THEORIES OF ORDERS ON THE SET OF WORDS

Dietrich Kuske

Abstract. It is shown that small fragments of the first-order theory of the subword order, the (partial) lexicographic path ordering on words, the homomorphism preorder, and the infix order are undecidable. This is in contrast to the decidability of the monadic second-order theory of the prefix order [M.O. Rabin, Trans. Amer. Math. Soc., 1969] and of the theory of the total lexicographic path ordering [P. Narendran and M. Rusinowitch, Lect. Notes Artificial Intelligence, 2000] and, in case of the subword and the lexicographic path order, improves upon a result by Comon & Treinen [H. Comon and R. Treinen, Lect. Notes Comp. Sci., 1994]. Our proofs rely on the undecidability of the positive \( \Sigma^1_1 \)-theory of \((\mathbb{N},+,\cdot)\) [Y. Matiyasevich, Hilbert’s Tenth Problem, 1993] and on Treinen’s technique [R. Treinen, J. Symbolic Comput., 1992] that allows to reduce Post’s correspondence problem to logical theories.

Mathematics Subject Classification. 03D35.

1. Introduction

Depending on the context, the set of words carries different interesting partial orders. Seen as a free monoid, the divisor or infix relation is most natural; seen as nodes of the complete \(n\)-ary tree, one looks at the predecessor relation of the tree which coincides with the prefix relation. In combinatorics and the theory of well quasi orders, the subword order is central. In some cases, this order coincides with the lexicographic path ordering that is of utmost importance in string rewriting. The homomorphism order is closely related to the order of \(k\)-partitions over \(NP\).

By Rabin’s Theorem [23], the theory of the prefix order \((\Sigma^*,\leq)\) is decidable (this holds even for the monadic second order theory). Comon & Treinen [6] and Narendran & Rusinowitch [22] considered structures \((\Sigma^*,(p_a)_{a\in\Sigma},\leq_{lpo})\) where \(p_a\) is a unary function that prefixes a word with the letter \(a\) and \(\leq_{lpo}\) is the lexicographic path ordering [9]. In case this order is total, the theory of this structure is

* These results were obtained while the author was affiliated with the Technische Universität Dresden.

1 Universität Leipzig, Germany; kuske@informatik.uni-leipzig.de © EDP Sciences 2005
decidable [22]; the $\Sigma_4$-fragment is undecidable if the order is partial [6]. The latter undecidability holds for $(\Sigma^*, (p_a)_{a \in \Sigma}, \leq)$ as well where $\leq$ is the subword relation [6]. Here, we are mainly interested in the order relation alone, i.e., in structures of the form $(\Sigma^*, \sqsubseteq)$ for some order relation $\sqsubseteq$. The existential theory turns out to be decidable in all cases since all finite partial orders can be embedded. For small alphabets, we show the full theory of the homomorphism preorder $(\Sigma^*, \preceq)$ to be decidable. Apart from these results, we prove the undecidability of small fragments of the theory of all the abovementioned partial orders for two-elements alphabets.

We start with the subword order $\imp$ where $u \imp v$ if $u$ results from $v$ by deleting some occurrences of letters. This relation has been studied extensively. It is a well order [15], the homotopy types of its intervals [11] and rational expressions for related Möbius-functions [2] have been calculated, it has been considered under counting aspects Chapter 6 of [19], in the context of Macaulay-posets [8,18] and of formal languages [14], and it can be used to show decidability results on “lossy channel systems” [12] and asynchronously cellular automata [17]. We reduce the positive $\Sigma_1$-fragment of arithmetic to the $\Sigma_3$-theory of the subword order $((a,b)^*, \imp)$ which proves the undecidability of this fragment (Th. 2.3).

In rewriting theory, it is desirable to orient a set of equations as a first step towards a terminating and confluent rewrite system. A typical example, where this is not possible, is the set of equations defining commutative groups: the commutativity law cannot be ordered in any way. A possible solution is to consider ordered rewriting: $s \cdot t$ is rewritten into $t \cdot s$ only in case $s < t$ for some order relation $\leq$. This can be extended by allowing more involved properties than $s < t$, e.g., arbitrary first-order formulas. To apply such a strategy in an automatic system, these properties have to be decidable. Refining the proof for the subword order, we show that the $\Sigma_2$-theory of $((a,b)^*, p_a, p_b, \leq_{lpo})$ is undecidable where $\leq_{lpo}$ is a partial lexicographic path ordering (Th. 3.5). This improves upon a result by Comon & Treinen [6] stating this result for the $\Sigma_4$-theory in case the alphabet contains at least three letters. For the pure ordered structure $((a,b)^*, \leq_{lpo})$, we obtain the undecidability of the $\Sigma_3$-theory.

In [16], Kosub & Wagner study the structure of $k$-partitions over NP. Generalizing the classes of the Boolean Hierarchy over NP, they define classes of $k$-partitions and investigate their order structure which turns out to be rather complicated in general. Any such class is given by a $\{1,2,\ldots,k\}$-labeled finite lattice. Their embedding conjecture states that the order on these classes is completely described by the homomorphism order between the defining labeled lattices. This conjecture is proved in some cases, in particular if the defining lattice is a chain, i.e., a word over an $k$-elements alphabet. Therefore, we turn attention to the “homomorphism preorder” on words: consider a word of length $n$ as a labeled linear order with $n$ elements (the labels come from the alphabet). Then $u \preceq v$ if there exists a homomorphism from the labeled linear order representing $u$ into the labeled linear order representing $v$. Equivalently, $u \preceq v$ if, after deleting repetitions in $u$, we obtain a subword of $v$. Interpreting the subword relation in the homomorphism preorder (of a larger alphabet), it follows that the $\Sigma_5$-theory of this preorder is
undecidable for alphabets with at least four elements (Th. 4.3); the full theory is
decidable for alphabets with at most two elements (cf. discussion after Th. 4.3).

Makanin [20] showed that the positive $\Sigma_1$-theory of the free monoid is decidable
(the extension to the full $\Sigma_1$-theory can be found in [5]). The positive $\Sigma_1$-theory of
the divisor or infix relation $\leq$ is easily reduced to the $\Sigma_1$-theory of the free monoid;
hence it is decidable as well. On the other hand, the positive $\Pi_2$-theory of $(\Sigma^*, \cdot)$
was shown to be undecidable by Durnev [10], but there is no obvious reduction
of this theory to the theory of the infix relation. To show the undecidability of
the $\Sigma_4$-theory of $(\Sigma^*, \leq)$ (cf. Th. 5.6), we use the ideas developed by Treinen in
[25]. There, he gives a general result stating that, provided formulas with certain
properties exist in a given theory, the underlying theory is undecidable. The point
is that the existence of these formulas allows to encode Post’s correspondence
problem in the theory. I decided not to start from his criteria, but to follow
his proof in the concrete setting of this particular partial order. The reasons
for this decision are two-fold: it should simplify the understanding since Post’s
correspondence problem is directly encoded into the theory, and it is not much
longer than showing that our formulas have the properties required by Treinen.

In the final section, we extend our focus to finite $\Sigma$-labeled forests. The analogon
of the subword relation is the embeddability: the forest $s$ is smaller than the forest
t if $s$ can be embedded into $t$. We show that this order relation has an undecidable
theory (Cor. 6.1).

I would like to thank Denis Lugiez for directing my attention to lexicographic
path orderings and pointing me to the results of Comon & Treinen, Ralf Treinen
for his pointer to Narendran & Rusinowitch’s work, and Victor Selivanov for his
continuous interest in the results to be reported in this article (although I could
not solve his original question).

Notation. Concerning first order logic, we only recall that $\Sigma_n$ stands for the set
of formulas that are logically equivalent to some formula in prenex normal form
with $n$ blocks of quantifiers (starting with a block of existential quantifiers); $\Pi_n$ is
the set of negations of formulas in $\Sigma_n$. By $B^\Sigma_n$, we denote the set of Boolean
combinations of formulas from $\Sigma_n$. The $\Sigma_n$-theory of a structure $S$ is the set of
sentences from $\Sigma_n$ that hold in $S$.

2. THE SUBWORD ORDER

For two words $u$ and $v$ over some alphabet $\Sigma$, we write $u \hookrightarrow v$ if $u$ is a subword
of $v$, i.e., if $u$ results from $v$ by deleting arbitrary many letters. Equivalently,
$u \hookrightarrow v$ if $u$ (seen as a $\Sigma$-labeled linear order) can be embedded into $v$.

**Theorem 2.1** (Comon & Treinen [6]). Let $a, b, \# \in \Sigma$ and let the function $p_\# : \Sigma^* \to \Sigma^*$ be defined by $w \mapsto \# w$. Then the $\Sigma_4$-theory of $S = (\Sigma^*, p_\#, \hookrightarrow, a, b)$ is
undecidable.

More precisely, Comon & Treinen show that the free monoid $(\{a, b\}^*, \cdot, a, b)$ can
be interpreted in $S$. All the formulas in this interpretation are at most $\Sigma_3$. Since
the positive $\forall^3\exists$-theory of the free monoid is undecidable [10], one obtains the
undecidability of the $\Sigma_4$-theory of $S$.

It is the aim of this section to sharpen the above result. In particular, we will
show that the $\Sigma_2$-theory of $(\Sigma^*, \hookrightarrow)$ (which is a reduct of Conom & Treinen’s
structure) is undecidable as soon as $\Sigma$ contains at least 2 elements.

But first, we prove that the existential theory of $(\Sigma^*, \hookrightarrow)$ is decidable.

**Proposition 2.2.** Let $\Sigma$ be some alphabet. Then the $\Sigma_4$-theory of $(\Sigma^*, \hookrightarrow)$ is
decidable.

**Proof.** Since $((\{a\})^*, \hookrightarrow) \cong (\mathbb{N}, \leq)$, this holds for $|\Sigma| = 1$. For larger alphabets,
your finite partial order can be embedded into $(\Sigma^*, \hookrightarrow)$: Let $\{p_1, p_2, \ldots, p_n\}, \leq$
be a finite partial order and choose $a, b, c \in \Sigma$ with $c \not\in \{a, b\}$ (in a later proof,
we will use that these three letters are mutually distinct). For $j = 1, 2, \ldots, n$, set
$w_j = abx_1abx_2abx_3 \ldots x_n$ with $x_i = c$ iff $p_i \leq p_j$, and $x_i = \varepsilon$ otherwise. For
any of the words $w_i$, the maximal subword from $\{a, b\}^*$ is $(ab)^n a$. Hence we get
$w_i \hookrightarrow w_j$ iff $w_i$ results from $w_j$ by the deletion of some occurrences of the letter $c$,
hence iff $p_i \leq p_j$. Hence the formula $\exists x_1 \exists x_2 \ldots \exists x_n : \psi$ where $\psi$ is quantifier-free
holds in $(\Sigma^*, \hookrightarrow)$ iff it holds in some finite partial order whose size can be restricted
to $n$. Since there are only finitely many such orders, the result follows. \hfill \Box

We now turn to the announced undecidability proof. Let $\Sigma = \{a, b\}$ and $M = (\Sigma^*, \hookrightarrow, \varepsilon, a, b, ab, ba, aa, bb, aba, bab)$. We will encode arithmetic by identifying a
natural number $n$ with the word $a^n$. Projections will be the main tool in this
section. E.g., the longest $a$-prefix of a word from $a^*ba^*$ is the projection to $a^*$
of its projection to $a^*b$. A word contains precisely $k$ occurrences of the letter $a$ iff
its projection to $a^*$ is $a^k$. Hence addition can be defined by “there is a word from
$a^*ba^*$ with longest $a$-prefix $a^m$ and longest $a$-suffix $a^n$ whose projection to $a^*$ is
$a^{m+n}$. To encode multiplication, we show that the binary relation “same length”
can be defined. This allows to define the word $b^m$ from $a^m$ and then, from $b^m$ and
$a^n$, the word $(ba^n)^m$. Its projection to $a^*$ is $a^{m+n}$.

First, we have to show that some auxiliary relations are definable in $M$. For a
word $w \in \Sigma^*$, let $\pi_a(w)$ denote the projection of $w$ to $a^*$, i.e., the largest element
of $a^*$ that embeds into $w$; $\pi_b(w)$ is defined similarly.

(S1) A word $w \in \Sigma^*$ belongs to $a^*$ iff it does not contain any occurrence of the
letter $b$, i.e., iff $b \not\hookrightarrow w$. Hence the sets $a^*$ and $b^*$ are $\Sigma_0$-definable in $M$.
(S2) $\pi_a(w)$ is the maximal word $u \in a^*$ embedding into $w$, i.e., $u = \pi_a(w)$ iff
$u \in a^* \land u \hookrightarrow w \land \forall x((u \hookrightarrow x \hookrightarrow w \land x \in a^*) \Rightarrow (u = x))$. Hence the set
of all pairs $(u, w) \in \Sigma^* \times \Sigma^*$ with $u = \pi_a(w)$ is $\Pi_1$-definable in $M$. The
projection to $b^*$ can be handled similarly.
(S3) Let $x = a^mba^n$ and $u \in a^*$. Then $u = a^m$ iff the following holds in $M$:

\[
\forall y, z \quad ((b \hookrightarrow y \hookrightarrow x \land ba \not\hookrightarrow y \land b \not\hookrightarrow z \hookrightarrow y) \Rightarrow (z \hookrightarrow u))
\]
\[\land \exists y \quad (b \hookrightarrow y \land ba \not\hookrightarrow y \land u \hookrightarrow y \hookrightarrow x).
\]

The condition in the first line expresses that $y \in a^*b^+$ is a subword of $x$
(and therefore contained in $a^*b$) and $z \in a^*$ is a subword of $y$. Hence (with
Theories of Orders on the Set of Words

57

\( x = a^m b a^n \), the length of \( z \) is bounded by \( m \). The conclusion says that \( u \) contains at least \( |z| \) occurrences of \( a \). Since \( z \) can take the value \( a^m \), we have that \( u \) is at least \( a^m \). The second line expresses that in particular \( y = ub \) is a subword of \( x \), i.e., that \( u \) contains at most \( m \) occurrences of \( a \). The formula above is \( B \Sigma_1 \).

Now we are in the position to show that \( S = \{(a^m, a^n, a^{m+n}) \mid m, n \in \mathbb{N} \} \) is definable: \( (u, v, w) \in S \) iff

\[
\exists x : \left( \begin{array}{c}
\frac{\ b \leftarrow x \land \neg(bb \leftarrow x) \land w = \pi_a(x)}{
\land u \in a^* \land v \in a^*}
\land u \text{ is the maximal } a^* \text{-prefix of } x
\land v \text{ is the maximal } a^* \text{-suffix of } x
\end{array} \right).
\]

The first three conjuncts state that \( x = a^m b a^n \) and \( w = a^{m+n} \) for some \( m, n \in \mathbb{N} \).

Together with the second line, \( x \) and \( u \) as well as \( x \) and \( v \) satisfy the assumption in (S3). Hence the third and fourth lines ensure \( u = a^m \) and \( v = a^n \) (which is \( B \Sigma_1 \)-expressible by (S3)). Thus, indeed, \( S \) is \( \Sigma_2 \)-definable.

We define some more auxiliary relations

(S4) A word \( w \in \Sigma^* \) belongs to \( \Sigma^* b \) iff

\[
\exists x (x \leftarrow w \land \forall y ((y \in a^* \land y \leftarrow w) \Rightarrow (y \leftarrow x)) \land b \leftarrow x \land ba \nrightarrow x).
\]

By the first conjunct, \( x \) results from \( w \) by deleting some letters. The second conjunct ensures that all occurrences of \( a \) are still present, i.e., that \( x \) results from \( w \) by deleting some occurrences of \( b \). The final two conjuncts express that the last letter of \( x \) is \( b \). Thus, indeed, this \( \Sigma_2 \)-formula holds iff \( w \in \Sigma^* b \). Similarly, the set \( a \Sigma^* \) is \( \Sigma_2 \)-definable.

(S5) \( w \in \Sigma^* \setminus (\Sigma^* b \Sigma^*) \) iff \( \forall u (bb, \pi_a(w) \leftarrow u \leftarrow w \Rightarrow bab \leftarrow u) \); the condition expresses that \( u \) results from \( w \) by deleting some occurrences of \( b \) and that at least two occurrences of \( b \) are left. The conclusion requires that these two occurrences of \( b \) are separated by some \( a \). To place this expression in \( \Sigma_2 \), we use the alternative formulation

\[
\exists x (x = \pi_a(w) \land \forall u (bb, x \leftarrow u \leftarrow w \Rightarrow bab \leftarrow u)).
\]

It is indeed \( \Sigma_2 \) since \( x = \pi_a(w) \) is expressible in \( \Pi_1 \) by (S2).

(S6) The set \( (ab)^+ = a \Sigma^* \cap \Sigma^* b \cap \Sigma^* \setminus (\Sigma^* a a \Sigma^* \cup \Sigma^* b b \Sigma^*) \) is \( \Sigma_2 \)-definable by (S4) and (S5). The same applies to \( (ab)^+ = (ab)^+ \cup \{ a \} \).

(S7) A pair of words \( (u, v) \) belongs to \( E = \{(a^n, b^n) \mid n \in \mathbb{N} \} \) iff there exists \( x \in (ab)^* \) with \( u = \pi_a(x) \) and \( v = \pi_b(x) \); hence \( E \) is \( \Sigma_2 \)-definable by (S2) and (S6).

(S8) Let \( u = b^m, v = a^n \) and \( z \in \Sigma^* \). Then \( z = a^{n_0} b a^{n_1} b a^{n_2} \ldots b a^{n_m} \) for some \( n_i \leq n \) iff

\[
\varphi_{(S8)}(z) \equiv (u = \pi_b(z) \land \forall x ((u \leftarrow x \leftarrow z \land aba \nrightarrow x) \Rightarrow (\pi_a(x) \leftarrow v))).
\]
The formula \( u = \pi_k(z) \) forces \( z \) to be of the form \( a^{n_0}b_{a^{n_1}}b_{a^{n_2}} \ldots b_{a^{n_m}} \) for some \( n_i \in \mathbb{N} \). Let \( x = b_{a^{n_i}}b_{a^{m-i}} \) with \( 0 \leq i \leq m \). Then the premise of the above implication is satisfied. The conclusion ensures \( a^{n_i} = \pi_a(x) \iff v = a^n \), i.e., \( n_i \leq n \). If, conversely, \( z \) is of the desired form and \( x \) satisfies the premise of the implication, then \( x = b_{a^k}b_{a^{m-i}} \) for some \( 0 \leq i \leq m \).

Since \( x \leftrightarrow z \), we get \( k \leq n_i \leq n \) and therefore \( \pi_a(x) \leftrightarrow v \). We can express \( \pi_a(x) \leftrightarrow v \) by the \( \Pi_1 \)-formula \( (\forall y (b_{a^k}y \leftrightarrow x \Rightarrow y \leftrightarrow v)) \). Note that it occurs in a positive position under the universal quantifier \( \forall x \), i.e., the second conjunct of the above formula is in \( \Pi_1 \). By (S2), the same applies to the first conjunct. Thus, the formula \( \varphi_{(S8)} \) is \( \Pi_1 \).

(S9) A triple of words \((u, v, w)\) belongs to the set \( \{(b_{a^m}, a^n, (ba)^m) \mid m, n \in \mathbb{N} \}\) iff \( u \in b^* \), \( v \in a^* \) and if \( w \) is the maximal element \( z \in b\Sigma^* \) satisfying the formula \( \varphi_{(S8)}(z) \) from (S8). This can be expressed as

\[
a \not\rightarrow u \wedge b \not\rightarrow v \wedge w \in b\Sigma^* \wedge \forall z ((z \in b\Sigma^* \wedge \varphi_{(S8)}(z)) \Rightarrow z \leftrightarrow w).
\]

The formula \( w \in b\Sigma^* \) is \( \Sigma_2 \) by (S4). The formula \( z \in b\Sigma^* \wedge \varphi_{(S8)}(z) \) is \( \Sigma_2 \) by (S4) and (S8). Since it occurs at a negative position under the universal quantification \( \forall z \), the last conjunct of the above formula is \( \Pi_2 \). Hence the whole formula above is \( B\Sigma_2 \).

Now we are in the position to show that \( P = \{a^m, a^n, a^{m-n} \mid m, n \in \mathbb{N} \} \) is definable as well: \((u, v, w) \in P \) iff

\[
\exists x, y : \left( (u, x) \in E \land (x, v, y) \in \{(b_{a^m}, a^n, (ba)^m) \mid m, n \in \mathbb{N} \} \land w = \pi_a(y) \right).
\]

The first conjunct under the existential quantifier states that \( u = a^m \) and \( x = b^m \) for some \( m \in \mathbb{N} \). By the second conjunct, \( v = a^n \) and \( y = (ba)^m \) for some \( n \in \mathbb{N} \). Hence, by the third conjunct, \( w = a^{m-n} \) as required. By (S7), the first conjunct is a \( \Sigma_2 \)-formula, by (S9), the second one is in \( B\Sigma_2 \), and by (S2), the last one is in \( \Pi_1 \). Hence, altogether, this formula is in \( \Sigma_3 \).

We showed that \( a^*, S, \) and \( P \) can be defined in \( M \). Since \( (a^*, S, P) \cong (\mathbb{N}, +, \cdot) \), this implies that the theory of \( M \) is undecidable [13].

**Theorem 2.3.** The \( \Sigma_3 \)-theory of \((a, b)^*, \leftrightarrow \) is undecidable.

**Proof.** So far, we found a \( \Sigma_3 \)-interpretation of \((\mathbb{N}, +, \cdot) \) in

\[
M = (\Sigma^*, \leftrightarrow, \varepsilon, a, b, ab, ba, aa, bb, aba, bab).
\]

Since the positive \( \Sigma_1 \)-theory of \((\mathbb{N}, +, \cdot) \) is undecidable by [21], the \( \Sigma_3 \)-theory of \( M \) is undecidable. As a first step, we want to reduce the \( \Sigma_3 \)-theory of \( M \) to that of \( M' = (\Sigma^*, \leftrightarrow, a, b, ab) \). For this, we show how to define \( ba \) etc. in \( M' \).

- \( \varepsilon \) is the least word \( w \) of \( M' \), a property expressible by a \( \Pi_1 \)-formula \( \varphi_{\varepsilon} \).
THEORIES OF ORDERS ON THE SET OF WORDS 59

• A word \( w \in \Sigma^* \) equals \( ba \) iff it is not \( ab \), and any of its proper subwords is a subword of \( a \) or of \( b \). This is expressed by the following \( \Pi_1 \)-formula:

\[
\varphi_{ba}(w) \equiv a, b \mapsto w \neq ab \land \forall x (x \mapsto w \iff (x = w \lor x \mapsto a \lor x \mapsto b)).
\]

• The word \( aa \) is the minimal element of \( a^* \setminus \{\varepsilon, a\} \), i.e., \( w = aa \) iff

\[
\varphi_{aa}(w) \equiv w \in a^* \land \forall x ((x \in a^* \land \neg \varphi_{\varepsilon}(x) \land x \not\equiv a) \Rightarrow (w \not\equiv x)).
\]

The \( \Pi_1 \)-formula \( \varphi_{ab} \) is defined similarly.

• The word \( aba \) is the least word \( w \) embedding \( ab \) and \( ba \), but not \( bb \), i.e., \( w = aba \) iff \( \varphi_{aba}(w) \equiv ab, ba \mapsto w \land b^2 \not\mapsto w \land \forall x ((ab, ba \mapsto x \land bb \not\mapsto x) \Rightarrow (w \not\equiv x)) \) which is a \( \Pi_1 \)-formula. Note that this is not a formula in the language of \( (\Sigma^*, \Longleftrightarrow, a, b, ab) \), but it mentions the additional constants \( ba \) and \( bb \). The \( \Pi_1 \)-formula \( \varphi_{bab} \) is defined similarly (using \( aa \) as an additional constant).

Now let \( \varphi \) be a \( \Sigma_3 \)-sentence in the language of \( M \). Then \( M \models \varphi \) iff \( M' \) satisfies

\[
\exists w_a, w_b, w_{aa}, w_{bb}, w_{aba}, w_{bab} : \left( \varphi_x(w_x) \land \varphi_{ba}(w_{ba}) \land \varphi_{aa}(w_{aa}) \land \varphi_{bb}(w_{bb}) \land \varphi_{aba}(w_{aba}) \land \varphi_{bab}(w_{bab}) \land \varphi' \right).
\]

Here \( \varphi' \) and \( \varphi'_x \) result from \( \varphi \) and \( \varphi_x \), resp., by replacing \( ab \) by \( w_{ab} \), etc. Since all the conjuncts are at most \( \Sigma_3 \)-formulas, the whole formula is \( \Sigma_3 \), i.e., we reduced the undecidable \( \Sigma_3 \)-theory of \( M \) to the \( \Sigma_3 \)-theory of \( M' \). It remains to get rid of the constants \( a, b \), and \( ab \). Since the models \( (\Sigma^*, \Longleftrightarrow, a, b, ab) \) and \( (\Sigma^*, \Longleftrightarrow, b, a, ba) \) are isomorphic (replacing any occurrence of \( a \) in a word \( w \) by \( b \) and vice versa is such an isomorphism), we cannot define the elements \( a, b, \) and \( ab \) in \( \Sigma_3 \), but we can define them “up to isomorphism”:

For a \( \Sigma_3 \)-sentence \( \varphi \) in the language of \( M' \), we consider the formula \( \exists \)

\[
\exists w_a, w_b, w_{ab} : \left( \begin{align*}
& w_a \not\leftrightarrow w_b \land w_b \not\leftrightarrow w_a \\
& \land \exists x \forall z ((x \leftrightarrow w_a) \Rightarrow (x = w_z \lor x \leftrightarrow w_a)) \\
& \land \exists x \forall z ((x \leftrightarrow w_b) \Rightarrow (x = w_z \lor x \leftrightarrow w_z)) \\
& \land \forall x ((x \leftrightarrow w_{ab}) \Rightarrow (x = w_{ab} \lor x \leftrightarrow w_a \lor x \leftrightarrow w_b)) \\
& \land \varphi'
\end{align*} \right),
\]

where \( \varphi' \) results from \( \varphi \) by replacing any occurrence of \( a \) by \( w_a \), \( b \) by \( w_b \), and \( ab \) by \( w_{ab} \).

The first three lines ensure that \( w_a \) and \( w_b \) are two distinct elements of \( \Sigma \). The fourth line holds iff \( w_{ab} \in \{w_a w_b, w_b w_a\} \). Hence we get \( \Sigma, \Longleftrightarrow, a, b, ab \cong (\Sigma, \Longleftrightarrow, w_a, w_b, w_{ab}) \) which implies \( M' \models \varphi \iff (\Sigma, \Longleftrightarrow) \models \exists \).

\[ \square \]

Corollary 2.4. Let \( \Sigma = \{a_1, a_2, \ldots, a_n\} \) be an alphabet with at least two elements. Then the \( \Sigma_3 \)-theory of the subword order \( (\Sigma^*, \Longleftrightarrow) \) is undecidable.
Proof. Let ϕ be a Σ_3-sentence in the language of (\{a, b\}^*, \hookrightarrow) and consider the following formula

\[ \exists (w_i)_{i \leq n} \left( \bigwedge_{1 \leq i < j \leq n} w_i \not\hookrightarrow w_j \land w_j \not\hookrightarrow w_i \land \forall x(x \hookrightarrow w_1 \iff (w = w_2 \lor w = w_1)) \right). \]

Here, the formula ϕ′ results from ϕ by simultaneous replacement of θxψ by \exists x(\bigwedge_{1 \leq i \leq n} \neg w_i \hookrightarrow x \land \psi) and of \forall xψ by \forall x(\bigwedge_{1 \leq i \leq n} \neg w_i \hookrightarrow x \Rightarrow \psi). Then (Σ^*, \hookrightarrow) \models ϕ if and only if (Σ^*, \hookrightarrow) \models ϕ. □

3. THE LEXICOGRAPHIC PATH ORDER

Let Γ be some finite functional signature (i.e., a finite set of function and constant symbols with associated arity) and T(Γ) the associated set of Γ-terms. Further, with any n-ary function symbol f ∈ Γ, one associates an n-ary operation on T(Γ) (also denoted f) with (t_1, ..., t_n) → f(t_1, ..., t_n). The signature Γ is unary if it consists of unary and constant function symbols, only. Any partial order ≤ on Γ defines a lexicographic path ordering ≤_{lpo} [9] on the set of Γ-terms T(Γ) (see also [1]). The actual definition of lexicographic path orderings is nontrivial and, for our technical arguments, only the following observation is of importance (it is folklore in the rewriting community):

Observation. Let Σ be some alphabet and set Γ_Σ = Σ ∪ \{⊥\} where the letters from Σ are unary and ⊥ is the only constant symbol. On Γ_Σ, consider the precedence ≤ with ⊥ < a for all a ∈ Σ and no further comparabilities hold. Then the structures (Σ^*, \hookrightarrow, Γ_Σ, ≤_{lpo}) (cf. Th. 2.1) and (T(Γ_Σ), Γ_Σ, ≤_{lpo}) are isomorphic.

For general signatures, the following is known.

Theorem 3.1 (Comon & Treinen [7]). Let Γ be a signature containing a constant, an at least unary and an at least binary symbol. Then there exists a total precedence ≤ on Γ such that the Σ_2-theory of the structure (T(Γ), Γ, ≤_{lpo}) is undecidable.

Any signature has to contain a constant for otherwise there were no terms. Most likely, one can discard the unary symbol from the signature and still get the result (cf. discussion at the end of [7]). But the proof makes crucial use of the binary symbol. A signature is unary if it consists of unary and constant symbols, only. Narendran & Rusinowitch showed that the binary symbol is crucial not only in the proof by Comon & Treinen, but for the result to hold:

Theorem 3.2 (Narendran & Rusinowitch [22]). Let Γ be a unary signature with total precedence ≤. Then the theory of (T(Γ), Γ, ≤_{lpo}) is decidable.

By Theorem 3.1, the signature has to be unary for this result to hold. From Theorem 2.1, one also gets that totality of the precedence relation is necessary as we indicate now.
The isomorphism of the structures \((\Sigma^*, (p_a)_{a \in \Sigma}, \hookrightarrow)\) and \((T(\Gamma \Sigma), \Gamma \Sigma, \leq_{\text{lpo}})\) and Theorem 2.1 imply

**Corollary 3.3** (Comon & Treinen [6]). Let \(\Gamma\) be a unary signature with at least three function symbols and one constant symbol. Then there exists a partial precedence \(\leq\) on \(\Gamma\) such that the \(\Sigma_4\)-theory of \((T(\Gamma), \leq_{\text{lpo}})\) is undecidable.

Our Corollary 2.4 allows to similarly derive the slightly stronger result

**Corollary 3.4.** Let \(\Gamma\) be a unary signature with at least two function symbols and one constant symbol. Then there exists a partial precedence \(\leq\) on \(\Gamma\) such that the \(\Sigma_4\)-theory of \((T(\Gamma), \leq_{\text{lpo}})\) is undecidable.

Note that, differently from Corollary 3.3, this result speaks about the reduct \((\Gamma)\) of the structure \((\Sigma, (p_a)_{a \in \Sigma}, \hookrightarrow)\). The second line ensures that any such word embeds into \(w\) even when the premise iff \(u \leftrightarrow v \land \pi_b(w) = u \land \exists x(w = bx)\)

\[\land \forall x((u \leftrightarrow x \leftrightarrow w \land aba \not\leftrightarrow x) \Rightarrow (\pi_a(x) \leftrightarrow v))\]

\[\land \forall x((u, v \leftrightarrow bx \land aba, av, ba \not\leftrightarrow bx) \Rightarrow (bx \leftrightarrow w))\]

\[\land \exists x \in (ba)^* \land u \leftrightarrow x \leftrightarrow w).\]

The first two conjuncts ensure \(u = b^m\) and \(v = a^n\) for some \(m, n \in \mathbb{N}\). Since \(\pi_b(w) = u\), the word \(w\) contains precisely \(m\) occurrences of \(b\) and starts with \(b\) (since \(\exists x(w = bx)\)). The second line ensures that any \(a\)-block in \(w\) has size at most \(n\) (cf. discussion in (S8)). Now consider the third line. A word \(x\) satisfies the premise iff

- \(bx\) contains the same number of occurrences of \(b\) as \(u\) and therefore \(w\) does (since \(u \leftrightarrow bx \land bu \not\leftrightarrow bx)\);
- \(bx\) contains the same number of occurrences of \(a\) as \(v\) does (since \(v \leftrightarrow bx \land av \not\leftrightarrow bx)\);
- \(bx\) contains precisely one \(a\)-block (since \(aba \not\leftrightarrow bx)\).

Thus, \(x\) satisfies the premise iff \(bx = b^i a^n b^{m-i}\) for some \(1 \leq i \leq m\). Hence the third line ensures that any such word embeds into \(w\), i.e., any nonempty \(a\)-block in \(w\) has size at least \(n\). The last line is meant to ensure that there is a nonempty \(a\)-block between any two consecutive \(b\)s and at the end of \(w\).
Using this formula instead of the formula from (S9) yields a Σ₂-description of the relation \( P = \{(a^n, a^n, a^n, m, n) \mid m, n \in \mathbb{N}\} \). Hence we have a Σ₂-interpretation of \((\mathbb{N}, +, \cdot)\) in the structure \( \mathcal{M} \). Since the positive Σ₁-theory of \((\mathbb{N}, +, \cdot)\) is undecidable, the Σ₂-theory of \( \mathcal{M} \) is undecidable. Let \( \varphi \) be a Σ₂-sentence in the language of \( \mathcal{M} \) and replace any occurrence of, e.g., \( ab \) in \( \varphi \) by \( p_a p_b(\varepsilon) \). This yields a Σ₂-sentence \( \varphi' \) in the language of the structure \( \mathcal{M}' = \{ (a, b)^*, p_a, p_b, \rightarrow, \varepsilon \} \) that holds in this latter structure iff \( \mathcal{M} \models \varphi \). Finally, consider \( \psi = \exists w (\forall w : (w \rightarrow w) \land \varphi') \) where \( \varphi' \) results from \( \varphi \) by replacing \( \varepsilon \) by \( w \). Then we have \( \mathcal{M} \models \varphi \iff (\{a, b\}^*, p_a, p_b, \rightarrow) \models \psi \). Since \( \psi \) is a Σ₂-sentence, considerations as in the proof of Corollary 2.4 yield

**Theorem 4.1.** If the alphabet \( \Sigma \) contains at most two letters, then the theory of \((\Sigma^*, \preceq)\) is decidable.

**Proof.** For one letter, we have only two repetition-free words (\( \varepsilon \) and \( a \)); hence the theory is decidable in this case. For two letters, the only repetition-free words are the elements of the set \( \{a, \varepsilon\}(ba)^*\{b, \varepsilon\} \). Its nonempty elements can naturally be identified with the elements of the set \( \{a, b\} \times \mathbb{N} \) by \( w \mapsto (\text{first letter of } w, |w|) \). Then \( u \rightarrow v \) iff they agree on their first letter and \( |u| \leq |v| \), or they don’t and \( |u| < |v| \). Hence for two letters, the theory of \((\text{RF}, \rightarrow)\) can be interpreted in the theory of \((\mathbb{N}, \preceq)\) which is decidable. □

4. THE HOMOMORPHISM PREORDER OF WORDS

Let \( u = u_1 u_2 \ldots u_n \) be some word of length \( n \). With \( u \), we associate the Σ-labeled linear order \( \hat{u} = \{(1, 2, \ldots, n), \leq, \lambda\} \) with \( \lambda(i) = u_i \). For two words \( u \) and \( v \), let \( u \preceq v \) denote the existence of a homomorphism from \( \hat{u} \) into \( \hat{v} \) (i.e., an order preserving function \( f \) from \( \{1, 2, \ldots, |u|\} \) to \( \{1, 2, \ldots, |v|\} \) with \( u_i = v_{f(i)} \)). For instance, \( u \rightarrow v \) implies \( u \preceq v \) for any two words \( u \) and \( v \). But also \( aab \preceq ab \) witnessed by the mapping \( f \) with \( f(1) = f(2) = 1 \) and \( f(3) = 2 \). The relation \( \preceq \) is a preorder that, to the knowledge of the author, appeared for the first time in [16] in the context of complexity theoretic considerations. Let \( \sim = \preceq \cap \geq \) be the associated equivalence relation. Then \( \preceq/\sim \) is a partial order on \( \Sigma^*/\sim \). The structure \((\Sigma^*/\sim, \preceq/\sim)\) is Σ₀-interpretable in \((\Sigma^*, \preceq)\). Showing that the Σ₀-theory of the former is undecidable therefore implies that the Σ₂-theory of the latter is undecidable.

Each \( \preceq/\sim \)-equivalence class contains precisely one repetition-free word (i.e., a word not containing \( aa \) as an infix for any letter \( a \)). For repetition-free words \( u \) and \( v \), we have \( u \preceq v \) iff \( u \rightarrow v \). Thus, the structure \((\Sigma^*/\sim, \preceq/\sim)\) is isomorphic to the structure \((\text{RF}, \rightarrow)\) where RF denotes the set of repetition-free words. We first prove some decidability results:

**Theorem 4.5.** Let \( \Gamma \) be some unary signature with at least two function symbols and one constant symbol. Then there exists a partial precedence \( \preceq \) on \( \Gamma \) such that the Σ₂-theory of \((T(\Gamma), \Gamma; \preceq_{\text{lopo}})\) is undecidable.
The case of three letter alphabets remains open, later we will show the undecidability for four letters.

**Proposition 4.2.** Let $\Sigma$ be some alphabet. Then the $\Sigma_1$-theory of $(\Sigma^*, \preceq)$ is decidable.

**Proof.** By the previous theorem, we can assume the existence of three distinct letters $a, b, c$ in $\Sigma$. Now the proof of Proposition 2.2 shows that the $\Sigma_1$-theory of (RF, $\rightarrow$) is decidable (since the embedding constructed there uses repetition-free words, only). Note that any $\sim$-equivalence class in $\Sigma^*$ is infinite. Hence the $\Sigma_1$-theory of $(\Sigma^*, \preceq)$ can be interpreted in that of its quotient (RF, $\rightarrow$). This ensures the result.

To get the undecidability result, we will interpret $(\{a, b\}^*, \rightarrow)$ in (RF, $\rightarrow$). For this to work, two letters do not suffice by Theorem 4.1: let $\Sigma = \{a, b, c, d\}$ and $\Gamma = \{a, b\}$. Then $X = (c\{a, b\})^*$ is a set of repetition-free words over $\Sigma$. Let $f$ be the monoid homomorphism from $\Gamma^*$ to $\Sigma^*$ with $a \mapsto ca$ and $b \mapsto cb$. Then $f$ is injective and onto $X$, hence it witnesses $(X, \rightarrow) \cong (\Gamma^*, \rightarrow)$. It therefore remains to show that $X$ is definable in (RF, $\rightarrow$). We will use the fact that a word $w \in \{a, b, c\}^*$ belongs to $X$ iff, for any factorization $w = x_1x_2$ of $w$ into two words, the last letter of $x_1$ or the first letter of $x_2$ equals $c$.

Similarly to the preceding sections, we work first in an extended model, namely in $\mathcal{M} = (\text{RF, } \rightarrow, a, b, c, d, da, ad, db, bd, dc, cd, dc d)$.  

(H1) Let $w \in \text{RF}$. Then $w$ belongs to $\{a, b, c\}^*$, to $\{a, b, c\}^* d$, or to $\{a, b, c\}^* dc$, resp., iff $d \not\rightarrow w$, iff $d \leftrightarrow w$ and $da, db, dc \not\rightarrow w$, or iff $dc \leftrightarrow w$, but $dc d, da, db \not\leftrightarrow w$, resp. Hence all these sets are $\Sigma_0$-definable.

(H2) Let $w, x \in \{a, b, c\}^* \cap \text{RF}$. Then $x \leftrightarrow \text{wdc}$ iff the following $\Pi_1$-formula holds
\[\forall y((y \in \{a, b, c\}^* dc \land w \leftrightarrow y) \Rightarrow x \leftrightarrow y).\]

First suppose that this formula holds. Note that $y = \text{wdc}$ satisfies the premise of the implication. Thus, $x \leftrightarrow \text{wdc}$ follows. So suppose $x \leftrightarrow \text{wdc}$ and let $y \in \{a, b, c\}^* dc$ with $w \leftrightarrow y$. If we have $x \leftrightarrow w$, then $x \leftrightarrow w \leftrightarrow y$ ensures $x \leftrightarrow y$. So suppose $x \not\leftrightarrow y$. Since $x \leftrightarrow \text{wdc}$ and $x \in \{a, b, c\}^* \cap \text{RF}$, there is a word $x'$ with $x = x'c$ such that the last letter of $x'$ is not $c$. Hence $x' \leftrightarrow w \leftrightarrow y \equiv y' dc$ implies $x' \leftrightarrow y'$ since the last letter of $x'$ is neither $d$ nor $c$. Hence $x = x'c \leftrightarrow y' dc = y$. This finishes the proof.

(H3) Let $w \in \{a, b, c\}^*$. We show that $c$ is the last letter of $w$ iff
\[\forall x((x \in \{a, b, c\}^* \land x \leftrightarrow \text{wdc}) \Rightarrow x \leftrightarrow w).\]

(The formula expresses that $w$ is the largest word from $\{a, b, c\}^* \cap \text{RF}$ embedding into $\text{wdc}$.) If $w = w'a$ or $w = w'b$, then $w \leftrightarrow wc \leftrightarrow \text{wdc}$, i.e., we showed $\sim \leftrightarrow$. Conversely, suppose $w = w'c$ and $x \in \text{RF} \cap \{a, b, c\}$ with $x \leftrightarrow \text{wdc}$. If the last letter of $x$ is not $c$, then $x \leftrightarrow w$. So let $x = x'c$ for some word $x'$. Since $x$ is repetition-free, the last letter of $x'$ belongs
to \(\{a, b\}\). Hence \(x′c = x \leftrightarrow wdc = w′cdc\) implies \(x′ \leftrightarrow w′\) and therefore \(x \leftrightarrow w\). Thus, indeed, \(w\) is maximal in \(\text{RF} \cap \{a, b, c\}^*\) with \(w \leftrightarrow wdc\).

Since the \(\Pi_1\)-subformula \(x \leftrightarrow wdc\) appears in a negative position under the universal quantification \(\forall x\), this formula is \(\Pi_2\).

Analogously, we can express by a \(\Pi_2\)-formula that \(w \in c\{a, b, c\}^* \cap \text{RF}\). For this, we refer to the set \(\{x \in \text{RF} \mid x \leftrightarrow cdw\}\) (cf. (H3)) and therefore to the set \(cd\{a, b, c\}^*\) (cf. (H2)). To define this latter one, we use the constants \(ad, bd\), and \(cd\) analogously to (H1).

Our next aim is to express that any odd letter of \(w\) equals \(c\). Since \(w\) does not end with \(c\) and is repetition-free, we showed \(w \in X\). Conversely, suppose \(w \in X\).

(H4) Let \(w \in \{a, b, c\}^* \cap \text{RF}\). Then \(x \in \text{RF}\) satisfies the following \(\Pi_1\)-formula: \(\varphi_0(w, x)\)

\[
d \leftrightarrow x \land w \leftrightarrow x \land \forall x′((d \leftrightarrow x′ \land w \leftrightarrow x′ \leftrightarrow x) \Rightarrow x = x′)
\]

iff there are words \(x_1, x_2 \in \text{RF}\) with \(w = x_1x_2\) and \(x = x_1dx_2\).

(H5) Let \(x = x_1dx_2\) with \(x_1x_2 \in \{a, b, c\}^* \cap \text{RF}\). Then \(z = x_1\) iff the following \(\Sigma_2\)-formula \(\varphi_1(x, z)\) is satisfied:

\[
z \in \{a, b, c\}^* \land \exists y \left( y \in \{a, b, c\}^* d \land y \leftrightarrow x \land \forall y′((y′ \in \{a, b, c\}^* d \land y′ \leftrightarrow x) \Rightarrow y′ \leftrightarrow y) \land z \leftrightarrow y \land \forall z′((z′ \in \{a, b, c\}^* \land z′ \leftrightarrow y) \Rightarrow (z′ \leftrightarrow z)) \right).
\]

In the first line, \(y \leftrightarrow x\) implies \(y \leftrightarrow x_1d\) since \(x\) contains only one \(d\) and the last letter of \(y\) equals \(d\). The second line therefore expresses that \(y\) is maximal with this property, i.e., \(y = x_1d\). Since \(z\) does not contain any \(d\), the third line says \(z \leftrightarrow x_1\). The last line therefore says that any \(d\)-free subword \(z′\) of \(x_1\) is a subword of \(z\), i.e., \(x_1 \leftrightarrow z\).

Let \(\varphi_2(x, z)\) be the analogous \(\Sigma_2\)-formula expressing \(z = x_2\).

Now we claim that a word \(w \in \text{RF} \cap \{a, b, c\}^*\) belongs to \(X = (c\{a, b\})^*\) iff

\[
\forall x, z_1, z_2 \left( (\varphi_0(w, x) \land \varphi_1(x, z_1) \land \varphi_2(x, z_2)) \Rightarrow (z_1 \in \{a, b, c\}^*c \lor z_2 \in c\{a, b, c\}^* \lor z_1 = w) \right)
\]

\[
\land w \notin \{a, b, c\}^*c
\]

\[
\lor (a \not\leftrightarrow w \land b \not\leftrightarrow w \land c \not\leftrightarrow w).
\]

Note that the last line is satisfied iff \(w = ε\). So, from now on, we consider only nonempty words \(w\). The premise in the first line is equivalent to \(z_1z_2 = w\) by (H4) and (H5), i.e., the universal quantification ranges over all factorizations of \(w\) into two words \(z_1\) and \(z_2\). First suppose that this formula holds. Let \(w = z_1z_2\) be a factorization in two nonempty words \(z_1\) and \(z_2\). Then, by the conclusion in the first line, \(z_1\) ends or \(z_2\) begins with \(c\). Hence, every other letter in \(w\) equals \(c\). If \(z_1\) in this factorization is empty, then \(z_2 \in c\{a, b, c\}^*\) since \(z_1 \neq w\). Hence \(w = z_2\) starts with \(c\). Thus, we showed that any odd letter of \(w\) equals \(c\). Since \(w\) does not end with \(c\) and is repetition-free, we showed \(w \in X\). Conversely, suppose
$w \in X \setminus \{ \varepsilon \}$. Let $w = z_1 z_2$ be any factorization. If $z_1$ is empty, we obtain $z_2 = w$ which begins with $c$. If both, $z_1$ and $z_2$ are nonempty, then either $z_1$ ends or $z_2$ starts with $c$. If $z_2$ is empty, then $z_1 = w$. Thus, we showed the implication in the first line.

The formulas in the premise are from $\Sigma_2$ by (H4) and (H5) and the formulas in the conclusion in $\Pi_2$ by (H3). Since the implication appears under the universal quantification $\forall$, $z_1, z_2$, the first conjunct is a $\Pi_2$-formula. Note that the second conjunct $w \not\in \{ a,b,c \}^c c$ is equivalent to $w \in \{ a,b,c \}^c a \lor w \in \{ a,b,c \} b$, i.e., it is $\Pi_2$ as well. Thus, the set $X$ is $\Pi_2$-definable in the structure $\mathcal{M}$. In other words, we found a $\Pi_2$-interpretation of $(\Gamma^+, \sim)$ in $\mathcal{M}$. Since the $\Sigma_3$-theory of the former is undecidable, the $\Sigma_5$-theory of $\mathcal{M}$ is undecidable.

We next define the constants $ad, db, bd, dc, cd$, and $dcd$ in the structure $\mathcal{M}' = (RF, \iff, a, b, c, d, da)$:

(H6) A word $w$ is of length at least $n$ if and only if there are mutually distinct $x_0 \iff x_1 \iff \ldots \iff x_{n-1} \iff w$. Hence the set of words of length $n$ is $B \Sigma_1$-definable in $\mathcal{M}'$.

(H7) $w = db$ if $|w| = 2$, $d, b \iff w$ and there are two distinct words $x \in RF$ of length 3 with $da, w \iff x$ (the other word $v$ of length 2 with $d, b \iff v$ is $v = bd$, but then $bda$ is the only word from RF of length 3 embedding $da$ and $v$). This formula is $\Sigma_2$. The word $dc$ can be defined similarly.

(H8) $w = ad$ if $w \neq da$, $a, d \iff ad$, and $|w| = 2$. The words $bd$ and $cd$ are defined similarly by $B \Sigma_1$-formulas. (Note that these formulas use the constants $db$ and $dc$ which are not in the language of the structure $\mathcal{M}'$.)

(H9) $w = dcd$ if $|w| = 3$, $dc, cd \iff dcd$ and there is a word $v$ of length 4 with $w, da \iff v$. (There is another word $w'$ of length 3 with $dc, cd \iff w'$, namely $dcd$. But for this one, we cannot construct $v'$ of length 4 with $dcd, ad, da \iff v'$.)

Thus, similarly to the first part of the proof of Theorem 2.3, the $\Sigma_5$-theory of $\mathcal{M}$ can be reduced to the $\Sigma_5$-theory of $\mathcal{M}'$. Considerations similar to those in the second part of the proof of Theorem 2.3 allow to interpret the $\Sigma_5$-theory of $\mathcal{M}$ in the $\Sigma_5$-theory of $(RF, \iff)$. Hence, we obtain

**Theorem 4.3.** Let $\Sigma$ be an alphabet with at least four elements. Then the $\Sigma_5$-theory of $(RF, \iff)$ and therefore that of $(\Sigma^*, \lesssim)$ is undecidable.

**Proof.** Above, we explained how to prove the result about $(RF, \iff)$ if $\Sigma$ contains precisely four letters. The proof of Corollary 2.4 yields the undecidability for larger alphabets. The model $(RF, \iff)$ is always isomorphic to $(\Sigma^*/\sim, \lesssim/\sim)$. Since $\sim$ is $\Sigma_0$-definable in $(\Sigma^*, \lesssim)$, we can $\Sigma_0$-interpret $(\Sigma^*/\sim, \lesssim/\sim)$ in $(\Sigma^*, \lesssim)$. Hence the $\Sigma_5$-theory of this latter structure is undecidable. \hfill $\square$

5. The Infix Order

For two words $u$ and $v$ over $\Sigma$, we write $u \leq v$ if $u$ is an infix of $v$, i.e., if there exist words $x, y$ such that $v = xuy$. In this section, we consider the theory of $(\Sigma^*, \leq)$. 
Note that in the partial order $(\Sigma^*, \leq)$, any word dominates only finitely many other words (i.e., any set $\{ x \in \Sigma^* \mid x \leq w \}$ is finite). In the spirit of Propositions 2.2 and 4.2, we first show that any partial order with this property embeds into the infix order:

**Lemma 5.1.** Let $\Sigma$ be some alphabet and $a, b \in \Sigma$. Let $(P, \preceq)$ be some at most countable partial order such that any set $\{ x \in P \mid x \preceq y \}$ is finite. Then $(P, \preceq)$ can be embedded into $(\Sigma^*, \leq)$.

**Proof.** Without loss of generality, we assume $P \subseteq \mathbb{N} \setminus \{0\}$. By induction on the size $k(y)$ of the set $\{ x \in P \mid x < y \}$, we define words $w_y$ as follows: if $k(y) = 0$, set $w_y = ab^y a$. Otherwise, choose any enumeration $x_1, x_2, \ldots, x_n$ of the set $\{ x \in P \mid x < y \}$ and define $w_y = ab^y a w_{x_1} w_{x_2} \ldots w_{x_n}$. Then $y \mapsto w_y$ is an order embedding of $(P, \preceq)$ into $(\Sigma^*, \leq)$. □

**Proposition 5.2.** Let $\Sigma$ be some alphabet. Then the $\Sigma_1$-theory of $(\Sigma^*, \leq)$ is decidable. If $\Sigma$ is a singleton, then the full theory of $(\Sigma^*, \leq)$ is decidable.

**Proof.** If $\Sigma$ is a singleton, $(\Sigma^*, \leq)$ is isomorphic to $(\mathbb{N}, \leq)$ whose theory is decidable. If $\Sigma$ contains at least two elements we can proceed as in Proposition 2.2 using Lemma 5.1. □

Our undecidability proof makes use of the following words over $\Sigma = \{ \alpha, \beta \}$:

$$a = \alpha^6 \beta \quad b = \alpha^5 \beta^2 \quad \# = \alpha^4 \beta^3 \quad \bot = \alpha^3 \beta^4 \quad \#' = \alpha^2 \beta^5 \quad \bot' = \alpha \beta^6.$$  

In particular, we will consider words over $\Gamma = \{ a, b, \#, \bot, \#, \bot' \}$ and use them to encode the solvability of an instance of Post’s correspondence problem. The encoding is based on ideas developed by Treinen [25]. To make the presentation self-contained, we only use his ideas, but do not refer to his results explicitly. The alphabet $\{ a, b \}$ will be the alphabet of the instance, and the alphabet $\{ \#, \bot, \#, \bot' \}$ will be used to encode the necessary operations.

We extend the structure $(\Sigma^*, \leq)$ by constants for all nonempty words of length at most 14: $M = (\Sigma^*, \leq, (w)_{w \in \Sigma^+, \|w\| \leq 14})$. A word $u$ is an upper neighbor of $v$ iff $u \preceq v$, $u \neq v$ and there is no word properly between these two.

**Lemma 5.3.** A word $w \in \Sigma^*$ of length at least 14 belongs to $\Gamma^*$ iff

- none of the words $\alpha^7$, $\beta^7$, $\alpha u \beta$ and $uv w$ with $u \in \Gamma$ and $v \in \Sigma^7 \setminus \Gamma$ is an infix of $w$;
- there are words $w' \in \Sigma^*$ and $u \in \Gamma$ such that $w'$ is an upper neighbor of $w$ in $(\Sigma^*, \leq)$ and $u \alpha v \beta \leq w'$; and
- there are words $w'' \in \Sigma^*$ and $v \in \Gamma$ such that $w''$ is an upper neighbor of $w$ in $(\Sigma^*, \leq)$ and $v \beta \beta \leq w''$.

Hence the set $\Gamma^*$ is $\Sigma_2$-definable in $M$.

**Proof.** Suppose $u_i \in \Gamma$ for $1 \leq i \leq n$ ($n \geq 2$) and $w = u_1 u_2 \ldots u_n$. Since all the words $u_i$ have length 7 and belong to $\alpha^7 \beta^7$, the word $w$ does not contain $\alpha^7$ or $\beta^7$ as an infix. Now let $u \in \Gamma$ and $x, y \in \Sigma^*$ with $xuy = w$. Then there is an index $i$.
such that \( x = u_1u_2 \ldots u_{i-1}, u_i = u, \) and \( y = u_{i+1}u_{i+2} \ldots u_n. \) Hence the last letter of \( x \) is \( \beta \) (i.e., \( u \alpha u \) is no infix of \( w \)) and the first letter of \( y \) is \( \alpha \) (i.e., \( u \beta \) is no infix of \( w \)). Since the prefix of \( y \) of length 7 belongs to \( \Gamma \), no word \( wv \) with \( v \in \Sigma^7 \setminus \Gamma \) is an infix of \( w \). Now let \( w' = \alpha w \) and \( u = u_1. \) Then \( w' \) is an upper neighbor of \( w, u \in \Gamma, \) and \( u \alpha u \) is an infix of \( w' \). The existence of \( w'' \) is shown similarly.

Conversely, let \( w, w', w'' \in \Sigma^* \) and \( u, v \in \Gamma \) satisfy all the requirements given in the lemma. Since \( u \alpha u \leq w' \) and \( u \alpha u \not\leq w, \) the word \( u \) is a prefix of \( w. \) Similarly, \( v \) is a suffix of \( w. \) Let \( u_i \in \Sigma^7 \) and \( x \in \Sigma^* \) with \( |x| < 7 \) and \( w = u_1u_2 \ldots u_n. \) We already showed \( u_i \in \Gamma \) for some \( i < n. \) Then \( u_iu_{i+1} \in \Gamma \) is an infix of \( w \) implying \( u_{i+1} \in \Gamma. \) In particular, the last letter of \( u_n = \alpha^i \beta^{7-a} \) is \( \beta. \) Hence \( \beta x \) is a suffix of \( w \) of length at most 7 and therefore of \( v \in \Gamma. \) This implies \( x = \beta^b \) for some \( b. \) Hence \( \alpha^i \beta^{7+b-a} \) is a suffix of \( w. \) Since no \( u/\beta \) for \( u \in \Gamma \) is an infix of \( w, \) we obtain \( 7 + b = a + 7 + b - a \leq 7, \) i.e., \( x \) is the empty word. Hence \( w \in \Gamma^+. \)

The first statement is quantifier-free. A quantifier alternation is needed in the second and the third statement in order to express that there are upper neighbors \( w' \) and \( w'' \) of \( w: \)

\[
\exists w' \left( w < w' \land \forall x (w < x \land x \leq w' \Rightarrow x = w') \right).
\]

(11) For \( u, v \in \Gamma^+ \), let \( \text{neighbor}(u, v) \) denote that there is \( c \in \Gamma \) with \( v \in \{cu, uc\}; \) it expresses that \( v \) is an upper neighbor of \( u \) in \((\Gamma^*, \leq). \) Then \( \text{neighbor}(u, v) \) holds iff

\[
\mathcal{M} \models u < v \land \neg \exists x_1, x_1, \ldots, x_7, x_8 (u = x_0 \land \bigwedge_{1 \leq i \leq 8} x_{i-1} < x_i \land x_8 \leq v),
\]

\( i.e., \) iff \( u \) is a proper infix of \( v \) and the length difference is at most 7 (since we assumed \( u, v \in \Gamma^+ \) from the very beginning, the length difference equals 7 in this case). Thus, the relation \( \text{neighbor} \subseteq \Gamma^* \times \Gamma^* \) is \( \Pi_1 \)-definable in \((\mathcal{M}, \Gamma^+)\) and therefore \( \Sigma_2 \)-definable in \( \mathcal{M} \) by Lemma 5.3. (12) Let \( M \subseteq \Gamma. \) Then a word \( w \in \Gamma^+ \) belongs to \( M^+ \) iff \( c \not\leq w \) for all \( c \in \Gamma \setminus M. \) Thus, any such set is \( \Sigma_0 \)-definable in \((\mathcal{M}, \Gamma^+)\) by the formula

\[
w \in \Gamma^+ \land \bigwedge_{c \in \Gamma \setminus M} c \not\leq w
\]

and therefore \( \Sigma_2 \)-definable in \( \mathcal{M}. \)

(13) A word \( w \in \Sigma^* \) belongs to \( \Sigma^* \setminus \Sigma^+ \setminus \Sigma^+ \) iff it contains \( \# \), but not \( \# \gamma \) for any \( \gamma \in \Sigma. \) Hence this set is quantifier free definable in \( \mathcal{M}. \) Similarly, the set \( \# \Sigma^* \setminus \Sigma^+ \setminus \Sigma^+ \) is \( \Sigma_0 \)-definable using the constants \( \alpha \# \) and \( \beta \# \) from the signature of \( \mathcal{M}. \)

(14) A word \( w \in \Sigma^* \) belongs to \( \# \{a, b\} \# \) iff it is an element of \( \{a, b, \#\}^* \) and its two maximal proper infixes (within \( \Gamma^+ \)) \( x_1 \) and \( x_2 \) satisfy \( x_1 \in \# \Sigma^* \setminus \Sigma^+ \setminus \Sigma^+ \) and \( x_2 \in \Sigma^* \setminus \# \Sigma^+ \) or vice versa (to accept this,
note that the two maximal proper infixes from $\Gamma^*$ of a word $a_1a_2\ldots a_n$ with $a_i \in \Gamma$ are $a_2a_3\ldots a_n$ and $\ldots$ let $u, v, w \in \{a, b\}^*$. Then, by (I6), we can express by a $\Sigma_2$-formula that $x = u#v$ and $x = w$.

Above, we saw that $w \in \{a, b\}^*$ as well as $\text{neighbor}(x_1, w)$ can be expressed in $\Sigma_2$ while $x_1 \in \#\Sigma^* \setminus \Sigma^* \setminus \Sigma^+$ and $x_2 \in \Sigma^* \setminus \Sigma^+$. Hence the set $\#\{a, b\}^*$ is $\Sigma_2$-definable in $\mathcal{M}$.

(15) Since $\#\{a, b\}^*$ is the intersection of the $\Sigma_2$-set $\{a, b, \#\}^*$ and the $\Sigma_0$-set $\#\Sigma^* \setminus \Sigma^+ \setminus \Sigma^*$, it is $\Sigma_2$-definable in $\mathcal{M}$. Similarly, the set $\{a, b\}^*$ is $\Sigma_2$.

(16) Let $x = x_1x_2 \in \{a, b\}^*\{a, b\}^*$ and $w \in \{a, b\}^*$. Then $w = x_i$ iff the largest infix $y \in \{a, b\}^*$ of $x$ is an upper neighbor of $w$ (within $\Gamma^*$):

$$\exists y \left( y \in \{a, b\}^* \land \text{neighbor}(w, y) \land y \leq x \land \forall z((z \in \Sigma^* \setminus \Sigma^* \setminus \Sigma^+ \land z \leq x) \Rightarrow z \leq y) \right).$$

The set $\{a, b\}^*$ and the relation neighbor are $\Sigma_2$-definable, and the set $\Sigma^* \setminus \Sigma^+ \setminus \Sigma^*$ is $\Sigma_0$-definable. Hence this formula is $\Sigma_2$. We can write down an analogous $\Sigma_2$-formula that holds iff $w = x_2$.

(17) Let $u, \overline{u} \in \{a, b\}^*$. Then $ua = \overline{u}$ iff

$$\exists x, x', x'' \left( \text{neighbor}(u, x) \land \text{neighbor}(x, x') \land \text{neighbor}(x', x'') \land x, x' \in \downset\{a, b\}^* \land x'' \in \Sigma^* \setminus \Sigma^+ \setminus \Sigma^+ \land a \# \leq x'' \land u < \overline{u} < x'' \right).$$

The first line expresses that $u < x < x' < x''$ is a maximal chain from $u$ to $x''$ within $\Gamma^*$, i.e., any element of this sequence results from the previous one by prefixing or suffixing by one element of $\Gamma$. Since $u \in \{a, b\}^*$ and $x, x' \in \downset\{a, b\}^*$, we get $x = \bot u$ and $x' = \bot uc$ for some $c \in \{a, b\}$. Since $\#$ is a suffix of $x''$, we also have $x'' = \bot uc\#$. Now $a\# \leq x''$ forces $c = a$. Finally, $u \leq \overline{u}$ says that $\overline{u}$ is a proper extension of $u$. Since this extension belongs to $\{a, b\}^*$ and is an infix of $x'' = \bot ua\#$, the formula expresses indeed $ua = \overline{u}$.

Since all the conjunctions in the first two lines are at most $\Sigma_2$, the whole formula is $\Sigma_2$-expressible.

Lemma 5.4. Let $I = (u_i, v_i)_{i \leq 7}$ be some instance of Post’s correspondence problem with $u_i, v_i \in \{a, b\}^*$. There is a $\Sigma_2$-formula $\rho(x, \overline{x})$ such that, for $x, \overline{x} \in \{a, b\}^*\{a, b\}^*$, we have $\mathcal{M} \models \rho(x, \overline{x})$ iff $x = u\#v$ and $\overline{x} = u_i\#v_i$ for some $i \leq 7$ and $u, v \in \Gamma^*$.

Proof. Let $x, \overline{x} \in \{a, b\}^*\{a, b\}^*$ and let $u, v, \overline{u}, \overline{v} \in \{a, b\}^*$. Then, by (16), we can express by a $\Sigma_2$-formula that $x = u\#v$ and $\overline{x} = \overline{u}\#\overline{v}$. Now suppose
THEORIES OF ORDERS ON THE SET OF WORDS 69

$u_1 = a_1a_2 \ldots a_n$ with $a_i \in \{a, b\}$. Then $\overline{u} = uu_1$ iff

$$\exists x_0, x_1, x_2, \ldots x_n \left( u = x_0 \land \bigwedge_{i=1}^{n} x_i = x_{i-1}a_i \land x_n = \overline{u} \right).$$

By (17), this is a $\Sigma_2$-formula. Hence the following is expressible in $\Sigma_2$:

$$\exists u, v, \overline{u}, \overline{v} \left( x = u\#v \land \overline{x} = \overline{u}\#\overline{v} \right).$$

(18) A word $w \in \Sigma^*$ belongs to $\perp \{a, b, \#, \perp\}^* \perp \{a, b, \#, \perp\}^* \perp$ if there are words $x'$ and $x''$ in the set $\{a, b, \#, \perp\}^*$ with $\perp \leq x'$, $x' \perp = x''$ and $\perp x'' = w$. To express $x' \perp = x''$, we proceed as in (17) using $\perp'$ instead of $\perp$ and $\#$' instead of $\#$. Symmetrically, we can express $\perp x'' = w$ by a $\Sigma_2$-formula. Hence membership in this set is expressible in $\Sigma_2$.

(19) A word $w \in \Sigma^*$ belongs to $\perp \{a, b, \#\}^* \perp \{a, b, \#\}^* \perp$ if it is an element of the language $\perp \{a, b, \#, \perp\}^* \perp \{a, b, \#, \perp\}^* \perp$ and there is no proper infix $x < w$ of $w$ with $x \in \perp \{a, b, \#, \perp\}^*$. In other words, $w$ belongs to this set iff

$$w \in \perp \{a, b, \#, \perp\}^* \perp \{a, b, \#, \perp\}^* \perp \forall x(x \leq w \land x \in \perp \{a, b, \#, \perp\}^* \perp \{a, b, \#, \perp\}^* \perp) \Rightarrow x = w).$$

Since $w \in \perp \{a, b, \#, \perp\}^* \perp \{a, b, \#, \perp\}^* \perp$ is expressible in $\Sigma_2$ and appears in a negative position in the second conjunct, this formula is $B\Sigma_2$.

**Proposition 5.5.** Let $I = (a_i, b_i)_{i \leq 7}$ be some instance of Post's correspondence problem with $a_i, b_i \in \Gamma^*$. There is a $\Sigma_4$-sentence $\varphi$ such that $M \models \varphi$ if $I$ has a solution. Since the formula $\varphi$ can be constructed effectively from $I$, the $\Sigma_4$-theory of $M$ is undecidable.

**Proof.** Let $\rho$ be the $\Sigma_2$-formula from Lemma 5.4. Similarly to (16), there exist $\Sigma_2$-formulas $\varphi_1$ and $\varphi_2$ such that $x = x_1 \perp x_2 \in \{a, b\}^* \perp \{a, b\}^*$ and $u \in \{a, b\}^*$ satisfy $\varphi_i(x, u)$ iff $u = x_i$ for $i = 1, 2$.

Now let

$$R = \{ \perp u \perp v \mid u, v \in \{a, b\}^* \# \{a, b\}^* \text{ and } M \models \rho(u, v) \}$$

and $x \in \perp \{a, b\}^* \# \{a, b\}^* \perp \{a, b\}^* \# \{a, b\}^* \perp$. Then $x \in R$ iff the following holds

$$\exists x_1, x_2, x_3, y \left( x = y \perp \land y = \perp x_1 \land \varphi_1(x_1, x_2) \land \varphi_2(x_1, x_3) \right).$$

The first line ensures $x = \perp x_1 \perp$. Hence $x_1 = u \perp v$ for some $u, v \in \{a, b\}^* \# \{a, b\}^*$. By the second line, $u = x_2$ and $v = x_3$. Hence, by the fourth line, this formula expresses indeed $x \in R$ (provided $x \in \perp \{a, b\}^* \# \{a, b\}^* \perp \{a, b\}^* \# \{a, b\}^* \perp$).
Note that this formula is $\Sigma_2$ by (I7) and Lemma 5.4. Now consider the following statement

$$\exists w \left( \begin{array}{l}
w \in \perp \{a, b, \perp, \#\}^* \perp \\
\land \forall x (x \leq w \Rightarrow (x \notin \{a, b\}^* \# \cup \perp \{a, b\}^* \perp)) \\
\land \forall x ((x \leq w \land x \in \perp \{a, b, \#\}^* \perp \{a, b, \#\}^* \perp) \Rightarrow x \in R) \\
\land \perp \# \perp \leq w \land \exists u (u \# u \leq w \land u \in \{a, b\}^*)
\end{array} \right).$$

We show that the PCP-instance $I$ has a solution iff this formula is satisfied in $M$. The conjunction of the first two lines expresses $x \in (\perp \# \#)^* \perp$, i.e.,

$$x = (\perp u_1 \# v_1)(\perp u_2 \# v_2)\ldots(\perp u_n \# v_n) \perp$$

for some $n \geq 1$ and $u_i, v_i \in \{a, b\}^*$. The last line expresses that there are $i, j \leq n$ with $u_i = v_i = \varepsilon$ and $u_j = v_j \neq \varepsilon$. Finally, the implication in the third line expresses that, for any $i < n$, we have $\perp u_i \# v_i \perp u_i+1 \# v_i+1 \perp \in R$, i.e., $u_i+1 = u_i a_k$ and $v_i+1 = v_i b_k$ for some $k \leq 7$. Therefore, indeed, $I$ has a solution iff this statement holds.

Next we show that the statement above is expressible by a $\Sigma_4$-formula. The first line is equivalent to

$$w \in \Gamma^* \land \# \perp \leq w \land \exists y, z (y = \perp x \land w = y \perp).$$

Since $w \in \Gamma^*$, $y = \perp x$, and $w = y \perp$ are $\Sigma_2$-expressible (cf. (I7)), the first line is $\Sigma_2$-expressible as well. The second conjunct is $\Pi_3$ since the conclusion is $\Sigma_2$. Now consider the third line. The condition of the implication is $B \Sigma_2$-expressible (I9) and the conclusion is $\Sigma_2$. Hence the third line is a $\Pi_3$-formula. The last conjunct is equivalent to

$$\exists y, u (\perp y \perp \leq w \land \perp \leq y \land (y, u) \text{ satisfies the two formulas from (I6)})$$

which is $\Sigma_2$. Thus, all the conjuncts are at most $\Pi_3$ which places the whole formula in $\Sigma_4$. \hfill \Box

**Theorem 5.6.** The $\Sigma_4$-theory of $(\{\alpha, \beta\}^*, \leq)$ is undecidable.

**Proof.** By Proposition 5.5, we have to reduce the $\Sigma_4$-theory of the extended structure $M$ to the $\Sigma_4$-theory of $(\Sigma^*, \leq)$. We proceed similarly to the proof of Theorem 2.3. Consider the structure $M_n = (\Sigma^*, \leq, (w)_{w \in \Sigma^+, |w| \leq n})$ for $n \in \mathbb{N}$. We will successively reduce the $\Sigma_4$-theory of $M_{n+1}$ to that of $M_n$. By Proposition 5.5, the $\Sigma_4$-theory of $M = M_{14}$ is undecidable. Hence, by induction, the undecidability of the $\Sigma_4$-theory of $M_0 = (\Sigma^*, \leq)$ will follow.

First assume $n \geq 2$ and let $w \in \Sigma^+$ with $|w| = n + 1$.

1. Suppose $w = \alpha^{n+1}$. Then $w$ is the unique word of length $n + 1$ whose only infix of length $n$ is $\alpha^n$. Hence $\alpha^{n+1}$ is the only word $w$ satisfying the
following $\Pi_1$-formula $\varphi_{\alpha^{n+1}}(w)$ in the structure $\mathcal{M}_n$:

$$\alpha^n < w \land \forall x (\alpha^n < x \leq w \Rightarrow x = w) \land \bigwedge_{v \in \Sigma^n \setminus \{\alpha^n\}} \neg v \leq w.$$ 

Similarly, $\beta^{n+1}$ is the unique word satisfying some $\Pi_1$-formula in $\mathcal{M}_n$.

(2) Suppose there is $i$ such that the letters no. $i$ and $i + 2$ in $w$ differ. Let $w_1$ and $w_2$ be the two infixes of $w$ of length $n$ (since $w$ does not contain to $\alpha^* \cup \beta^*$, there are two such distinct infixes). Then there are $a, b \in \Sigma$ with $w = aw_1 = w_2b$. Suppose $v$ is another word of length $n + 1$ containing both, $w_1$ and $w_2$. Then there are $c, d \in \Sigma$ with $w_1c = dw_2$. Since $w = w_2b$, letter no. $i$ in $w$ equals letter no. $i$ in $w_2$. Since $w_1c = dw_2$, it equals letter no. $i + 1$ in $w_1$. Now $aw_1 = w$ implies that it equals letter no. $i + 2$ in $w$, contradicting our assumption on $i$ and $w$. Hence $w$ is the only word of length $n + 1$ containing both, $w_1$ and $w_2$. More formally, it is the only word satisfying the following $\Pi_1$-formula $\varphi_w$ in the structure $\mathcal{M}_n$:

$$w_1, w_2 < w \land \forall x (w_1 < x \leq w \Rightarrow x = w).$$

(3) Finally, suppose $\alpha^2$ and $\beta^2$ are no infix of $w$. Then $w \in \{(\alpha\beta)^m, (\beta\alpha)^m\}$ (with $2m = n + 1$ if $n$ is odd) or $w \in \{(\alpha\beta)^m \alpha, (\beta\alpha)^m \beta\}$ (with $2m = n$ if $n$ is even). Suppose $w$ starts with $\alpha$ and let $w'$ be the prefix of length $n$ of $w$. The following distinguishes $w$ from the other element of the respective set: there is an upper neighbor in $(\Sigma^*, \leq)$ containing $\alpha^2 \beta$ as an infix. Thus, $(\alpha\beta)^m ((\alpha\beta)^m \alpha, \text{resp.})$ is the only word $w$ satisfying the following $\Sigma_2$-formula $\varphi_w$:

$$\alpha^2, \beta^2 \not\leq w$$
$$\land \quad w' \leq w \land \forall y (w' < y \leq w \Rightarrow y = w)$$
$$\land \quad \exists y (w, \alpha^2 \beta < y \land \forall x (w < x \leq y \Rightarrow x = y)).$$

Since this formula uses the constant $\alpha^2 \beta$, it belongs to the language of the structure $\mathcal{M}_n$ for $n \geq 3$, only. If $n = 2$, it is a formula in the language of the extended structure $(\mathcal{M}_2, \alpha^2 \beta)$. If the first letter of $w$ is $\beta$, we can derive an analogous formula.

Now let $\varphi$ be some $\Sigma_4$-sentence in the language of $\mathcal{M}_{n+1}$. Then let $\mathcal{F}$ be the following $\Sigma_4$-sentence

$$\exists (x_w)_{w \in \Sigma^{n+1}} \left( \bigwedge_{w \in \Sigma^{n+1}} \varphi_w(x_w) \land \varphi' \right)$$

where $\varphi'$ is obtained from $\varphi$ by replacing any occurrence of the constant $w \in \Sigma^{n+1}$ by the variable $x_w$. Provided $n \geq 3$, this is a $\Sigma_4$-sentence in the language of $\mathcal{M}_n$ and we have $\mathcal{M}_n \models \mathcal{F}$ iff $\mathcal{M}_{n+1} \models \varphi$. If $n = 2$, the formulas $\varphi_{\alpha^2 \alpha}$ and $\varphi_{\beta^2 \alpha}$ contain occurrences of the constant $\alpha^2 \beta$ and $\beta^2 \alpha$, resp. Replacing them by $x_{\alpha^2 \beta}$
and \( x_{\beta \alpha} \), resp., turns \( \varphi \) into a sentence in the language of \( M_2 \) with \( M_2 \models \varphi \) iff \( M_3 \models \varphi \).

So far, we reduced the undecidable \( \Sigma_4 \)-theory of \( M \) to the \( \Sigma_4 \)-theory of \( M_2 \) which is therefore undecidable as well. Next, we reduce this latter theory to the \( \Sigma_4 \)-theory of the structure \( M' = (\Sigma^*, \leq, \alpha, \beta, \alpha \beta) \). As above, it suffices to produce \( \Pi_1 \)-formulas defining \( \beta \alpha, \alpha^2 \) and \( \beta^2 \) in this structure:

\[
\begin{align*}
\text{w} = \beta \alpha & \iff M' \models w \neq \alpha \beta \land \alpha < w \land \forall x (\alpha < x \leq w \Rightarrow x = w) \\
\text{w} = \alpha^2 & \iff M' \models \beta \leq w \land \alpha < w \land \forall x (\alpha < x \leq w \Rightarrow x = w) \\
\text{w} = \beta^2 & \iff M' \models \alpha \leq w \land \beta < w \land \forall x (\beta < x \leq w \Rightarrow x = w).
\end{align*}
\]

The word \( \alpha \beta \) cannot be defined in the structure \( M_1 \) since taking the mirror image of a word is an automorphism of \( M_1 \) that maps \( \alpha \beta \) to \( \beta \alpha \).

For a \( \Sigma_4 \)-sentence \( \varphi \) in the language of \( M' \), we consider the formula \( \varphi' \)

\[
\exists x_{\alpha \beta} : (\varphi' \land \forall x (x \leq x_{\alpha \beta} \Rightarrow (x = x_{\alpha \beta} \lor x \leq \alpha \lor x \leq \beta)))
\]

where \( \varphi' \) results from \( \varphi \) by replacing any occurrence of \( \alpha \beta \) by \( x_{\alpha \beta} \). The universally quantified statement ensures \( x_{\alpha \beta} \in \{\alpha \beta, \beta \alpha\} \). Hence \( (\Sigma^*, \leq, \alpha, \beta, \alpha \beta) \cong (\Sigma^*, \leq, \alpha, \beta, x_{\alpha \beta}) \) and therefore

\[
(\Sigma^*, \leq, \alpha, \beta, \alpha \beta) \models \varphi \iff (\Sigma^*, \leq, \alpha, \beta, x_{\alpha \beta}) \models \varphi'.
\]

But this implies \( M' \models \varphi \) iff \( M_4 \models \varphi' \), i.e., we reduced the undecidable \( \Sigma_4 \)-theory of \( M' \) to the \( \Sigma_4 \)-theory of \( M_1 \).

Finally, let \( \varphi \) be a \( \Sigma_4 \)-sentence in the language of \( M_1 \). Consider the following \( \Sigma_4 \)-sentence \( \varphi' \) in the language of \( (\Sigma^*, \leq) \):

\[
\exists x_\alpha, x_\beta \left( \varphi' \land \exists x_\alpha \forall x (x < x_\alpha \iff (x = x_\alpha \lor x = x_\alpha)) \right)
\]

where \( \varphi' \) is obtained from \( \varphi \) by replacing any occurrence of \( \alpha \) or \( \beta \) by \( x_\alpha \) or \( x_\beta \), resp.

\[\square\]

**Corollary 5.7.** Let \( \Sigma = \{a_1, a_2, \ldots, a_n\} \) be an alphabet with at least two elements. Then the \( \Sigma_4 \)-theory of the infix order \( (\Sigma^*, \leq) \) is undecidable.

**Proof.** This can be proved as Corollary 2.4. \[\square\]

6. **Forests**

A forest is a finite \( \Sigma \)-labeled partial order \( (V, \leq, \lambda) \) where any of the sets \( \{x \in V \mid x \leq y\} \) is linearly ordered. For two forests \( s \) and \( t \), let \( s \hookrightarrow t \) denote the existence of an embedding of \( s \) into \( t \) (i.e., of an injective mapping \( f : V_s \to V_t \) such that \( \lambda_s(v) = \lambda_t(f(v)) \)) and \( v \leq w \iff f(v) \leq f(w) \) for any \( v, w \in V_s \). By Kruskal’s theorem, \( \hookrightarrow \) is a well quasi order on the set \( \mathcal{F}_\Sigma \) of all forests. Note that
any term from $T(\Gamma)$ can be seen as a forest with $\Sigma = \Gamma$. By [3], the positive $\Sigma_1$-theory of $(T(\Gamma), \Gamma, \rightarrow)$ is decidable. We show that the related structure $(\mathcal{F}_{\Sigma}, \hookrightarrow)$ has an undecidable theory.

**Corollary 6.1.** Let $\Sigma$ be a finite alphabet with at least two elements. Then the theory of $(\mathcal{F}_{\Sigma}, \hookrightarrow)$ is undecidable.

**Proof.** As before, we identify a word $w \in \{a, b\}^*$ with the labeled linear order of length $|w|$ where $i$ is mapped to the $i$th letter of $w$. In this sense, $\{a, b\}^*$ is a subset of $\mathcal{F}_{\Sigma}$ — we show that it is definable which implies the undecidability by Theorem 2.3.

We identify the letter $a \in \Sigma$ with the singleton tree whose only node is labeled $a$. The empty forest is the only one that does not embed any other forest. A forest $t$ is of size at most $n$ iff there is no sequence of distinct forests $t_0 \leftarrow t_1 \leftarrow \ldots \leftarrow t_n \leftarrow t$. Thus, for any $n$, the set of forests of size at most $n$ is definable. For $a, b \in \Sigma$ let an $ab$-forest be a forest of size 2 that embeds $a$, $b$, and no further forests of size 1. For $a, b \in \Sigma$, let $t_{ab}$ be the disjoint union of the trees $a$ and $b$. Further, $\ell_{ab}$ is the 2-elements linear order whose minimal node is labeled $a$ and the other one carries $b$. Then $t_{bb}$ and $\ell_{bb}$ are the only $bb$-forests, and $t_{ab}, \ell_{ab}$, and $\ell_{ba}$ are the only $ab$-forests for $a \neq b$. We want to distinguish $t_{ab}$ from the other $ab$-forests.

First, let $a \neq b$ and let $t$ be any $ab$-forest. We consider the set $M(t)$ of forests $t'$ of size 3 such that no $bb$-forest embeds into $t'$ and $t$ is the only $ab$-forest that embeds into $t'$. Then $M(t_{ab})$ contains just 2 elements while $M(\ell_{ab})$ is a three-elements set.

Hence $\ell_{ab}$ as well as the set $\{\ell_{ab}, \ell_{ba}\}$ are definable for $a \neq b$. Then $\ell_{ab}$ is the unique $bb$-forest that embeds into some forest $t$ of size 3 with $\ell_{ab}, \ell_{ba} \hookrightarrow t$. Hence, $\ell_{bb}$ and therefore $t_{bb}$ are definable.

Hence $\{a, b\}^*$ is the set of forests $t$ satisfying

$$\bigwedge_{c \in \Sigma \setminus \{a, b\}} c \not\hookrightarrow t \wedge t_{ab}, t_{aa}, t_{bb} \not\hookrightarrow t.$$ 

Thus, the theory of $(\{a, b\}^*, \hookrightarrow)$ can be interpreted in the theory of $(\mathcal{F}_{\Sigma}, \hookrightarrow)$ which is therefore undecidable by Theorem 2.3. □

### 7. Open Questions

For some partial orders on the set of words, we showed the undecidability of small fragments of the first-order theory. In this context, the following cases are open.

1. The $\Sigma_2$-theory of $(\Sigma^*, \hookrightarrow)$ for $|\Sigma| \geq 2$.
2. The $\Sigma_n$-theory of $(\Sigma^*, \hookrightarrow)$ for $2 \leq n \leq 4$ and $|\Sigma| \geq 4$. Nothing is known for $|\Sigma| = 3$ beyond the $\Sigma_1$-theory, smaller alphabets have decidable full theories.
3. The $\Sigma_n$-theory of $(\Sigma^*, \hookrightarrow)$ for $2 \leq n \leq 3$ and $|\Sigma| \geq 2$.

I would have liked some results on the homomorphism preorder of forests [24] since this question by V. Selivanov initiated the research reported in this paper.
References


Communicated by V. Diekert.
Received May 26, 2004. Accepted February 3, 2005.