Generating All Minimal Petri Net Unsolvable Binary Words

Evgeny Erofeev[1⋆], Kamila Barylska[2⋆⋆], Łukasz Mikulski[2⋆⋆], Marcin Piątkowski[2⋆⋆]

[1] Parallel Systems, Department of Computing Science
Carl von Ossietzky Universität, D-26111 Oldenburg, Germany
evgeny.erofeev@informatik.uni-oldenburg.de
[2] Faculty of Mathematics and Computer Science
Nicolaus Copernicus University, 87-100 Toruń, Poland
{kamila.barylska,lukasz.mikulski,marcin.piatkowski}@mat.umk.pl

Abstract. Sets of finite words, as well as some infinite ones, can be described using finite systems, e.g. automata. On the other hand, some automata may be constructed with use of even more compact systems, like Petri nets. We call such automata Petri net solvable. In this paper we consider the solvability of singleton languages over a binary alphabet (i.e. binary words). An unsolvable (i.e. not solvable) word w is called minimal if each proper factor of w is solvable. We present a complete language-theory characterisation of the set of all minimal unsolvable binary words. The characterisation utilises morphic-based transformations which expose the combinatorial structure of those words, and allows to introduce a pattern matching condition for unsolvability.
Keywords: Binary words, labelled transition systems, Petri nets, synthesis

1 Introduction

To deal with infinite sets of words we need to specify them in a finite way. Finite automata which are known as a classical model for describing regular languages, are equivalent to finite labelled transition systems [8]. Some sets may be expressed with use of even more compact system models.

In this paper we investigate the synthesis problem with a specifications given in the form of labelled transition systems. The sought system model is a place/transition Petri net [11], with its reachability graph as a natural bridge between specification and implementation. Namely, we are concerned with finding a net, which reachability graph is isomorphic to a given labelled transition system.

⋆ This work is supported by the German Research Foundation through the Research Training Group (DFG GRK 1765) SCARE (www.scare.uni-oldenburg.de).
⋆⋆ This work is supported by the Polish National Science Center under the grant No.2013/09/D/ST6/03928.

To address this issue one may use the theory of regions [3]. For a given labelled transition system, the solution of a number of linear inequations systems provided by the theory of regions exists if and only if there exists an implementation in a net form. Moreover, solutions of such linear inequations systems are usually utilised during the synthesis of the resulting system (see Synet [4] and APT [12]).

Our aim is to initiate a combinatorial approach and to provide a complete characterisation of a generative nature for a special kind of labelled transition systems – non-branching and acyclic transition systems having at most two labels (i.e. binary words) [1]. More precisely, we characterise all minimal unsolvable binary words.

The paper is organized as follows. First we give some basic notions and notations concerning labelled transition systems, Petri nets and theory of regions. After that we present a necessary condition for minimal unsolvability, which allows to formulate possible shapes of minimal unsolvable words in the form of extended regular expressions [5]. In section 4 we introduce the notion of (base) extendable and non-extendable binary words. In the following sections we provide the main results of this paper: a generic characterisation of all minimal unsolvable binary words and its utilization for an efficient verifying procedure. We conclude the paper with a short section containing some directions for further research.

2 Basic notions

In this section we introduce notions used throughout the paper.

Words
A *word over alphabet* T is a finite sequence $w \in T^*$, and it is *binary* if $|T| = 2$. For a word w and a letter t, $\#_t(w)$ denotes the number of times t occurs in w. A word $w' \in T^*$ is called a *subword* (or *factor*) of $w \in T^*$ if $\exists u_1, u_2 \in T^* \colon w = u_1 w' u_2$. In particular, w' is called a *prefix* of w if $u_1 = \varepsilon$, a *suffix* of w if $u_2 = \varepsilon$, and an *infix* of w if $u_1 \neq \varepsilon$ and $u_2 \neq \varepsilon$.

A mapping $\phi : \Sigma_1^* \to \Sigma_2^*$ is called a *morphism* if we have $\phi(u \cdot v) = \phi(u) \cdot \phi(v)$ for every $u, v \in \Sigma_1^*$ whenever all operations are defined. A morphism ϕ is uniquely determined by its values on the alphabet. Moreover, ϕ maps the neutral element of Σ_1^* into the neutral element of Σ_2^*.

Transition systems
A *finite labelled transition system* (or simply *lts*) with initial state is a tuple $TS = (S, \to, T, s_0)$ with nodes S (a finite set of states), edge labels T (a finite set of letters), edges $\to \subseteq (S \times T \times S)$, and an initial state $s_0 \in S$. A label t is enabled at $s \in S$, denoted by $s[t\rangle$, if $\exists s' \in S \colon (s, t, s') \in \to$. A state s' is reachable from s through the execution of $\sigma \in T^*$, denoted by $s[\sigma\rangle s'$, if there is a directed path from s to s' which edges are labelled consecutively by σ. The set of states reachable from s is denoted by $[s\rangle$. A sequence $\sigma \in T^*$ is allowed, or firable, from a state s, denoted by $s[\sigma\rangle$, if there is some state s'

such that $s[\sigma\rangle s'$.[1] Two labelled transition systems $TS_1 = (S_1, \rightarrow_1, T, s_{01})$ and $TS_2 = (S_2, \rightarrow_2, T, s_{02})$ are isomorphic if there is a bijection $\zeta\colon S_1 \rightarrow S_2$ with $\zeta(s_{01}) = s_{02}$ and $(s, t, s') \in \rightarrow_1 \Leftrightarrow (\zeta(s), t, \zeta(s')) \in \rightarrow_2$, for all $s, s' \in S_1$.

A word $w = t_1 t_2 \dots t_n$ of length $n \in \mathbb{N}$ uniquely corresponds to a finite transition system $TS(w) = (\{0, \dots, n\}, \{(i-1, t_i, i) \mid 0 < i \leq n \wedge t_i \in T\}, T, 0)$.

Petri nets
An *initially marked Petri net* is denoted as $N = (P, T, F, M_0)$ where P is a finite set of places, T is a finite set of transitions, F is the flow function $F\colon ((P \times T) \cup (T \times P)) \rightarrow \mathbb{N}$ specifying the arc weights, and M_0 is the initial marking (where a marking is a mapping $M\colon P \rightarrow \mathbb{N}$, indicating the number of tokens in each place). A *side-place* is a place p with $p^\bullet \cap {}^\bullet p \neq \emptyset$, where $p^\bullet = \{t \in T \mid F(p,t) > 0\}$ and ${}^\bullet p = \{t \in T \mid F(t,p) > 0\}$. N is *pure* or *side-place free* if it has no side-places. A transition $t \in T$ is enabled at a marking M, denoted by $M[t\rangle$, if $\forall p \in P\colon M(p) \geq F(p,t)$. The firing of t at marking M leads to M', denoted by $M[t\rangle M'$, if $M[t\rangle$ and $M'(p) = M(p) - F(p,t) + F(t,p)$. This can be extended, as usual, to $M[\sigma\rangle M'$ for sequences $\sigma \in T^*$, and $[M\rangle$ denotes the set of markings reachable from M. The reachability graph $RG(N)$ of a bounded (such that the number of tokens in each place does not exceed a certain finite number) Petri net N is the labelled transition system with the set of vertices $[M_0\rangle$, initial state M_0, label set T, and set of edges $\{(M, t, M') \mid M, M' \in [M_0\rangle \wedge M[t\rangle M'\}$. If a labelled transition system TS is isomorphic to the reachability graph of a Petri net N, we say that N *PN-solves* (or simply *solves*) TS, and that TS is *synthesisable* to N. We say that N solves a word w if it solves $TS(w)$. A word w is then called *solvable*, otherwise it is called *unsolvable*.

Solvability
Region theory constitutes the most common tool for proving solvability of labelled transition systems. Let $(S, \rightarrow, T, s_0)$ be an lts and $N = (P, T, F, M_0)$ be a Petri net, which we hope to synthesise. The synthesis comprises solving systems of linear inequalities in integer numbers. Those inequalities guaranty satisfiability of the following properties:

State separation property (*ssp* in short)
: For every pair $s, s' \in S$ of distinct states $(s \neq s')$ there exists a place $p \in P$ such that $M(p) \neq M'(p)$ for markings M and M' corresponding to s and s'.

Event/state separation property (*essp* in short)
: For every state-transition pair $s \in S$ and $t \in T$ with $\neg(s[t\rangle)$ there exists a place $p \in P$ such that $M(p) < F(p,t)$ for the marking M corresponding to state s.

Note that if the lts is defined by a word w then the state separation property is easy to satisfy by introducing a counter place. On the other hand, satisfiability of event/state separation property, for every state-transition pair $s \in S$ and $t \in T$ with $\neg(s[t\rangle)$, requires a place preventing t at s. In the case of binary word $w \in \{a,b\}^*$ such a place $p \in P$ is of the form depicted in figure 1.

[1] For compactness, in case of long formulas we write $|_r\, \alpha\, |_s\, \beta\, |_t$ instead of $r\ [\alpha\rangle\ s\ [\beta\rangle\ t$.

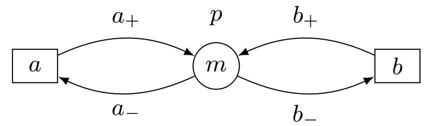


Fig. 1. A general form of a place p containing initially m tokens and preventing a transition (a or b) to satisfy essp.

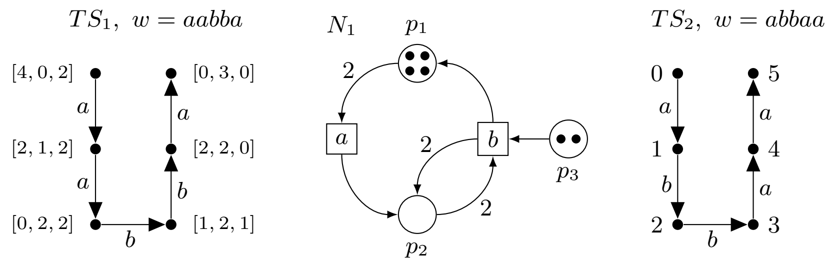


Fig. 2. N_1 solves TS_1. No solution of TS_2 exists.

The labelled transition systems TS_1 and TS_2 depicted in figure 2 correspond to the words *aabba* and *abbaa*, respectively. The former is PN-solvable, since the reachability graph of N_1 is isomorphic to TS_1, while the latter contains an unsolvable event/state separation problem (see [1] for detailed explanation). Note that word *abbaa*, isomorphic to TS_2, is the shortest binary word (modulo swapping a/b) which is not PN-solvable. However, its reverse (*aabba*) is solvable.

Minimal unsolvable words

If w is PN-solvable, then all of its subwords w' are. To see this, let the Petri net solving w be executed up to the state before w', take this as the new initial marking, and add a pre-place with $\#_a(w')$ tokens to a and a pre-place with $\#_b(w')$ tokens to b. Thus, the unsolvability of any proper subword of w entails the unsolvability of w. For this reason, the notion of a *minimal unsolvable word* (*muw* in short) is well-defined, namely, as an unsolvable word all of which proper subwords are solvable. A complete list of minimal unsolvable words up to length 110 can be found, amongst some other lists, in [10].

3 Structurel classification of minimal unsolvable words

Throughout this section we investigate possible shapes of minimal unsolvable words in details. In [1,2] some necessary and some sufficient properties of solvable and of unsolvable words have already been described. In this section we shall provide known facts about minimal unsolvable words, which are true modulo swapping a and b, only in one form for the sake of succinctness. From these facts we then deduce some important restrictions for the possible shapes of those words.

Proposition 1. [1] SUFFICIENT CONDITION FOR UNSOLVABILITY

If a word over $\{a, b\}$ has a subword of the form (1)*, then it is not PN-solvable.*

$$\boxed{(\ a\ b\ \alpha\ )\ b^*\ (\ b\ a\ \alpha\ )^+\ a\ , \qquad \textit{with } \alpha \in T^*} \tag{1}$$

Remark: Let us notice that for a fixed α the language described by the expression $(ab\alpha)b^*(ba\alpha)^+a$ is regular. However in our case α is an arbitrary but fixed binary word and we consider all words of the form (1) for all possible α's. The language obtained this way is obviously not regular (nor even context-free).

In the following, $u, v \in \{a, b\}^*$. For a decomposition $w = u|_s av$, let us call b *separable at s* iff we can construct a Petri net with transitions a and b and one place p such that w can be fired completely and at s, b is not enabled. In the present paper, we rely on the main result proved in a companion paper [2], which will here be used in the following form:

Lemma 1. [2] CHARACTERISATION OF SEPARABLE STATES

For a word $w \in \{a, b\}^*$ let $w = u|_s av$ be an arbitrary decomposition. Then, b is separable at s iff $\forall_{\alpha,\beta,\gamma,\delta}\ (w = \alpha b\beta|_s a\gamma b\delta \ \Rightarrow\ \#_b(b\beta)\cdot\#_a(a\gamma) > \#_a(b\beta)\cdot\#_b(a\gamma))$.

Besides these general structural restrictions, there are known conditions for (un)solvability, which allow to restrict possible shapes of minimal unsolvable words being applied step by step.

Proposition 2. [1] SOLVABILITY OF av AND vb IMPLIES SOLVABILITY OF avb

If both av and vb are solvable, then avb is also solvable.

This implies that each minimal unsolvable word either starts and ends with a or starts and ends with b. Also, if a muw w starts (and ends) with a then b is always separated in w.

Lemma 2. b IS ALWAYS SEPARATED IN MUW $a\alpha$

If w is muw and starts with a, there is no violations of *essp* for b in w.

From the following fact we get that minimal unsolvable word either starts with ab or with ba.

Proposition 3. [1] SOLVABLE WORD CAN BE PREFIXED BY STARTING LETTER

If a word av is PN-solvable then aav is, too.

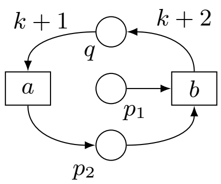
Let w be a minimal unsolvable binary word. We now have two possible cases: either w ends with a single a (or b), or it has many (more than one) a's (b's, respectively) at the end. So far we know $\boxed{w = abua \text{ (or } w = baub).}$ Due to the following statement, we get bu (or au, respectively) either has no aa or no bb.

Proposition 4. [1] NO aa AND bb INSIDE A MINIMAL UNSOLVABLE WORD

If a minimal non-PN-solvable word is of the form $w = a\alpha a$, then either α does not contain the factor aa or α does not contain the factor bb.

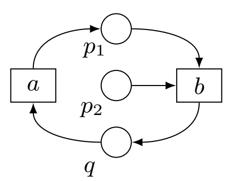
Assume, bu has neither factors aa nor bb inside. The following two cases for a muw w are possible: $\boxed{ab(ab)^k aa \quad \text{or} \quad ab(ab)^k a, \quad \text{where } k \geq 0}$

Petri nets N_1 and N_2 in figure 3 solve the first and the second of these forms, respectively. From proposition 4 and this observation we deduce that, in minimal unsolvable word $w = a\alpha a$, α has either the factor aa or the factor bb, but never both.



$m\begin{pmatrix} p_1 \\ p_2 \\ q \end{pmatrix} = \begin{pmatrix} k+1 \\ 0 \\ k+1 \end{pmatrix}$;

N_1



$m\begin{pmatrix} p_1 \\ p_2 \\ q \end{pmatrix} = \begin{pmatrix} 0 \\ k+1 \\ 1 \end{pmatrix}$

N_2

Fig. 3. N_1 solves $ab(ab)^k aa$. N_2 solves $ab(ab)^k a$.

Thus, w has one of the following forms (modulo a/b), where $x_i > 0$ for $1 \leq i \leq n$:

1. $ab^{x_1}ab^{x_2}a \ldots ab^{x_n}a$: starts and ends with a, single a at the end, no aa;
2. $aba^{x_1}ba^{x_2}b \ldots ba^{x_n}ba$: starts and ends with a, single a at the end, no bb;
3. $ab^{x_1}ab^{x_2}a \ldots ab^{x_n}aa$: starts and ends with a, many a at the end, no aa inside;
4. $aba^{x_1}ba^{x_2}b \ldots ba^{x_n}a$: starts and ends with a, many a at the end, no bb.

All those patterns can be comprised into the following three general forms of muw w (modulo swapping a/b and with bb appearing inside):

$$ab^{x_1}ab^{x_2}a \ldots ab^{x_n}a \quad \text{with } x_i > 0 \text{ for } 1 \leq i \leq n, \quad \text{for 1;} \tag{2}$$

$$bab^{x_2}ab^{x_3}a \ldots ab^{x_n} \quad \text{with } x_i > 0 \text{ for } 2 \leq i \leq n, \quad \text{for swapped 2, 4;} \tag{3}$$

$$ab^{x_1}ab^{x_2}a \ldots ab^{x_n}aa \quad \text{with } x_i > 0 \text{ for } 1 \leq i \leq n, \quad \text{for 3.} \tag{4}$$

In the rest of this section we will try to figure out these forms more precisely.

Consider first the form (4): $w = ab^{x_1}ab^{x_2}a \ldots ab^{x_n}aa$ with $x_i > 0$ for $1 \leq i \leq n$. Since w necessarily has bb as a factor, $x_i \geq 2$ for some $1 \leq i \leq n$. If $n = 1$ then $x_1 \geq 2$. We shall prove now that if $n > 1$ then $x_1 = 2$, $x_2 = \ldots = x_n = 1$. Let $j = \max\{1 \leq i \leq n \mid x_i \geq 2\}$. For the subword $v = \underbrace{ab^{x_j - 1}}_{\alpha} | \underbrace{ba \ldots aba}_{\beta} a$ of w, where $x_j \geq 2$ and $x_{j+1} = \ldots = x_n = 1$, we have $\#_a(\beta) \cdot \#_b(\alpha) = (n - j + 1) \cdot (x_j - 1) \geq 1 \cdot (n - j + 1) = \#_a(\alpha) \cdot \#_b(\beta)$, implying v is not solvable, due to lemma 1. If $j > 1$, v is a proper subword of w, which contradicts minimal unsolvability of w. Hence, $x_i \leq 1$ for $i > 1$. Thus, there are two possibilities for w of the form (4):

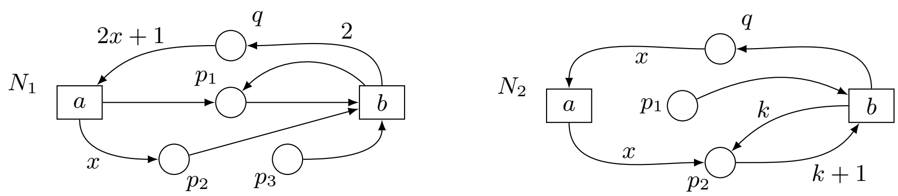
$$\boxed{ab^x aa, \text{ with } x > 2 \quad \text{or} \quad abb(ab)^k aa, \text{ with } k \geq 0} \tag{4'}$$

To understand shapes (2) and (3), the following *balancing property* will be useful.

Lemma 3. [2] Block lengths differ by at most 1

Let $w \in a^*b^+(ab^+)^*(a|\varepsilon)$ be a word that contains both bab^xa and abb^xb with $x \geq 1$ as subwords. Then, w is not solvable.

Let us now study pattern (2). It is easy to see that words corresponding to pattern (2) are solvable for $n = 1$. Consider the partial instance, $n = 2$, of this pattern. The words of the following two classes $\boxed{ab^{x+1}ab^xa \quad \text{or} \quad ab^{x-k}ab^xa \quad \text{with } 0 \leq k < x,}$ are solvable, and Petri nets N_1 and N_2 in figure 4 are possible solutions for words of the first and of the second of these forms, respectively. Thus, if $w = ab^{x_1}ab^{x_2}a$ is minimal unsolvable, then $x_1 - x_2 \geq 2$.



$$m\begin{pmatrix} p_1 \\ p_2 \\ p_3 \\ q \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 2x+1 \\ 2x+1 \end{pmatrix} \qquad\qquad m\begin{pmatrix} p_1 \\ p_2 \\ q \end{pmatrix} = \begin{pmatrix} 2x-k \\ 0 \\ x+k \end{pmatrix}$$

Fig. 4. N_1 solves $ab^{x+1}ab^xa$. N_2 solves $ab^{x-k}ab^xa$.

Lemma 4. [1] Side-place-free solvability with few initial b's

If $u = b^{x_1}ab^{x_2}a \ldots ab^{x_n}a$ is solvable and $x_1 \leq \min\{x_2, \ldots, x_n\}$, then u is solvable side-place-freely.

Lemma 5. [1] Solving au from u

Suppose $u = b^{x_1}ab^{x_2}a \ldots ab^{x_n}a$ is solvable side-place-freely. Then au is solvable.

Consider an arbitrary minimal unsolvable word $w = ab^{x_1}ab^{x_2}a \ldots ab^{x_n}a$ of the form (2) with $n \geq 3$, $x_i > 0$ for $1 \leq i \leq n$. Let $x = \min\{x_i \mid 2 \leq i \leq n\}$. Due to lemma 3, $x_i \in \{x, x+1\}$ for $2 \leq i \leq n$, and then $x_1 \leq x+2$. If $x_1 < x+1$, by lemmata 4 and 5, the word w is solvable, contradicting the choice. Hence, $x+1 \leq x_1 \leq x+2$, and $\min\{x_i \mid 1 \leq i \leq n\} = x$. We now show $x_n = x$. Two cases are possible:
Case 1: $x_1 = x+2$. If $x_n = x+1$, then $x_j = x$ for some $1 < j < n$, which by lemma 3 contradicts the minimality of w. Hence, $x_n = x$, and w follows the pattern $ab^{x+2}a(b^{x+1}a)^+b^xa$.
Case 2: $x_1 = x+1$. By contraposition, assume $x_n = x+1$. Then, $x_j = x$ for some $2 \leq j \leq n-1$. Let $j_1 = \max\{j \mid x_j = x\}$. Assume a is not separated from some state s_k in w (b is separated by lemma 2). If $k < j_1$, then, by lemma 1, for

$$w \;=\; \underbrace{a\, b^{x_1}\, a \ldots a\, b^{x_k-1}}_{\alpha} |_{s_k} \; \underbrace{\overbrace{b\, a \ldots\, b^{x_{j_1}}}^{\beta'}\; a \ldots\; b^{x_n}}_{\beta}\; a$$

we have

$$\#_a(\beta) \cdot \#_b(\alpha) \geq \#_a(\alpha) \cdot \#_b(\beta) \quad \Longleftrightarrow \quad \frac{\#_b(\alpha)}{\#_a(\alpha)} \geq \frac{\#_b(\beta)}{\#_a(\beta)},$$

where $\#_a(\alpha) \neq 0$ by the form of w, and $\#_a(\beta) \neq 0$ due to $j_1 \leq n-1$. From the choice of j_1, $\#_b(\beta) \big/ \#_a(\beta) \geq \#_b(\beta') \big/ \#_a(\beta')$, implying

$$\frac{\#_b(\alpha)}{\#_a(\alpha)} \geq \frac{\#_b(\beta)}{\#_a(\beta)} \geq \frac{\#_b(\beta')}{\#_a(\beta')} \quad \Longrightarrow \quad \#_a(\beta') \cdot \#_b(\alpha) \geq \#_a(\alpha) \cdot \#_b(\beta').$$

According to lemma 1, this means unsolvability of the proper subword $\alpha\beta' a$ of w, which contradicts minimality of w. Assume now $k \geq j_1$. Then in

$$w \;=\; \underbrace{a\, b^{x_1}\; a\; \ldots a\, b^{x_{j_1}}\; a\; \ldots\; b^{x_k - 1}}_{\alpha} |_{s_k} \; \underbrace{b\; a\; \ldots\; b^{x_n}}_{\beta}\; a,$$

by lemma 1, we have

$$\#_a(\beta) \cdot \#_b(\alpha) \geq \#_a(\alpha) \cdot \#_b(\beta) \quad \Longleftrightarrow \quad \frac{\#_b(\alpha)}{\#_a(\alpha)} \geq \frac{\#_b(\beta)}{\#_a(\beta)},$$

where $\#_a(\alpha) \neq 0$ by the form of w, and $\#_a(\beta) \neq 0$ because a can be separated "inside" the last group of b's with a place p having $\#_b(w) \cdot n$ tokens on it initially, the weight of the arc from p to a is $\#_b(w)$, and the weight of the arc from b to p is 1. On the other hand, thanks to the choice of x_{j_1}, we have $x+1 > \#_b(\alpha) \big/ \#_a(\alpha)$ and $\#_b(\beta) \big/ \#_a(\beta) > x+1$, which is a contradiction. Hence, $x_n = x$.

From the consideration above we can deduce that all minimal unsolvable words of the form (2) match one of the following three refined patterns

$$\boxed{\begin{array}{l} ab^{x+k}ab^{x}a, \text{ with } x > 0,\ k > 2 \quad \text{or} \\ ab^{x+2}(ab^{x+1})^{*}ab^{x}a, \text{ with } x > 0 \quad \text{or} \\ ab^{x_1}ab^{x_2}a \ldots ab^{x_n}a, \text{ with } x_1 = x+1,\ x_n = x,\ x_i \in \{x, x+1\} \text{ for } x > 0,\ n \geq 3 \end{array}} \tag{2'}$$

The last pattern to be studied in details is (3). Binary words of the form (3) are obviously solvable for $n = 2$. We now consider arbitrary minimal unsolvable word $w = bab^{x_2}ab^{x_3}a \ldots ab^{x_n}$ with $n \geq 3$ and $x_i > 0$ for $2 \leq i \leq n$ of the form (3). Let $x = \min\{x_i \mid 2 \leq i \leq n-1\}$. Due to lemma 3, $x_i \in \{x, x+1\}$ for all $2 \leq i \leq n-1$, and then $x_n \leq x+2$. Assume $x_n \leq x$. Consider state s in w

$$w \;=\; \underbrace{b\; a\; b^{x_2}\; a \ldots\; a\; b^{x_k}}_{\alpha}\; |_s\; \underbrace{\overbrace{a\; \ldots\; b^{x_{n-1}-1}}^{\beta'}\; b\; a\; b^{x_n - 1}}_{\beta}\; b,$$

from which b is not separated (a is always separated by lemma 2). b can be separated from the state right after the first b with a place p having an arc from a to p with weight $\max\{x_i \mid 2 \leq i \leq n\}$, an arc from p to b with weight 1, and initially 1 token on it. Hence, $k \neq 1$. Transition b can easily be separated at the very end of w by an input place p of b, having $\#_b(w)$ tokens on p initially. Hence, $k \neq n$. If $k = n-1$, we have

$$\#_a(\alpha) \cdot \#_b(\beta) = (n-2) \cdot (x_n - 1) < 1 \cdot (1 + x_2 + \ldots + x_{n-1}) = \#_a(\beta) \cdot \#_b(\alpha),$$

which, due to the minimal unsolvability of w, contradicts lemma 1. Hence, $k < n-1$. From lemma 1, because of minimal unsolvability of w, we have

$$\#_a(\alpha) \cdot \#_b(\beta) \geq \#_a(\beta) \cdot \#_b(\alpha) \quad \Longleftrightarrow \quad \frac{\#_b(\beta)}{\#_a(\beta)} \geq \frac{\#_b(\alpha)}{\#_a(\alpha)},$$

where $\#_a(\beta) \neq 0$ because of $k < n-1$, and $\#_a(\alpha) \neq 0$ due to $k > 1$. Since we assumed $x_n \leq x$,

$$\frac{\#_b(\beta')}{\#_a(\beta')} \geq \frac{\#_b(\beta)}{\#_a(\beta)} \quad \Longleftrightarrow \quad \#_a(\alpha) \cdot \#_b(\beta') \geq \#_a(\beta') \cdot \#_b(\alpha).$$

Due to lemma 1, $\alpha\beta' b$ is not solvable. Since it is a proper subword of w, we get a contradiction to the minimality of w. Thus $x+1 \leq x_n \leq x+2$. We now demonstrate $x_2 = x$. Consider two possible cases:

Case 1: $x_n = x+2$. Take $j = \max\{i \mid x_i = x\}$. Then for the subword u

$$u \;=\; \underbrace{b\;a\;b^{x_j}\;(a\;b^{x+1})^k}_{\alpha} \;|_s\; \underbrace{a\;b^{x_n-1}}_{\beta}\;b.$$

of w with $k \geq 0$, the following inequality is satisfied

$$\#_b(\beta) \cdot \#_a(\alpha) = (x+1) \cdot (k+1) \geq (1 + x + (x+1) \cdot k) \cdot 1 = \#_b(\alpha) \cdot \#_a(\beta).$$

This means u is unsolvable. If $j > 2$, u is a proper subword of w, contradicting minimality of w. Hence, in this case $x_2 = x$, $x_i = x+1$ for $2 < i < n$.

Case 2: $x_n = x+1$. Let $j_1 = \min\{i \mid x_i = x\}$. By the definition of x, $j_1 \neq n$. By contraposition, assume $x_2 = x+1$. Consider state s_k in w after the group of b^{x_k}, such that b is not separated at s_k (a is always separated by lemma 2). If $k > j_1$, then, by lemma 1, for

$$w \;=\; \underbrace{b\;a\;b^{x_2}\;a\;b^{x_3-1}\;\overbrace{b\;a\;\ldots\;b^{x_{j_1}}\;a\;\ldots\;b^{x_k}}^{\alpha'}}_{\alpha} \;|_{s_k}\; \underbrace{a\;\ldots\;b^{x_n-1}}_{\beta}\;b$$

the following inequality holds

$$\#_b(\beta) \cdot \#_a(\alpha) \geq \#_a(\beta) \cdot \#_b(\alpha) \quad \Longleftrightarrow \quad \frac{\#_b(\beta)}{\#_a(\beta)} \geq \frac{\#_b(\alpha)}{\#_a(\alpha)},$$

where $\#_a(\beta) \neq 0$ by the choice of s_k, $\#_a(\alpha) \neq 0$ due to the fact b can be separated from the state after the first b. As $x_2 = x+1$ and $x_{j_1} = x$, we have $\#_b(\alpha) \big/ \#_a(\alpha) \geq \#_b(\alpha') \big/ \#_a(\alpha')$. From

$$\frac{\#_b(\beta)}{\#_a(\beta)} \geq \frac{\#_b(\alpha')}{\#_a(\alpha')} \quad \Longrightarrow \quad \#_b(\beta) \cdot \#_a(\alpha') \geq \#_a(\beta) \cdot \#_b(\alpha'),$$

according to lemma 1, it follows that the proper subword $\alpha'\beta b$ of w is unsolvable, contradicting minimality of w. Suppose $k \leq j_1$. Then, by lemma 1, for

$$w \;=\; \underbrace{b\;a\;b^{x_2}\;a\;\ldots\;b^{x_k}}_{\alpha}\;|_{s_k}\;\underbrace{a\;\ldots\;b^{x_{j_1}-1}\;b\;a\;\ldots\;b^{x_n-1}}_{\beta}\;b$$

the following inequality is satisfied

$$\#_b(\beta) \cdot \#_a(\alpha) \geq \#_a(\alpha) \cdot \#_b(\beta) \quad \Longleftrightarrow \quad \frac{\#_b(\beta)}{\#_a(\beta)} \geq \frac{\#_b(\alpha)}{\#_a(\alpha)},$$

with $\#_a(\beta) \neq 0$ thanks to the special form of the word, and $\#_a(\alpha) \neq 0$ due to $k < n$. On the other hand, due to $x_n = x+1$ and by the choice of j_1, we have $x+1 > \#_b(\beta) \big/ \#_a(\beta)$, and $\#_b(\alpha) \big/ \#_a(\alpha) > x+1$, which is a contradiction. Thus, $x_2 = x$, and we deduce the following refinement of pattern (3)

$$\boxed{\begin{array}{l} bab^x(ab^{x+1})^*ab^{x+2}, \text{ with } x > 0 \quad \text{ or} \\ bab^{x_2}ab^{x_3}a\ldots ab^{x_n}, \text{ with } x_2 = x,\ x_n = x+1,\ x_i \in \{x, x+1\} \text{ for } x > 0,\ n \geq 3 \end{array}} \tag{3'}$$

Notice that sets of words generated by all patterns (2')-(4') are mutually disjoint. In the following section we divide them into classes of extendable and non-extendable words.

4 Generative nature of minimal unsolvable binary words

In this section we provide a complete characterisation of minimal unsolvable binary words. The general idea is to split the whole set into two classes: extendable (which are origins for more complex minimal unsolvable words) and non-extendable (which might be also seen as origins of more complex unsolvable, but not minimal, binary words). In the former class we distinguish the simplest extendable muw's, i.e. the words in which the factor α from (1) is of the form a^i or b^i. Such words are called base extendable. After introducing the class of base extendable words, we provide an extension operation based on simple morhisms, which are prefix codes. The code nature is used in subsequent section, where we define the converse procedure, called compression.

4.1 Base extendable and non-extendable words

The following definitions must be understood modulo swapping a/b.

Definition 1. Base extendable words
A word $u \in \{a,b\}^*$ is called *base extendable* if it is of the form

$$\begin{aligned} &abw(baw)^k a \ \text{ with } \ w = b^j,\ j > 0,\ k \geq 1, \quad \text{or} \\ &baw(abw)^k b \ \text{ with } \ w = b^j,\ j \geq 0,\ k \geq 1. \end{aligned} \tag{5}$$

The class of base extendable words is denoted by $\mathcal{BE}$. □ 1

Definition 2. Non-extendable words
A word $u \in \{a,b\}^*$ is called *non-extendable* if it is of the form

$$abb^j b^k bab^j a \ \text{ with } \ j \geq 0,\ k \geq 1.$$

The class of all non-extendable words is denoted by $\mathcal{NE}$. □ 2

We now establish that all words from classes $\mathcal{BE}$ and $\mathcal{NE}$ are minimal unsolvable.

Lemma 6. Minimal unsolvability of base extendable and non-extendable words
If w belongs to class $\mathcal{BE}$ or $\mathcal{NE}$, then it is unsolvable and minimal with that property.

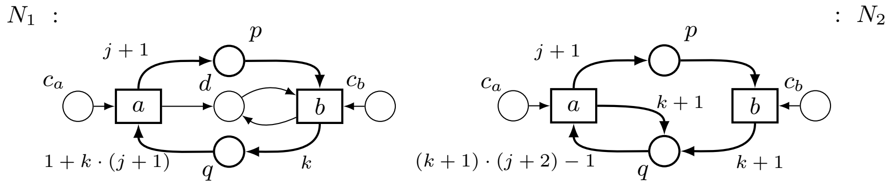
Proof: Let us notice that a word w is a muw if and only if w is unsolvable and every proper prefix and every proper suffix of w is solvable. Every word w from $\mathcal{BE} \cup \mathcal{NE}$ is of the form 1, hence unsolvable. We shall prove the minimality of w by indicating Petri nets solving its proper prefix and suffix.

CASE 1 (base extendable words):

(a) $w = abb^j(bab^j)^k a$

Consider first an arbitrary (modulo swapping a/b) base extendable word of the form $w = abb^j(bab^j)^k a$ with $j \geq 0$ and $k \geq 1$. This form satisfies (1) with $\alpha = b^j$, the star * being repeated zero times, and the plus $^+$ being repeated k times. Due to proposition 1, all binary words of this form are unsolvable.

The maximal proper prefix $abb^j(bab^j)^k$ of this word can be solved by Petri net N_1 in figure 5. Place q in this net enables the initial a, and then disables it unless b has been fired $j+2$ times. After the execution of block bb^jb there are $k-1$ tokens more than a needs to fire on place q. These surplus tokens allow a to be fired after each sequence b^jb, but not earlier. Place p has initially 1 token on it, which is necessary to execute block bb^jb after the first a, and this place has only $j+1$ tokens after each next a, preventing b at states where a must occur. Place d



$$M\begin{pmatrix} p \\ q \\ d \\ c_a \\ c_b \end{pmatrix} = \begin{pmatrix} 1 \\ 1+k\cdot(j+1) \\ 0 \\ k+1 \\ (j+1)(k+1) \end{pmatrix} \qquad M\begin{pmatrix} p \\ q \\ c_a \\ c_b \end{pmatrix} = \begin{pmatrix} j+2 \\ 0 \\ k+1 \\ (k+1)(j+1) \end{pmatrix}$$

Fig. 5. N_1 solves the prefix $abb^j(bab^j)^k$. N_2 solves the suffix $bb^j(bab^j)^k a$.

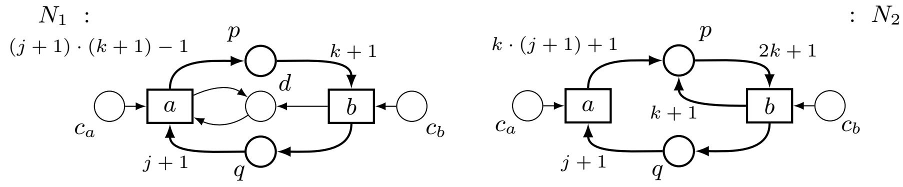
prevent premature occurence of b at the very beginning of the prefix, and places c_a and c_b restrict the total number of firings of a and b respectively.

For the general form of maximal proper suffix $bb^j(bab^j)^k a$ of w, one can consider Petri net N_2 on the right-hand side of figure 5 as a possible solution. Indeed, place q prevents premature occurrences of a in the first block $bb^j b$, and enables a only after this and each next block $b^j b$. Doing so, it collects one additional token after each $b^j b$, which allows this place to enable the very last a after sequence b^j. The initial marking allows to execute the sequence $bb^j b$ at the beginning, and at most $j+1$ b's in a row after that, thanks to place p. Place c_b restricts the total number of b's allowing only block b^j at the end. Thus we deduce that any word of the form $abb^j(bab^j)^k a$ with $j > 0$ and $k \geq 1$ is muw.

(b) $w = bab^j(abb^j)^k b$

We can similarly examine arbitrary (modulo swapping a/b) base extendable word of another form $w = bab^j(abb^j)^k b$ with $j \geq 0$ and $k \geq 1$. w satisfies (1) with swapped a and b, $\alpha = b^j$, the star * being repeated zero times, and the plus $^+$ being repeated k times. Due to proposition 1, all binary words of this form are unsolvable. Petri nets N_1 and N_2 in figure 6 are possible solutions for maximal proper prefix and for maximal proper suffix of w, respectively.

Remark (On special structure of Petri nets which solve prefixes and suffixes): Petri net N_1 in figure 5, which solves maximal proper prefix $abb^j(bab^j)^k$ of word $w = abb^j(bab^j)^k a$ from class $\mathcal{BE}$, has a special structure. Place d serves for preventing undesirable b in the very beginning of w, and places c_a and c_b restrict the total number of a and b, correspondingly. So, the internal structure of the word, being executed by N_1, is determined by two places p and q, which prevent when and only if the necessity b and a, respectively. In what follows, we will call the part of N_1 consisting of these two places (and transitions) a *core part* . So, Petri net N_2 if figure 5 has a core part made of places p and q. Similarly, such parts are formed by places p and q for both nets in figure 6. In future



$$M\begin{pmatrix} p \\ q \\ d \\ c_a \\ c_b \end{pmatrix} = \begin{pmatrix} k+1 \\ j+1 \\ 0 \\ k+1 \\ (k+1)(j+1) \end{pmatrix} \qquad M\begin{pmatrix} p \\ q \\ c_a \\ c_b \end{pmatrix} = \begin{pmatrix} 0 \\ j+2 \\ k+1 \\ (k+1)(j+1) \end{pmatrix}$$

Fig. 6. N_1 solves the prefix $bab^j(abb^j)^k$. N_2 solves the suffix $ab^j(abb^j)^kb$.

consideration we shall sometimes concentrate only on such core parts, as the other necessary places may be added in an uncomplicated way and does not influence the main behaviour of the nets.

CASE 2 (non-extendable words):

We now demonstrate that any (modulo swapping a/b) binary word of the form $w = abb^jb^kbab^ja$ with $j \geq 0$ and $k \geq 1$ from class $\mathcal{NE}$ is minimal unsolvable. w satisfies (1) with $\alpha = b^j$, the star * being repeated k times, and the plus $^+$ being repeated only once. Due to proposition 1, w is unsolvable. To show minimality of w, we provide Petri nets N_1 and N_2 (see figure 8) solving its maximal proper prefix and maximal proper suffix, respectively. $\square$ 6

Example 1. Let us consider a word $w = abbbaba$, which is of the form (1), with $\alpha = b$, the star * being repeated zero times, and the plus $^+$ being repeated just once. By definition 1, w is a base extendable word with $j = 1$ and $k = 1$. The word w is unsolvable (by proposition 1) and minimal with that property. We show the minimality by introducing Petri nets solving a proper prefix $abbbab$ and a proper suffix $bbbaba$ of w. Those Petri nets, constructed on the basis of the proof of lemma 6, are depicted in figure 7.

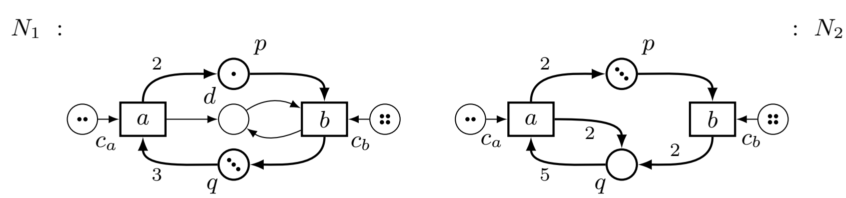
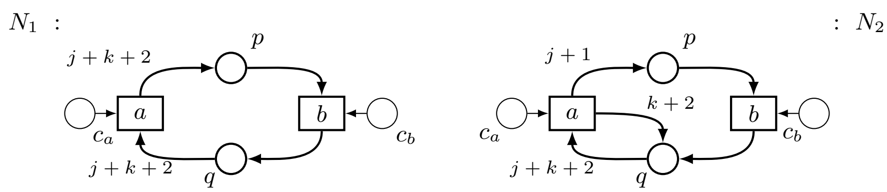


Fig. 7. N_1 solves the prefix $abbbab$. N_2 solves the suffix $bbbaba$.

Notice that both Petri nets contain core parts consisting of places p and q, which are responsible for the required behaviour of the nets, as well as auxiliary places – a delay place d and counter places c_a and c_b.



$$M\begin{pmatrix} p \\ q \\ c_a \\ c_b \end{pmatrix} = \begin{pmatrix} 0 \\ j+k+2 \\ 2 \\ 2\cdot(j+1)+k \end{pmatrix} \qquad M\begin{pmatrix} p \\ q \\ c_a \\ c_b \end{pmatrix} = \begin{pmatrix} j+k+2 \\ 0 \\ 2 \\ 2\cdot(j+1)+k \end{pmatrix}$$

Fig. 8. N_1 solves the prefix $abb^jb^kbab^j$. N_2 solves the suffix $bb^jb^kbab^ja$.

4.2 Extension operation and extendable words

Let us now explain how some minimal unsolvable words can be obtained from other minimal unsolvable words. For this purpose we use the following notion of *extension operation*:

Definition 3. Extension operation

For a word $u = xwx$ ($w \in \{a,b\}^*$, $x \in \{a,b\}$) an extension operation E is defined as follows:

$$E(awa) = \bigcup_{i=1}^{\infty} \Big\{abM_{a,i}(w)a^{i+1},\ aM_{b,i}(wa)\Big\},$$
$$E(bwb) = \bigcup_{i=1}^{\infty} \Big\{baM_{b,i}(w)b^{i+1},\ bM_{a,i}(wb)\Big\},$$

where $M_{a,i}$ and $M_{b,i}$ are morphisms defined as follows

$$M_{a,i} = \begin{cases} a \mapsto a^{i+1}b \\ b \mapsto a^ib \end{cases} \qquad \text{and} \qquad M_{b,i} = \begin{cases} a \mapsto b^ia \\ b \mapsto b^{i+1}a \end{cases}.$$

$\square$ 3

In what follows, for a given $w \in \{a,b\}^*$, we shall call $u \in E(w)$ an *extension* of w.

We are now ready to define a class of *extendable* minimal unsolvable words.

Definition 4. Extendable words

For a word $w \in \{a, b, \}^*$

1. if $w \in E(v)$ for some base extendable v, then w is extendable,
2. if $w \in E(v)$ for some extendable v, then w is extendable,
3. there are no other extendable words.

The class of all extendable words is denoted by $\mathcal{E}$. □ 4

Lemma 7. Unsolvability of extendable words

Let $u \in \{a, b\}^*$ be of the form $abv(bav)^k a$ or $bav(abv)^k b$ ($k > 0$). Then $E(u)$ is a set of PN-unsolvable words.

Proof: Let $u = abv(bav)^k a$ ($k > 0$). Then

$$\begin{aligned} E(u) = \bigcup_{i \in N} \Big\{ & aba^i b M_i^{(a)}(v) \Big(a^i b a^{i+1} b M_i^{(a)}(v) \Big)^k a^{i+1}, \\ & ab^{i+1} a M_i^{(b)}(v) \Big(b^{i+1} a b^i a M_i^{(b)}(v) \Big)^k b^i a \Big\} = \\ = \bigcup_{i \in N} \Big\{ & ab(a^i b M_i^{(a)}(v) a^i) \Big(ba(a^i b M_i^{(a)}(v) a^i) \Big)^k a, \\ & ab(b^i a M_i^{(b)}(v) b^i) \Big(ba(b^i a M_i^{(b)}(v) b^i) \Big)^k a \Big\} = \\ = \bigcup_{i \in N} \Big\{ & abv_i^{(a)} \Big(bav_i^{(a)} \Big)^k a, abv_i^{(b)} \Big(bav_i^{(a)} \Big)^k a \Big\}. \end{aligned}$$

Therefore, by proposition 1, $E(u)$ is a set of PN-unsolvable words. The case $u = bav(abv)^k b$ can be proved similarly. □ 7

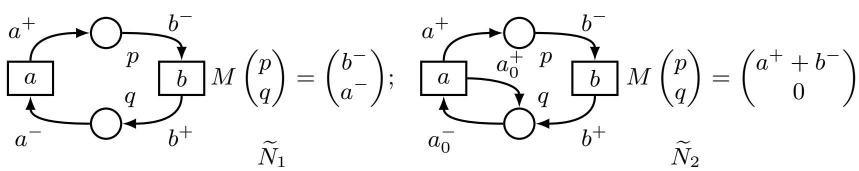


Fig. 9. Core parts of Petri nets: $\widetilde{N}_1$ for a net solving prefix, $\widetilde{N}_2$ for a net solving suffix.

Transformations of core part w.r.t. morphisms

As it has been demonstrated above, for every base extendable word w there are Petri nets N_1 and N_2, which solve maximal proper prefix w_1 and maximal proper suffix w_2 of w, respectively. These nets N_1 and N_2 have a special structure: so called "core" parts $\widetilde{N}_1$ and $\widetilde{N}_2$ (general patterns of $\widetilde{N}_1$ and $\widetilde{N}_2$ are depicted in figure 9) determine internal order of firings of a's and b's during execution of w_1 and w_2, while the remaining parts of N_1 and N_2 take responsibility of correct implementation of the beginnings and the ends of w_1 and w_2. Applying operation E to w, one can easily obtain new minimal unsolvable word w'. Moreover, applying appropriate transformation (which is determined by the particular morphism that has been used to gain w' from w) to $\widetilde{N}_1$ or to $\widetilde{N}_2$, one derives new core part $\widetilde{N}'_1$ or $\widetilde{N}'_2$, which correctly implements the internal structure of maximal proper prefix w'_1 or maximal proper suffix w'_2 of w', respectively. In table 1 the correspondence between morphisms from definition 3 and such transformations of nets is provided for general forms of $\widetilde{N}_1$ and $\widetilde{N}_2$. This fact is confirmed throughout the proof of the following lemma

	$M_{a,i}$	$M_{b,i}$
$\widetilde{N}_1$	$a^+ \longmapsto a^+ + b^-$	$a^+ \longmapsto a^+ + i \cdot (a^+ + b^-)$
	$b^- \longmapsto b^- + i \cdot (a^+ + b^-)$	$b^- \longmapsto a^+ + b^-$
	$b^+ \longmapsto b^+ + i \cdot (a^- + b^+)$	$b^+ \longmapsto a^- + b^+$
	$a^- \longmapsto a^- + b^+$	$a^- \longmapsto a^- + i \cdot (a^- + b^+)$
	$M(p) \longmapsto b^- + i \cdot (a^+ + b^-)$	$M(p) \longmapsto a^+ + b^-$
	$M(q) \longmapsto a^- + b^+$	$M(q) \longmapsto a^- + i \cdot (a^- + b^+)$
$\widetilde{N}_2$	$a^+ \longmapsto a^+ + b^-$	$a^+ \longmapsto a^+ + i \cdot (a^+ + b^-)$
	$b^- \longmapsto b^- + i \cdot (a^+ + b^-)$	$b^- \longmapsto a^+ + b^-$
	$b^+ \longmapsto b^+ + i \cdot (a_0^- + b^+ - a_0^+)$	$b^+ \longmapsto b^+ + a_0^- - a_0^+$
	$a_0^- \longmapsto a_0^- + b^+$	$a_0^- \longmapsto a_0^- + i \cdot (b^+ + a_0^- - a_0^+)$
	$a_0^+ \longmapsto a_0^+$	$a_0^+ \longmapsto a_0^+$
	$M(p) \longmapsto b^- + (i+1) \cdot (a^+ + b^-)$	$M(p) \longmapsto a^+ + (i+1) \cdot (a^+ + b^-)$
	$M(q) \longmapsto 0$	$M(q) \longmapsto 0$

Table 1. Correspondence between morphisms and transformations

Lemma 8. MINIMALITY OF EXTENDABLE WORDS

If $w \in \mathcal{E}$, then w is minimal unsolvable.

Proof: *(Sketch)* By lemma 7, any extendable word is unsolvable. According to definition 4, for every $w \in \mathcal{E}$ there is a sequence $w_0, w_1, \ldots, w_r$ such that $w_0 \in \mathcal{BE}$, $w_j \in \mathcal{E}$ and $w_j \in E(w_{j-1})$ for $1 \leq j \leq r$, and $w_r = w$. We will argument by induction on r, and check the existence of Petri nets, solving maximal proper prefix and suffix of w. Every base extendable word w_0 is minimal unsolvable, and there are Petri nets N_1^0 and N_2^0 with core parts and additional parts, which solve the maximal proper prefix and suffix of w_0. Suppose, for $1 \leq j \leq r-1$, there are Petri nets N_1^j and N_2^j doing similar job for w_j, and which have been obtained from N_1^{j-1} and N_2^{j-1}, respectively, with the appropriate transformation of core part. The particular morphism $M_{x,i}$ with $x \in \{a, b\}$, that has been used to derive w_j from w_{j-1}, determines this transformation uniquely. Inductive step consists of proving that N_1^r and N_2^r obtained from N_1^{r-1} and N_2^{r-1}, respectively, solve maximal proper prefix and suffix of w_r. Having morphism $M_{x,i}$, the transformation and two core parts (new and old), it can be directly checked that place p disables/enables transition b in prefix of w_{r-1} as a place of (core part of) N_1^{r-1} if one only if it does the same as the place of (core part of) N_1^r at the corresponding state in prefix of w_r. Similarly, for place q and transition

a, and also for suffixes of w_{r-1} and w_r with nets N_2^{r-1} and N_2^r. Additional parts of nets N_1^r and N_2^r can be implemented with a place "from initial to non-initial" transition, having zero tokens initially and "enough many" tokens after, and a place which is a simple counter for the (total) number of firings. □ 8

Let us note that the extension operation being applied to an extendable word, produces another extendable word which is unsolvable and minimal. On the other hand, from a non-extendable word this operation derives unsolvable but not minimal words.

Example 2. Observe again the word $w = abbbaba$. From the previous considerations (see example 1) we know that this words is base extendable, and therefore is a muw. By the application of the extension operation, using the morphism $M_{a,1} = \begin{cases} a \mapsto aab \\ b \mapsto ab \end{cases}$ we obtain a word $w_{a,1} = ab\,ababa\,ba\,ababa\,a$, which is of the form (1) with $\alpha = ababa$, the star * being repeated zero times, and the plus $^+$ being repeated just once, hence – by proposition 1 – unsolvable. On the basis of the Petri nets of figure 7, and according to table 1 we construct Petri nets (depicted in figure 10) solving the maximal proper prefix *abababababa...* *ababababaababa* and the maximal proper suffix *babababaababaa* of $w_{a,1}$. Thus, $w_{a,1}$ is a minimal unsolvable word.

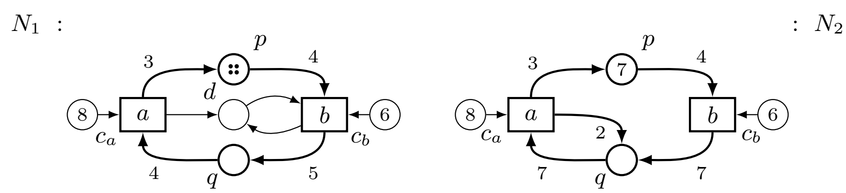


Fig. 10. N_1 solves the prefix *ababababaababa* and N_2 solves the suffix *babababaababaa* of $w_{a,1} = ababababaababaa$.

Lemma 9. Unsolvability of extensions of non-extendable words

If $w \in \mathcal{NE}$, then extension $u \in E(w)$ is unsolvable but not minimal unsolvable.

Proof: Argumentation modulo swapping a/b. Consider arbitrary $w \in \mathcal{NE}$, where $w = abb^j b^k bab^j a$ with $j \geq 0$, $k \geq 1$. Depending on a particular morphism $M_{x,i}$ with $x = a$ or $x = b$ for some $i \geq 1$, extension $u_x \in E(w)$ of $w = aw_1 a$ can be

$$u_a = aM_{a,i}(w_1)a^{i+1} = a\ a^i b\ (a^i b)^j\ (a^i b)^k\ a^i b\ a^{i+1} b\ (a^i b)^j\ a^{i+1} =$$
$$= a\ (a^i b)^{k-1}\ a^{i-1}\ ab\ \underbrace{a^i b\ (a^i b)^j\ a^i}_{\alpha_a} \mid ba\ \underbrace{a^i b\ (a^i b)^j\ a^i}_{\alpha_a}\ a,$$

or

$$u_b = aM_{b,i}(w_1a) = a\ b^{i+1}a\ (b^{i+1}a)^j\ (b^{i+1}a)^k\ b^{i+1}a\ b^ia\ (b^{i+1}a)^j\ b^ia =$$
$$= (ab^{i+1})^k\ ab\ \underbrace{b^ia\ (b^{i+1}a)^j\ b^i}_{\alpha_b} \mid ba\ \underbrace{b^ia\ (b^{i+1}a)^j\ b^i}_{\alpha_b}\ a$$

respectively. By proposition 1, word $ab\alpha_b ba\alpha_b a$ is unsolvable, which means unsolvability of u_b. Due to $k \geq 1$, $ab\alpha_b ba\alpha_b a$ is a proper subword of u_b. Hence, u_b is not minimal unsolvable. Analogously, unsolvability of $ab\alpha_a ba\alpha_a a$ implies non-minimal unsolvability of u_a. □ 9

5 Generation-based classification of minimal unsolvable words

Consider minimal unsolvable words w.r.t. the classification obtained earlier. All possible patterns from (2)–(4), and more precisely their refined variants from (2')–(4'), can be distinguished into base extendable

$ab(ba)^{k+1}a$, with $k \geq 0$, for the second pattern from (4'),

$abb^x(bab^x)^ka$, with $x > 0, k > 0$, for the second pattern from (2'),

$bab^x(abb^x)^kb$, with $x > 0, k > 0$, for the first pattern from (3'),

non-extendable

$abb^{x-1}baa$, with $x > 2$ for the first pattern from (4'),

$abb^xb^{k-1}bab^xa$, with $x > 0$, $k > 2$ for the first pattern from (2'),

and the rest, which we call $\mathcal{C}$ (*compressible*)

$ab^{x_1}ab^{x_2}a \ldots ab^{x_n}a$, with $x_1 = x+1$, $x_n = x$, $x_i \in \{x, x+1\}, x > 0$, $n \geq 3$, for the third pattern from (2'),

$bab^{x_2}ab^{x_3}a \ldots ab^{x_n}$, with $x_2 = x$, $x_n = x+1$, $x_i \in \{x, x+1\}, x > 0$, $n \geq 3$, for the second pattern from (3').

From this classification we derive that the class of all minimal unsolvable words $\mathcal{MUW} = \mathcal{BE} \cup \mathcal{NE} \cup \mathcal{C}$, where $\mathcal{BE}$, $\mathcal{NE}$ and $\mathcal{C}$ are mutually disjoint classes. Note, that since all words from class $\mathcal{E}$ are unsolvable and minimal with that property, and $\mathcal{E}$ is disjoint with $\mathcal{BE}$ and $\mathcal{NE}$, we have $\mathcal{E} \subseteq \mathcal{C}$.

5.1 Morphic compression and reducibility

In the previous section we showed how to construct new minimal unsolvable words on the basis of extendable words. The purpose of this section is to introduce an inverse transformation, which allows to compress longer minimal unsolvable words into shorter ones.

Definition 5. Compression function

For a word $v = xux$ ($u \in \{a,b\}^*$, $x \in \{a,b\}$) a *compression function* C is defined as follows:

$$\begin{aligned} C(abua^{i+1}) &= aM_{a,i}^{-1}(u)a, \quad C(baub^{i+1}) = bM_{b,i}^{-1}(u)b, \\ C(auba) &= aM_{b,i}^{-1}(uba), \qquad C(buab) = bM_{a,i}^{-1}(uab), \end{aligned} \tag{6}$$

where $i \geq 1$ and $M_{a,i}$, $M_{b,i}$ are morphisms defined as follows:

$$M_{a,i}^{-1} : \begin{cases} a^{i+1}b & \mapsto a \\ a^i b & \mapsto b \end{cases} \quad \text{and} \quad M_{b,i}^{-1} : \begin{cases} b^i a & \mapsto a \\ b^{i+1}a & \mapsto b. \end{cases}$$ □ 5

It is easy to see that among all possible forms from the classification of minimal unsolvable words, function C can only be applied to patterns from class $\mathcal{C}$. Moreover, the form of the word explicitly defines the particular morphism $M_{x,i}^{-1}$ which is used when applying C to the word. Let us also notice that since $\mathcal{E} \subseteq \mathcal{C}$, all words from class $\mathcal{E}$ are compressible with function C.

From definitions 3 and 5 it is clear that $M_{x,i}$ is reciprocal to $M_{x,i}^{-1}$ for $x \in \{a,b\}$, $i \geq 1$. The following lemma establishes that the extension operation E and the application of compression function C are complement to each other in the following sense

Lemma 10. Compression and extension functions

1. *If $v \in \mathcal{BE} \cup \mathcal{E}$ and $u \in E(v)$, then $C(u) = v$;*
2. *If $u \in \mathcal{C}$ and $v = C(u)$, then $u \in E(v)$.*

Proof: 1. Let $v = xv_1x$, where $x \in \{a,b\}$. Hence, for distinct $x, y \in \{a,b\}$ and $i \geq 1$, we have two possible cases:

- $u = xyM_{x,i}(v_1)x^{i+1}$. By compression function definition,
$$C(u) = C(xyM_{x,i}(v_1)x^{i+1}) = aM_{x,i}^{-1}(M_{x,i}(v_1))a = av_1a = v.$$
- $u = xM_{y,i}(v_1x)$. By compression function definition,
$$C(u) = C(xM_{y,i}(v_1x)) = C(xM_{y,i}(v_1)y^ix) = xM_{y,i}^{-1}(M_{y,i}(v_1)y^ix) = xv_1x = v.$$

2. W.l.o.g., u starts and ends with $x \in \{a,b\}$. Due to definition 5 of function C and class $\mathcal{C}$, u uniquely determines which compression morphism can be applied to it. Two cases are possible:

- $v = C(u) = xM_{x,i}^{-1}(u_1)x$ for $u = xyu_1x^{i+1}$, $x \neq y \in \{a,b\}$. Then,
$$E(v) = \bigcup_{j=1}^{\infty} \{xyM_{x,j}(M_{x,i}^{-1}(u_1))x^{i+1}, xM_{y,j}(M_{x,i}^{-1}(u_1)x)\}.$$
As $u = xyM_{x,j}(M_{x,i}^{-1}(u_1))x^{i+1}$ for $j = i$, hence $u \in E(v)$.
- $v = C(u) = xM_{y,i}^{-1}(u_1xy^ix)$ for $u = xu_1xy^ix$, $x \neq y \in \{a,b\}$. Then,
$$E(v) = \bigcup_{j=1}^{\infty} \{xyM_{x,j}(M_{y,i}^{-1}(u_1x))x^{i+1}, xM_{y,j}(M_{y,i}^{-1}(u_1xy^ix))\}.$$
As $u = xM_{y,j}(M_{y,i}^{-1}(u_1xy^ix))$ for $j = i$, hence $u \in E(v)$. □ 10

5.2 Compression of a muw is an unsolvable word

The following technical lemmata will be helpful in the further considerations.

Lemma 11. *Suppose $w = \alpha|_s b^{m-1}|_{\tilde{s}} ba\beta$, with $m \geq 1$. If a is not separable at state s, then it is not separable at state $\tilde{s}$, as well.*

Proof: By contrapostion, assume there is a Petri net $N = (P, T, F, M_0)$ with a place $p \in P$ such that w can be fired completely, and $M_{\tilde{s}}(p) < F(p, a)$. Since a is enabled at the state right after $\tilde{s}$, b effectively brings tokes on p. Hence, $M_s(p) \leq M_{\tilde{s}}(p) < F(p, a)$, i.e. a is separable at state s with place p, contradiction. $\square$ 11

Lemma 12. *If $w = ab^{x_1}ab^{x_2}a \ldots ab^{x_n}a$, with $x_1 = x+1$, $x_n = x$, $x_i \in \{x, x+1\}$, $x > 0$, $n \geq 3$, is a minimal unsolvable word, and separation failure occurs in group b^{x_k}, then $x_k = x + 1$.*

Lemma 13. *If $w = bab^{x_2}ab^{x_3}a \ldots ab^{x_n}$, with $x_2 = x$, $x_n = x+1$, $x_i \in \{x, x+1\}$, $x > 0$, $n \geq 3$, is a minimal unsolvable word, and separation failure occurs after group b^{x_k}, then $x_k = x$.*

Consider arbitrary minimal unsolvable word $w = aw_1 = ab^{x_1}ab^{x_2}a \ldots ab^{x_n}a$ from class $\mathcal{C}$, with $x_1 = x + 1$, $x_n = x$, $x_i \in \{x, x + 1\}$, $x > 0$, $n \geq 3$. According to the special form of w, compression function C can merely be applied to w in form $C(w = aw_1) = aM_{b,x}^{-1}(w_1)$. Note that $u = C(w)$ is also unsolvable. Due to lemma 12, for state s in

$$w = \underbrace{a\ b^{x_1}\ a\ \ldots\ a\ b^{x_k - 1}}_{\alpha}\ |_s\ \underbrace{b\ a\ \ldots\ a\ b^{x_n}}_{\beta}\ a,$$

from which a is not separated, we have $x_k = x + 1$. By lemma 1,

$$(n - k) \cdot (x_1 + x_2 + \cdots + x_k - 1) \geq k \cdot (x_{k+1} + \cdots + x_n + 1)$$

Assume, there are l groups of b^x in α (except the part of b^{x_k}), and m groups of b^x in β. Due to the form of w, we have $0 \leq l < k - 1$ and $0 < m \leq n - k$. Hence,

$$\begin{aligned}
&\#_a(\beta) \cdot \#_b(\alpha) \geq \#_a(\alpha) \cdot \#_b(\beta) \quad \Longleftrightarrow \\
&\Longleftrightarrow \quad (n - k) \cdot (k \cdot (x + 1) - l - 1) \geq k \cdot ((n - k) \cdot (x + 1) - m + 1) \quad \Longleftrightarrow \\
&\Longleftrightarrow \quad k \cdot l + k \cdot m - n \cdot l - n \geq 0.
\end{aligned}$$

After applying compression function to w, due to the definition of C and $M_{b,x}^{-1}$, for every sequence $b^x a$ and for every sequence $b^{x+1}a$ in w, we obtain a and b in u, respectively. Hence, u has $n + 1$ letters at all, starts with ab and ends with a thanks to the definition of C and the shape of w, and, by lemma 12, has b on $(k + 1)$-th position:

$$u \ = \ \underbrace{a\ b \ldots}_{\alpha'}\ |_{s'}\ \underbrace{b\ \ldots}_{\beta'}\ a,$$

where $|\alpha'| = k$, $|\beta'| = n - k$. Moreover, $\#_a(\alpha') = l$ and $\#_a(\beta') = m$. Thus, we have $\#_a(\beta') \cdot \#_b(\alpha') = m \cdot (k - l)$ and $\#_a(\alpha') \cdot \#_b(\beta') = l \cdot (n - k - m)$. Then,

$$\begin{aligned} \#_a(\beta') \cdot \#_b(\alpha') - \#_a(\alpha') \cdot \#_b(\beta') &= k \cdot l + k \cdot m - n \cdot l \geq \\ &\geq k \cdot l + k \cdot m - n \cdot l - n \geq 0. \end{aligned}$$

Due to lemma 1, this implies unsolvability of u.

Let now consider arbitrary minimal unsolvable word $w = bab^{x_2}ab^{x_3}a \dots ab^{x_n}$ from class $\mathcal{C}$, with $x_2 = x$, $x_n = x + 1$, $x_i \in \{x, x + 1\}$, $x > 0$, $n \geq 3$, and check that $u = C(w)$ is unsolvable as well. The form of w explicitly determines that $C(w = bw_1b^{x+1}) = bM^{-1}_{b,x}(w_1)b$. By lemma 13, for state s from which b is not separated in

$$w = \underbrace{b\ a\ b^{x_2}\ a\ \dots\ b^{x_k}}_{\alpha} |_s \underbrace{a\ b^{x_{k+1}}\ a\ \dots\ a\ b^{x_n-1}}_{\beta}\ b,$$

we have $x_k = x$. From lemma 1,

$$(k - 1) \cdot (x_{k+1} + \dots + x_n - 1) \geq (1 + x_2 + \dots + x_k) \cdot (n - k).$$

Assume, there are l groups of b^{x+1} in α and m groups of b^{x+1} in β. Due to the form of w, we have $0 \leq l < k$ and $0 \leq m \leq n - k$, and

$$\begin{aligned} &(k - 1) \cdot (x \cdot (n - k) + m) \geq (1 + x \cdot (k - 1) + l) \cdot (n - k) \iff \\ &\iff k \cdot m - m - n + k - l \cdot n + l \cdot k \geq 0. \end{aligned}$$

After applying compression function C to w, according to the definition of $M^{-1}_{b,x}$, for every sequence $b^{x+1}a$ and every sequence b^xa in w, we obtain a and b in u, respectively. Hence, u has n letters at all, starts with ba and ends with b, by definition of function C and special shape of w, and, by lemma 13, has a on k-th position:

$$u = \underbrace{ba\dots}_{\alpha'} |_{s'} \underbrace{a\dots}_{\beta'} b,$$

where $|\alpha'| = k - 1$, $|\beta'| = n - k$. Moreover, $\#_b(\alpha') = l$ and $\#_b(\beta') = m$. Thus, $\#_a(\alpha') \cdot \#_b(\beta') = (k - 1 - l) \cdot m$ and $\#_b(\alpha') \cdot \#_a(\beta') = l \cdot (n - k - m)$. Then,

$$\begin{aligned} \#_a(\alpha') \cdot \#_b(\beta') - \#_b(\alpha') \cdot \#_a(\beta') &= k \cdot m - m - l \cdot n + l \cdot k \geq \\ &\geq k \cdot m - m - l \cdot n + l \cdot k + k - n \geq 0. \end{aligned}$$

By lemma 1, this means u is unsolvable.

So far, we have shown that the compression of any word from $\mathcal{C}$ is unsolvable. Suppose that $\mathcal{C} \setminus \mathcal{E} \neq \emptyset$. Take some shortest word $u \in \mathcal{C} \setminus \mathcal{E}$ and let $w = C(u)$. Since w is unsolvable, two cases are possible:
Case 1: w is a minimal unsolvable word. Due to the choice of u as shortest in $\mathcal{C} \setminus \mathcal{E}$, and the fact that w is shorter than u, we have $w \notin \mathcal{C} \setminus \mathcal{E}$. Hence, w belongs

to one of disjoint classes $\mathcal{BE}, \mathcal{NE}, \mathcal{E}$. If $w \in \mathcal{BE}$ or $w \in \mathcal{E}$, then, by definition 4 and lemma 10, $u \in E(w) \subseteq \mathcal{E}$, which contradicts the choice of $u \in \mathcal{C} \setminus \mathcal{E}$. If $w \in \mathcal{NE}$, then by Lemma 9 $u \in E(w)$ is not a minimal unsolvable word, contradicting minimality of u.

Case 2: w is not a minimal unsolvable word. We shall prove that u is also not a minimal unsolvable word. Assume now, $w = w_1 v w_2$, where v is a minimal unsolvable word and $w_1 w_2 \neq \epsilon$, and that w has been obtained from u using compression morphism $M_{x,i}^{-1}$, where $x \in \{a, b\}$. Since v is a proper subword of w, and w is shorter than u, then $v \notin \mathcal{C} \setminus \mathcal{E}$. From the minimal unsolvability of v we have $v \in \mathcal{BE} \cup \mathcal{E} \cup \mathcal{NE}$. Hence, any extension v' of v is unsolvable (possibly not minimal in case $v \in \mathcal{NE}$). For $x \neq y$, where $x, y \in \{a, b\}$, we have either $v = x v_1 x$, or $v = y v_1 y$. Consider these two possibilities.

1. $v = x v_1 x$. In this case, according to definition 3, we consider extension $v' = xyM_{x,i}(v_1)x^{i+1} \in E(v)$. Suppose both w_1 and w_2 are non-empty words. Hence, $M_{x,i}(v) = x^{i+1}yM_{x,i}(v_1)x^{i+1}y$ is a proper subword of u. As v' is a subword of $M_{x,i}(v)$, we get a contradiction to the minimal unsolvability of u. Assume, $w_1 = \epsilon$. Then, being a proper prefix of w, after extension v will be morphed to $xyM_{x,i}(v_1)x^{i+1}y$, which again has v' as a subword, implying contradiction to the minimality of u. If $w_2 = \epsilon$, extension u of w with morphism $M_{x,i}$ has a proper subword $x^{i+1}yM_{x,i}(v_1)x^{i+1}$, and hence, contains v' as well. This contradicts minimal unsolvability of u.
2. $v = y v_1 y$. Let now $v' = yM_{x,i}(v_1 y) \in E(v)$. In case w_1 is non-empty word, $M_{x,i}(v) = x^i y M_{x,i}(v_1 y)$ is a proper subword of u, and contains v' as a factor. This contradicts minimality of u. If $w_1 = \epsilon$, u has v' as a proper prefix, which again contradicts minimal unsolvability of u.

Thus, $\mathcal{C} = \mathcal{E}$, which establishes the first of main results of the paper

Theorem 1. Generative nature of minimal unsolvable binary words

Let w be a minimal Petri net unsolvable binary word. Then we have the following exclusive alternatives:

- *w is a non-extendable word ($w \in \mathcal{NE}$),*
- *w is a base extendable word ($w \in \mathcal{BE}$),*
- *w is an extendable word ($w \in \mathcal{E}$).*

Generation of maximal partial solutions of minimal unsolvable words

In the last case of the alternative from theorem 1 (case $w \in \mathcal{E}$), applying function C to w consecutively, we can recover sequence of minimal unsolvable words $w_0, w_1, \ldots, w_r$, such that $w_0 \in \mathcal{BE}$, $w_r = w$, $w_i \in \mathcal{E}$ and $w_{i-1} = C(w_i)$ for $1 \leq i \leq r$. Moreover, starting from a word w_0, its maximal proper prefix and maximal proper suffix, and Petri nets solving them (in special forms, that have been provided in the paper), using appropriate transformations, we can derive Petri nets solving maximal proper prefix and maximal proper suffix of w_i for all $1 \leq i \leq r$.

Example 3. Let us consider word $v = ba\,aabaaabaa\,ab\,aabaaabaa\,b$. It is unsolvable by proposition 1, because it is of the form $ba\alpha\, a^*\,(ab\alpha)^+\,b$ (which is exactly the form (1) – modulo swapping a/b) with $\alpha = aabaaabaa$, the star * being repeated zero times, and the plus $^+$ being repeated just once. We now aim to compress v with function C. It can be easily seen that the word could be written in the form

$v = b(aaab)(aaab)(aaab)(aab)(aaab)(aab)$, hence we need to consider the morphism $M_{a,2}^{-1} : \begin{cases} aaab & \mapsto a \\ aab & \mapsto b \end{cases}$, and by the compression we obtain a word $v_{a,2}^{-1} = baaabab$. Let us notice that $v_{a,2}^{-1}$ is dual to the word $w = abbbaba$ (see example 1), modulo swapping a/b, hence it is a minimal unsolvable word. Function C cannot be applied to $w = C(v)$, which accord with the fact that $w \in \mathcal{BE}$.

Moreover, starting with the word $w = abbbaba$, together with Petri nets solving its proper prefix and suffix (see figure 7) and applying the morphism $M_{b,2}$: $\begin{cases} a & \mapsto bba \\ b & \mapsto bbba \end{cases}$ we obtain the word $w_{b,2} = ab\,bbabbbabb\,ba\,bbabbbabb\,a$ which is dual to v modulo swapping a/b. By the previous considerations we can easily construct Petri nets solving the maximal proper prefix and the maximal proper suffix of $w_{b,2}$, hence, by swapping letters we can obtain Petri nets for a proper prefix and a proper suffix of v. Such nets are depicted in figure 11. Now we can state that the word v is not only unsolvable, but also minimal with that property.

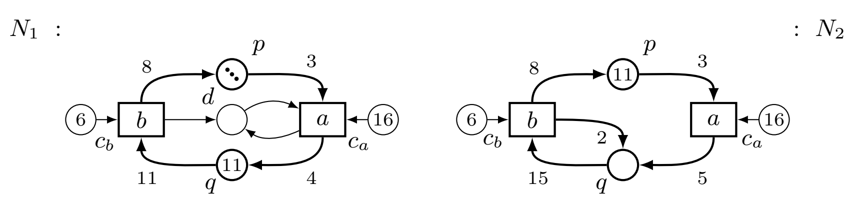


Fig. 11. N_1 solves the prefix $baaabaaabaaabaabaaabaa$ and N_2 solves the suffix $aaabaaabaaabaabaaabaab$ of $v = baaabaaabaaabaabaaabaab$.

6 Algorithm for checking unsolvability

The classification of minimal unsolvable words presented in sections 3 and 4 leads to an efficient algorithm for verifying solvability/unsolvability of a binary word. By definition 2 all non-extendable words are of the form (Ia) ab^xab^ya or (Ib) ba^xba^yb, where $x > y + 2$, $y \geq 0$, and by definition 1 and 3 all extendable words (including base extendable ones) are of the form (IIa) $abw(baw)^ka$ or (IIb) $baw(abw)^kb$, where $k \geq 1$ and $w \in \{a, b\}^*$.

Recall that a word $v \in \{a, b\}^*$ containing a minimal unsolvable word as a factor is also unsolvable. Moreover, due to theorem 1, v is unsolvable if it contains at least one of the patterns (Ia) (Ib), (IIa) or (IIb). Therefore, checking the solvability of a binary word can be reduced to a pattern-matching problem.

The algorithm described below takes a binary word v as an input and returns true if v is solvable and false otherwise (i.e. any of the above mentioned patterns was found inside v).

As the first step we search for the patterns (Ia) and (Ib). We scan the input word from left to right comparing the sizes of the two blocks of consecutive b's between any three consecutive occurrences of a and the sizes of the two blocks of consecutive a's between any three consecutive occurrences of b. This can be done in $O(n)$ time and $O(1)$ space.

The second step is to search for the patterns (IIa) and (IIb). It utilizes the Knuth-Morris-Pratt failure function called also the border table (see [6]). For any position i in v it contains the length of the longest factor u, which is at the same time a proper prefix and a proper suffix of $v[1..i]$. Such a factor is called a border of $v[1..i]$. For the relation between borders and periods of a word see for instance [7].

The search for the patterns (IIa) and (IIb) is performed as follows. For any possible pair of letters $v[i..i+1] = ab$ ($v[i..i+1] = ba$ respectively) we temporarily swap $v[i]$ with $v[i+1]$ and then build the border table for the suffix of v starting at position i. After discovering a repetition $v[i..j]$ (i.e. difference between j and the lenght of the border divides $j - i$) we check whether it is followed by a (b respectively) and report the occurrence of the pattern if needed.

The border table for a single suffix of the input word v can be constructed in $O(n)$ time and $O(n)$ space (see [6]). We have to process at most $O(n)$ suffixes of v, therefore the second step and the whole algorithm runs in $O(n^2)$ time and $O(n)$ space.

7 Conclusion

In this paper we studied the class of binary words which can not be generated by any injectively-labelled Petri net, and which are minimal with that property. We examined in detail all possible shapes of such words, obtaining extended regular expressions for them. The presented classification of minimal unsolvable words resulted in the construction of a pattern-matching based algorithm for checking the solvability/unsolvability for binary words. Moreover, we introduced the extension and compression functions, which could be foundations of a fixed-point procedure for the generation of the set of all minimal unsolvable binary words. The non-extendable and base extendable words are defined by simple parametrized formulas (see definitions 2 and 1). Choosing all possible values of the parameters j and k we can generate all non-extendable and base extendable words of a given length. Then by using recursive calls of extension and compression function we can generate all extendable words of a given length.

References

1. K. Barylska and E. Best and E. Erofeev and Ł. Mikulski and M. Piątkowski: On Binary Words Being Petri Net Solvable. **Proc. of ATAED** (2015).
2. E. Best, E. Erofeev, U. Schlachter, H. Wimmel: Characterising Petri Net Solvable Binary Words. Number 01/16 in Berichte aus dem Department für Informatik, pp. 1-20. Universität Oldenburg, January 2016. ISSN 1867-9218.
3. E. Badouel and L. Bernardinello and Ph. Darondeau: Petri Net Synthesis. **Springer** (2009).
4. B. Caillaud: `http://www.irisa.fr/s4/tools/synet` (2002).
5. C. Câmpeanu and K. Salomaa and S. Yu: A Formal Study Of Practical Regular Expressions **Int. J. Found. Comput. Sci.** 6(13) (2003)
6. T.H. Cormen, C.E. Leiserson, R.L. Rivest, C.Stein: Introduction to Algorithms (third edition). **The MIT Press** (2009).
7. M. Crochemore and L. Ilie and W. Rytter: Repetitions in strings: Algorithms and combinatorics **Theoretical Computer Science** 410(50) (2009).
8. M. Droste and R. M. Shortt: From Petri nets to automata with concurrency. **Applied Categorical Structures** 10.2 (2002).
9. C. Dufourd, A. Finkel and P. Schnoebelen: Reset nets between decidability and undecidability **Proc. of ICALP** (1998).
10. M. Piątkowski et al.: `http://folco.mat.umk.pl/unsolvable-words` (2015).
11. W. Reisig: Understanding Petri Nets - Modeling Techniques, Analysis Methods, Case Studies **Springer** (2013).
12. U. Schlachter et al.: `http://github.com/CvO-Theory/apt` (2013).

Appendix

Lemma 2. b IS ALWAYS SEPARATED IN MUW $a\alpha$
If w is a minimal unsolvable word and starts with a, there is no violations of essp *for b in w.*

Proof: By contraposition, assume $w = a \ldots |_s a \ldots a$, and b is not separated from state s. If there is no b in w before state s, b can be separated from s with place p having zero tokens initially, the weight of the arc from a to p is 1, and p being a side-condition for b with both arc having weight equal to the number of occurrences of a before the first b in w. Hence, there is at least one b before s. If there is no b after state s, one can separate b from s with an input place p for b, having $\#_b(w)$ tokens initially, and the weight of the arc from p to b equal to 1. Thus, there is at least one b after s in w. As b is not separable at s, for some decomposition $w = a\alpha b\beta|_s a\gamma b\delta$, by lemma 1, we have $\#_b(b\beta)\cdot\#_a(a\gamma) \leq \#_a(b\beta)\cdot\#_b(a\gamma)$. The inequality means that the proper subword $b\beta a\gamma b$ of w is unsolvable, contradicting minimality of w. $\square$

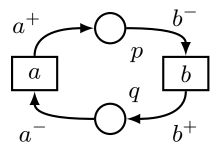
Lemma 8. MINIMALITY OF EXTENDABLE WORDS
If $w \in \mathcal{E}$, then w is minimal unsolvable.

Proof: Let $w \in \mathcal{E}$ be an arbitrary extendable word. By lemma 7, w is unsolvable. Let now check its minimality. According to definition 4, there is a sequence $w_0, w_1, \ldots, w_r$ such that $w_0 \in \mathcal{BE}$, $w_j \in \mathcal{E}$ and $w_j \in E(w_{j-1})$ for $1 \leq j \leq r$, and $w_r = w$. We will argument by induction on the length r of this sequence. From the previous consideration we know that the base extendable word w_0 is minimal unsolvable, and there are Petri nets N_1^0 and N_2^0 with core part and additional part, which are solutions for the maximal proper prefix and the maximal proper suffix of w_0. Assume now, that for every $1 \leq j \leq r-1$, there are Petri nets N_1^j and N_2^j which are solutions for the maximal proper prefix and the maximal proper suffix of w_j, and which have been obtained from N_1^{j-1} and N_2^{j-1}, respectively, with the appropriate transformation from table 1 (this transformation is uniquely defined by the particular morphism $M_{x,i}$ with $x \in \{a,b\}$, that has been used to derive w_j from w_{j-1}). We now prove, that knowing morphism $M_{x,i}$ with $x \in \{a,b\}$, which is used for producing w_r from w_{r-1}, and using the corresponding transformation, Petri nets N_1^r and N_2^r, which are derivatives of N_1^{r-1} and N_2^{r-1}, are indeed solutions for the maximal proper prefix and the maximal proper suffix of w_r.

Let us consider the case of producing N_1^r from N_1^{r-1}, when $w_{r-1} = aw'a$ and $w_r = aM_{b,i}(w'a)$, for some $i \geq 1$. Having the core part $\widetilde{N}_1^{r-1}$ (see figure 12) of the solution N_1^{r-1} for aw', with the transformations of the arcweights and the new initial marking

$$\begin{array}{lcl} a^+ & \longmapsto & a^+ + i\cdot(a^+ + b^-) \qquad b^- \longmapsto \quad a^+ + b^- \\ a^- & \longmapsto & a^- + i\cdot(a^- + b^+) \qquad b^+ \longmapsto \quad a^- + b^+ \\ m\begin{pmatrix} p \\ q \end{pmatrix} & = & \begin{pmatrix} a^+ + b^- \\ a^- + i\cdot(a^- + b^+) \end{pmatrix} \end{array} \tag{7}$$

$\widetilde{N}_1^{r-1}$:



$M\begin{pmatrix} p \\ q \end{pmatrix} = \begin{pmatrix} b^- \\ a^- \end{pmatrix}$;

Fig. 12. Core part of Petri net N_1^{r-1} solving maximal proper prefix of w_{r-1}.

for morphism $M_{b,i}$ we can construct the new core part $\widetilde{N}_1^r$ for aw'', where $aw''a = w_r$. Let now check, that the constructed core part implements the internal part of aw''. We shall show, place p prevents all undesirable b inside aw'' and enables all b that are to occur, and the similar for place q and transition a. Since we have used morphism $M_{b,i}$ for extension operation, we have a special form of extension $w_r = ab^{x_1}ab^{x_2}a \dots ab^{x_n}a \in E(w_{r-1})$, with $x_j \in \{i, i+1\}$. By contraposition, assume p disables some b that must occur at state s in $aw'' = ab^{x_1}a \dots ab^{x_k-m} \mid_s b^m a \dots$, where s is the leftmost state in aw'' with this property, and $k \geq 1$. By (7), each firing of a brings $a^+ + i \cdot (a^+ + b^-)$ tokens on place p, and b consumes $a^+ + b^-$ tokens on every its occurrence. Hence p can only disable the last but one b in a group b^{i+1}, i.e. $x_k = i+1$ and $m = 1$. Assume, there are l groups of b^{i+1} in $ab^{x_1}a \dots ab^{x_k-1} \mid_s$. By the initial assumption, marking of p at state s is less than the weight of the arc from p to b, i.e.

$$\begin{aligned} M_s(p) = (a^+ + b^-) + k \cdot (a^+ {+}\, i \cdot (a^+ + b^-)) - \\ -k \cdot i \cdot (a^+ + b^-) - l \cdot (a^+ + b^-) < a^+ + b^- \quad \iff \\ \iff \quad (k - l) \cdot a^+ {+} (1 - l) \cdot b^- < b^- \end{aligned}$$

On the other hand, the marking of place p in net $\widetilde{N}_1^{r-1}$, before applying transformation (7), at state s_1 of $w_{r-1} = a \dots |_{s_1} b \dots a$, where the b right after s_1 corresponds to the block $b^{x_k}a$ in w_r, is $M_{s_1}(p) = b^- + (k - l) \cdot a^+ - l \cdot b^-$, since every sequence $b^{i+1}a$ in w_r corresponds to b in w_{r-1}, and every sequence $b^i a$ corresponds to a. Hence, $M_{s_1}(p) < b^-$, which contradicts the assumption that the net $\widetilde{N}_1^{r-1}$ solves the word aw'. Thus, place p after transformation (7), allows all necessary occurrences of b. Notice here, that place p allows b to fire initially also.

We now have to show, p disables b at all states where a has to occur, except the initial one. Suppose a contrary, i.e. there is a state s in $aw'' = ab^{x_1}a \dots ab^{x_k} \mid_s a \dots ab^{x_n}$, with $k \geq 1$, such that $M_s(p) \geq a^+ + b^-$. W.l.o.g. let s to be the leftmost (except the initial) state with that property. Assume $x_k = i + 1$. Consider state s' in $ab^{x_1}a \dots \mid_{s'} ab^{x_k} \mid_s a \dots ab^{x_n}a$. Then

$$\begin{aligned} M_s(p) = M_{s'}(p) + a^+ {+}\, i \cdot (a^+ + b^-) - (i+1) \cdot (a^+ + b^-) \geq a^+ + b^- \quad \iff \\ \iff \quad M_{s'}(p) \geq b^- + (a^+ + b^-). \end{aligned}$$

The last inequality means that b is not separated at state s'. If $k = 1$, then, by (7), $M_{s'}(p) = M(p) = a^+ + b^-$, which contradicts the last inequality. If $k > 1$, then we get a contradiction to the choice of s. Hence, $x_k = i$. Let l be the number of blocks b^{i+1} in $ab^{x_1}a \dots ab^{x_k}|_s$. Then

$$\begin{aligned} M_s(p) = (a^+ + b^-) + k \cdot (a^+ + i \cdot (a^+ + b^-)) - \\ - k \cdot i \cdot (a^+ + b^-) - l \cdot (a^+ + b^-) \geq a^+ + b^- \quad \Longleftrightarrow \\ \Longleftrightarrow \quad (k - l) \cdot a^+ + (1 - l) \cdot b^- \geq b^-. \end{aligned}$$

Since w_r has been obtained using morphism $M_{b,i}$, sequence $b^{x_k}a$ corresponds to letter a in w_{r-1}. Therefore, in $w_{r-1} = a \dots |_{s_1} a \dots$, where s_1 fits the state right before $b^{x_k}a$ in w_r, we have b is not separated at state s_1, which contradicts the assumption that $\widetilde{N}_1^{r-1}$ solves aw'. Thus, in the net $\widetilde{N}_1^r$ that was derived from $\widetilde{N}_1^{r-1}$ by (7), p disables b whenever and only if it is necessary inside aw''.

For separating b at the initial marking, one can construct additional place p_1, having 0 tokens on it initially, and being a pure input place for transition b and pure output place for transition a with unit arcweights. For restricting the total number of occurrences of b, it is enough to construct place p_2 with $\#_b(w^r)$ tokens on it initially, which is a pure input place for b with the arcweight equal to 1.

Let us now consider place q and transition a. First we will show that q allows a to fire at each state where this is necessary. It is clear that initially q enables a. By contraposition, assume there is a state s in $aw'' = ab^{x_1}ab^{x_2}a \dots ab^{x_k} \mid_s ab^{x_{k+1}}a \dots$, with $k \geq 1$, such that q disables a at s. Due to (7), each firing of b brings $a^- + b^+$ tokens on q. Hence $x_k = i$. Suppose there are l blocks b^{i+1} in $ab^{x_1}a \dots ab^{x_k} \mid_s$. Then, we have

$$\begin{aligned} M_s(q) \ &= \ a^- + i \cdot (a^- + b^+) - k \cdot (a^- + i \cdot (a^- + b^+)) + \\ &+ k \cdot i \cdot (a^- + b^+) + l \cdot (a^- + b^+) < a^- + i \cdot (a^- + b^+) \quad \Longleftrightarrow \\ &\Longleftrightarrow \quad a^- + l \cdot b^+ - (k - l) \cdot a^- < a^- \end{aligned}$$

Due to the fact that $aw''a$ has been obtained from $aw'a$ using morphism $M_{b,i}$, block $b^{x_k}a$ corresponds to a right after the state s' in $w_{r-1} = a \dots \mid_{s_1} a \dots$. The last inequality means $M_{s_1}(q) < a^-$ which contradicts the assumption that $\widetilde{N}_1^{r-1}$ solves the word aw'. Thus, place q after the transformation (7) allows each mandatory firing of a.

We now demonstrate that q disables a at every place, where b has to occur. By contraposition, suppose there is a state s in $aw'' = ab^{x_1}a \dots ab^{x_k - m} \mid_s b^m a \dots$, with $k, m > 0$, at which a is enabled by place q. W.l.o.g. let s be the leftmost state in aw'' with that property. Due to the initial marking of q provided in (7), $k > 1$. Hence, for state s and place q we have

$$\begin{aligned} M_s(q) \ &= \ a^- + i \cdot (a^- + b^+) - k \cdot (a^- + i \cdot (a^- + b^+)) \\ &+ (x_1 + \dots + x_k - m) \cdot (a^- + b^+) \geq a^- + i \cdot (a^- + b^+) \end{aligned}$$

If $x_{k-1} = i$, then

$$\begin{aligned} M_{s_1}(q) \ &= \ a^- + i \cdot (a^- + b^+) - (k - 1) \cdot (a^- + i \cdot (a^- + b^+)) \\ &+ (x_1 + \dots + x_{k-1} - m) \cdot (a^- + b^+) \geq a^- + i \cdot (a^- + b^+) + a^- \end{aligned}$$

implying that a is enabled by q at state s_1 in $aw'' = ab^{x_1}a \dots ab^{x_{k-1}-m} \mid_{s_1} b^m a \dots$, which contradicts the choice of s. Then, $x_{k-1} = i + 1$. This means, the block $b^{x_k}a$ corresponds to letter b in $aw'a$, and state s in aw'' corresponds to the state s_0 in $aw' = a \dots \mid_{s_0} b \dots$. On the other hand,

$$\begin{aligned} M_s(q) &= a^- + i \cdot (a^- + b^+) - k \cdot (a^- + i \cdot (a^- + b^+)) \\ &\quad + (x_1 + \dots + x_k - m) \cdot (a^- + b^+) \geq a^- + i \cdot (a^- + b^+) \iff \\ &\iff \; a^- - (k - l) \cdot a^- + l \cdot b^+ \geq a^- + (m - 1) \cdot (a^- + b^+) \end{aligned}$$

Since $m \geq 1$, we have $M_{s_0}(q) \geq a^-$ in the net $\widetilde{N}_1^{r-1}$, implying that a is enabled at state s_0. This contradicts the fact that $\widetilde{N}_1^{r-1}$ solves aw'. Thus, q disables a at every state in aw'' where b has to occur.

Redundant occurrence of b at the very beginning of aw'', that is not handled by p, can be easily restricted by place p_1, having zero tokens initially, the arc weight from a to p_1 is $i + 1$ and the arc weight from p_1 to b is 1. The length of execution performed by $\widetilde{N}_1^r$ can be simply restricted with letter-counting place, having no inputs and a single output for each transition, and the initial number of tokens equal to the length of aw''. As the result, we have Petri net N_1^r, solving exactly aw'', with a core and additional part.

The other three possible cases from table 1 can be checked analogously. □

Lemma 10. *Suppose $w = ab^{x_1}a \dots ab^{x_n}a$ is a minimal unsolvable word. If a is not separated at some state s in $\dots ab^{x_k-m}|_s b^m a \dots$, then a is not separated at state $\tilde{s}$ in $\dots ab^{x_k-1}|_{\tilde{s}} ba \dots$ as well.*

Proof: By lemma 1, for

$$w \;=\; \overbrace{\underbrace{a\ b^{x_1}\ a\ \dots\ a\ b^{x_k-m}}_{\alpha}\ |_s\ b^{m-1}}^{\alpha'}\ \underbrace{|_{s'}\ \overbrace{b\ a\ \dots\ b^{x_n}}^{\beta'}}_{\beta}\ a$$

the following holds true

$$\#_a(\beta) \cdot \#_b(\alpha) \geq \#_a(\alpha) \cdot \#_b(\beta) \quad \iff \quad \frac{\#_b(\alpha)}{\#_a(\alpha)} \geq \frac{\#_b(\beta)}{\#_a(\beta)},$$

where $\#_a(\alpha) \neq 0$ and $\#_a(\beta) \neq 0$. Due to $\#_b(\alpha') \geq \#_b(\alpha)$, $\#_b(\beta') \leq \#_b(\beta)$, and $\#_a(\alpha) = \#_a(\alpha')$, $\#_a(\beta) = \#_a(\beta')$, we have

$$\frac{\#_b(\alpha')}{\#_a(\alpha')} \geq \frac{\#_b(\beta')}{\#_a(\beta')} \quad \Longrightarrow \quad \#_a(\beta') \cdot \#_b(\alpha') \geq \#_a(\alpha') \cdot \#_b(\beta'),$$

implying a is not separated at state s', according to lemma 1. □

Lemma 11. *If $w = ab^{x_1}ab^{x_2}a \dots ab^{x_n}a$, with $x_1 = x+1$, $x_n = x$, $x_i \in \{x, x+1\}$, $x > 0$, $n \geq 3$, is a minimal unsolvable word, and separation failure occurs in group b^{x_k}, then $x_k = x + 1$.*

Proof: By lemma 11, a is not separated at some state s in

$$w \;=\; \underbrace{\overbrace{a\,b^{x_1}\;a\;\ldots\;a\,b^{x_{k-1}-1}}^{\alpha'}\;|\;b\;a\;b^{x_k-1}}_{\alpha}\;|_s\;\overbrace{\underbrace{b\;a\;\ldots\;a\;b^{x_{n-1}}}_{\beta}\;a\;b^{x_n}}^{\beta'}\;a,$$

which implies, according to lemma 1, that

$$\begin{aligned}(x_1+\ldots+x_k-1)\cdot(n-k) \;&\geq\; (1+x_{k+1}+\ldots+x_n)\cdot k \iff\\ \frac{x_1+\ldots+x_k-1}{k} \;=\; \frac{\#_b(\alpha)}{\#_a(\alpha)} \;&\geq\; \frac{\#_b(\beta)}{\#_a(\beta)} \;=\; \frac{1+x_{k+1}+\ldots+x_n}{n-k},\end{aligned}$$

where $\#_a(\alpha)\neq 0$ and $\#_a(\beta)\neq 0$. Assume now, by contraposition, that $x_k = k$. Since for every $1 \leq i \leq 0$ we have $x \leq x_i \leq x+1$, then ${\#_b(\alpha')}\big/{\#_a(\alpha')} \geq {\#_b(\alpha)}\big/{\#_a(\alpha)}$, where $\#_a(\alpha')\neq 0$ because w starts with a. From $x_1 = x+1$, it follows $k>1$. Due to $x_n = x = x_k$, ${\#_b(\beta')}\big/{\#_a(\beta')} = {\#_b(\beta)}\big/{\#_a(\beta)}$, where $\#_a(\beta')\neq 0$ since $k>1$. Thus, ${\#_b(\alpha')}\big/{\#_b(\alpha')} \geq {\#_b(\beta')}\big/{\#_a(\beta')}$, which implies, by lemma 1, unsolvability of $\alpha'\beta' a$, contradicting minimality of w. $\square$

Lemma 12. *If $w = bab^{x_2}ab^{x_3}a\ldots ab^{x_n}$, with $x_2 = x$, $x_n = x+1$, $x_i \in \{x, x+1\}$, $x>0$, $n\geq 3$, is a minimal unsolvable word, and separation failure occurs after group b^{x_k}, then $x_k = x$.*

Proof: For state s in w, from which b is not separated,

$$w \;=\; \underbrace{\overbrace{b\;a\;b^{x_2-1}\;b\;a\;\ldots\;a\;b^{x_{k-1}-1}}^{\alpha'}\;|\;a\;b^{x_k}}_{\alpha}\;|_s\;\overbrace{\underbrace{a\;\ldots\;a\;b^{x_{n-1}-1}\;b\;a\;b^{x_n-1}}_{\beta}}^{\beta'}\;b$$

according to lemma 1, we have

$$\begin{aligned}(k-1)\cdot(x_{k+1}+\ldots+x_n-1) &\geq (1+x_2+\ldots+x_k)\cdot(n-k) \iff\\ \frac{x_{k+1}+\ldots+x_n-1}{n-k} \;=\; \frac{\#_b(\beta)}{\#_a(\beta)} \;&\geq\; \frac{\#_b(\alpha)}{\#_a(\alpha)} \;=\; \frac{1+x_2+\ldots+x_k}{k-1},\end{aligned}$$

where $\#_a(\beta)\neq 0$ since β starts with a, and $\#_a(\alpha)\neq 0$ because $k>1$. By contraposition, assume $x_k = k+1$. Since for all $2\leq i\leq n$ we have $x\leq x_i\leq x+1$, ${\#_b(\alpha')}\big/{\#_a(\alpha')} \leq {\#_b(\alpha)}\big/{\#_a(\alpha)}$, where $\#_a(\alpha')\neq 0$ because $k>2$. From $x_n = x+1 = x_k$ it follows ${\#_b(\beta)}\big/{\#_a(\beta)} = {\#_b(\beta')}\big/{\#_a(\beta')}$, where $\#_a(\beta')\neq 0$ due to β' starts with a. Hence, ${\#_b(\beta')}\big/{\#_a(\beta')} \geq {\#_b(\alpha')}\big/{\#_a(\alpha')}$. Due to lemma 1, this implies unsolvability of $\alpha'\beta' b$, contradicting minimality of w. $\square$