3.4. *If (2) holds then T is not rigid.*

Proof. Let $t(x_1, x_2) = m(u\alpha(x_1), x_2)$. Then, using (6), (2), and 7, we have in T

$$t(x_1, x_2) = m(u\alpha(x_1), x_2) = m(v\alpha(x_2), x_1) = m(u\alpha(x_2), x_1) = t(x_2, x_1)$$

i.e. t is flabby in T , and T is not rigid. \square

Now we define a linear-regular interpretation $I : T_0 \rightarrow T$ as follows

$$I(l) = m(u\alpha(x_1), x_2), \quad I(r) = m(v\alpha(x_1), x_2), \quad I(m) = m(x_1, x_2).$$

Lemma 3.5. *$I : T_0 \rightarrow T$ is a linear-regular interpretation. It is conservative iff (2) does not hold.*

Proof. We have in T

$$\bar{I}(l)(x_1, x_2) = m(u\alpha(x_1), x_2) = m(v\alpha(x_2), x_1) = \bar{I}(l)(x_2, x_1)$$

and hence I is an interpretation.

If (2) holds then we have in T

$$\bar{I}(l(x_1, x_2)) = m(u\alpha(x_1), x_2) = m(v\alpha(x_2), x_1) = \bar{I}(r(x_1, x_2))$$

But clearly $T_0 \not\vdash l(x_1, x_2) = r(x_1, x_2)$. So I is not conservative.

Now, we assume that $T \not\vdash u(x) = v(x)$ and we shall show that I is conservative. Let s, s' be two terms in T_0 such that

$$T \vdash \bar{I}(s) = \bar{I}(s').$$

First, we want to show that the above equality can be deduced without use of the equations (5). Let D be a derivation of $\bar{I}(s) = \bar{I}(s')$ in T that contains minimal number of applications of equations (5). If D does not use (5), we are done. If the equation (5) is used in D , it is used to either part of the string of unary symbols u or v of a subterm $m(u\alpha(t_1), t_2)$ or $m(v\alpha(t_1), t_2)$, respectively. Suppose the first rewrite step using the equation (5) in the derivation D is applied to the subterm $m(u\alpha(t_1), t_2)$ rewriting it to some other subterm $m(u'\alpha(t_1), t_2)$. The rewrite steps concerning the subterm with ‘this occurrence’ of m as the root symbol will concern the subterms u' and t_1, t_2 parts only and possibly m but only if u' will be rewritten to either u or v . By assumption, u cannot be rewritten to v , so it can only be rewritten back to u . In fact, as at the end of the derivation we get a term of form $\bar{I}(s')$ (with all strings of unary symbols from G being equal either u or v), u' has to be eventually rewritten back to u . But this means that we can shorten the derivation D by eliminating all those rewrite steps from u to u' and back to u again. As this contradicts the minimality of D , we can assume that D contains only rewrite steps that use the equation (6). But then the derivation D of $\bar{I}(s) = \bar{I}(s')$ in T can be used to build a derivation D' of $s = s'$ in T_0 . We need to change the rewrite steps using the equation (6) in D to rewrite steps in the corresponding positions using the equality (4) in D' . Thus $T_0 \vdash s = s'$. Since terms s, s' where arbitrary, I is conservative. \square

Special terms of T are terms in the image of the function $\bar{I} : Tr(T_0) \rightarrow Tr(T)$. The set of special terms is denoted by $Sp(T)$. The function

$$\widehat{(-)} : Tr(T) \longrightarrow Sp(T)$$

is defined, for $t = t(x_1, \dots, x_n) \in Tr(T)$ as follows

$$\hat{t} = \begin{cases} x_i & \text{if } t = x_i \\ \hat{t}' & \text{if } t = g(t') \text{ where } g \in G \cup \{\alpha\} \\ m(u\alpha(\hat{t}_1), \hat{t}_2) & \text{if } t = m(w\alpha(t_1), t_2) \text{ and } T \vdash u(x) = w(x) \\ m(v\alpha(\hat{t}_1), \hat{t}_2) & \text{if } t = m(w\alpha(t_1), t_2) \text{ and } T \vdash v(x) = w(x) \text{ and not (2)} \\ m(\hat{t}_1, \hat{t}_2) & \text{if } t = m(t_1, t_2), \text{ and none of the above applies.} \end{cases}$$

The following Lemma lists some properties of $\widehat{(-)}$ that were used in the proof of the main theorem.

Lemma 3.6. *We have*

1. $\widehat{(-)}$ is onto;
2. $\widehat{\bar{I}(s)} = \bar{I}(s)$, for any term s of T_0 ;
3. for any term t of T , the variables in terms t and \widehat{t} are the same and they occur in the same order; $t : \bar{x}^n$ is a linear-regular term iff $\widehat{t} : \bar{x}^n$ is;
4. if $T \vdash t = t'$ then $T \vdash \widehat{t} = \widehat{t}'$, for any terms t, t' in T .

Proof. 1. and 2. is obvious.

To show 3. one can verify by induction on the construction of terms that no clause in the definition of $\widehat{(-)}$ changes the variables or their order.

We shall show 4. by induction on the complexity of the term t . If t is a variable then the thesis is obvious.

If $t = w(m(t_1, t_2))$ where w is a (non-empty) sequence of unary symbols of T then, as no derivation changes the number of symbols in terms, $t' = w'(m(t'_1, t'_2))$ where w' is a sequence of unary symbols of T . The derivation D from t to t' consists of steps that either change unary symbols over the first m in the term using equations (5) or does not involve those symbols at all. Thus if we drop from the derivation D all the rewrite steps that change symbols over the first m the resulting derivation proves $w(m(t_1, t_2)) = w(m(t'_1, t'_2))$ never using symbols from w . Thus the same derivation proves also $m(t_1, t_2) = m(t'_1, t'_2)$. Using inductive hypothesis we get

$$\widehat{t} = m(\widehat{t_1}, \widehat{t_2}) = m(\widehat{t'_1}, \widehat{t'_2}) = \widehat{t'}$$

If $t = m(t_1, t_2)$ and $t' = z(m(t'_1, t'_2))$, then by the above we can assume that the sequence of the unary symbols z is empty. We have to consider three cases concerning the form of the term t_1 :

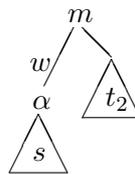
1. $t_1 = w(\alpha(s))$ and $T \vdash u(x) = w(x)$;
2. $t_1 = w(\alpha(s))$ and $T \vdash v(x) = w(x)$;
3. t_1 is not in the above form.

As the cases 1. and 2. are similar we shall consider cases 1. and 3 only.

We start with Case 3, as it is much simpler. In that case to the leading symbol m in term t the rule (6) is never applied. Thus all the derivations of $T \vdash t = t'$ can be split into two separate derivations, one for $T \vdash t_1 = t'_1$ and one for $T \vdash t_2 = t'_2$. Thus again using inductive hypothesis we get

$$\widehat{t} = m(\widehat{t_1}, \widehat{t_2}) = m(\widehat{t'_1}, \widehat{t'_2}) = \widehat{t'} \quad \square$$

It remains to consider Case 1. The term t looks as follows

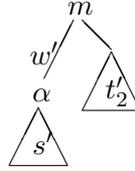


Then the derivation D of $t = t'$ has three kinds of rewrite steps:

1. using equation (6) to the root symbol m in the term;
2. using equations (5) to change something in the sequence of unary symbols over the first α on the left;
3. using either kinds of equations to rewrite something in subterm s or t_2 .

The rewrite steps of the third kind are independent of the rewrite steps of the first and second kind. Thus we can assume that we first do the rewrite steps of the first and second kind and after that the rewrite steps of the third kind. It is also not difficult to note that the rewrite steps of the first kind can be moved so that they are performed one after the other. Any two rewrite steps of the first kind done one immediately after the other do not change the term. We can eliminate all but possibly one rewrite step of the first kind from D and still have a derivation of $t = t'$. Now we assume that D is a derivation with at most one step of the first kind, in between the rewrite steps of the second kind, with all the rewrite steps of the third kind at the end.

Thus we have two cases depending whether there is one rewrite steps of the second kind or none. In both cases the term t' is of form



If there are no rewrite step of the first kind in D then the derivation D consists of three independent derivations in T of the equations

$$w = w', \quad s = s', \quad t_2 = t'_2.$$

Thus using inductive assumption we get

$$\widehat{t} = m(u(\alpha(\widehat{s}), \widehat{t}_2)) = m(u(\alpha(\widehat{s}'), \widehat{t}'_2)) = \widehat{t}'$$

If there is one rewrite step of the first kind in D then the derivation D consists of two independent derivations in T of the equations

$$s = s', \quad t_2 = t'_2.$$

and moreover two derivation of either $w = u$ and $v = w'$ or, if $T \vdash u = v$, two derivations $w = v$ and $u = w'$. Between the latter two derivations there is one rewrite step of the first kind. Again using inductive assumption we get

$$\widehat{t} = m(u(\alpha(\widehat{s}), \widehat{t}_2)) = m(v'(\alpha(\widehat{s}'), \widehat{t}'_2)) = \widehat{t}'$$

where

$$v' = \begin{cases} u & \text{if } T \vdash u = v \\ v & \text{otherwise.} \end{cases}$$

□

References

- [BN] F. Baader, T. Nipkow, *Term rewriting and all that*, Cambridge University Press, (1998).
- [CJ1] A. Carboni, P. T. Johnstone, *Connected limits, familial representability, and Artin, glueing*, *Mathematical Structures in Comp. Science* (1995), vol 5, pp. 441-459.
- [CJ2] A. Carboni, P. T. Johnstone: Corrigenda for ‘Connected limits, familial representability and Artin glueing’. *Mathematical Structures in Computer Science* 14(1): 185-187 (2004)
- [J] A. Joyal, *Foncteurs analytiques et espèces de structures*, *Lecture Notes Math.* 1234, Springer (1986), pp. 126-159.
- [M] A. A. Markov, *On impossibility of certain algorithms in the theory of associative systems*, (in Russian) *Dokl. Akad. Nauk SSSR* 55, pp. 587-590. [English translation in *C. R. Acad. Sci. URSS*, 55, pp. 533-586]
- [P] E. Post, *Recursive Unsolvability of a Problem of Thue*, *J. Symbolic Logic*, vol. 12 (1947) pp. 1-11.
- [SZ] S. Szawiel, M. Zawadowski, *Theories of analytic monads*, arXiv:1204.2703v1 [math.CT].