The First-Order Theory of One Step Rewriting in Linear Noetherian Systems is Undecidable

Sergei Vorobyov
March 4, 1997

Max-Planck-Institut für Informatik
Im Stadtwald, D-66123, Saarbrücken, Germany (e-mail: sv@mpi-sb.mpg.de)

Abstract. We construct a finite linear finitely terminating rewrite rule system with undecidable theory of one step rewriting.

1 Preliminaries

Given a functional signature Σ with constants and a finite rewrite rule system R, consider the model $M = \langle T(\Sigma), \mathbf{R}\rangle$, where $T(\Sigma)$ is the Herbrand universe over Σ and $\mathbf{R} = \{\langle s,t\rangle \mid s,t \in T(\Sigma) \wedge s \to_R t\} \subseteq T(\Sigma) \times T(\Sigma)$ is the one step rewrite relation on $T(\Sigma)$ generated by R. The presence of constants in Σ is necessary to guarantee that $T(\Sigma)$ is not empty.

Let $\mathcal{L}$ be the first-order language *without equality* containing the only binary relation symbol R. The *first-order theory of one step rewriting* in R is the set of all sentences (closed formulas) of $\mathcal{L}$ true in M. Notice that the only non-logical symbol used in formulas of the theory is R, and the symbols of Σ are *not allowed* in formulas.

The aim of this note is to give an example of a *finite linear finitely terminating* system with undecidable theory of one step rewriting. Until now it was an open problem as to whether such systems exist. All systems with undecidable theories of one step rewriting known so far were *diverging* [2,3], where self-reducibility of terms was used in an essential way to detect properties of terms. At RTA'96 H. Ganzinger asked whether finite termination is indispensable for undecidability. The answer appears to be negative. Obtaining linearity does not represent any substantial difficulty, so the system we construct is *simultaneously linear and finitely terminating.*

2 Reduction

We will show that *dyadic words* and the *dyadic word concatenation* (i.e., concatenation of words in a two-letter alphabet) can be represented by means of formulas of $\mathcal{L}$ for an appropriate system R with desirable properties. The undecidability of the theory of one step rewriting in R then follows by the well-known

Theorem 1 (Quine, [1]). *The first-order theory of dyadic concatenation is undecidable.* □

We employ the same reduction as in [3]. However, to detect properties of terms by means of a one step reducibility relation in a linear finitely terminating system we use a different approach based on rewriting diagrams. Very schematically the idea may be described as follows. Suppose, we need to determine whether the first and the second subterms of a term $f(s,t)$ are equal by using the one step rewriting relation in a linear finitely terminating system. We can construct the following system, where g is an auxiliary ternary function symbol and c_1, c_2, c_3 are auxiliary constants: $f(x,y) \to g(x,y,c_1)$, $f(x,y) \to g(x,y,c_2)$, $g(x,y,c_1) \to g(x,y,c_2)$, $g(x,y,c_1) \to g(x,y,c_3)$, $g(x,y,c_2) \to g(y,x,c_3)$. Now the first and second subterms in $f(s,t)$ (without internal occurrences of f) are equal if and only if $f(s,t)$ satisfies the formula $\Phi(u) \equiv \forall v \exists w, z (R(u,v) \Rightarrow R(u,w) \wedge (R(v,w) \vee R(w,v)) \wedge R(v,z) \wedge R(w,z))$, where R is the one step reducibility relation in the above system. We thus distinguish the needed property by a "diamond-like" rewrite diagram. We use the other "fan-like" diagrams of the form $\Psi_n(u) \equiv \exists x_1, \ldots, x_n (\bigwedge_{i=1}^{n} R(u,x_i) \wedge \bigwedge_{i=1}^{n-1} R(x_i,x_{i+1}))$ to distinguish other needed properties of terms by means of the one step rewriting relation in a linear finitely terminating system.

3 Signature

We will use the following signature Σ of function symbols:

1. ε, a constant to denote the empty word and the empty list;
2. $a()$, $b()$, both unary to represent the letters A and B;
3. $c(,)$, binary for the list constructor *cons*;
4. $\langle ,, \rangle$, ternary constructor for triples;
5. $0()$, $1()$, $2()$, $3()$, $E()$, all unary auxiliary symbols.

4 Representing Words

Let us represent words over the dyadic (binary) alphabet $\{A, B\}$ as terms of signature $\{a, b, \varepsilon\}$, where a, b are unary function symbols and ε is a constant as follows:

- ε represents the empty word;
- if a term t represents a word α then the term $a(t)$ represents the word $A\alpha$ and the term $b(t)$ represents the word $B\alpha$.

From now on for brevity we will often call terms built of a, b, ε *words.*

5 Concatenation

Let terms s and t represent words α and β respectively. Then the term $s[t/\varepsilon]$, i.e., s with its unique occurrence of ε replaced with t, represents the concatenation of the words α and β.

6 Concatenation Witnesses

We need to express the fact that for terms r, s, t representing words, the concatenation of r and s equals t. This can be done as follows. To check whether $rs = t$ we start with r, s, t and stepwise erase equal symbols in the beginning of r and t. The equality $rs = t$ holds iff we arrive at ε, s, s. This leads to the following

Definition 2 (Concatenation Witnesses). Call a term

$$\begin{array}{l} \mathit{0(c(}\langle x_1, y_1, z_1\rangle, \\ \quad c(\langle x_2, y_2, z_2\rangle, \\ \quad\; c(\langle x_3, y_3, z_3\rangle, \\ \qquad \dots \\ \qquad c(\langle x_{n-1}, y_{n-1}, z_{n-1}\rangle, \\ \qquad\; c(\langle x_n, y_n, z_n\rangle, \varepsilon) \\ \qquad)\dots)))), \end{array} \tag{1}$$

representing a sequence of triples $\langle x_1, y_1, z_1\rangle, \dots, \langle x_n, y_n, z_n\rangle$, a *witness of concatenation* of r, s, t if and only if

- x_i, y_i, z_i (for $i = 1, \dots, n$) are terms built of ε, a, and b (i.e., words);
- $x_1 \equiv r$, $z_1 \equiv t$, and $y_i \equiv s$ for $i = 1, \dots, n$;
- $x_n \equiv \varepsilon$; (2)
- $y_n \equiv z_n$; (3)
- for all $i = 1, \dots, n-1$
  - either $x_i \equiv a(x_{i+1})$ and $z_i \equiv a(z_{i+1})$, (4)
  - or $x_i \equiv b(x_{i+1})$ and $z_i \equiv b(z_{i+1})$. (5)

Remark 3. The outermost 0() the added for technical reasons, which will become clear shortly. □

Obviously, we have the following simple

Proposition 4. *The concatenation of words α, β equals γ if and only if for the terms r, s, t representing α, β, γ there exists a (unique) witness of concatenation of r, s, t.* □

7 Convention on Rewriting Sequences

We represent a sequence of $n \geq 1$ elements

$$e_1, e_2 \dots, e_{n-1}, e_n$$

as a term

$$0(c(e_1, c(e_2, \dots, c(e_{n-1}, c(e_n, \varepsilon)) \dots))).$$

In the sequel to simplify notation and readability we will operate with rewrite rules over sequences, like

$$\langle x, y, z\rangle, \langle u, v, w\rangle \;\rightarrow\; \langle u, v, w\rangle, x, y, \langle x, y, z\rangle$$

keeping in mind that this is just a syntactically sugared version of otherwise non-understandable and bulky

$$c(\langle x, y, z\rangle, c(\langle u, v, w\rangle, x') \;\rightarrow\; c(\langle u, v, w\rangle, c(x, c(y, c(\langle x, y, z\rangle, x')))),$$

(where x' is a fresh variable).

Similarly, by writing

$$\langle x, y, z\rangle, \varepsilon \rightarrow \; \langle z, y, x\rangle, x, y, \varepsilon$$

we will mean the rule

$$c(\langle x, y, z\rangle, \varepsilon) \;\rightarrow\; c(\langle z, y, x\rangle, c(x, c(y, \varepsilon))),$$

which applies to the *last* element of a sequence.

8 Plan of the Proof

We will write the needed formula $Conc(x, y, z)$, which expresses the fact that the concatenation of words represented by x, y equals the word represented by z, in the following form:

$$Conc(x, y, z) \;\equiv_{df}\; \exists w \Big(C(w) \wedge P(x, y, z, w) \wedge W(w) \Big), \tag{6}$$

where:

1. $\exists w$ expresses "there exists a (candidate for) concatenation witness...",
2. $C(w)$ expresses that w is "correct", e.g., does not contain senseless subterms like $c(c(x, y, z), u)$ or $a(c(x, y, z))$, etc.; it guarantees that w satisfies conditions of Definition 2, except equality conditions (3) — (5);
   (See Section 10, Definition 9.)
3. $P(x, y, z, w)$ says that w is of the form $0(c(\langle x, y, z\rangle, w')$, i.e., w starts with the triple $\langle x, y, z\rangle$ (we need to say that w is a concatenation witness for x, y, and z);
   (See Section 18, Definition 19.)
4. $W(w)$ guarantees that w satisfies the equality conditions (3) — (5) from Definition 2.
   (See Section 17, Definition 14.)

Thus the formula (6) is going to express concatenation by means of existence of a concatenation witness, as specified by Definition 2.

It does not matter which part of $Conc$ to describe first. Let us start with the correctness formula $C(w)$ and then proceed to the most interesting part $W(w)$ in Sections 13 — 17 and to the subformula $P(x, y, z, w)$ in Section 18.

9 Correct and Senseless Terms

First we define correct terms with the aim to write the formula $C(w)$ in (6). It is easier to define correct terms as terms that are not senseless. So, we start by specifying senseless terms.

Definition 5 (Senseless Terms). A term of signature Σ is called *senseless* if and only if it contains a subterm of one of the following forms:

1. (a) $s(f(\ldots))$
   for $s \in \{a, b\}$ and $f \in \Sigma \backslash \{a, b, \varepsilon\}$;
   - (Reason: terms constructed with a, b are words, and cannot contain subterms starting with something except a, b, ε.)
2. (a) $\langle f(\ldots), u, v\rangle$,
   (b) $\langle u, f(\ldots), v\rangle$,
   (c) $\langle u, v, f(\ldots)\rangle$
   for some $f \in \Sigma \backslash \{a, b, \varepsilon\}$;
   - (Reason: the only meaningful function symbols in the argument positions to the triple constructor $\langle , , \rangle$ are a, b, ε, cf., Definition 2.)
3. (a) $c(f(\ldots), t)$
   for some $f \in \Sigma \backslash \{\langle , , \rangle\}$;
   (b) $c(t, f(\ldots))$
   for some $f \in \Sigma \backslash \{c, \varepsilon\}$;
   - (Reason: we only accept right-flattened sequences of triples as witnesses, cf., (1) of Definition 2.)
4. (a) $c(\langle s(x), y, z\rangle, \varepsilon)$
   for $s \in \{a, b\}$;
   - (Reason: a term containing $c(\langle s(x), y, z\rangle, \varepsilon)$ cannot be a witness, because a witness should necessarily end with $c(\langle \varepsilon, y, z\rangle, \varepsilon)$.)
5. (a) $c(\langle s(x), y, \varepsilon\rangle, v)$
   for $s \in \{a, b\}$;
   - (Reason: the triple $\langle a(x), y, \varepsilon\rangle$ cannot occur in a witness, cf., (4), (5) of Definition 2.)
6. (a) $c(\langle a(x), y, b(z)\rangle, v)$,
   (b) $c(\langle b(x), y, a(z)\rangle, v)$;
   - (Reason: the triple $\langle a(x), y, b(z)\rangle$ cannot occur in a witness, cf., (4), (5) of Definition 2.)
7. (a) $f(0(x))$
   for some auxiliary $f \in \{0, 1, 2, 3, E\}$;
   (b) $0(f(\ldots))$
   for some $f \in \Sigma \backslash \{c\}$.
   - (Reason: we would not like accept terms with something except $0(c(\ldots))$ in head position; cf., Definition 2.)

A term of signature Σ is called *correct* if and only if it is not senseless. $\square$

A useful property of non-senseless (=correct) terms is that almost certainly they have structure very close to the structure of witnesses (see Definition 2):

Lemma 6. *A non-senseless (correct) term t*

1. *either does not contain occurrences of the function symbol* $0()$ *(hence, does not contain* 0*, hence cannot satisfy the predicate* $P(x,y,z,w)$ *for any* x*,* y*,* z*,* w*, see below Section 18),*
2. *or has the form*

$$
\begin{array}{l}
0(\mathrm{c}(\langle x_1, y_1, z_1\rangle, \\
\quad \mathrm{c}(\langle x_2, y_2, z_2\rangle, \\
\quad\; \mathrm{c}(\langle x_3, y_3, z_3\rangle, \\
\qquad \ldots \\
\qquad \mathrm{c}(\langle x_{n-1}, y_{n-1}, z_{n-1}\rangle, \\
\qquad\; \mathrm{c}(\langle \varepsilon, y_n, z_n\rangle, \varepsilon) \\
\qquad)\ldots)))),
\end{array}
\tag{7}
$$

where:

- x_i*,* y_i*,* z_i *(for* $i = 1, \ldots, n$*) are terms built of* ε*,* a*, and* b *(words);*
- x_i *and* z_i *(for* $i = 1, \ldots, n-1$*) start with the same symbol* $s \in \{a, b\}$*.*

Proof. If a non-senseless term contains an occurrence of 0, then this occurrence should be the head one, by clauses 7a 7b of Definition 5. Afterwards it suffices to argue by induction on the structure of a term by applying the clauses of Definition 5. □

Remark 7. Notice that a correct term satisfying the second alternative of Lemma 6 satisfies almost all requirements of Definition 2, with the exception of (3), (4) and (5). □

We will construct the rewrite rules allowing for defining the predicate "to be a senseless term" by a formula of the language $\mathcal{L}$ containing the only binary predicate symbol R (see Section 1). Then negating this formula we will get the subformula $C(w)$ of (6).

10 Error Detecting Rules (Determining Senselessness)

Now we introduce error detecting rules, which allow us to determine senseless terms, as specified in Definition 5. These rules will reduce senseless terms in a specific way by creating distinguished rewrite diagrams, impossible for correct terms. This will permit us to write the needed subformula $C(w)$ of (6) by using the only binary predicate R for the one step reducibility relation in our system.

We are going to introduce the rules like $a(c(x,y)) \rightarrow E^i(\varepsilon)$, where x, y are variables, $i = 1, \ldots, 6$, $E^1(t) = E(t)$, and $E^{i+1}(t) = E(E^i(t))$, for each of the cases enumerated in Definition 5 of senseless terms. We also need the auxiliary rule $E(E(x)) \rightarrow E(x)$.

Our intention with these rules is as follows. If a term t contains a senseless subterm of the form $a(c(u,t))$, it can be reduced by the 6 rules with E^i on the right to six different terms $t_1, \ldots, t_6$, with that property that t_{i+1} reduces to t_i by the rule $E(E(x)) \rightarrow E(x)$. Thus a senseless term t satisfies the formula

$$\exists x_1, \ldots, x_6 \Big(\bigwedge_{i=1}^{6} R(t, x_i) \wedge \bigwedge_{i=1}^{5} R(x_{i+1}, x_i) \Big),$$

whereas no correct (non-senseless) term can satisfy the same property.

Definition 8 (Error Detecting Rules). We define the error detecting rules in 1-1-correspondence to the clauses of Definition 5 of senseless terms. In the rules below $i = 1, \ldots, 6$, and the ellipses $\ldots$ should be replaced by the lists of fresh variables of appropriate lengths.

1. (a) $s(f(\ldots)) \rightarrow E^i(\varepsilon)$ (8)
   for all $s \in \{a, b\}$, $f \in \Sigma \backslash \{a, b, \varepsilon\}$;
2. (a) $\langle f(\ldots), u, v \rangle \rightarrow E^i(\varepsilon)$, (9)
   (b) $\langle u, f(\ldots), v \rangle \rightarrow E^i(\varepsilon)$, (10)
   (c) $\langle u, v, f(\ldots) \rangle \rightarrow E^i(\varepsilon)$ (11)
   for all $f \in \Sigma \backslash \{a, b, \varepsilon\}$;
3. (a) $c(f(\ldots), x) \rightarrow E^i(f(\ldots))$ (12)
   for all $f \in \Sigma \backslash \{\langle,,\rangle\}$;
   (b) $c(x, f(\ldots)) \rightarrow E^i(f(\ldots))$ (13)
   for all $f \in \Sigma \backslash \{c, \varepsilon\}$;
4. (a) $c(\langle s(x), y, z \rangle, \varepsilon) \rightarrow E^i(\varepsilon)$ (14)
   for all $s \in \{a, b\}$;
5. (a) $c(\langle s(x), y, \varepsilon \rangle, v) \rightarrow E^i(\varepsilon)$ (15)
   for all $s \in \{a, b\}$;
6. (a) $c(\langle a(x), y, b(z) \rangle, v) \rightarrow E^i(\varepsilon)$, (16)
   (b) $c(\langle b(x), y, a(z) \rangle, v) \rightarrow E^i(\varepsilon)$; (17)
7. (a) $f(0(x)) \rightarrow E^i(\varepsilon)$ (18)
   for all auxiliary $f \in \{0, 1, 2, 3, E\}$;
   (b) $0(f(\ldots)) \rightarrow E^i(\varepsilon)$ (19)
   for all $f \in \Sigma \backslash \{c\}$;

We finally add the auxiliary rule

$$E(E(x)) \rightarrow E(x). \qquad (20)$$

11 Expressing Subformula $C(w)$ of (6)

We have everything necessary to write the correctness subformula $C(w)$ of (6):

Definition 9 (Subformula $C(w)$ of (6)). Define the formula

$$SENSELESS(w) \ \equiv_{df} \ \exists x_{1,2,3,4,5,6} \Big(\bigwedge_{i=1}^{6} R(w, x_i) \wedge \bigwedge_{i=1}^{5} R(x_{i+1}, x_i) \Big), \qquad (21)$$

and the subformula $C(w)$ of (6) by

$$C(w) \ \equiv_{df} \ \neg SENSELESS(w). \qquad (22)$$

Lemma 10 (Adequacy of $C(w)$). *A ground term t of signature Σ satisfies the formula $SENSELESS(t)$ if and only if t is senseless according to Definition 5. Equivalently, a ground term t of signature Σ is correct (non-senseless) if and only if it satisfies the formula $C(t)$.*

Proof. If a term is senseless according to Definition 5, then by construction of erroneous rules and the definition of the formula $SENSELESS$ in (21), the term t should satisfy $SENSELESS(t)$. Conversely, if a term t is correct then the erroneous rules do not apply, and t satisfies $C(t)$. $\square$

12 Further Rules

We will now introduce three groups of rules that will allow us, assuming that a candidate for concatenation witness w is correct (i.e., satisfies $C(w)$) to check the following:

1. Main Rules I – to check conditions (4) and (5) of Definition 2.
2. Main Rules II – to check condition (3) of Definition 2.
3. Parameter Rules – to check that w is of the form $0(c(\langle x, y, z\rangle))$.

The way we introduce these rules is motivated by the desire to maintain the following properties summarized in Lemma 11. These properties are essential for the correctness of representation of binary concatenation and also for keeping the rules of different groups non-interacting. This is crucial as soon as we would like to make the validity of Lemma 10 (and other properties in the sequel) insensitive to adding new rules.

Lemma 11 (Crucial Lemma). *For a correct term t:*

1. *if $s \to t_1$ and $s \to t_2$ by rules of the same group at different occurrences, then neither $t_1 \to t_2$, nor $t_2 \to t_1$.*

2. if $s \to t_1$ and $s \to t_2$ by rules of different groups, then neither $t_1 \to t_2$, nor $t_2 \to t_1$.

The proof that these properties hold are guaranteed by the construction of rules below and are easily checked simultaneously with the rules introduction. In each case the reader is invited to make a stop a get convinced that the rules are introduced in a way to keep Lemma 11 valid.

13 Main Rules I

Assume that the subformulas $C(w)$ and $P(x, y, z, w)$ of (6) guarantee that w is as specified by the second clause of Lemma 6. The subformula $C(w)$ alone cannot distinguish between the alternatives of Lemma 6, but together with $P(x, y, z, w)$, see Section 18, they do the job.

Suppose we are given a term as in the second clause of Lemma 6. Such a term "almost" satisfies all the conditions of the Definition 2, except for the conditions (3) (equality in the last element in the sequence) and (4), (5) on adjacent triples.

Our aim is to invent linear and finitely terminating rewrite system that would allow us to write the test $W(w)$ of conditions (4) and (5) as a formula with the only predicate R for the one step rewrite relation in this system.

Let s be either a or b. Consider the following 10 rules (we align corresponding arguments to improve readability):

$$\langle s(x), y, s(z)\rangle, \quad \langle x', y', z'\rangle \to \langle x, y, s(z)\rangle, s(\varepsilon), \ \varepsilon, \ \langle x', y', z'\rangle \tag{23}$$
$$\langle s(x), y, s(z)\rangle, \quad \langle x', y', z'\rangle \to \langle s(x), y, z\rangle, \ \varepsilon, \ s(\varepsilon), \langle x', y', z'\rangle \tag{24}$$

$$\langle x, y, s(z)\rangle, \ s(\varepsilon), \ \varepsilon, \ \langle x', y', z'\rangle \to \langle s(x), y, z\rangle, \ \varepsilon, \ s(\varepsilon), \langle x', y', z'\rangle \tag{25}$$

$$\langle x, y, s(z)\rangle, \ s(\varepsilon), \ \varepsilon, \ \langle x', y', z'\rangle \to \langle x, y, z\rangle, \ s(\varepsilon), s(\varepsilon), \langle x', y', z'\rangle \tag{26}$$
$$\langle s(x), y, z\rangle, \ \varepsilon, \ s(\varepsilon), \langle x', y', z'\rangle \to \langle x', y', z'\rangle, \ s(\varepsilon), s(\varepsilon), \ \langle x, y, z\rangle \tag{27}$$

Notice the "swapping trick" in the last rule. Finite termination of this group of rules is obvious, see also Section 19.

14 Rewrite Diagram I

The above rules give the following rewriting diagram (which simplifies their understanding):

$$\begin{array}{ccc}
 & \langle s(x), y, s(z)\rangle, \langle x', y', z'\rangle & \\
 \swarrow & & \searrow \\
\langle x, y, s(z)\rangle, \ s(\varepsilon), \ \varepsilon, \ \langle x', y', z'\rangle & \to & \langle s(x), y, z\rangle, \ \varepsilon, \ s(\varepsilon), \ \langle x', y', z'\rangle \quad (28) \\
\downarrow & & \downarrow \\
\langle x, y, z\rangle, \ s(\varepsilon), \ s(\varepsilon), \ \langle x', y', z'\rangle & & \langle x', y', z'\rangle, \ s(\varepsilon), \ s(\varepsilon), \ \langle x, y, z\rangle \quad (29)
\end{array}$$

Notice the following simple but useful property we will extensively exploit:

Proposition 12. *Two terms in the last line* coincide *if and only if* $x = x', y = y'$*, and* $z = z'$*.* □

Notice that the rules (23), (24) applied to a correct term at the same occurrences yield incorrect terms t_1, t_2 such that $t_1 \to t_2$. It is easy to check that the reduction of t_1, t_2 to the *same term* by erroneous rules (12), (13) is *impossible* by the construction of the right-hand sides of these rules (where we retained $f(\ldots)$). The reduction of t_1, t_2 to the *same term* is only possible by the rules (26), (27), provided that $x = x', y = y'$, and $z = z'$.

15 Main Rules II

5 rules similar to (23)–(27) should be added to check that the last element of the witness candidate sequence is a triple of the form $\langle \varepsilon, z, z \rangle$ with equal second and third elements (condition (3) of Definition 2):

$$\begin{array}{lcll}
\langle \varepsilon, y, z \rangle, \quad \varepsilon & \to & \langle \varepsilon, y, z \rangle, a(\varepsilon), \ \varepsilon, \ \varepsilon & (30) \\
\langle \varepsilon, y, z \rangle, \quad \varepsilon & \to & \langle \varepsilon, y, z \rangle, b(\varepsilon), \ \varepsilon, \ \varepsilon & (31) \\
& & & \\
\langle \varepsilon, y, z \rangle, a(\varepsilon), \varepsilon, \varepsilon & \to & \langle \varepsilon, y, z \rangle, b(\varepsilon), \ \varepsilon, \ \varepsilon & (32) \\
& & & \\
\langle \varepsilon, y, z \rangle, a(\varepsilon), \varepsilon, \varepsilon & \to & \langle \varepsilon, y, z \rangle, a(\varepsilon), a(\varepsilon), \varepsilon & (33) \\
\langle \varepsilon, y, z \rangle, b(\varepsilon), \varepsilon, \varepsilon & \to & \langle \varepsilon, z, y \rangle, a(\varepsilon), a(\varepsilon), \varepsilon & (34)
\end{array}$$

Again, notice the "swapping" in the last rule. Appropriate terms $a(\varepsilon)$, $b(\varepsilon)$ are added to guarantee finite termination, and to avoid rewriting of the right-hand sides of (30), (31) to the same term by erroneous rules (12), (13).

16 Rewrite Diagram II

Similarly, the above rules (30)–(34) give the following rewrite diagram:

$$\begin{array}{ccccl}
 & & \langle \varepsilon, y, z \rangle, \ \varepsilon & & \\
 & \swarrow & & \searrow & \\
\langle \varepsilon, y, z \rangle, a(\varepsilon), \ \varepsilon, \ \varepsilon & & \longrightarrow & \langle \varepsilon, y, z \rangle, b(\varepsilon), \ \varepsilon, \ \varepsilon & (35) \\
\downarrow & & & \downarrow & \\
\langle \varepsilon, y, z \rangle, a(\varepsilon), a(\varepsilon), \ \varepsilon & & & \langle \varepsilon, z, y \rangle, a(\varepsilon), a(\varepsilon), \varepsilon & (36)
\end{array}$$

Again notice the following simple but useful

Proposition 13. *Two terms in the last line* coincide *if and only if* $y = z$*.* □

17 Expressing the $W(w)$ Subformula of (6)

Definition 14 (Subformula $W(w)$ of (6)). Define the formula $W(w)$ as:

$$W(w) \equiv_{df} \forall w_1 \Big(R(w, w_1) \Rightarrow \exists w_2, w_3 \Big[R(w, w_2) \wedge (R(w_1, w_2) \vee R(w_2, w_1)) \wedge R(w_1, w_3) \wedge R(w_2, w_3) \Big] \Big)$$

(where R is the binary predicate symbol of the language $\mathcal{L}$ interpreted as a one step rewriting relation in the system we construct.) □

Propositions 12 and 13 imply that $W(w)$ so defined satisfies the following crucial property:

Proposition 15. *If w is a witness then the formula $W(w)$ is true.*

If w satisfies $C(w)$, has form $0(c(\langle s, t, u \rangle, \ldots)$, and satisfies $W(w)$, then w is a witness of concatenation of s, t, u.

Proof. By inspection. w_1 and w_2 correspond in some order to terms in (28) (or (35)), w_3 corresponds to (equal) terms in (29) (or (36)). Here it is important to notice that whenever w satisfies the premises of the second claim, every subterm of w of the form $c(s, t)$ is reducible by one of the main rules (23), (24), (30), (31), so the premise of $W(w)$ is always true; hence the conclusion is also true guaranteeing the equality constraints (3) — (5). □

Remark 16. Notice that the second claim of Proposition 15 depends on correctness of w expressed by $C(w)$ occurring conjunctively in (6) and also on the form $0(c(\langle \ldots \rangle, \ldots))$ of w, guaranteed by $P(x, y, z, w)$ (see Section 18), also occurring conjunctively in (6).

18 Arguments: the $P(x, y, z, w)$ Subformula of (6)

We must express that w is a witness of concatenation of words x, y, z, i.e., starts with the triple $\langle x, y, z \rangle$, i.e., w has form $0(c(\langle x, y, z \rangle, w')$.

We will need the following auxiliary formulas describing fan-like rewrite diagrams.

Definition 17. For $n \geq 3$ define the formulas $Fan_n(u, u_n)$ as follows:

$$Fan_n(u, u_n) \equiv_{df} \exists u_1 \ldots u_{n-1} \Big(\bigwedge_{i=1}^{n} R(u, u_i) \wedge \bigwedge_{i=1}^{n-1} R(u_i, u_{i+1}) \wedge$$

$$\wedge \neg \exists u_0 (R(u, u_0) \wedge R(u_0, u_1)) \wedge \neg \exists u_{n+1} (R(u, u_{n+1}) \wedge R(u_n, u_{n+1})) \Big).$$

Definition 18 (Argument Detecting Rules). Let us add the following rules to our system for $s \in \{a, b\}$ (note that the left-hand sides of the rules starting with 0 are prepared by the previous applications of the rules (23)–(27) and (30)–(34)):

$$\begin{array}{rcll} 0(c(\langle x,y,z\rangle, s(\varepsilon), s(\varepsilon), v) & \to & 1(1(x)) & (37) \\ 0(c(\langle x,y,z\rangle, s(\varepsilon), s(\varepsilon), v) & \to & 1(x) & (38) \\ 0(c(\langle x,y,z\rangle, s(\varepsilon), s(\varepsilon), v) & \to & x & (39) \\ 1(x) & \to & x & (40) \end{array}$$

(Notice that $Fan_3(0(c(\langle x,y,z\rangle, s(\varepsilon), s(\varepsilon), v), x)$ is true, provided x is irreducible. Neither Fan_4, nor Fan_5 is true for the same arguments.)

$$\begin{array}{rcll} 0(c(\langle x,y,z\rangle, s(\varepsilon), s(\varepsilon), v) & \to & 2(2(2(y))) & (41) \\ 0(c(\langle x,y,z\rangle, s(\varepsilon), s(\varepsilon), v) & \to & 2(2(y)) & (42) \\ 0(c(\langle x,y,z\rangle, s(\varepsilon), s(\varepsilon), v) & \to & 2(y) & (43) \\ 0(c(\langle x,y,z\rangle, s(\varepsilon), s(\varepsilon), v) & \to & y & (44) \\ 2(y) & \to & y & (45) \end{array}$$

(Notice that $Fan_4(0(c(\langle x,y,z\rangle, s(\varepsilon), s(\varepsilon), v), y)$ is true, provided y is irreducible. Neither Fan_3, nor Fan_5 is true for the same arguments.)

$$\begin{array}{rcll} 0(c(\langle x,y,z\rangle, s(\varepsilon), s(\varepsilon), v) & \to & 3(3(3(3(z)))) & (46) \\ 0(c(\langle x,y,z\rangle, s(\varepsilon), s(\varepsilon), v) & \to & 3(3(3(z))) & (47) \\ 0(c(\langle x,y,z\rangle, s(\varepsilon), s(\varepsilon), v) & \to & 3(3(z)) & (48) \\ 0(c(\langle x,y,z\rangle, s(\varepsilon), s(\varepsilon), v) & \to & 3(z) & (49) \\ 0(c(\langle x,y,z\rangle, s(\varepsilon), s(\varepsilon), v) & \to & z & (50) \\ 3(z) & \to & z & (51) \end{array}$$

(Notice that $Fan_5(0(c(\langle x,y,z\rangle, s(\varepsilon), s(\varepsilon), v), z)$ is true provided y is irreducible. Neither Fan_3, nor Fan_4 is true for the same arguments.) □

Now the technical role of the leading 0 in (1) becomes completely clear. The rules (37)–(51) starting with 0 may apply only in a topmost position. We exclude 0 in the internal positions considering them incorrect, see Definition 5. Notice that the rules (37)–(51) cannot apply to a correct term if it does not contain 0 (in the head position). Moreover, these rules are applicable only after the full normalization by the main rules (23)–(27) and (30)–(34).

We are now ready to define the subformula $P(x, y, z, w)$ of (6).

Definition 19 (Subformula $P(x,y,z,w)$ of (6)). Define the formula $P(x,y,z,w)$ as follows:

$$\begin{array}{ll} P\ (x,y,z,w) & \equiv_{df} \\ \exists w_1, w_2, w_3 & \Big(R(w,w_1) \wedge R(w,w_2) \wedge \\ & (R(w_1,w_2) \vee R(w_2,w_1)) \wedge R(w_1,w_3) \wedge R(w_2,w_3) \wedge \\ & Fan_3(w_3,x) \wedge Fan_4(w_3,y) \wedge Fan_5(w_3,z)\Big). \end{array}$$

(where R is the binary predicate symbol of the language $\mathcal{L}$ interpreted as a one step rewriting relation in the system we construct.) □

As a result we have the following simple

Proposition 20. *A correct term w equals $0(c(\langle x,y,z\rangle,r))$ (for some term r) if and only if $P(x,y,z,w)$ is true.*

Proof. By inspection. □

Notice that if a correct term does not start with 0, the above formula cannot be true, because fans may result only by applications of (37)–(51).

19 Finite Termination

Definition 21 (Weights). A subterm occurrence in a term of signature Σ is assigned (below ... stand for sequences of terms of appropriate length):

- weight 4 if it has form
  - $c(\langle\ldots\rangle, c(\langle\ldots\rangle,\ldots))$ or
  - $c(\langle\ldots\rangle,\varepsilon)$;
- weight 3 if it has form
  - $c(\langle\ldots\rangle, c(s(\varepsilon), c(\varepsilon, c(\langle\ldots\rangle,\ldots))))$ (for $s \in \{a,b\}$) or
  - $c(\langle\ldots\rangle, c(a(\varepsilon), c(\varepsilon,\varepsilon)))$;
- weight 2 if it has form
  - $c(\langle\ldots\rangle, c(\varepsilon, c(s(\varepsilon), c(\langle\ldots\rangle,\ldots))))$ (for $s \in \{a,b\}$) or
  - $c(\langle\ldots\rangle, c(b(\varepsilon), c(\varepsilon,\varepsilon)))$;
- weight 1 if it has form
  - $c(\langle\ldots\rangle, c(s(\varepsilon), c(s(\varepsilon), c(\langle\ldots\rangle,\ldots))))$ (for $s \in \{a,b\}$) or
  - $c(\langle\ldots\rangle, c(a(\varepsilon), c(a(\varepsilon),\varepsilon)))$;
- weight 0 otherwise.

The *weight of a term* of signature Σ, denoted $weight(t)$, is the sum of weights of all occurrences of subterms in t. □

It is immediate to check that the following property holds:

Proposition 22. *The main rules (23) — (27) and (30) — (34) decrease weights of terms.* □

The other rules may leave the weights unchanged. We need additional complexity measures.

Definition 23. For $\Sigma' \subseteq \Sigma$ the *Σ'-length* of a term t of signature Σ is the number of occurrences of symbols from Σ' in t. □

Proposition 24. *The parameter rules (37) — (51) and the error detecting rules (8) — (19) decrease $\Sigma \backslash \{E, \varepsilon\}$-lengths of terms.*

Proof. By inspection. □

The auxiliary error detecting rule (20) does not change neither weights, nor $\Sigma \backslash \{E, \varepsilon\}$-lengths. However, it decreases Σ-lengths. Thus, combining Propositions 22 — 24 we get the desired

Lemma 25 (Finite Termination). *Define the complexity measure of a term t of signature Σ as follows:*

$$|t| \;\equiv_{df}\; \langle weight(t),\ \Sigma \backslash \{E, \varepsilon\}\text{-}length(t),\ \Sigma\text{-}length(t) \rangle$$

The rewrite rule system consisting of rules (8) — (20), (23) — (27), (30) — (34), (37) — (51) decreases the complexity measure of terms of signature Σ with respect to the lexicographic ordering on ω^3, henceforth, is finitely terminating.

Proof. Straightforward from Propositions 22 — 24. The main rules (23) — (27) and (30) — (34) decrease weights of terms. The other rules, except (20), do not increase weights, but decrease $\Sigma \backslash \{E, \varepsilon\}$*-lengths*. The rule (20) leaves weights and $\Sigma \backslash \{E, \varepsilon\}$*-lengths* unchanged, but decreases Σ-lengths. □

20 Correctness

From the explanation we supplied for the rewrite rules introduced it is immediate that the following is true.

Proposition 26. *If w is a witness of concatenation of terms x, y, z then w, x, y, z satisfy the matrix $C(w) \wedge P(x, y, z, w) \wedge W(w)$ of (6). Henceforth, the formula $Conc(x, y, z)$ is true.* □

The converse requires some additional effort.

Lemma 27. *If the formula (6) is true for terms x, y, z of signature Σ then x, y, z represent words X, Y, Z, and the concatenation of X and Y equals Z.*

Proof. Suppose, the formula (6) is true for terms x, y, z of signature Σ. It means that there exists a term w of signature Σ such that the matrix $C(w) \wedge P(x, y, z, w) \wedge W(w)$ of (6) is true.

1. $C(w)$ is true means, by Definitions 9, that the error detecting rules (8) — (19) do not apply to w (still, the rule (20) $E(E(x)) \to E(x)$ may apply, but this will be excluded by the further analysis);
2. it follows that w does not contain senseless patterns enumerated in Definition 5;
3. $P(x, y, z, w)$ is true means, by Proposition 20, that w has form $0(c(\langle x, y, z\rangle, t))$; henceforth, satisfies the second clause of Lemma 6 (consequently, $E(E(x)) \to E(x)$ cannot apply to w);
4. finally, $W(w)$ is true for $w \equiv 0(c(\langle x, y, z\rangle, t))$ means that w satisfies the conditions (3), (4) and (5) of Definition 2;
5. henceforth, w is a witness of concatenation of x, y, z. □

21 Conclusion

The claim in the title of this note is thus a consequence to Theorem 1 due to Quine as follows. Consider the model $M = \langle T(\Sigma), \mathbf{R}\rangle$, where $T(\Sigma)$ is the Herbrand universe over Σ and $\mathbf{R} = \{\langle s, t\rangle \mid s, t \in T(\Sigma) \wedge s \to_R t\} \subseteq T(\Sigma) \times T(\Sigma)$ is the one step rewrite relation on $T(\Sigma)$ generated by the rewrite system R we introduced. The definable submodel of M consisting of elements m satisfying $\exists e Conc(e, m, m)$ with the predicate $Conc(,,)$ is isomorphic to the set of dyadic words with concatenation predicate, and thus Theorem 1 applies.

By a similar reduction from the Post correspondence problem or from the halting problem for two-register machines, and by using quantifiers more sparingly we can obtain a stronger

Theorem 28. *The $\exists\forall\exists$-theory of one step rewriting in a finite linear finitely terminating system is undecidable, in general.*

Proof. See [4]. □

Acknowledgments. Suggestions of Harald Ganzinger and anonymous referees helped to eliminate several errors and improve the presentation.

References

1. W. V. Quine. Concatenation as a basis for arithmetic. *J. Symb. Logic*, 11(4):105–114, 1946.
2. R. Treinen. The first-order theory of one step rewriting is undecidable. In *Rewriting Techniques and Applications'96*, Lect. Notes Comput. Sci., pages 276–285. Springer-Verlag, 1996.
3. S. Vorobyov. The elementary theory of one-step rewriting is undecidable (note). Unpublished draft, see `http://www.mpi-sb.mpg/~sv/`, Section "On Trees and Rewriting", 1995.
4. S. Vorobyov. ∃∀∃-theories of one step rewriting in linear noetherian systems are undecidable. Available at `http://www.mpi-sb.mpg.de/~sv`, November 1996.