EQUATIONS IN WORDS : AN ALGORITHMIC CONTRIBUTION

Jean Néraud

Abstract

We study the special class of equations in words of type (R, w), where R is a two variable generalized regular expression, without constant, and where w is a constant word. We show that the problem may be solved by applying a $O(|w| \ln^2 |w|)$ time algorithm.

1 Introduction

In Combinatoric on words, the question of deciding whether an arbitrary word (or, equivalently, all the words in a finite family) belongs to a given recursive language L takes a prominent part for the problem it generates. Indeed, in spite of the simplicity of the preceding statement, practical conditions lead to various problems, with a large range of corresponding computational complexity [13]. In a first hand, several general problems are known to be NP-complete, even undecidable, and in another hand, with special instances, famous efficient algorithms have been implemented. Actually, between these two poles, there exists a large gap of open problems. This feature is particularly well illustrated when considering the framework of pattern matching.

The most famous example is certainly the so-called "string matching" problem, which consists in deciding whether a given word u appears as factor in a given "text" w. In other words, the question consists in deciding whether $w \in \Sigma^* u \Sigma^*$, where Σ^* stands for the free monoid generated by Σ, the basic alphabet. With this special case of instance, many famous linear-time algorithms have been implemented (cf e.g. [16], [7], [14]). Actually the implementation of new improvements remains a challenging question.

Another classical question corresponds to construct efficient membership tests to languages of type $L = \Sigma^* L(R) \Sigma^*$, where $L(R)$ stands for the set of all the words which are described by the regular expression R. In [25], an $O(|R||w|)$-time algorithm has been proposed for solving this problem (in a classical way, $|R|$ denotes the length of R). Moreover, with special classes of regular patterns, fast algorithms allow to compute all the occurrences of the pattern R in w (cf e.g. [12], [3], [9]).

Received by the editors March 1993, revised December 1993.
Communicated by M. Boffa.
AMS Mathematics Subject Classification : 68R15.
Keywords : free monoid, word, factor, period, morphism, equation, solution, pattern, algorithm, complexity.

Approximate pattern matching is also concerned, and led to a lot of challenging combinatorical algorithms (e.g. [26], [21], [18]).

Languages described by "generalized regular expression" (GRE for short), a more general class of languages, are also concerned. Practically, this notion of GRE is illustrated in the commands of the text editors of the UNIX system. Formally, given two finite disjoint sets, say Σ, the alphabet of the "constants", and Δ, the alphabet of the "variables", we consider a regular expression, say R, over $\Delta \cup \Sigma$. Given a third alphabet Γ, we define the (Γ, Σ)-language described by R, namely $L_{(\Gamma,\Sigma)}(R)$, as the set of all the words $\phi(t) \in \Sigma^*$, which satisfy the two following conditions :

- t is an arbitrary word in the regular language described by R over $\Sigma \cup \Delta$.
- ϕ stands for any morphism from $(\Delta \cup \Sigma)^*$ into $(\Sigma \cup \Gamma)^*$ satisfying $\phi(a) = a$, for every "constant" $a \in \Sigma$.

For instance, take $\Gamma = \Sigma = \{a, b\}$, $\Delta = \{X\}$ and consider the GRE $R = X^*abX^*$. By definition, for every integer pair (n, p), the word $W = X^n abX^p$ belongs to the regular subset described by R in $(\Delta \cup \Sigma)^*$. As a consequence, the words $(aba)^2ab(aba)^3$, and a^5aba^2 belong to $L_{(\Gamma,\Sigma)}(R)$. Indeed, such strings may be constructed by substituting aba to X, or a to X, in the word $W \in L_{\Delta\cup\Sigma}(R)$.

From the point of view of the computational complexity, as shown in [1] (p. 289), given R, an arbitrary GRE, and given an input word w, deciding whether $w \in \Sigma^* L_{(\Gamma,\Sigma)}(R)\Sigma^*$ is NP-complete. The best known results concerning restrictions relate to "periodicities", i.e. patterns of type X^q. Notice that, in this case, the morphim ϕ which defines the substitution, must be non-erasing, i.e. $\phi(X)$ must be different of the empty word. With such a type of GRE, several efficient $O(|w| \ln |w|)$ algorithms have been implemented ([8], [4], [20], [24]).

As another example, the problem of deciding whether the "rank" of a finite set of words $E \subseteq \Sigma^*$ is not greater than an arbitrary integer k, comes down to decide whether E may be described by a pattern of type $(X_1 + X_2 + ... + X_k)^*$. For instance, consider the set $E = \{abcba, abcbaabc, abcbaabcbaabc\}$. Since $E \subseteq \{abc, ba\}^*$, the rank of E is at most 2. In the general case, this problem of "rank" is also NP-complete [22]. When considering an arbitrary set of words $E \subseteq \Sigma \cup \Sigma^2$, (i.e. a set of words w, with $|w| \in \{1, 2\}$), the question may be easily decided in quadratic time moreover, in the case where we fix the integer k to 2, we constructed a $O(n \ln m)$-time algorithm [23], where n stands for the sum of the lengths of the words in E, and where m stands for the length of the longest word in E.

Another "difficult" question consists in computing a "descriptive" pattern for a finite set of words [2]. For instance, take $\Sigma = \Delta = \{a, b\}$ and consider the pattern $R = XabXa$. By substituting ba (aba, a) to X, it is easy to verify that R allows to describe all the words in the finite set $E = \{baabbaa, abaababaa, aabaa\}$. Moreover, it can be shown that, given another GRE, say S, if $E \subseteq L_{(\Sigma,\Sigma)}(S)$, then the language $L_{(\Sigma,\Sigma)}(S)$ cannot be a strict subset of $L_{(\Sigma,\Sigma)}(R)$, the language described by R. Unformally, R is a "closer" pattern describing the set of words E. As in the preceding case, the problem of computing such a pattern is NP-complete, moreover, we notice that in the case of a constant number of variables, it may be solved in polynomial time [2], [15].

The framework of equations in words is also concerned. Such an equation consists in fact in a pair of star-free GRE, (R, S), and given a third alphabet Γ, the problem consists in deciding whether the corresponding languages $L(R)$ and $L(S)$ have a non-empty intersection. Once more, as shown in [2], this is an NP-complete problem, moreover, in the general case, only a five exponential height time algorithm allows actually to compute a solution [19].

Our paper consists in a contribution, for drawing the limit of equations which may be solved by fast time algorithms. We present a $O(|w| \ln^2 |w|)$-time algorithm for solving an arbitrary equation of type (R, w), where $R \in \{X, Y\}^*$, and where w is a constant word.

Choosing such a class of instances must not appear as arbitrary. Indeed, our method allows to decide whether a finite language E may be "generated" by a two variable pattern R : a question directly connected to the preceding "pattern language". Moreover, our method is a first step for solving more general classes of equations.

The two fundamental combinatorical concepts of "overlapping" and "repetitions" (Section 2) play a prominent part in the constructions. Another important feature consists in describing the solutions by solving associated linear diophantine systems.

In Section 3, we study the case where the GRE R belongs to the set $XY\{X,Y\}^* \cap \{X,Y\}^*YX$, or belongs to the set $X^2\{X,Y\}^*$. We show how to compute candidates for the "periods" of the "solutions" $\phi(X)$, $\phi(Y)$. - indeed, we establish that these periods allow to compute each solution.

The case of a GRE of type $XY\Delta^* \cap \Delta^*XY$ is studied in Section 4. Once more we determine candidates for the solutions by examining the overlaps of w.

As a conclusion of our study, in Section 5 we draw the scheme of our main algorithm for solving an arbitrary two unknown equation (R, w) $(R \in \{X, Y\}^*$, $w \in \Sigma^*)$. This algorithm takes account of the special cases which were avoided in Section 3 and Section 4.

2 Preliminaries

2.1 Definitions and notations

We adopt the standard notations of the free monoid theory : given a word w in Σ^* (the free monoid generated by Σ), we denote by $|w|$ its length, the empty word being the word of length 0. Given two words $u, w \in \Sigma^*$, we say that u is a *factor* (resp. *prefix*, *suffix*) of w iff we have $w \in \Sigma^* u \Sigma^*$ ($u\Sigma^*$, $\Sigma^* u$). If $w \in \Sigma^+ u \Sigma^+$ (resp. $u\Sigma^+$, $\Sigma^+ u$), we say that u is an *interior factor* (*proper prefix*, *proper suffix*).

If u is a prefix (suffix) of w, then we denote by $u^{-1}w$ (wu^{-1}) the unique word v such that $w = uv$ $(w = vu)$. An *overlap* of w is a factor which is both proper prefix and suffix of w. Given a non-empty word $p \in \Sigma^*$, we say that it is a *period* of w iff w is a prefix of a word in p^+. The overlaps of w and its periods are in one-to-one correspondence (cf e.g. [16]).

The *primitive root* of a non-empty word w is the shortest word r such that $w \in r^+$ (if $w = r$, we say that w is a *primitive word*). As a direct consequence of the Defect theorem (cf e.g. [17] p. 6) :

Claim 2.1 *If x is a primitive word, then it cannot be an interior factor of x^2.*

The following result is of folklore in the litterature :

Theorem 2.1 (Fine and Wilf) *Let x, y be two words. Assume that two powers x^p, y^q of x and y have a common prefix of length at least equal to $|x| + |y| - \gcd(|x|, |y|)$. Then the words x and y are powers of a common word.*

2.2 A special class of equations in words

Consider the following general problem :

Instance : -Δ, a finite alphabet of "variables"
-Σ , a finite alphabet of "constants", with $\Delta \cap \Sigma = \emptyset$
-Γ, a third alphabet
-R, S, two regular expression upon $\Delta \cup \Sigma$

Question : Decide whether or not there exists a non-erasing morphism
$\phi\ : (\Delta \cup \Sigma)^* \rightarrow (\Gamma \cup \Sigma)^*$ (i.e. ε not in $\phi(\Sigma \cup \Delta)$)
such that the two following conditions hold :
-for every letter $a \in \Sigma$, we have $\phi(a) = a$
-$\phi(L(R)) \cap \phi(L(S)) \neq \emptyset$.

As shown in [1], this problem is NP-complete. The pair (R, S) is called an *equation*, and we say that the preceding mapping ϕ is a *solution* of the equation (R, S).
In our paper, we consider EQUA2, the restriction which corresponds to the following instances :

- Δ is two-variable alphabet {X,Y}
- $R \in \Delta^*$, and $S = w$ is a single word, in Σ^*

With such equations, the solutions are necessarily morphisms from Δ^* into Σ^*. Clearly, such a morphism ϕ is completely determined by the words $\phi(X)$ and $\phi(Y)$. Without loss of generality, we shall assume that we have $R \in X\Delta^*$.

2.3 Overlaps and prefix squares : two fundamental results

In a classical way, given a word t there exists a subset of $\Sigma^* \times \Sigma^+$, namely $OVL(t)$ such that the following property holds :

Condition 2.1 *(i) for each pair of words $(r, s) \in OVL(t)$, rs is a primitive word. (ii) for each overlap t' of t, there exists a pair of words $(r, s) \in OVL(t)$ such that $t' \in (rs)^+r$, with rs the shortest period of t.*

Moreover, according to [16] or [11] :

Claim 2.2 *We have $|OVL(t)| \leq \log_\Phi |t|$, where Φ stands for the golden ratio.*

Given an arbitrary word $t \in \Sigma^*$, denote by $LSQR(t)$ the set of the words $r \in \Sigma^*$ which satisfy the following condition :

Condition 2.2 *(i) r is a primitive word.*
(ii) r^2 is a prefix of t.

According to [10] :

Claim 2.3 *We have $|LSQR(t)| \leq \log_\Phi |t|$.*

Clearly, by considering suffixes of t, we may define the set $RSQR(t)$, with similar properties. From an algorithmic point of view, in a classical way :

Claim 2.4 *Given a word $t \in \Sigma^*$, computing the sets $OVL(t)$, $LSQR(t)$, $RSQR(t)$ may be done in time $O(|t|)$ by applying the algorithm of Knuth Morris and Pratt (KMP-algorithm).*

2.4 Convention of implementation

Clearly, we may assume that $|R| \leq |w|$. From an algorithmic point of view, we represent words by linked lists of characters, sets of words being represented by lists of words.
In a similar way, linear diophantine equations (inequations) will be represented by linked lists of integers. Linear systems will be implemented by lists of equations. With these representations, binary operations like union of sets, concatenation of words, conjunction or disjunction of linear systems will be easily done by concatenating lists.

2.5 Equation in lengths

Let ϕ be a solution of Equation (R, w). Denote by $|R|_X$ the number of occurrences of the letter X in the word $R \in \Delta^*$. Clearly the lengths of the words $\phi(X)$, $\phi(Y)$ satisfy the following "equation in lengths" :

$$|R|_X|\phi(X)| + |R|_Y|\phi(Y)| = |w| \tag{1}$$

As a consequence :

Claim 2.5 *Given a positive integer d, there exists at most one solution ϕ such that we have $|\phi(X)| = d$.*

Indeed, let m be the greatest integer such that X^m is a prefix of R. Clearly, $\phi(X)$ is the prefix of w with length d, and $\phi(Y)$ is the prefix of $d^{-m}w$ with length $\frac{|w|-|R|_X|\phi(X)|}{|R|_Y}$.

2.6 The case of "non-coding" solution

According to the Defect theorem, given a solution ϕ, if $\phi(\Delta)$ is not a unique decipherable set, then the words $\phi(X)$ and $\phi(Y)$ have a common primitive root, say x. More precisely, there exists a pair of positive integers, namely (i, j), such that $\phi(X) = x^i$ and $\phi(Y) = x^j$.
As a consequence, solving Problem EQUA2 comes down to decide whether there exists an integer pair (i, j), such that $w = x^{|R|_X i + |R|_Y j}$, x being the primitive root of

w. Trivially, this will be done in time $O(|w|)$ (indeed, the corresponding pairs (i,j) are the solutions of following diophantine equation :

$$i,j>0,\quad |R|_X i+|R|_Y j=\left[\frac{|w|}{|x|}\right]$$

In Section 3, and Section 4, we shall restrict our search to "unique decipherable" solutions, i.e. morphisms ϕ such that $\phi(\Delta)$ is a unique decipherable set (or, for short a "code").

2.7 Special cases of equations

In this section, we consider two special cases of equations which may be easily solved. In Section 3 and Section 4, we shall avoid these particular cases.

Equations of type (X^nY^m,w)

First, we notice that if $n=m=1$, then the solutions are all the morphisms ϕ such that $\phi(X)=u$, $\phi(Y)=v$, with $uv=w$.
Now, we assume that $\max\{m,n\}>1$. Given a word $v\in LSQR(w)$ $(RSQR(w))$, we denote by $n(v)$ $(m(v))$ the greatest integer such that $v^{n(v)}$ $(v^{m(v)})$ is a prefix (suffix) of w. Exactly one of the three following cases may occur :

- If $n\geq 2$, and $m=1$, then the problem consists in deciding whether there exists a word $x\in LSQR(w)$ and a positive integer i such that $ni\leq n(x)$ (we shall have $\phi(X)=x^i$, and $\phi(Y)=x^{-ni}w$). According to the properties which were mentioned above, the method requires time $O(|w|\ln|w|)$.
- Clearly, a similar result holds if $n=1$, and $m\geq 2$.
- Now, assume that $m,n\geq 2$. With this condition, the problem consists in deciding whether there exists a pair of words $(x,y)\in LSQR(w)\times RSQR(w)$, and a pair of positive integers (i,j) such that both the three following properties holds :
$$i.n\leq n(x),\;\; j.m\leq m(y),\;\; n|x|i+m|y|j=|w| \qquad (2)$$
Clearly, it is decidable in time $O(|w|\ln^2|w|)$.

Equations of type $((XY)^n,w)$

Trivially, such an equation has solutions iff there exists a word t such that $w=t^n$. The corresponding solutions are all the morphisms ϕ such that $\phi(X)=u$, $\phi(Y)=v$, with $t=uv$.

3 The cases where $R\in XY\Delta^*\cap\Delta^*YX$ or $R\in X^2\Delta^*$

Before to explain our algorithm, let's draw a theoretical study. Assume that we get a unique decipherable solution ϕ. We shall establish necessary conditions which must be satisfied by the words $\phi(X)$ and $\phi(Y)$.
Let $u,v,r,s\in\Sigma^*$ such that the following propreties hold :

Condition 3.3 *(i) uv and rs are primitive words.*
(ii) We have $v \neq \varepsilon$ and $s \neq \varepsilon$.
(iii) vu is not a prefix of rs.
(iv) uv is not a suffix of sr.

Moreover, given a morphism $\phi : \{X, Y\}^* \to \Sigma^*$, and given a tuple of non-negative integers (i, j, j', k), with $i \geq 1$ and $k \geq 1$, we consider the following condition :

Condition 3.4 *(i)* $\phi(X) = (uv)^i u$.
(ii) $\phi(Y) = (vu)^j (rs)^k r(uv)^{j'}$.

We say that the tuple (ϕ, i, j, j', k) satisfies Condition 3.4, with respect to the tuple of words (u, v, r, s). In fact, given a non-erasing morphism ϕ, there exists at least one tuple (u, v, r, s) such that Condition 3.4 holds. Indeed, let x be the shortest period of $\phi(X)$, let u be the shortest word such that $\phi(X) \in x^+u$, and let $v = u^{-1}x$. Define the following words y, y', y'' :
- y' is the shortest word such that $\phi(Y) \in (vu)^* y'$.
- y'' is the shortest word such that $y' \in y''(uv)^*$.
- If $y'' \neq \varepsilon$, then y is the shortest period of y''. Otherwise, we set $y = \varepsilon$.
With the condition $y = \varepsilon$, we set $r = s = \varepsilon$, otherwise, let r be the shortest word such that $y'' \in y^+r$, and let $s = r^{-1}y \in \Sigma^+$. By construction, the tuple (u, v, r, s) satisfies Condition 3.3. Moreover, we have $\phi(X) \in (uv)^+u$ and $\phi(Y) \in (vu)^*(rs)^+r(uv)^*$.

3.1 The case where the tuple (u, v, r, s) is given

We shall establish two lemma.

Lemma 3.1 *With the condition of Section 3, given the words $w \in \Sigma^*$ and $R \in \{X, Y\}^*$, and given the tuple of words (u, v, r, s) of Condition 3.3, with $u = \varepsilon$, there exist :*
- a finite set of integers K,
- and a subset I of $\Sigma^+ \times \Sigma^+$,
with constant cardinalities, such that, for every tuple (ϕ, i, j, j', k) satisfying Condition 3.4, if $\phi(R) = w$ then at least one of the two following conditions holds :
(i) The integer k belongs to K.
(ii) The corresponding pair of words $(\phi(X), \phi(Y))$ belongs to I.

Proof of Lemma 3.1 Let (ϕ, i, j, j', k) be a tuple satisfying Condition 3.4 with respect to the tuple of words (u, v, r, s). Assume that we have $i \in \{0, 1\}$. By definition, this determines two corresponding candidates for the word $\phi(X) = v^i$. According to Claim 2.5, there exists at most two corresponding candidates for the pair $(\phi(X), \phi(Y))$. Let I_0 be the set with elements these pairs of words.
Now we assume that $i \geq 2$. Moreover, we assume that $k \geq 2$ (we set $K_0 = \{0, 1\}$), and we set $y = (rs)^k r$.
Since $\phi(\Delta)$ is a unique decipherable set, it is the same for the set $\{v, y\}$. Moreover, since the word $\phi(R)$ belongs to $\{v, y\}^*$, there exists a unique sequence of non-negative integers $(h_0, h_1, ..., h_n)$ (with $n \geq 1$) such that $\phi(R) = v^{h_0} y v^{h_1} y ... y v^{h_n}$. Since we assume that $i \geq 2$:

Claim 3.6 *for each $a \in [0, n]$, if $h_a \neq 0$ then necessarily one of the two following conditions holds :*
(3.6.i) $h_a \geq 2$
(3.6.ii) $h_a = 1$ and $j + j' \leq 1$

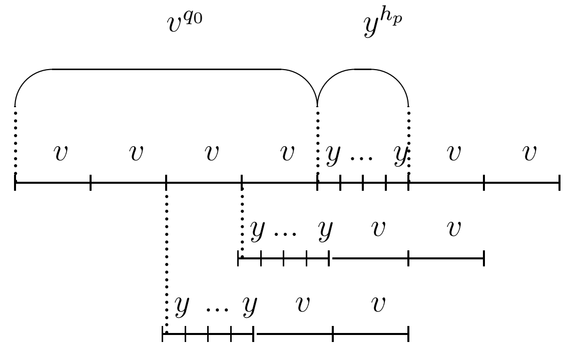
Similarly, there exists a unique sequence of non-negative integers $(m_0, ..., m_n)$ such that $R = X^{m_0}YX^{m_1}Y...YX^{m_n}$. Since $R \in X\Delta^*$, we have necessarily $m_0 > 0$, thus $h_0 > 0$.

a) A constraint on the integer h_0

First, we notice that at least one of the integers m_a is positive (otherwise, we should have $R \in Y^*$, which corresponds to a one-unknown equation).
Let p be the smallest positive integer such that $h_p > 0$.
According to Claim 3.6, exactly one of the two following cases may occur :

- **(3.6.i) The case where $h_p \geq 2$**
With this condition, the word $v^{h_0}y^pv^2$ is a prefix of $\phi(R)$ (recall that we assume that R is not prefix of a word in X^+Y^+, this type of equation being studied in Section 2.7). Two cases may occur :
- If $|v| \leq |y|$ then, since v cannot be a prefix of y, the integer h_0 is necessarily the greatest integer such that v^{h_0} is a prefix of w.
- If $|v| > |y|$ then, according to the theorem of Fine and Wilf, since $\{v, y\}$ is a unique decipherable set, the longest common prefix between y^p and a word in v^+ is necessarily a proper prefix of v^2. Moreover, according to Claim 2.1, the word v cannot be an interior factor of v^2 (cf Figure 1). As a consequence, in each case the following property holds :
$$h_0 \in [q_0 - 2, q_0] \tag{3}$$
where q_0 stands for the greatest integer such that v^{q_0} is a prefix of w. Set $h_0 = m_0 i + j$, $w' = v^{-h_0}w$ and denote by p_{max} the greatest integer such that $(rs)^{p_{max}}r$ is a prefix of w'.

- **(3.6.ii) The case where $h_p = 1$**
This case corresponds to the conditions $m_p \leq 1$ and $j + j' \leq 1$. More precisely :
- If $m_p = 1$, we have necessarily $j = j' = 0$, and $i = 1$. But this is a contradiction with our condition $i \geq 2$.
- If $m_p = 0$, $j = 0$ and $j' = 1$, then we have necessarily $p = 1$ (indeed, if $p \geq 2$, the word $v^{h_0}y^2$ is a prefix of w, hence we have $j + j' = 0$, a contradiction with $j = 0$ and $j' = 1$). This implies that the word $X^{m_0}YX$ is necessarily a prefix of R (indeed, we assume that R is not a prefix of a word in X^+Y^+). We have $\phi(Y) = vy$ and $\phi(X) = v$. According to Claim 2.5, this leads to determine a corresponding singleton I_1, with $(\phi(X), \phi(Y)) \in I_1$.
- As in the preceding case, if $m_p = 0$, $j = 1$ and $j' = 0$, then we have $p = 1$, thus the word $v^{h_0}yv$ is a prefix of w. As in the case (3.6.i), if $|v| \leq |y|$, then h_0 is necessarily the greatest integer such that v^{h_0} is a prefix of w. Otherwise, according to Claim 2.1, the word v cannot be an interior factor of v^2. This implies that we have $h_0 \in \{q_0 - 1, q_0\}$, where q_0 stands for the greatest integer



According to Claim 2.1, and since $\{y, v\}$ is a code, at most one of these three positions may occur

Figure 1: $h_0 \in [q_0 - 2, q_0]$

such that v^{q_0} is a prefix of w. But we have $h_0 = m_0 i + j = m_0 i$. This leads to determine precisely at most two candidates for the integer i thus, according to Claim 2.5, a corresponding set I_2, with $|I_2| \leq 2$, such that $(\phi(X), \phi(Y)) \in I_2$

In the next of the proof of our Lemma, we shall assume that $h_p \geq 2$.

b) The case where $r = \varepsilon$

With this condition, since $R \in X^+ Y^p X \Delta^*$, the word $(s^k)^p v^{h_p}$ is a prefix of w'. Moreover, recall that assume $h_p \geq 2$. Consequently, since v cannot be a prefix of y, and since v is a primitive word, we have $pk = z$, where z stands for the unique integer such that $s^z v^2$ is a prefix of w'. Set $K_1 = \{\frac{z}{p}\}$.

c) The case where $r \neq \varepsilon$

If $h_1 = 0$, since $(rs)^2$ is prefix of y, the word $(rs)^k r (rs)^2$ is a prefix of w'. Since $rs \neq sr$, we have $k = p_{max}$. Set $K_2 = \{p_{max}\}$.
Now, we assume that $h_1 \neq 0$ thus, according to Claim 3.6.(i), $p = 1$ and $h_1 \geq 2$. Necessarily, the word $(rs)^k rv$ is a prefix of w'. According to the theorem of Fine and Wilf, we may define a unique integer q_{cycle}, as indicated in the following :

If there exists a word $t \in v^+ \cap (sr)^* s$, then q_{cycle} is the unique integer such that $v^{q_{cycle}} = t$. Otherwise, we set $q_{cycle} = 0$.

Moreover, if q_{cycle} is a positive integer, then we denote by τ the unique integer such that $v^{q_{cycle}} = (sr)^\tau s$.
Comparing the integers h_1 and q_{cycle} leads to consider two new cases :

- **Condition** $h_1 \neq q_{cycle}$
  Necessarily, the word $(rs)^k rv^2$ is a prefix of w'. Since v and rs are primitive words, we have $(sr)^* \cap v^* = \emptyset$. As a consequence, if $|v| \geq |rs|$ then, according

to Claim 2.1, since v cannot be an interior factor of v^2, we have $k = z_1$, where z_1 stands for the greatest integer such that $(rs)^{z_1}rv^2$ is a prefix of w'. Set $K_3 = \{z_1\}$
Now, we assume that we have $|v| < |rs|$. With this condition, exactly one of the two following cases may occur :

- **The case where $\phi(R) = v^{h_0}yv^{h_1}$**
This condition necessarily implies that $R = X^{m_0}YX^{m_1}$, with $m_0, m_1 > 0$. According to Property (3), we have $m_0i+j \in [q_0-2, q_0]$. In a similar way, by considering the reversed words, we have also : $m_1i + j' \in [q'_0 - 2, q'_0]$, where q'_0 stands for the greatest integer such that $v^{q'_0}$ is a suffix of w. This leads to determine at most 9 pairs of integers (q_0, q'_0), thus at most 9 corresponding candidates for the word $y = v^{-q_0}wv^{-q'_0}$. Since we have $y = (rs)^k r$, once more, this determines a corresponding set K_3, with $|K_3| \leq 9$.
- **The case where $v^{h_0}yv^{h_1}y$ is a prefix of $\phi(R)$**
This condition implies that the word $(rs)^k rv^{h_1}(rs)^2$ is a prefix of w'. In fact, we are in a condition similar to the preceding condition of Section a) in the proof, Case (3.6.i) (by substituting v to y and sr to v). Consequently, we obtain $k \in K'_3 = [p_{max} - 2, p_{max}]$. Finally, we substitute to K_3 the union of the preceding sets K_3, K'_3.

• **Condition $h_1 = q_{cycle}$**
With the condition (i) of Claim 3.6, the integer q_{cycle} is necessarily greater than 1. According to Theorem 2.1, this implies that we have $\tau \leq 1$, thus $|v| < |rs|$.

Moreover, long prefixes of w' may belong to $(rs)^+r \cap (yv^{h_1})^+$. A clever examination of these prefixes leads to consider the following new cases :

- **The case where $R = X^{k_0}(YX^{k_1})^{k_2}YX^{k_3}YS$, with $S \in \Delta^*$, $k_2 > 0$ and $k_3 < k_1$**
With this condition, the word $w'' = (yv^{q_{cycle}})^{k_2}yv^{j'+k_3i+j}y$ is a prefix of w'. Since we have $j' + k_3i + j < j' + k_1i + j = q_{cycle}$, the word $v^{j'+k_3i+j}$ is a proper prefix of $v^{q_{cycle}}$. Moreover, since $k_3 < k_1$, w'' does not belong to $(rs)^+r$.
Consequently, we obtain :
$((rs)^k r(sr)^\tau s)^{k_2}(rs)^k r = (rs)^z r$, with $z \in \{p_{max}, p_{max} - \tau\}$.
This implies that the integer k satisfies the following condition :
$$k_2(k + \tau + 1) + k \in \{p_{max}, p_{max} - 1\} \tag{4}$$
This leads to determine a new set of integer, namely K_4, with $|K_4| \leq 2$.
- **The case where $R = X^{k_0}(YX^{k_1})^{k_2}YX^{k_3}$, with $k_2 > 0$, and $k_3 < k_1$**
With this condition, the word $w'' = (yv^{q_{cycle}})^{k_2}yv^{j'+k_3i}$ is a prefix of w'. As in the preceding case, the word $v^{j'+k_3i}$ is a prefix of the word $v^{q_{cycle}}$. Consequently the integer k satisfies Equation (4), thus it belongs to the preceding set K_4.

- **The case where $R = X^{k_0}(YX^{k_1})^{k_2}X^{k_3}YS$, with $S \in \Delta^*$, and $k_2, k_3 > 0$**
Since we have $q_{cycle} = j' + k_1 i + j$, the word $(yv^{q_{cycle}})^{k_2-1}yv^{j'+k_1 i+k_3 i+j}y$ i.e. $(yv^{q_{cycle}})^{k_2}v^{k_3 i}y$ is prefix of w'. This implies that $(yv^{q_{cycle}})^{k_2}v^{k_3 i}(rs)^2$ is also a prefix of w'. According to Claim 2.1, the word rs (v) cannot be an interior factor of $(rs)^2$ (v^2). Moreover, we have $(rs)^* \cap v^* = \emptyset$. As a consequence, we have $(yv^{q_{cycle}})^{k_2} = (rs)^{z_0}$, where z_0 stands for the greatest integer such that $(rs)^{z_0}$ is a prefix of w'. Consequently, the integer k satisfies the condition :
$$k_2(k + \tau + 1) = z_0 \tag{5}$$
This leads to determine a corresponding set K_4.
- **The case where $R = X^{k_0}(YX^{k_1})^{k_2}X^{k_3}$, with $k_2, k_3 > 0$**
We have $w' = (yv^{q_{cycle}})^{k_2-1}yv^{j'+(k_1+k_3)i}$. Moreover, exactly one of the three following cases occurs :
- $k_3 i < j$. The word $v^{j'+(k_1+k_3)i}$ is a proper prefix of $v^{q_{cycle}} = (sr)^\tau s$. This implies that the integer k satisfies the following condition :
$$(k + \tau + 1)(k_2 - 1) + k \in \{z_0, z_0 - 1\} \tag{6}$$
the integer z_0 being defined as indicated above. Let K'_1 be the set of the corresponding integers k.
- $k_3 i = j$. Since we have $v^{j'+(k_1+k_3)i} = v^{q_{cycle}}$, we have $w' = (yv^{q_{cycle}})^{k_2}$. As a consequence, the integer k satisfies the following equality :
$$(k + \tau + 1)k_2 = z_0 \tag{7}$$
Let $K'_2 = \{\frac{z_0-(\tau+1)k_2}{k_2}\}$.
- $k_3 i > j$. We have $v^{j'+(k_1+k_3)i} = v^{q_{cycle}}v^{k_3 i-j}$. Moreover, since $q_{cycle} > 1$, and since $v^{q_{cycle}} = (sr)^\tau s$, we have $|v| < |sr|$. According to Condition 3.3, the word $v^{k_3 i-j}$ cannot be a prefix of rs, and rs cannot be a prefix of $v^{k_3 i-j}$. This implies that the integer k satisfies Condition (7). Let K'_3 be the set of the corresponding integers k. Moreover, we set $K_4 = K'_1 \cup K'_2 \cup K'_3$.

Now, we denote by K the union of the preceding sets $K_a (0 \le a \le 4)$ which were defined above, for each of the integers $h_0 \in [q_0 - 2, q_0]$. Moreover, we set $I = I_0 \cup I_1 \cup I_2$. By construction the sets K and I satisfy the conditions of Lemma 3.1. This completes the proof of our lemma.

■

We now consider the case where u is not the empty word. The following result is similar to Lemma 3.1

Lemma 3.2 *With the condition of Section 3, let $w \in \Sigma^*$, $R \in \{X, Y\}^*$. Assume that one of the three following conditions holds :*
- $R \in X^2\{X, Y\}^*$
- $R \in \{X, Y\}^* X^2$
- $R \in XY\{X, Y\}^* \cup \{X, Y\}^* YX$.

Given a tuple of words (u, v, r, s) satisfying Condition 3.3, with $u \neq \varepsilon$, there exist :
- a finite set of positive integers K,
- and a finite subset I of $\Sigma^+ \times \Sigma^+$,
with constant cardinalities, such that, for every tuple (ϕ, i, j, j', k) satisfying Condition 3.4 with respect to (u, v, r, s), if $\phi(R) = w$, then at least one of the two following conditions holds :
(i) $k \in K$
(ii) $(\phi(X), \phi(Y)) \in I$.

Proof of Lemma 3.2

As for Lemma 3.1, the case where $i = 1$ ($k = 1$) leads to define a corresponding set I_0 (K_0).
In the next, we assume that $i, k \geq 2$, and we set $y = (rs)^k r$. Notice that if $y \in (vu)^+ v$ then, according to Condition 3.3, we have in fact $y = v$. This determines a unique integer $k = \frac{|v|-|r|}{|rs|}$. Set $K_1 = \{k\}$.
Now, we assume that $y \neq v$.

1) The case where X^2 is a prefix of R
With this condition, the word $(uv)^i u(uv)^2$ is necessarily a prefix of w. According to the Defect theorem, we have in fact $vu \neq uv$. As a consequence, i is necessarily the greatest integer such that $(uv)^i u$ is a prefix of w. This determines a unique word $\phi(X)$. According to Claim 2.5, this leads to determine a unique singleton I_1 such that $(\phi(X), \phi(Y)) \in I_1$ [1].

2) The case where $R \in XY\Delta^* \cap \Delta^* YX$
First, we notice that since vu is a primitive word, and since it cannot be a prefix of y, as in the proof of Lemma 3.1, necessarily, we have :

$$i + j \in [q_0 - 2, q_0] \tag{8}$$

where q_0 stands for the greatest integer such that $(uv)^{q_0} u$ is a prefix of w.
By examining the suffixes of R and w, we get a similar property :

$$i + j' \in [q'_0 - 2, q'_0] \tag{9}$$

where q'_0 stands for the greatest integer such that $(uv)^{q'_0} u$ is a suffix of w.
As a consequence, we get a constant number of candidates (at most 9) for the pair of integers $(h, h') = (i + j, i + j')$. We now consider one of these candidates (h, h'). First, we notice that according to the preceding equalities, if $j \leq 1$ or $j' \leq 1$, we directly get the integer i. According to Claim 2.5, this leads to define a set I_1 with elements the corresponding pairs of candidates $(\phi(X), \phi(Y))$. Now, we assume that both the integers j, j' are greater than 1.
Let $w_0 = ((uv)^h u)^{-1} w$, and let $w' = w_0((uv)^{h'} u)^{-1}$. According to the structure of the word $R \in XY\Delta^* \cap \Delta^* YX$, different cases may occur :

[1] Clearly, if X^2 is a suffix of R, a similar conclusion may be obtain by considering the suffixes of w

a) The case where $R \in XY^2\Delta^*$

With this condition, the word $y(uv)^{j'}(vu)^j y$ is a prefix of w'.

- If $|uv| \geq |sr|$, since $j' \geq 2$, and since vu is a primitive word, according to Claim 2.1, we have $k = k_1$, where k_1 stands for the unique integer such that $(rs)^{k_1}r(uv)^2$ is a prefix of w'. Set $K_1 = \{k_1\}$.

- If $|uv| < |sr|$ then, according to the theorem of Fine and Wilf, the longest common prefix between the word $(uv)^{j'}(vu)^j$ and a word in $(sr)^+$ is in fact prefix of the word $(sr)^4$.
  - If $(uv)^{j'}(vu)^j$ is not a prefix of any word in $(sr)^+$, then we have $k \in K_1$, with $K_1 = [p_{max} - 4, p_{max}]$ (as in Lemma 3.1, p_{max} stands for the greatest integer such that $(rs)^{p_{max}}r$ is a prefix of w').
  - Otherwise, once more according to the theorem of Fine and Wilf, j' is the greatest integer such that $(uv)^{j'}$ is a prefix of $(sr)^4$. This leads to determine a unique integer i, thus a corresponding singleton I_1 such that $(\phi(X), \phi(Y)) \in I_1$.

b) The case where $R \in XYX\Delta^*$

With this condition, the word $y(uv)^2$ is necessarily a prefix of w'. Consequently, if $|uv| \geq |sr|$, according to Claim 2.1, k is the unique integer such that $(rs)^k r(uv)^2$ is a prefix of w'. Now, we assume that $|uv| < |sr|$.
As in the proof of Lemma 3.1, if $(uv)^*u \cap (sr)^* \neq \emptyset$, the we denote by q_{cycle} the unique integer (if it exists) such that $(uv)^{q_{cycle}}u \in (sr)^*$. We shall distinguish the following new different cases :

- $R \in XYXY\Delta^*$
  The word $(rs)^k r(uv)^{j'+i+j}u(rs)^2$ is a prefix of w'. As a consequence :
  - If $(uv)^{j'+i+j}u$ does not belong to $(sr)^+s$ then, necessarily, the integer k belongs to the interval $K_1 = [p_{max} - 2, p_{max}]$ (as indicated above, p_{max} stands for the greatest integer such that $(rs)^{p_{max}}r$ is a prefix of w').
  - If $(uv)^{j'+i+j}u \in (sr)^+s$ then, according to the theorem of Fine and Wilf, there exist a unique positive integer q_{cycle} such that $(uv)^{q_{cycle}}u \in (sr)^*s$. As a consequence, the tuple (i, j, j') satisfies the linear diophantine system :

  $$i + j = h,\ i + j + j' = q_{cycle},\ i + j' = h' \qquad (10)$$

  Clearly, this system has a unique solution (i, j, j'). As a consequence of Claim 2.5, this determines a unique singleton I_1, such that the pair of words $(\phi(X), \phi(Y))$ belongs to I_1.

- **$R \in XYX^pY\Delta^*$, with $p \geq 3$** [2]
  We set $f = (uv)^{h'}u((uv)^i u)^{p-2}(uv)^h u$. By definition, the word $yf(rs)^2$ is a prefix of w'.

[2] Since we assume that $R \in XY\Delta^* \cap \Delta^*YX$, the condition $R \in XYX^p$, with $p \geq 1$, does not hold

- First, we assume that the word f belongs to $(sr)^+s$. This condition implies $|uv| < |sr|$ (otherwise, according to the Theorem of Fine and Wilf, since $k, i \geq 2$, we should have $uv = rs$, a contradiction with Condition 3.3). As a consequence, the word uv is necessarily a proper prefix of sr.
  * Assume that $(sr)^2s$ is a prefix of f.
    Since $uv \neq vu$, and since $rs \notin (uv)^*$, we have either $sr \in (uv)^{h'}u$ or $sr \in (uv)^{h'}(u(uv)^i)^+$. With the first condition, we obtain $i = h$, a contradiction with the fact that both the integers j, j' are greater than 1. Hence we have $sr \in (uv)^{h'}(u(uv)^i)^+$. But by considering the reversed words, since $f \in (sr)^*s$, we have also $rs \in (u(uv)^i)^+(uv)^{h'}$. According to Claim 2.1, since uv is a primitive word, we obtain :
    $$h = h', \quad s = (uv)^{h'}u, \quad r \in ((uv)^i v)^+$$
    As a consequence, i is the unique integer such that the primitive root of r is equal to $\phi(X) = (uv)^i v$. This leads to determine a corresponding singleton I_1, with $(\phi(X), \phi(Y)) \in I_1$.
  * Now, we consider the case where f is a prefix of $(sr)^2s$, that is $f = s$ or $f = srs$. Since we get the integer pair (h, h'), we obtain two candidates for the word $g = ((uv)^{h'}u)^{-1}f((uv)^h u)^{-1} = ((uv)^i u)^{p-2}$. Since we get the integer p, this leads to determine a unique integer i, thus a new set I_1' with elements the corresponding candidates $(\phi(X), \phi(Y))$. We finally substitute I_1 to the union of I_1 and I_1'.
- Now, we assume that we have $f \notin (sr)^+s$. Since rs is a primitive word, and since $yf(rs)^2$ is a prefix of w', as for Relation (8), we obtain $k \in K_2$, with $K_2 = [p_{max} - 2, p_{max}]$.

- $R \in XYX^2Y\Delta^*$
  With this condition, the word $f = (uv)^{h'}u(uv)^h u$ is a prefix of $y^{-1}w'$.
  - First, we consider the case where f does not belong to $(sr)^+s$. In a similar way, we obtain $k \in K_2 = [p_{max} - 4, p_{max}]$.
  - Now, we assume that there exists an integer τ such that $f = (sr)^\tau s$ (according to the theorem of Fine and Wilf, we have $\tau \leq 4$).
  We notice that since the integers h, h' were given, no new constraints on the tuple (i, j, j') may be directly obtained.
  Let d be the greatest integer such that $(XYX)^d$ is a prefix of R. Set $T = (XYX)^{-d}R$. According to the structure of the word $T \in \Delta^*$, exactly one of the following cases occurs :

  - $T \in X^2\Delta^*$. We have $(\phi(XYX))^d X^2 = gy(uv)^{h'}u(uv)^i u(uv)^i u$, with $g = (uv)^h u(yf)^{d-1}$. Since we have $i < h$, and since the word $(uv)^{h'}u(uv)^i u$ is a proper prefix of f, the word $(uv)^{h'}u(uv)^i u(uv)^i u$ cannot belong to $(sr)^+s$. More precisely, the longest common prefix between $(uv)^{h'}u(uv)^i u(uv)^i u$, and a word in $(sr)^+s$ is necessarily prefix of f. This implies that we have $(yf)^{d-1}y = (rs)^z r$, with $z \in [p_{max} - 6, p_{max}]$. This determines a constant number of candidates for the length of y thus, a set K_2 of at most seven candidates for the integer k.

$$\underbrace{(u\,v)^h uy\,\overbrace{(uv)^{h'}u(uv)^h u}^{\mathrm{f}}\,y\,\overbrace{(uv)^{h'}u(uv)^h u}^{\mathrm{f}}\,y(uv)^{h'}}_{\phi(\mathrm{XYX})^{\mathrm{d}}}\,\underbrace{(uv)^i u}_{\phi(\mathrm{X})}\,\underbrace{(uv)^i u}_{\phi(\mathrm{X})}$$

– $T \in XY^2\Delta^*$. We have $(\phi(XYX))^d XY^2 = g(uv)^{j'}(vu)^j y(uv)^{j'}$, with $g = (uv)^h u(yf)^d y$. Since we have $j' < h'$, and since $j \geq 2$, the word $(uv)^{j'}(vu)^j$ cannot belong to the set $(sr)^+ s$.
According to the theorem of Fine and Wilf, the greatest integer n such that $(sr)^n$ is a prefix of $(uv)^{j'}(vu)^j$ is not greater than 2. Consequently, we have $(yf)^d y = (rs)^z r$, with $z \in [p_{max} - 2, p_{max}]$. As in the preceding case, this determines a corresponding set K_2 of candidates for the integer k.

$$\underbrace{(u\,v)^h uy\,\overbrace{(uv)^{h'}u(uv)^h u}^{\mathrm{f}}\,y\,\overbrace{(uv)^{h'}u(uv)^h u}^{\mathrm{f}}\,y(uv)^{j'}}_{\phi((\mathrm{XYX})^{\mathrm{d}}\mathrm{XY})}\,\underbrace{(vu)^j y(uv)^{j'}}_{\phi(\mathrm{Y})}$$

– $T \in Y\Delta^*$. We have $(\phi(XYX))^d Y = gy(uv)^{h'+j}uy(uv)^{j'}$, with $g = (uv)^h u(yf)^{d-1}$. Since we have $vu \neq uv$, the word $(uv)^{h'+j}$ cannot be a prefix of f thus it cannot be prefix of a word in $(sr)^+$. Moreover, according to the theorem of Fine and Wilf, the longest common prefix between $(uv)^{h'+j}$, and an arbitrary word in $(sr)^+ s$, is a prefix of $(sr)^2$. As a consequence we have $(yf)^{d-1}y = (rs)^z r$, with $z \in [p_{max} - 2, p_{max}]$. Once more, this determines a two element set of candidates K_2 with $k \in K_2$.

Let $K = K_0 \cup K_1 \cup K_2$, and $I = I_0 \cup I_1$. Clearly the sets I and K satisfy the conditions of our lemma. This completes the proof.

■

We notice that the preceding study leads to an effective construction of the preceding set K and I. Moreover, according to (3), (8) (9) :

Lemma 3.3 *Let $w \in \Sigma^+$, and let $R \in \{X, Y\}^*$. With the condition of Section 3, denote (m, m') the unique pair of non-negative integers such that $R \in X^m Y\Delta^* \cap \Delta^* Y X^{m'}$.*
Let (u, v, r, s) be a tuple satisfying Condition 3.3, and let (ϕ, i, j, j', k) be a tuple satisfying Condition 3.4 with respect to (u, v, r, s). Set $y = (rs)^k r$.
If $y \neq v$ then the following property holds :
(i) If $u \neq \varepsilon$ and $max(m, m') \geq 2$, then there exists a unique singleton $I' \subseteq \Sigma^+ \times \Sigma^+$ such that $(\phi(X), \phi(Y)) \in I'$.
(ii) Otherwise [3], there exists a subset H of $\mathbf{N}^2$, with constant cardinality, such that, for every solution ϕ, there exists a unique pair of integers $(h, h') \in H$ which satisfies the following system :

$$mi + j = h, \quad m'i + j' = h' \tag{11}$$

Moreover, the set H is depends only of the pair (u, v).

[3] This condition is expressed by $u = \varepsilon$ or $u \neq \varepsilon$ and $m = n = 1$

By definition, given an integer $k \in K$, we directly get the word y. We now explain how y, and the preceding pair of words (r, s), allow to compute corresponding candidates for the words $\phi(X)$ and $\phi(Y)$.

3.2 The case where the tuple (u, v, y) is given

As we shown it above, given a candidate for the period of $\phi(X)$, and a candidate for the period of $\phi(Y)$, there exist two sets, with constant cardinalities, namely I and K, such that either $(\phi(X), \phi(Y)) \in I$, or the preceding integer k belongs to K. In the first case, by computing the word $\phi(R)$, it will be easy to verify whether the corresponding morphism ϕ is a solution.
In the case where only the integer k is given (thus the word $y = (rs)^k r$ is given), the following result gives precisions concerning the pair $(\phi(X), \phi(Y))$.

Lemma 3.4 *With the condition of Section 3, given $w \in \Sigma^+$, $R \in \{X, Y\}^*$, and given the set K of Lemma 3.1 or Lemma 3.2, the following property holds :*
Given an integer $k \in K$, there exist :
- a finite set $J \in \Sigma^+ \times \Sigma^+$, with constant cardinality,
- and a linear system of diophantine constraints (T),
such that, if $\phi(R) = w$ then one at least of the following conditions holds :
(i) the tuple (i, j, j') satisfies System (T).
(ii) the pair $(\phi(X), \phi(Y))$ belongs to J.
Moreover, with Condition (i), if the system (T) has more than one solution then all the corresponding morphisms ϕ are solutions of Problem EQUA2.

Proof of Lemma 3.4

Let $k \in K$, and let $y = (rs)^k r$. If the condition (i) of Lemma 3.3 holds, then we directly get the set J. Without loss of generality, we may assume that only the condition (ii) in Lemma 3.3 holds. With this restriction, we notice that if $0 \leq j \leq 1$ or $0 \leq j' \leq 1$ then, as a consequence of System (11), we determine directly the integer i thus, according to Claim 2.5, the pair $(\phi(X), \phi(Y))$. Let J_0 be the corresponding set of candidates for the pair $(\phi(X), \phi(Y))$ (we have $|J_0| \leq 4|H|$). In all the next of our proof, we assume that both the integers j, j' are greater than 1.

a) The case where $u = \varepsilon$. By definition, we have $\phi(X) = v^i$. Moreover, as in the preceding proofs, we may assume that $i \geq 2$ (otherwise, we obtain a new set of candidates, namely J_1 for the pair $(\phi(X), \phi(Y))$). Clearly, there exists a unique sequence of non-negative integers $(m_0, ..., m_n)$ such that $R = X^{m_0}Y....YX^{m_n}$. In a similar way, given the solution ϕ, there exists a unique sequence of integers $(h_0, ..., h_n)$, such that $\phi(R) = v^{h_0}.y....yv^{h_n}$. In fact, for each integer $a \in [1, n]$, we have $h_a \geq 2$. (indeed, we have $h_a \geq min\{i, j + j'\} \geq 2$). More precisely, since v cannot a prefix of y, and since it is a primitive word :

- With the notation of Lemma 3.3, we have $h_0 = h$.
- For each integer $a \in [1, n-1]$, h_a is the unique integer such that $v^{h_a}yv^2$ is a prefix of the word $(v^{h_0}y...yv^{h_{a-1}}y)^{-1}w$.

- We have $j' + m_n i = h_n (= h')$.

As a consequence, the tuple of integers (i, j, j') satisfies the following system of linear diophantine equations :

$$m_0 i + j = h_0, \quad j' + m_a i + j = h_a \ \ (1 \leq a \leq n-1), \quad j' + m_n i = h_n \qquad (T)$$

First, we consider the case where :

$$R = (X^m Y X^{m'})^n, \quad w = (v^h y v^{h'})^n$$

With such a condition, our system (T) is equivalent to :

$$mi + j = h, \quad m'i + j' = h'$$

and it is esay to see that each solution of (T) leads to determine a corresponding solution of Problem EQUA2.
In all the other cases, System (T) has at most one solution (i, j, j'). Clearly, this solution leads to determine a unique set J_1, such that the corresponding pair of words $(\phi(X), \phi(Y))$ belongs to J_1.
Set $J = J_0 \cup J_1$. With this notation, we obtain the conclusion of Lemma 3.4.

b) The case where $u \neq \varepsilon$, with $y \neq v$. Since we assume that the condition (ii) of Lemma 3.3 holds, necessarily, we have $max\{m, m'\} \leq 1$, hence the word R belongs to $XY\Delta^*$. We notice that if XYX is a prefix of R, the word $(uv)^h uy(uv)^{h'} u$ is a prefix of w. Howether, no other constraint than System (11) may be directly obtained.
Let d be the greatest integer such that the word $(XYX)^d$ is a prefix of R and let $S = (XYX)^{-d} R$. According to the structure of S, different cases may occur :

- If $S = \varepsilon$, then every tuple (i, j, j') which is solution of System (11) leads to determine a solution ϕ of Problem EQUA2.

- Assume that $S \in Y\Delta^*$. Notice that necessarily, we have $d \geq 1$ (indeed, the word XY is a prefix of R). Let $w_1 = ((uv)^h uy(uv)^{h'} u)^{d-1}$, $w_2 = (uv)^h u$, and $w'' = (w_1 w_2)^{-1} w$. With this notation, the word $y(uv)^{h'+j} uy(uv)^2$ is a prefix of w''. Denote by q_1 the greatest integer such that $y(uv)^{q_1} u$ is a prefix of w''. Trivially, we have $2 \leq h' + j \leq q_1$.

  - The case where $|uv| \geq |y|$.
    Assume that we have $h' + j \leq q_1 - 2$. With this condition, since the word $y(uv)^{h'+j} uy(uv)^2$ is a prefix of w", necessarily, the word yuv is a proper prefix of vuv. But according to Claim 2.1, since uv is a primitive word, we have $y = v$, a contradiction with the condition of Case b). Consequently, we have $h' + j \in \{q_1 - 1, q_1\}$.
  - The case where $|uv| < |y|$.
    Since vu cannot be a prefix of y, we obtain $h' + j = q_1$.

  In each case, according to Claim 2.5, we determine a unique set J_1, with $|J_1| \leq 1$, and such that $(\phi(X), \phi(Y)) \in J_1$.

- Now, we assume that $S \in X^2\Delta^*$. Since X^2 cannot be a prefix of R, once more we have $d \geq 1$. With the preceding notation, the word $y(uv)^{h'}u(uv)^i u(uv)^2$ is a prefix of w''. Since $uv \neq vu$, we have $i = q_2$, where q_2 stands for the greatest integer such that $y(uv)^{h'}u(uv)^{q_2}u$ is a prefix of w''. This determines a corresponding singleton J_1.

- The last case corresponds to XY^2 being a prefix of R (indeed, since the integer d is maximal, the word XYX cannot be a prefix of S). Let $w_1' = ((uv)^h uy(uv)^{h'}u)^d$, and let $w_1'' = (w_1'w_2)^{-1}w$. Since the word $y(uv)^{j'}(vu)^j y$ is a prefix of w_1'', with $j \geq 2$, and since $vu \neq uv$, we have $j' = q_3$, where q_3 is the greatest integer such that $(uv)^{q_3}$ is a prefix of w_1''. Once more, this determines a new singleton J_1 such that $(\phi(X), \phi(Y)) \in J_1$.

We set $J = J_0 \cup J_1$, and (T)=(11). Once more we obtain the conclusion of our lemma.

c) The case where $y = v$. (According to Condition 3.3, we have $u \neq \varepsilon$). Notice that, since $\phi(Y) = (vu)^{j+j'}v$, without loss of generality, we may assume that $j' = 0$. With this condition, for every solution ϕ, we have $\phi(XY) = (uv)^{i+j+1}$.
There exists a unique sequence of words $(Z_a)_{1 \leq a \leq n}$, which satisfies the following properties :

- $R = Z_1 ... Z_n$,
- For each $a \in [1, n]$, we have $Z_a \in (XY)^+ \cup (XY)^*X \cup (YX)^+ \cup (YX)^*Y$.
- for each $a \in [1, n-1]$:
  - If $Z_a \in (XY)^+$ then $Z_{a+1} \in Y\Delta^*$
  - If $Z_a \in (XY)^+X$ then $Z_{a+1} \in X\Delta^*$
  - If $Z_a \in (YX)^+$ then $Z_{a+1} \in X\Delta^*$
  - If $Z_a \in (YX)^+Y$ then $Z_{a+1} \in Y\Delta^*$
  - If $Z_a = X$ then $Z_{a+1} \in X\Delta^* \cup \{\varepsilon\}$
  - If $Z_a = Y$ then $Z_{a+1} \in Y\Delta^* \cup \{\varepsilon\}$

For each integer $a \in [1, n]$, we set $w_a = \phi(Z_a)$. Since uv and vu are primitive words, and since we assume that both the integers i, j are greater than 1, we obtain the following property :

Condition 3.5 *If $Z_a \in (XY)^+$ ($(XY)^+X$, $(YX)^+$, $(YX)^+Y$), then w_a is the longest prefix of $(w_1 ... w_{a-1})^{-1}w$ which belongs to $(uv)^+$, ($(uv)^+u$, $(vu)^+$, $(vu)^+v$).*

As a consequence, if $Z_a \in (XY)^d$ ($(XY)^dX$, $(YX)^d$, $(YX)^dY$), with $d > 0$, then the pair (i, j) satisfies the equation (12) ((13), (12), (14)), which is defined as indicated the following :

$$(i + j + 1)|uv|d = |w_a| \tag{12}$$

$$((i + j + 1)d + i)|uv| + |u| = |w_a| \tag{13}$$

$$((i+j+1)d+j)|uv|+|v|=|w_a| \tag{14}$$

Let (T) be the conjunction of the corresponding equations for all the integers $a \in [1,n]$. By definition, if $Z_n = X$ (Y) then, necessarily we have $Z_{n-1} = X$ (Y). Let $a \in [1,n]$:

- If $Z_a = X$ and $Z_{a+1} = X$, then the preceding integer i is the greatest one such that $(uv)^i u$ is a prefix of $(w_1...w_{a-1})^{-1}w$. Let J_1 be the singleton with element the corresponding pair of words $(\phi(X), \phi(Y))$.
- If $Z_a = Y$ and $Z_{a+1} = Y$, then we have $j = q_1$, where q_1 is the greatest integer such that $(vu)^{q_1}$ is a prefix of $(w_1...w_{a-1})^{-1}w$. Let J_1 be the corresponding set of candidates $(\phi(X), \phi(Y))$.
- Now, we assume that $Z_n \notin \{X, Y\}$.
  - In the case where $R \in \{XY, YX\}^+ \cup ((XY)^d X)^+$, the system (T) is equivalent to one of the preceding equations (12), (13), (14). Conversely, each solution of (T) leads to a corresponding solution of EQUA2.
  - Otherwise, the resulting system has at most one solution (i,j). This determines a unique singleton J_1 such that $(\phi(X), \phi(Y)) \in J_1$.

Set $J = J_0 \cup J_1$. With these notations, once more we obtain the conclusion of Lemma 3.4. This completes the proof.

■

Notice that if (T) has a unique solution then, by computing the word $\phi(R)$, it will be easy to decide whether the corresponding morphism ϕ is solution of Problem EQUA2.

Example 3.5 *Let* $R = X^4(YX^2)^2YX^3$ *and* $w = (a^3b)^5(a(a^3b)^6)^3$.
Assume that $u = \varepsilon$, $v = a^3b$ *and* $y = a$. *With the notation in the proof of Lemma 3.4, Case a), we have :*
$h_0 = 5$, $h_1 = h_2 = h_3 = 6$, $m_0 = 4$, $m_1 = 2$, $m_3 = 3$. *The tuple* (i, j, j') *is solution of the linear system :*
$4i + j = 5$, $\quad j' + 2i + j = 6$, $\quad j' + 3i = 6$. *This system has a unique solution :* $(i, j, j') = (1, 1, 3)$, *which corresponds to the following morphism :*
$\phi : X \to a^3b, \quad Y \to a^3ba(a^3b)^3$

3.3 How to obtain candidates for the pairs of words (u, v), (r, s)

Let $w \in \Sigma^+$, and $R \in \{X, Y\}^*$, and let ϕ be a solution of Equation (R, w). In Section 3.1, we have seen that there exist a tuple (u, v, r, s), and a tuple of integers (i, j, j', k), such that (ϕ, i, j, j', k) satisfies Condition 3.4 with respect to (u, v, r, s). We have also explained how to determine the integers i, j, j', k, given the tuples (u, v, r, s).
Now, we shall see how to compute candidates for the tuple (u, v, r, s).
More precisely, given the equation (R, w), and a solution ϕ, we shall prove that there

exists a set Q, with $|Q| = O(\ln^2 |w|)$, and such that the preceding tuple (u, v, r, s) belongs to Q.

- First, we assume that $R \in XY\Delta^* \cap \Delta^*YX$. By definition, the word $\phi(X)$ is necessarily an overlap of w. According to Condition 2.1 :

  Claim 3.7 *Given a solution ϕ of Problem EQUA2, there exists a pair of words $(u, v) \in OVL(w)$, such that $\phi(X) \in (uv)^*u$.*

- Now, assume that $R \in X^2\Delta^*$. Since $(\phi(X))^2$, is a prefix of w, there exists a primitive word v such that the word $\phi(X)$ belongs to v^+.

  Claim 3.8 *Given a solution of EQUA2, there exists a (primitive) word $v \in LSQR(w)$, such that $\phi(X) \in v^+$ (thus $\phi(X) \in (uv)^+u$, with $u = \varepsilon$).*

- Clearly, if $R \in \Delta^*X^2$, a similar conclusion holds by considering the suffixes. Moreover, if $R \in Y^2\Delta^* \cup \Delta^*Y^2$, by exchanging the letters X and Y, a similar study may be done.

In all the cases, according to Claim 2.2 or Claim 2.3, we get a set Q, such that there exists a pair of words $(u, v) \in Q$, with $\phi(X) \in (uv)^*u$.

Now, we assume that we get the preceding pair of words (u, v). As in Section 3.1, we may define corresponding words y', y'', y and a pair of words (r, s) such that the tuple (u, v, r, s) satisfies Condition 3.3, and such that the morphism ϕ satisfies Condition 3.4 with respect to (u, v, r, s).
Given an instance of Problem EQUA2, and given the preceding pair of words (u, v), we shall explain how to determine a set $T_{(u,v)}$, with elements candidates for the pair (r, s). In fact, two cases may occur :
- Assume that $y = v$. Clearly, we have $(r, s) \in OVL(v)$.
- Now, we assume that $y \neq v$, moreover, without loss of generality, we may assume that the condition (ii) of Lemma 3.3 holds (otherwise, we directly get the pair $(\phi(X), \phi(Y))$).
According to Lemma 3.3, given the pair of words (u, v), there exists a set H, with constant cardinality, such that $(mi + j, j' + m'i) = (h, h') \in H$. Moreover, it is important to recall that the set H depends only of the pair (u, v).
Set $w_1 = ((uv)^h u)^{-1} w$ and $w' = w_1((uv)^{h'} u)^{-1}$ (clearly, we get a constant number of candidates for the word w'). By construction, the word y is an overlap of one of these candidates. Consequently, by definition, the pair of words (r, s) belongs to the union of the corresponding sets $OVL(w')$, namely U.

Now, we denote by $T_{(u,v)}$ the union of the preceding set $OVL(v)$ with the set U. According to Claim 2.2, we have $|T_{(u,v)}| \sim \ln |w|$ moreover, by construction, the pair (r, s) belongs to $T_{(u,v)}$.

Let $Q_{(u,v)}$ be the set of the corresponding tuples (u, v, r', s') for all the pairs of words $(r', s') \in T_{(u,v)}$, and let Q be the union of the preceding sets $Q_{(u',v')}$ for all the words $(u', v') \in OVL(w)$. By construction :

Claim 3.9 *(i) we have $|Q| \sim \ln^2 |w|$.*
(ii) For every solution ϕ of Problem EQUA2, there exists a tuple $(u, v, r, s) \in Q$, such that Condition 3.3 holds, and such that ϕ satisfies Condition 3.4 with respect to the tuple (u, v, r, s).

3.4 Algorithmic interpretation

With the conditions of Section 3, Claim 3.9 leads to an algorithm for deciding if Problem EQUA2 has a solution. Indeed, for each candidate $(u, v, r, s) \in Q$, we shall apply the results of Section 3.1 and Section 3.2 for computing the corresponding tuple of integers (i, j, j', k).

The main sheme of the corresponding algorithm is described bellow. This algorithm makes use of two functions, namely TEST1 and TEST2. The main feature of these functions is to verify whether the candidates ϕ, which was determined by the preceding sets H, I, J, is a solution of our equation (R, w).

Function TEST1 **: boolean;**
input : finite set of pairs of words L, and a boolean variable *answer* ;

```
for each pair (φ(X), φ(Y)) ∈ L do
    compute the prefix w' of φ(R) with length |w| ; {Step 1}
    if w' = w then answer ← TRUE {Step 2}
    endif
endfor
TEST1 ← answer
endfunction ;
```

Clearly, Step 1 and Step 2 require time $O(|w|)$. Consequently, applying Function TEST1 requires time $O(|w||L|)$.

Function TEST2 **: boolean;**
input : - linear diophantine system (T), with at most three unknowns ;
- pair of words $(u, v) \in \Sigma^* \times \Sigma^+$;
- boolean variable *answer* ;

```
by substituting the variables, compute the set S of solutions (i, j, j') ; {Step 1}
if |S| = 1 then
    by applying Claim 2.5 compute L = {(φ(X), φ(Y))} ; {Step 2}
    answer ← TEST1(L) {Step 3}
else if |S| > 1 then answer ← TRUE
endif ;
TEST2 ← answer
endfunction ;
```

In Step 1, we apply in time $O(|R|)$ the algorithm of Gauss-Jordan for computing the set of solutions S (recall that we assume that $|R| \le |w|$). Since Step 2 requires time $O(w)$, and since Step 3 requires time $O(|w||L|)$, with $|L| = 1$, applying Function TEST2 requires time $O(|w|)$.

Algorithm 1

```
answer ← FALSE;
compute the set Q of the tuples (u, v, r, s) as indicated above ;
```

for each tuple $(u, v, r, s) \in Q$ **do**
compute the preceding sets $I, I' \subseteq \Sigma^+ \times \Sigma^+$, and $K \subseteq \mathbf{N}$;
$answer \leftarrow TEST1(I \cup I')$; **{Step 1}**

for each integer $k \in K$ **do**
compute the set J and the system (T) ;
$answer \leftarrow TEST1(J)$; **{Step 2}**
$answer \leftarrow TEST2(u, v, (T))$ **{Step 3}**
endfor
endfor
endalgorithm

Complexity of Algorithm 1

1. Computing all the pairs (u, v) may be done in time $O(|w|)$ by applying the KMP-algorithm [16]. In a similar way, given a pair (u, v), computing the corresponding pairs (r, s) may be done in time $O(|w|)$. Since we get $O(\ln |w|)$ candidates for the pair (u, v), the computation of all the tuples candidates (u, v, r, s) may be done in time $O(|w| + |w| \ln |w|)$, thus in time $O(|w| \ln |w|)$.

2. Given a tuple (u, v, r, s) applying the constructions in the proof of the preceding lemma takes time $O(|w|)$. Particularly, computing the coefficients of the diophantine systems lays upon the two following methods.

   (a) Given two words t, t', determine the greatest integer n such that t^n is a prefix of t'.

   (b) Given three words t, t', t", determine a (minimal) integer n such that $t^n t'$ is a prefix of t'' (this last operation being done by applying the KMP-algorithm).

3. Since the cardinalities of the sets I, I', J are constant, in Step 1 and Step 2 applying function TEST1 requires time $O(|w|)$. In a similar way, in Step 3, applying function TEST2 may be done in time $O(|w|)$.

We also notice that if the preceding system (T) has more than one solution, then we may complete our algorithm in such a way that all the corresponding tuples (i, j, j') are computed. This allows in fact to give a representation of all the solutions of the input equation, the candidates $(\phi(X), \phi(Y))$ being examined in an exhaustive way. As a consequence :

Claim 3.10 *With the condition of Section 3, deciding whether the equation* (R, w) *has a solution may be done in time* $O(|w| \ln^2 |w|)$.

4 The case where $R \in XY\Delta^* \cap \Delta^* XY$

With this condition given a solution ϕ, the word $\phi(XY)$ is necessarily an overlap of w. This implies that there exists a pair of words $(\alpha, \beta) \in OVL(w)$, and a positive integer k such that we have $\phi(XY) = (\alpha\beta)^k \alpha$.

4.1 The case where $\phi(XY)$ is given

We may "simplify" our equation, as indicated in the following result :

Lemma 4.1 *Assume that the word R does not belong to the set $(XY + YX)^+(\varepsilon + YXY)$. Then there exists a pair of words $(S, t) \in \Delta^* \times \Sigma^*$ such that both the two following conditions holds :*
(i) The word S belongs to $(X^2 + Y^2)\Delta^+$.
(ii) Every solution ϕ of the equation (R, w) such that $\phi(XY) = (\alpha\beta)^k\alpha$ is a solution of the equation (S, t).

Proof of Lemma 4.1

Let d be the greatest integer such that $(XY)^d$ is a prefix of R, and let $T_1 = (XY)^{-d}R$. Let $s = \phi(XY)$, and let $t_1 = s^{-d}w$. If $T_1 \in (X^2 + Y^2)\Delta^+$, then we get our result, by considering the equation (T_1, t_1).
Otherwise we denote by d' be the greatest integer such that the set $(XY + YX)^{d'}$ contains a prefix of T_1 and let $S = (XY + YX)^{-d'}T_1$. We have $\phi(YX) = s'$, where s' stands for the prefix of t_1 with length $|s|$. Let $t = s'^{-d'}t_1$. [4]
By construction, the word S belongs to $(X^2+Y^2)\Delta^+$. Moreover, since ϕ is a solution of the equation (T_1, t_1), it is also a solution of the equation (S, t). This completes the proof of our lemma.

■

Example 4.2 *Let $R = XYXYYXXYY^2XY$, $w = abaabaaababaaaaba$ and $s = \phi(XY) = aba$.*
We have $T_1 = YXXYY^2XY$, $t_1 = aababaaaaba$, and $s' = \phi(YX) = aab$.
This implies that ϕ is solution of the equation $(Y^2XY, aaaba)$.

Remark 4.3
1) Assume that word R belongs to $(XY + YX)^+ \setminus (XY)^+$. The construction in the proof of Lemma 4.1 leads to determine two words, namely s and s', such that $\phi(XY) = s$ and $\phi(YX) = s'$.
This implies that the solutions of Equation (R, t) are all the morphisms ϕ such that we have $\phi(X)s'\phi(Y) = s^2$. The problem comes down to determine the different occurrences of the word s' in s^2 : once more that will be done, in time $O(|w|)$, by applying the KMP-algorithm.

2) Now, assume that $R \in (XY + YX)^*YXY$. Since we have $S = Y$, we directly get the word $\phi(Y) = t_1$. According to Claim 2.5, this leads to compute a set I, with $(\phi(X), \phi(Y)) \in I$.

Algorithmic interpretation

Assume that we get both the word $\phi(XY)$, and a primitive word v such that $\phi(X) \in v^+$. With the notation of Condition 3.4, we have $\phi(X) = v^i$ and $\phi(XY) = v^jyv^{j'}$, with v not a prefix of y, nor a suffix of y. Since y is the shortest word such that

[4] Since we assume that ϕ is a unique decipherable morphism, we have $s \neq s'$.

$\phi(Y) \in v^+yv^+$, it is easily computable. After that, we may apply the construction in the proof of Lemma 3.4 for computing the correspondings set J and the corresponding system T.
Clearly, since X, Y play a symetrical role, a similar conclusion may be done if $\phi(Y) = v^+$. Since we have $v \in LSQR(t)$, we get $O(\ln |w|)$ candidates v. Consequently :

Claim 4.11 *Assume that* $(XY+YX)^+(\varepsilon+YXY)$. *Given the word* $\phi(XY)$ *deciding whether* ϕ *is a solution of our equation* (R, w) *requires time* $O(|w| \ln |w|)$.

The corresponding algorithm is described as follows :

```
Function TEST3 : boolean ;
input :   - finite set of words L such that φ(XY) ∈ L ;
          - boolean variable answer ;

    for each z ∈ L do
        compute the words S and t of Lemma 4.1 ;
        if S = ε then apply the method in Remark 4.3
        else if S = Y then
                compute the corresponding set J of Remark 4.3
                answer ← TEST1(K)
            else for each word v ∈ LSQR(t) do
                    t1 ← the shortest word such that z = v+t1 ;
                    y ← the shortest word such that t1 = yv+;
                    compute the sets J and the system (T) as indicated
in the proof of Lemma 3.4 ;
                    answer ← TEST1(J) ;
                    answer ← TEST2(ε, v, (T)) ;
                endfor
            endif
        endif
    endfor ;
    TEST3 ← answer
endfunction ;
```

4.2 The case where the period of $\phi(XY)$ is given, with $|\phi(X)| \geq |\phi(Y)|$

Let (u, v) be a pair of words in $\Sigma^* \times \Sigma^+$, such that uv is a primitive word. Given a non-erasing morphism ϕ, and given a pair of integers (i, j), we consider the following condition :

Condition 4.6 *(i)* $\phi(X) = (uv)^i u$
(ii) $\phi(Y) = (vu)^j$

We say that the tuple (ϕ, i, j) satisfies Condition 4.6 with respect to the pair of words (u, v).

Lemma 4.4 *Let $R \in XY\Delta^* \cap \Delta^*XY$, and let $w \in \Sigma^*$. Given a pair of words $(u, v) \in \Sigma^* \times \Sigma^+$, with uv a primitive word, there exist :*
- a singleton $H \subseteq \Sigma^* \times \Sigma^+$,
- a two element set $K \subseteq \Sigma^+$,
- and a diophantine system (U),
such that, for every morphism $\phi : \Delta^* \rightarrow (\Sigma \cup \Delta)^*$, if $\phi(R) = w$ and if $\phi(XY) \in (uv)^+u$, then one at least of the three following conditions holds :
(i) $(\phi(X), \phi(Y)) \in H$.
(ii) there exists a solution (i, j) of (U) such that the tuple (ϕ, i, j) satisfies Condition 4.6, with respect to the pair of words (u, v).
(iii) $\phi(XY) \in K$.
Moreover, with Condition (ii), if the system (U) has more than one solution (i, j), than all the corresponding morphisms ϕ are solutions of Equation (R, w).

Proof of Lemma 4.4

Let k_{max} be the greatest integer such that $(uv)^{k_{max}}u$ is a prefix of w. Recall that we set $\phi(XY) = (uv)^k u$.
Set $K_0 = [0, 3] \cup [k_{max} - 2, k_{max}]$. Assume that the integer k does not belong to K_0, i.e. $k \in [4, k_{max} - 3]$. Since $k \geq 4$, and since $|\phi(X)| \geq |\phi(Y)|$, the word $(uv)^2$ is a prefix of $\phi(X)$.

a) The case where $u \neq \varepsilon$. Necessarily, the word $\phi(Y)$ is a suffix of $(uv)^k u$. Since $k \leq k_{max} - 2$, and since $(uv)^2$ is a prefix of $\phi(X)$, the word XYY is necessarily a prefix of R (indeed, the word $(vu)^2$ is a prefix of $(\phi(XY))^{-1}w$ moreover, we have $vu \neq uv$). This leads to consider two new cases :

- **vu is a suffix of $\phi(Y)$**
  This condition implies that the word vu is both prefix and suffix of $\phi(Y)$. But vu is a primitive word and $\phi(Y)$ is suffix of a word in $(uv)^+u$. As a consequence, there exists a pair of positive integers (i, j) such that the tuple (ϕ, i, j) satisfies Condition 4.6.
  Clearly, for every positive integer n, the word $\phi(XY^n)$ belongs to $(uv)^+u$.
  - If one of the two integers i, j is not greater than 1, then, according to Claim 2.5, we directly get corresponding candidates for the pair $(\phi(X), \phi(Y))$. Let H_0 be the set with elements these candidates.
  - Now, we assume that both the integers i, j are greater than 1.
  Let $(d_1, d_2, ..., d_m)$ be the longest sequence of positive integers such that $R = XY^{d_1}XY^{d_2}...XY^{d_m}S$, with $S \in \{\varepsilon, X\}$ or $S \in X^2\Delta^*$. Since $\phi(R) = w$, and since uv is a primitive word, there exists a unique sequence of words $(w_1, ..., w_m)$, a unique sequence of positive integers $(k_1, k_2, ..., k_m)$, and a word $s \in \{\varepsilon\} \cup \phi(X^2)\Delta^*$, such that each of the following properties holds :

$$\begin{gathered} k_p \geq 4 \\ w_a = \phi(XY^{d_a}) = (uv)^{k_a}u \quad (a \in [1, m]) \\ w = w_1.w_2...w_m s \end{gathered} \tag{15}$$

  In fact, k_1 is the greatest integer such that $(uv)^{k_1}u$ is a prefix of w and, for each integer $a \in [2, m]$, k_a is the greatest integer such that $(uv)^{k_a}u$ is a prefix

of the word $(w_1...w_{a-1})^{-1}w$.
According to (15), for each integer $a \in [1, m]$, we have :

$$|uv|i + |u| + jd_a|vu| = k_a|uv| + |u| \tag{16}$$

Moreover :
- If $S = \varepsilon$ then (i, j) is solution of the following system :

$$i + jd_a = k_a \quad (1 \leq a \leq m) \tag{17}$$

- If $S = X$, we have $\phi(X) = (w_1 \cdots w_m)^{-1}w$. This determines a unique word $\phi(X)$ thus, according to Claim 2.5 a unique singleton H_1 such that $(\phi(X), \phi(Y)) \in H_1$.
- Otherwise, necessarily the word $(uv)^i u.(uv)^i u$ is a prefix of $s = (w_1...w_m)^{-1}w$. Hence i is the unique integer such that $(uv)^i u(uv)^2$ is a prefix of s. According to Claim 2.5, this determines a new set H_1, such that $(\phi(X), \phi(Y)) \in H_1$.

- **$\phi(Y)$ is a proper suffix of vu**
  Let d be the greatest integer such that the word XY^d is a prefix of R. As we said it above (cf the begining of Case a)), we have $d \geq 2$.
  - If $d = 2$, since $k \leq k_{max} - 3$, and since $(uv)^2$ is a prefix of the word $\phi(X)$, necessarily, we have $\phi(Y) = v$. Let H_2 be the corresponding singleton with $(\phi(X), \phi(Y)) \in H_2$.
  - Now, we assume that we have $d > 2$, thus $d - 1 \geq 2$.
  According to the theorem of Fine and Wilf, and since we have $k \leq k_{max} - 3$, the word $\phi(Y^{d-1})$ is necessarily a proper prefix of $(vu)^2$. Consequently, we obtain $\phi(Y^{d-1}) \in \{v, vuv\}$. This leads to determine at most two candidates for the word $\phi(Y)$. According to Claim 2.5, this leads also to determine a new set $H_2 \in \Sigma^+ \times \Sigma^+$.
  Let $H = H_1 \cup H_2$. With this notation, the set H satisfies Condition (i) in our lemma. Moreover, System (17) satisfies the condition (ii) in the lemma.

b) The case where $u = \varepsilon$

First, we notice that the word v cannot be a prefix of $\phi(Y)$. Indeed, if v is a prefix of $\phi(Y)$, according to Claim 2.1, since the word $\phi(XY)$ belongs to v^+ and since v is a primitive word, the words $\phi(Y)$ and $\phi(X)$ belong to v^+, a contradiction with the fact that ϕ is a unique decipherable morphism.
Let (r, s) be the unique pair of words which satisfies the two following conditions :

Condition 4.7 *(i)* $0 \leq |r| < |v|$
(ii) $\phi(X) \in v^+r$
(iii) $v = rs$

Let d be the greatest integer such that $(XY)^d$ is a prefix of R. Since $R \in XY\Delta^* \cap \Delta^*XY$, and since $R \neq (XY)^d$, at most one of the two following cases may occur :

- **$(XY)^d X^2$ is a prefix of R**
  Since v is a primitive word, and since v^2 is a prefix of $\phi(X)$, there exists a unique integer n such that $v^n rv^2$ is a prefix of w (otherwise, we should

have $rv = vr$, thus $r = v$, a contradiction with the fact that ϕ is a unique decipherable morphism). Moreover, we have $\phi((XY)^d X) = v^n r$. This leads to directly get the word $\phi(XY)$. We set $K_1 = \{v^{[\frac{n}{d}]}\}$.

- $(XY)^d Y$ **is a prefix of** R (since $R \in XYX\Delta^*$, we have in fact $d \geq 1$)
  Since $R \in XY\Delta^* \cap \Delta^* XY$, there exists an integer $p \geq 1$ such that $R \in (XY)^d Y^p X\Delta^*$.
  Recall that v cannot be a prefix of $\phi(Y)$.
  - Assume that $|\phi(Y)| < |v|$.
  Since the longest common prefix between a word in v^+ and the word $\phi(Y)^p$ is necessarily a prefix of v^2, we have $\phi(XY) = v^k$, with $dk \in [k_{max} - 2, k_{max}]$. Let K_1 be the corresponding set of candidates for $\phi(XY)$.
  - If $|\phi(Y)| \geq |v|$, then we have $\phi(Y) \in sv^+$. Since rs is a primitive word, according to Claim 2.1, we have $\phi(XY) = v^{dk}$, with $dk \in [k_{max}-1, k_{max}] \subseteq K_1$.

Set $H = H_0 \cup H_1$, and $K = K_0 \cup K_1$. By construction, the set H (K) satisfies the condition (i) ((iii)) of Lemma 4.4. This completes the proof.

■

Now, we assume that we have $\phi(XY) = (uv)^k u$, with $|\phi(X)| < |\phi(Y)|$. Given a word $t \in \Sigma^*$, denote by $\tilde{t}$ the returned word (mirror image) of t. Let ϕ' be the morphism defined by $\phi'(\tilde{X}) = \widetilde{\phi(X)}$ and $\phi'(\tilde{Y}) = \widetilde{\phi(Y)}$. We have $\tilde{R} \in \tilde{Y}\tilde{X}\{\tilde{X}, \tilde{Y}\}^* \cap \{\tilde{X}, \tilde{Y}\}^* \tilde{Y}\tilde{X}$, and $\phi'(\tilde{Y}\tilde{X}) = (\tilde{u}\tilde{v})^k \tilde{u}$, with $|\phi'(\tilde{Y})| > |\phi'(\tilde{X})|$. By substituting $\tilde{Y}$ to X and $\tilde{X}$ to Y, we are in a case similar to the case of Section 4.2 for the equation $(\tilde{R}, \tilde{w})$. Particularly, Condition 4.6 is expressed as follows :

Condition 4.8 *(i)* $\phi'(\tilde{Y}) = (\tilde{u}\tilde{v})^i \tilde{u}$
(ii) $\phi'(\tilde{X}) = (\tilde{v}\tilde{u})^j$

Consequently, the result of Lemma 4.4 holds.

4.3 Algorithmic interpretation

Given a word $R \in XY\Delta^* \cap \Delta^* XY$, and given an arbitrary word $w \in \Sigma^*$, the preceding results lead to an algorithm for deciding whether Equation (R, w) has a solution or not. We now indicate its main steps :

Algorithm 2
$answer \leftarrow FALSE$;
$Q \leftarrow OVL(w)$; $Q' \leftarrow OVL(\tilde{w})$;

{ The case where $|\phi(X)| \geq |\phi(Y)|$ };
for each pair $(u, v) \in Q$ **do**
$k_{max} \leftarrow$ the greatest integer such that $(uv)^{k_{max}} u$ is a prefix of w ;
compute the sets H, K and the system (U), as indicated in the proof of Lemma 4.4 ;
$K \leftarrow K \cup [0, 3] \cup [k_{max} - 3, k_{max}]$;
$answer \leftarrow$ TEST1(H) ;
$answer \leftarrow$ TEST2$(u, v, (U))$;

$answer \leftarrow$ TEST3(K)
endfor

{ The case where $|\phi(X)| < |\phi(Y)|$ };
Apply the same the process with $\tilde{w}, \tilde{R}$ and Q'
endalgorithm ;

According to Claim 2.2, we have $|Q| = O(\ln|w|)$. Moreover, applying Function TEST1 and Function TEST2 requires time $O(|w|)$. Since applying Function TEST3 requires time $O(|w|\ln|w|)$, applying Algorithm 2 requires time $O(|w| + \ln|w|(|w| + |w|\ln|w|))$, thus time $O(|w|\ln^2|w|)$.

5 Concluding the preceding study

In this section, we consider an arbitrary two-unknown equation (R, w), with $R \in \{X, Y\}^*$, and $w \in \Sigma^*$. As a consequence of the preceding study, we now present the main sheme of our algorithm for deciding whether or not the equation (R, w) has a solution. This algorithm takes into account of all the special cases of equations and morphisms that we have mentionned above.

Algorithm 3
$answer \leftarrow FALSE$;

{ **The case of an erasing solution** }
$x \leftarrow$ the prefix of w with length $[\frac{w}{|R|_X}]$;
if $w = x^{|R|_X}$ **then** $answer \leftarrow TRUE$ { $\phi(X) = x, \phi(Y) = \varepsilon$ }
endif ;
$y \leftarrow$ the prefix of w with length $[\frac{w}{|R|_Y}]$;
if $w = y^{|R|_Y}$ **then** $answer \leftarrow TRUE$ { $\phi(Y) = y, \phi(X) = \varepsilon$ }
endif ;

{ **The case of a non-coding solution** }
$x \leftarrow$ the primitive root of w **;** $k \leftarrow [\frac{|w|}{x}]$;
if $k \geq 2$ **then**
if the equation $(i, j > 0,\ |R|_X i + |R|_Y j = k)$ has a solution **then**
$answer \leftarrow TRUE$ { $\phi(X) = x^i, \phi(Y) = x^j$ }
endif
endif ;

{ **Special classes of equations**}
if $R \in X^+Y^+$ **or** $R \in (XY)^+$ **then**
compute the variable $answer$ by applying the results of Section 2.7

{ **The general case**}
else if $R \in XY\Delta^* \cap YX\Delta^*$ **or** $R \in \{X^2, Y^2\}\Delta^* \cup \Delta^*\{X^2, Y^2\}$ **then**
apply Algorithm 1
else apply Algorithm 2 {The case where $R \in XY\Delta^* \cup \Delta^*XY$ }
endif
endif
endalgorithm ;

In each of the special cases, deciding whether or not Equation (R, w) has a solution requires time $O(|w|)$. Moreover, applying Algorithm 2 and Algorithm 3 requires time $O(|w| \ln^2 |w|)$. As a consequence, we get our main result :

Theorem 5.1 *Given a word $w \in \Sigma^*$, and given a word $R \in \{X, Y\}^*$, deciding whether there exists a morphism ϕ such that $\phi(R) = w$ may be implemented so that it requires time $(O(|w| \ln^2 |w|)$.*

We finally notice that our algorithms allow to give a complete description of all the solutions of PAT2. Indeed, searching the candidates is done in an exhaustive way.

Acknowledgement

The author is grateful to one of the anonymous referees, for detailed and usefull comments.

References

[1] A. Aho, Algorithms for Finding Patterns in Strings in : the Handbook of Computer Science, J. van Leeuwen editor, Elsevier Science Publisher, Amsterdam (1990).

[2] D. Angluin, Finding Patterns Common to a Set of Strings *Journ. of Computer and Syst. Sci.* **21** (1980) 46–62.

[3] A. Aho, M. Corasick, Efficient String Matching : An Aid to Bibliographic Search, *Comm. ACM* **18** (6) (1975) 333–340.

[4] A. Apostolico, F.P. Preparata, Optimal off-line detection of repetitions in a string, *Theoret. Comput. Sci.* **22** (1983) 297–315.

[5] K. Baker, Open problems on avoidable and unavoidable patterns, manuscript (Université de Rouen, France) (1992).

[6] J. Berstel, D.Perrin, "Theory of Codes", Academic Press (1985).

[7] R.S. Boyer, J.S. Moore, A fast string searching algorithm, *Comm. ACM* **20** (10) (1977) 62–72.

[8] M. Crochemore, An optimal algorithm for computing the repetitions in a word, *Information Proc. Letters* **12** (1981) 244–250.

[9] M. Crochemore, J. Néraud, Unitary monoid with two generators : an algorithmic point of view, in : *proceedings of CAAP'90* Lectures Notes in Computer Science **431**, Springer Verlag, New York/Berlin (1990).

[10] M. Crochemore, W. Rytter, Periodic prefixes of strings, in : *acts of Sequences'91* (1991).

[11] J.-P. Duval, Contribution à la combinatoire du monoide libre, Thèse de Doctorat d'Etat, Université de Rouen, France (1980).

[12] M.J. Fisher, M.S. Paterson, String Matching and other products, in : R.M. Karp ed., Complexity of Computation, *SIAM-AMS Proceedings (Amer. Mathematical Soc. Providence, RI)* **7** (1974) 113–125.

[13] M. Garey, D. Johnson, Computers and intractability, A guide to the theory of NP-completeness, W.H. Freeman and Company, San Francisco (1979).

[14] Z. Galil, J. Seiferas, Saving space in fast string-matching, *SIAM J. of Computer* (1980) 417–438.

[15] K.P. Jantke, Polynomial time inference of general pattterns languages, in : *Proceedings Symposium of Theoretical aspects of Computer Science* Lectures notes in Computer Science **166**, Springer-Verlag, New York/Berlin (1984) 314–325.

[16] D. Knuth, J. Morris, V. Pratt, Fast pattern matching in string, *SIAM Journal of Computation* **6** (2) (1977) 323–350.

[17] M. Lothaire, "Combinatorics on words", Encyclopedia of Mathematics and appl., Addison Wesley Publish. Company (1983).

[18] G. Landau, U. Vishkin, Fast string Matching with k Differences, *Journal of Comput. and Systeme Sci.* **37** (1988) 63–78.

[19] G.S. Makanin, The problem of solvability of equations in a free semigroup, *Mat. Sb.* **103** (1977) 147–236 (English trans. in : *Math USSR Sb.* **32**, 129–280).

[20] G. Main, J. Lorentz, Linear time recognition of squarefree strings, in "Combinatoric Algorithms on Words", A. Apostolico and Z. Galil editor, NATO ASI, Springer Verlag, Berlin (1985).

[21] E. Myers, W. Miller, Approximate matching of regular expressions, *Bulletin of Mathematical Biology* **51** (1) (1989) 5–37.

[22] J. Néraud, Elementariness of a finite set of words is co-NP-complete, *Theoretical Informatics and Applications* **24** (5) (1990) 459–470.

[23] J. Néraud, Deciding whether a finite set of words has rank at least two, *Theoretical Computer Science* **112** (1993) 311–337.

[24] O. Rabin, Discovering repetitions in strings, in : "Combinatoric Algorithms on Words", A. Apostolico and Z. Galil editor, NATO ASI, Springer Verlag, Berlin (1985).

[25] K. Thomson, Regular Expression Search Algorithm, *Comm. of ACM* **11** (6) (1968).

[26] R. Wagner, J. Seiferas, Correcting counter-automaton-recognizable languages, *SIAM J. of comput.* **7** (3) (1978).

Jean Néraud
LIR, Université de Rouen
LITP, Institut Blaise Pascal
Université de Rouen
Faculté des Sciences
F-76821 Mont Saint Aignan
France