Math. Struct. in Comp. Science (2014), vol. 24, iss. 6, e240605, 10 pages. © Cambridge University Press 2014
doi:10.1017/S096012951300087X

Rigidity is undecidable

MIKOŁAJ BOJAŃCZYK[†], STANISŁAW SZAWIEL[‡]
and MAREK ZAWADOWSKI[‡]

[†]*Institute of Informatics, University of Warsaw,*
S. Banacha 2, 02-097 Warszawa, Poland
Email: bojan@mimuw.edu.pl
[‡]*Institute of Mathematics, University of Warsaw,*
S. Banacha 2, 02-097 Warszawa, Poland
Email: {szawiel;zawado}@mimuw.edu.pl

Received 28 April 2012; revised 6 September 2013

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

1. Introduction

Szawiel and Zawadowski (2014) showed that the category of polynomial monads is equivalent to the category of rigid equational theories, thereby solving a problem stated in Carboni and Johnstone (2004). 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 only once. For example, the theories 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 and m with arities 0, 1 and 2, respectively, contains the usual axioms for monoids and, additionally, the equations

$$i(i(x_1)) = x_1$$
$$i(m(x_1, x_2)) = m(i(x_2), i(x_1)).$$

A linear-regular theory is rigid if and only if for any term $t(x_1, \ldots, x_n)$ and permutation $\sigma \in S_n$, if

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

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 is thus a global property of linear-regular theories. In this paper we show that the problem of whether an equational theory T with finite set of linear-regular axioms is rigid is undecidable.

https://doi.org/10.1017/S096012951300087X Published online by Cambridge University Press

2. Preliminaries

When dealing with equational theories, we will mostly follow the terminology of Baader and Nipkow (1998). However, we want to specify what variables might occur in a term, so we deal with terms in context, and we use the word 'equation' for what Baader and Nipkow (1998) call an 'identity'.

By an *equational theory*, we mean a pair of sets $T = (L, A)$, where $L = \bigcup_{n\in\omega} L_n$ and L_n is the set of n-ary operations. The sets of operations of different arities are disjoint. The set $\mathcal{T}r(L, \vec{x}^n)$ of terms over L in context

$$\vec{x}^n = \langle x_1, \ldots, x_n \rangle$$

is the usual set of terms built using symbols from L and variables from $\vec{x}^n$. We write $t : \vec{x}^n$ for a term t over L in context $\vec{x}^n$. The set A is a set of equations of L in context $t = s : \vec{x}^n$, that is, both $t : \vec{x}^n$ and $s : \vec{x}^n$ are terms over L in context for $n \in \omega$.

If we do not specify the context of a term explicitly, we mean that the context consists of variables explicitly occurring in the term. As in Baader and Nipkow (1998), we often think of a term as a tree labelled 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 Baader and Nipkow (1998, Definition 3.1.8). When possible, a simple derivation will be presented as a sequence of equations.

A morphism of equational theories, an *interpretation*

$$I : T \to T' = (L', A'),$$

is a set of functions

$$I_n : L_n \to \mathcal{T}r(L', \vec{x}^n)$$

for $n \in \omega$. Moreover, we require that I preserves the equations, that is, 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 the I_ns to functions

$$\bar{I}_n : \mathcal{T}r(L, \vec{x}^n) \to \mathcal{T}r(L', \vec{x}^n)$$

for $n \in \omega$ as follows (we will usually drop the index n in $\bar{I}_n$). We have

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

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

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

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

https://doi.org/10.1017/S096012951300087X Published online by Cambridge University Press

symbols as provably equivalent terms, that is,

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

for any $n \in \omega$ and $f \in L_n$. An interpretation $I : T \to T'$ is *conservative* if and only if for any equation $s = t : \vec{x}^n$ of L, 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 and only if every variable in $\vec{x}^n$ occurs in t exactly once. An equation $s = t : \vec{x}^n$ is *linear-regular* if and only if 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 $\phi : (n] \to (k]$ is a term in context, denoted by $\phi \cdot t : \vec{x}^k$, 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* if and only if all the consequences of T are consequences of linear-regular consequences of T. An interpretation is a *linear-regular interpretation* if and only if it interprets function symbols as linear-regular terms.

A theory $T = (L, A)$ is a *rigid theory* if and only if it is linear-regular and for any linear-regular term in context $t : \vec{x}^n$, if $A \vdash t = \sigma \cdot t : \vec{x}^n$, 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 as to ensure 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 (Szawiel and Zawadowski 2014). The main result of the current paper says that even if we restrict ourselves to finitely axiomatisable linear-regular theories, the problem of whether or not such theories are rigid is still undecidable.

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

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

for a non-identity permutation $\sigma \in S_n$. Thus, a theory is rigid if and only if it does not contain flabby terms.

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

Proof (sketch). It is well known that the word problem for monoids is undecidable (Markov 1947; Post 1947), and 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. We shall then prove a series of Lemmas in the remaining part of the paper that make the construction and argument more precise.

https://doi.org/10.1017/S096012951300087X Published online by Cambridge University Press

We begin the proof by defining a simple theory T_0 that is rigid (*cf.* Lemma 3.2). For an arbitrary instance of the word problem for monoids,

$$\bigwedge_{i \in n} u_i = v_i \vdash u = v \tag{2}$$

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

An easy argument shows that if equation (2) holds, there is an obvious flabby term in T and hence T is not rigid (*cf.* Lemma 3.5). To complete the proof, we shall also need the converse.

Next we define a linear-regular interpretation $I : T_0 \to T$ that is conservative if and only if equation (2) does not hold (*cf.* Lemma 3.6). The terms in the image of

$$\bar{I} : \mathcal{T}r(T_0) \to \mathcal{T}r(T)$$

are called special, and the set of special terms is denoted by $\mathcal{S}p(T)$. We construct a function

$$\widehat{(-)} : \mathcal{T}r(T) \longrightarrow \mathcal{S}p(T)$$

sending all terms of T to the special terms such that (*cf.* Lemma 3.7):

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

Having established the above, in order to get a contradiction, we shall assume that equation (2) does not hold but T is still not rigid. Let $t(x_1, \ldots, x_n)$ be a flabby term in T and $\sigma \in S_n$ such that (1) holds. Then, by Lemma 3.7,

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

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

$$\bar{I}(s)(x_1, \ldots, x_n) = \hat{t}(x_1, \ldots, x_n).$$

Thus

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

and since I is conservative,

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

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

We shall now fill in the details of the above argument.

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

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

https://doi.org/10.1017/S096012951300087X Published online by Cambridge University Press

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, so it contains no non-trivial equations. In particular, it is rigid. □

We now fix an instance of the word problem for monoids. Let u_i, v_i, u and v be words over the alphabet $G = \{g_1, \ldots, g_n\}$ for $i \in m$. The problem is to decide whether equation (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 $w = g_{k_1} \ldots g_{k_m}$ is a word over G, then $w(x)$ denotes the corresponding term $g_{k_1} \ldots g_{k_m}(x)$ of T. The axioms of T are

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

and, moreover,

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

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

Lemma 3.3.

(1) For any two words w_1 and w_2 over G, we have

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

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 labelled m. In particular, no derivation changes the number of symbols m.

Remark 3.4. Property (3) says that in the derivations in T we can trace the identity of each symbol m – we shall use this when arguing about derivations.

Lemma 3.5. If equation (2) holds, then T is not rigid.

Proof. Let

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

Then, using equations (6), (2) and (7), we have in T

$$\begin{aligned} t(x_1, x_2) &= m(u\alpha(x_1), x_2) \\ &= m(v\alpha(x_2), x_1) \\ &= m(u\alpha(x_2), x_1) \\ &= t(x_2, x_1), \end{aligned}$$

that is, t is flabby in T, so T is not rigid. □

https://doi.org/10.1017/S096012951300087X Published online by Cambridge University Press

We now define a linear-regular interpretation $I : T_0 \to T$ as follows:

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

Lemma 3.6. $I : T_0 \to T$ is a linear-regular interpretation. It is conservative if and only if equation (2) does not hold.

Proof. We have in T

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

so I is an interpretation.

If equation (2) holds, we have in T

$$\begin{aligned}\bar{I}(l(x_1, x_2)) &= m(u\alpha(x_1), x_2)\\ &= m(v\alpha(x_1), x_2)\\ &= \bar{I}(r(x_1, x_2)).\end{aligned}$$

But it is clear that $T_0 \nvdash l(x_1, x_2) = r(x_1, x_2)$, so I is not conservative.

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

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

We want to show first that the above equality can be deduced without using equations (5). Let D be a derivation of $\bar{I}(s) = \bar{I}(s')$ in T that contains the minimal number of applications of equations (5). If D does not use equations (5), we are done. If an equation (5) is used in D, it is used for a 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 an 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 the 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, since at the end of the derivation we get a term of the form $\bar{I}(s')$ (with all strings of unary symbols from G being equal to either u or v), u' must eventually be 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. Since this contradicts the minimality of D, we can assume that D only contains rewrite steps that use 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 equation (6) in D to rewrite steps in the corresponding positions using equation (4) in D'. Thus, $T_0 \vdash s = s'$. Hence, since the terms s and s' were arbitrary, I is conservative. □

https://doi.org/10.1017/S096012951300087X Published online by Cambridge University Press

As mentioned above, special terms of T are terms in the image of the function

$$\bar{I} : \mathcal{T}r(T_0) \to \mathcal{T}r(T),$$

and the set of special terms is denoted by $\mathcal{S}p(T)$. The function

$$\widehat{(-)} : \mathcal{T}r(T) \longrightarrow \mathcal{S}p(T)$$

is defined for $t = t(x_1, \ldots, x_n) \in \mathcal{T}r(T)$ as follows:

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

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

Lemma 3.7. 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; $t : \vec{x}^n$ is a linear-regular term if and only if $\widehat{t} : \vec{x}^n$ is.
(4) If $T \vdash t = t'$, then $T \vdash \widehat{t} = \widehat{t'}$, for any terms t, t' in T.

Proof.

(1) This part is obvious.
(2) This part is obvious.
(3) To show this part, we just verify by induction on the construction of terms that no clause in the definition of $\widehat{(-)}$ changes the variables or their order.
(4) We use induction on the complexity of the term t:
   — If t is a variable, 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 do 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

$$w(m(t_1, t_2)) = w(m(t'_1, t'_2))$$

   without using any symbols from w. Thus, the same derivation also proves

$$m(t_1, t_2) = m(t'_1, t'_2).$$

https://doi.org/10.1017/S096012951300087X Published online by Cambridge University Press

Using the induction hypothesis, we then get

$$\begin{aligned}\widehat{t} &= m(\widehat{t_1, t_2}) \\ &= m(\widehat{t'_1, t'_2}) \\ &= \widehat{t'}.\end{aligned}$$

— 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 for the form of the term t_1:

(a) $t_1 = w(\alpha(s))$ and $T \vdash u(x) = w(x)$.

(b) $t_1 = w(\alpha(s))$ and $T \vdash v(x) = w(x)$.

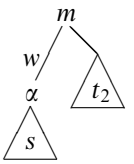
(c) t_1 does not have either of the above forms.

Cases (a) and (b) are similar, so we shall only consider cases (a) and (c). We will begin with case (c), as it is much simpler.

In case (c), the rule (6) is never applied to the leading symbol m in term t. 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 the induction hypothesis, we get

$$\begin{aligned}\widehat{t} &= m(\widehat{t_1}, \widehat{t_2}) \\ &= m(\widehat{t'_1}, \widehat{t'_2}) \\ &= \widehat{t'}.\end{aligned}$$

For case (a), the term t is of the form



so the derivation D of $t = t'$ has three kinds of rewrite step:

(i) rewrites using equation (6) for the root symbol m in the term;

(ii) rewrites using equations (5) to change something in the sequence of unary symbols over the first α on the left;

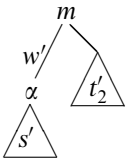
(iii) rewrites using either kind of equation to rewrite something in subterm s or t_2.

The rewrite steps of the third kind are independent of the rewrite steps of the first and second kind, so we can assume that we do the rewrite steps of the first and second kind first, and then the rewrite steps of the third kind. It is also not difficult to see 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, so we can eliminate all but possibly one rewrite step of the first kind from D and still have a derivation of $t = t'$. So we can now assume that D is a derivation with at most one step of

https://doi.org/10.1017/S096012951300087X Published online by Cambridge University Press

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 to consider, depending on whether there is one rewrite step of the second kind or none. In both cases, the term t' has the form



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

$$w = w'$$
$$s = s'$$
$$t_2 = t'_2.$$

Thus, using the induction hypothesis, we get

$$\begin{aligned}\widehat{t} &= m(u(\alpha(\widehat{s}), \widehat{t_2}) \\ &= m(u(\alpha(\widehat{s'}), \widehat{t'_2}) \\ &= \widehat{t'}.\end{aligned}$$

If there is one rewrite step of the first kind in D, then, possibly after some reorganisation of the independent step, the derivation D in T consists of

(i) a derivation of $w = u$ by steps of the second kind;

(ii) one rewrite step of the first kind;

(iii) a derivation of $v = w'$ by steps of the second kind;

(iv) two independent derivations in T of the equations $t_2 = s'$ and $s = t'_2$ by steps of the third kind.

Using the induction hypothesis again, we get

$$\begin{aligned}\widehat{t} &= m(u(\alpha(\widehat{s}), \widehat{t_2})) \\ &= m(v'(\alpha(\widehat{t_2}), \widehat{s})) \\ &= m(v'(\alpha(\widehat{s'}), \widehat{t'_2})) \\ &= \widehat{t'}\end{aligned}$$

where

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

This completes the proof. □

References

Baader, F. and Nipkow, T. (1998) *Term rewriting and all that*, Cambridge University Press.

https://doi.org/10.1017/S096012951300087X Published online by Cambridge University Press

Carboni, A. and Johnstone, P. T. (1995) Connected limits, familial representability and Artin glueing. *Mathematical Structures in Computer Science* **5** 441–459.

Carboni, A. and Johnstone, P. T. (2004) Corrigenda for 'Connected limits, familial representability and Artin glueing'. *Mathematical Structures in Computer Science* **14** (1) 185–187.

Joyal, A. (1986) Foncteurs analytiques et espéces de structures. In: Labelle, G. and Leroux, P. (eds.) Combinatoire énumerative. *Springer-Verlag Lecture Notes in Mathematics* **1234** 126–159.

Markov, A. A. (1947) On the impossibility of certain algorithms in the theory of associative systems (in Russian). *Doklady Akademii Nauk SSSR* **55** (7) 587–590. (English translation: *Comptes Rendus de l'Academie des Sciences de l'URSS* (1948) **55** 533–586.)

Post, E. (1947) Recursive Unsolvability of a Problem of Thue. *Journal of Symbolic Logic* **12** 1–11.

Szawiel, S. and Zawadowski, M. (2014) Theories of analytic monads. *Mathematical Structures in Computer Science* (to appear).

https://doi.org/10.1017/S096012951300087X Published online by Cambridge University Press