# The Hardness of Solving Simple Word Equations 

Joel D. Day ${ }^{1}$, Florin Manea ${ }^{2}$, and Dirk Nowotka ${ }^{3}$

1 Kiel University, Department of Computer Science, Kiel, Germany jda@informatik.uni-kiel.de<br>2 Kiel University, Department of Computer Science, Kiel, Germany flm@informatik.uni-kiel.de<br>3 Kiel University, Department of Computer Science, Kiel, Germany<br>dn@informatik.uni-kiel.de


#### Abstract

We investigate the class of regular-ordered word equations. In such equations, each variable occurs at most once in each side and the order of the variables occurring in both left and right hand sides is preserved (the variables can be, however, separated by potentially distinct constant factors). Surprisingly, we obtain that solving such simple equations, even when the sides contain exactly the same variables, is NP-hard. By considerations regarding the combinatorial structure of the minimal solutions of the more general quadratic equations we obtain that the satisfiability problem for regular-ordered equations is in NP. The complexity of solving such word equations under regular constraints is also settled. Finally, we show that a related class of simple word equations, that generalises one-variable equations, is in P .


1998 ACM Subject Classification F.2.2 Nonnumerical Algorithms and Problems, F.4.3 Formal Languages

Keywords and phrases Word Equations, Regular Patterns, Regular Constraints

Digital Object Identifier 10.4230/LIPIcs.MFCS.2017.18

## 1 Introduction

A word equation is an equality $\alpha=\beta$, where $\alpha$ and $\beta$ are words over an alphabet $\Sigma \cup X$ (called the left, respectively, right side of the equation); $\Sigma=\{\mathrm{a}, \mathrm{b}, \mathrm{c}, \ldots\}$ is the alphabet of constants and $X=\left\{x_{1}, x_{2}, x_{3}, \ldots\right\}$ is the alphabet set of variables. A solution to the equation $\alpha=\beta$ is a morphism $h:(\Sigma \cup X)^{*} \rightarrow \Sigma^{*}$ that acts as the identity on $\Sigma$ and satisfies $h(\alpha)=h(\beta)$. For instance, $\alpha=x_{1} \mathrm{ab} x_{2}$ and $\beta=\mathrm{a} x_{1} x_{2} \mathrm{~b}$ define the equation $x_{1} \mathrm{ab} x_{2}=\mathrm{a} x_{1} x_{2} \mathrm{~b}$, whose solutions are the morphisms $h$ with $h\left(x_{1}\right)=\mathrm{a}^{k}$, for $k \geq 0$, and $h\left(x_{2}\right)=\mathrm{b}^{\ell}$, for $\ell \geq 0$.

The study of word equations (or the existential theory of equations over free monoids) is an important topic found at the intersection of algebra and computer science, with significant connections to, e.g., combinatorial group or monoid theory [19, 18, 2], unification [25, 11, 12], and, more recently, data base theory $[9,8]$. The problem of deciding whether a given word equation $\alpha=\beta$ has a solution or not, known as the satisfiability problem, was shown to be decidable by Makanin [20] (see Chapter 12 of [17] for a survey). Later it was shown that the satisfiability problem is in PSPACE by Plandowski [22]; a new proof of this result was obtained in [14], based on a new simple technique called recompression. However, it is conjectured that the satisfiability problem is in NP; this would match the known lower bounds: the satisfiability of word equations is NP-hard, as it follows immediately from, e.g., [4]. This hardness result holds in fact for much simpler classes of word equations, like quadratic equations (where the number of occurrences of each variable in $\alpha \beta$ is at most two), as shown in [3]. There are also cases when the satisfiability problem is tractable. For

© Joel D. Day, Florin Manea, and Dirk Nowotka;
licensed under Creative Commons License CC-BY
42nd International Symposium on Mathematical Foundations of Computer Science (MFCS 2017). Editors: Kim G. Larsen, Hans L. Bodlaender, and Jean-Francois Raskin; Article No. 18; pp. 18:1-18:14
instance, word equations with only one variable can be solved in linear time in the size of the equation, see [13]; equations with two variables can be solved in time $\mathcal{O}\left(|\alpha \beta|^{5}\right)$, see [1].

In most cases, the NP-hardness of the satisfiability problem for classes of word equations was shown as following from the NP-completeness of the matching problem for corresponding classes of patterns with variables. In the matching problem we essentially have to decide whether an equation $\alpha=\beta$, with $\alpha \in(\Sigma \cup X)^{*}$ and $\beta \in \Sigma^{*}$, has a solution; that is, only one side of the equation, called pattern, contains variables. The aforementioned results [4, 3] show, in fact, that the matching problem is NP-complete for general $\alpha$, respectively when $\alpha$ is quadratic. Many more tractability and intractability results concerning the matching problem are known (see [24, 6, 7]). In [5], efficient algorithms were defined for, among others, patterns which are regular (each variable has at most one occurrence), non-cross (between any two occurrences of a variable, no other distinct variable occurs), or patterns with only a constant number of variables occurring more than once.

Naturally, for a class of patterns that can be matched efficiently, the hardness of the satisfiability problem for word equations with sides in the respective class is no longer immediate. A study of such word equations was initiated in [21], where the following results were obtained. Firstly, the satisfiability problem for word equations with non-cross sides (for short non-cross equations) remains NP-hard. In particular, solving non-cross equations $\alpha=\beta$ where each variable occurs at most three times, at most twice in $\alpha$ and exactly once in $\beta$, is NP-hard. Secondly, the satisfiability of one-repeated variable equations (where at most one variable occurs more than once in $\alpha \beta$, but arbitrarily many other variables occur only once) having at least one non-repeated variable on each side, was shown to be trivially in P .

In this paper we mainly address the class of regular-ordered equations, whose sides are regular patterns and, moreover, the order of the variables occurring in both sides is the same. This seems to be one of the structurally simplest classes of equations whose number of variables is not bounded by a constant. One central motivation for studying these equations with a simple structure is that understanding their complexity and combinatorial properties may help us to identify a boundary between classes of word equations whose satisfiability is tractable and intractable. Moreover, we wish to gain a better understanding of the core reasons why solving word equations is hard. In the following, we overview our results, methods, and their connection to existing works from the literature.

Lower bounds. Our first result closes the main problem left open in [21]. Namely, we show that it is (still) NP-hard to solve regular (ordered) word equations. Note that in these word equations each variable occurs at most twice: at most once in every side. They are particular cases of both quadratic equations and non-cross equations, so the reductions showing the hardness of solving these more general equations do not carry over. To begin with, matching quadratic patterns is NP-hard, while matching regular patterns can be done in linear time. Showing the hardness of the matching problem for quadratic patterns in [3] relied on a simple reduction from 3-SAT, where the two occurrences of each variable were used to simulate an assignment of a corresponding variable in the SAT formula, respectively to ensure that this assignment satisfies the formula. To facilitate this final part, the second occurrences of the variables were grouped together, so the equation constructed in this reduction was not non-cross. Indeed, matching non-cross patterns can be done in polynomial time. So showing that solving non-cross equations is hard, in [21], required slightly different techniques. This time, the reduction was from an assignment problem in graphs. The (single) occurrences of the variables in one side of the equation were used to simulate an assignment in the graph, while the (two) occurrences of the variables from the other side were used for two reasons:
to ensure that the previously mentioned assignment is correctly constructed and to ensure that it also satisfies the requirements of the problem. For the second part it was also useful to allow the variables to occur in one side in a different order as in the other side.

As stated in [21], showing that the satisfiability problem for regular equations seems to require a totally different approach. Our hardness reduction relies on some novel ideas, and, unlike the aforementioned proofs, has a deep word-combinatorics core. As a first step, we define a reachability problem for a certain type of (regulated) string rewriting systems, and show it is NP-complete (in Lemma 7). This is achieved via a reduction from the strongly NP-complete problem 3-Partition [10]. Then we show that this reachability problem can be reduced to the satisfiability of regular-ordered word equations; in this reduction (described in the successive Lemmas 9, 10, and 11), we essentially try to encode the applications of the rewriting rules of the system into the periods of the words assigned to the variables in a solution to the equation. In doing this, we are able to only use one occurrence of each variable per side, and moreover to even have the variables in the same order in both sides.

Our reduction suggests the ability of this simple class of equations to model other natural problems in rewriting, combinatorics on words, and beyond. In this respect, our construction seems interesting with respect to the expressibility of word equations, as studied in [15].

Upper bounds. A consequence of the results in [23] is that the satisfiability problem for a certain class of word equations is in NP if the lengths of the minimal solutions of such equations (where the length of the solution defined by a morphism $h$ is the image of the equation's sides under $h$ ) are at most exponential. With this in mind, we show Lemma 14, which gives us an insight in the combinatorial structure of the minimal solutions of quadratic equations: if we follow around the minimal solutions the positions that are fixed inside the images of the variables by each terminal of the original equation (in order, starting with that terminal), we obtain sequences that should not contain repetitions. Consequently, in Proposition 17, we give a simple and concise proof of the fact that the image of any variable in a minimal solution to a regular-ordered equation is at most linear in the size of the equation. It immediately follows that the satisfiability problem for regular-ordered equations is in NP. While this result was expected, the approach we use to obtain it seems rather interesting to us, and also a promising approach to showing that other, more complicated, classes of restricted word equations can be solved in NP-time. For instance, it is an open problem to show this for arbitrary regular or quadratic equations. It is worth noting that our polynomial upper bound on length of minimal solutions of regular-ordered equations does not hold even for slightly relaxed versions of such equations. More precisely, non-cross equations $\alpha=\beta$ where the order of the variables is the same in both sides and each variable occurs exactly three times in $\alpha \beta$, but never only on one side, may already have exponentially long minimal solutions (see Proposition 2). To this end, it seems even more surprising that it is NP-hard to solve equations with such a simple structure (regular-ordered), which, moreover, have quadratically short solutions. As such, regular-ordered equations seem to be among the structurally simplest word-equations, whose satisfiability problem is intractable.

Extending our ideas, we settle the complexity of solving regular-ordered equations with regular constraints (as defined in [3], where each variable is associated with an NFA), which is in NP for regular-ordered equations whose sides contain exactly the same variables, or when the languages defining the scope of the variables are all accepted by NFAs with at most $c$ states, where $c$ is a constant. For regular-ordered equations with regular constraints without these restrictions, the problem remains PSPACE-complete.

Finally, we use again a reasoning on the structure of the minimal solutions of equations, similar to the above, to show that if we preserve the non-cross structure of the sides of the
considered word equations, but allow only one variable to occur an arbitrary number of times (all the others occur exactly once in total, and hence in at most one side), we get a class of equations whose satisfiability problem is in P . This problem is related to the one-repeated variable equations considered in [21]; in this case, we restrict the equations to a non-cross structure of the sides, but drop the condition that at least one non-repeated variable should occur on each side. Moreover, this problem generalises the one-variable equations [13], while preserving the tractability of their satisfiability problem. Last, but not least, this result shows that the pattern searching problem, in which, given a pattern $\alpha \in\left(\Sigma \cup\left\{x_{1}\right\}\right)^{*}$ containing constants and exactly one variable $x_{1}$ (occurring several times) and a text $\beta \in\left(\Sigma \cup\left\{x_{1}\right\}\right)^{*}$ containing constants and the same single (repeated) variable, we check whether there exists an assignment of $x_{1}$ that makes $\alpha$ a factor of $\beta$, is tractable; indeed, this problem is the same as checking whether the word equation $x_{2} \alpha x_{3}=\beta$, with $\alpha, \beta \in\left(\Sigma \cup\left\{x_{1}\right\}\right)^{*}$, is satisfiable.

## 2 Preliminaries

Let $\Sigma$ be an alphabet. We denote by $\Sigma^{*}$ the set of all words over $\Sigma$; by $\varepsilon$ we denote the empty word. Let $|w|$ denote the length of a word $w$. For $1 \leq i \leq j \leq|w|$ we denote by $w[i]$ the letter on the $i^{\text {th }}$ position of $w$ and $w[i . . j]=w[i] w[i+1] \cdots w[j]$. A word $w$ is $p$-periodic for $p \in \mathbb{N}$ (and $p$ is called a period of $w$ ) if $w[i]=w[i+p]$ for all $1 \leq i \leq|w|-p$; the smallest period of a word is called its period. By extension, for a word $w$ of period $p$, we sometimes call $w[1 . . p]$ the period of $w$. Let $w=x y z$ for some words $x, y, z \in \Sigma^{*}$, then $x$ is called prefix of $w, y$ is a factor of $w$, and $z$ is a suffix of $w$. Two words $w$ and $u$ are called conjugate if there exist non-empty words $x, y$ such that $w=x y$ and $u=y x$. The powers of $w$ are defined by $w^{0}=\varepsilon$, $w^{n}=w w^{n-1}$ for $n \geq 1$, and $w^{\omega}=w w \cdots$, an infinite concatenation of the word $w$.

Let $\Sigma=\{\mathrm{a}, \mathrm{b}, \mathrm{c}, \ldots\}$ be an alphabet of constants and let $X=\left\{x_{1}, x_{2}, x_{3}, \ldots\right\}$ be an alphabet of variables. We assume that $X$ and $\Sigma$ are disjoint. A word $\alpha \in(\Sigma \cup X)^{*}$ is usually called pattern. For a pattern $\alpha$ and a letter $z \in \Sigma \cup X$, let $|\alpha|_{z}$ denote the number of occurrences of $z$ in $\alpha ; \operatorname{var}(\alpha)$ denotes the set of variables from $X$ occurring in $\alpha$. A morphism $h:(\Sigma \cup X)^{*} \rightarrow \Sigma^{*}$ with $h(a)=a$ for every $a \in \Sigma$ is called a substitution. We say that $\alpha \in(\Sigma \cup X)^{*}$ is regular if, for every $x \in \operatorname{var}(\alpha)$, we have $|\alpha|_{x}=1$; e.g., a $x_{1} \mathrm{a} x_{2} \mathrm{c} x_{3} x_{4} \mathrm{~b}$ is regular. Note that $L(\alpha)=\{h(\alpha) \mid h$ is a substitution $\}$ (the pattern language of $\alpha$ ) is regular when $\alpha$ is regular, hence the name of such patterns. The pattern $\alpha$ is non-cross if between any two occurrences of the same variable $x$ no other variable different from $x$ occurs, e.g., $\mathrm{a} x_{1} \mathrm{ba} x_{1} x_{2} \mathrm{a} x_{2} x_{2} \mathrm{~b}$ is non-cross, but $x_{1} \mathrm{~b} x_{2} x_{2} \mathrm{~b} x_{1}$ is not.

A word equation is a tuple $(\alpha, \beta) \in(\Sigma \cup X)^{+} \times(\Sigma \cup X)^{+}$; we usually denote such an equation by $\alpha=\beta$, where $\alpha$ is the left-hand side (LHS, for short) and $\beta$ the right-hand side (RHS) of the equation. A solution to an equation $\alpha=\beta$ is a substitution $h$ with $h(\alpha)=h(\beta)$, and $h(\alpha)$ is called the solution word (defined by $h$ ); the length of a solution $h$ of the equation $\alpha=\beta$ is $|h(\alpha)|$. A solution of shortest length to an equation is also called minimal.

A word equation is satisfiable if it has a solution and the satisfiability problem is to decide for a given word equation whether or not it is satisfiable. The satisfiability problem for general word equations can be solved non-deterministically in time polynomial in $n \log N$, where $n$ is the length of the equation and $N$ the length of its minimal solution [23]. The next result follows.

- Lemma 1. Let $\mathcal{E}$ be a class of word equations. Suppose there exists a polynomial $P$ such that for any equation in $\mathcal{E}$ its minimal solution, if it exists, has length at most $2^{P(n)}$ where $n$ is the length of the equation. Then the satisfiability problem for $\mathcal{E}$ is in NP.

A word equation $\alpha=\beta$ is regular or non-cross, if both $\alpha$ and $\beta$ are regular or both $\alpha$ and $\beta$ are non-cross, respectively; $\alpha=\beta$ is quadratic if each variable occurs at most twice in $\alpha \beta$. We call a regular or non-cross equation ordered if the order in which the variables occur in both sides of the equation is the same. That is, if $x$ and $y$ are variables occurring both in $\alpha$ and $\beta$, then all occurrences of $x$ occur before all occurrences of $y$ in $\alpha$ if and only if all occurrences of $x$ occur before all occurrences of $y$ in $\beta$. Note, however, that variables may occur only in one side of a regular or non-cross ordered equation. For instance $x_{1} x_{1} \mathrm{a} x_{2} x_{3} \mathrm{~b} x_{4}=x_{1} \mathrm{a} x_{1} x_{2} \mathrm{~b} x_{3}$ is ordered non-cross, while $x_{1} x_{1} \mathrm{a} x_{3} x_{2} \mathrm{~b}=x_{1} \mathrm{a} x_{1} x_{2} \mathrm{~b} x_{3}$ is still non-cross but not ordered. Next we give an example of very simple word equations whose minimal solution has exponential length, whose structure follows that in [16, Theorem 4.8].

- Proposition 2. The minimal solution to the word equation $x_{n} \mathrm{a} x_{n} \mathrm{~b} x_{n-1} \mathrm{~b} x_{n-2} \cdots \mathrm{~b} x_{1}=$ $\mathrm{a} x_{n} x_{n-1}^{2} \mathrm{~b} x_{n-2}^{2} \mathrm{~b} \ldots \mathrm{~b} x_{1}^{2} \mathrm{ba}{ }^{2}$ has length $\Theta\left(2^{n}\right)$.

For a word equation $\alpha=\beta$ and an $x \in \operatorname{var}(\alpha \beta)$, a regular constraint (for $x$ ) is a regular language $L_{x}$. A solution $h$ for $\alpha=\beta$ satisfies the regular constraint $L_{x}$ if $h(x) \in L_{x}$. The satisfiability problem for word equations with regular constraints is to decide on whether an equation $\alpha=\beta$ with regular constraints $L_{x}, x \in \operatorname{var}(\alpha \beta)$, given as an NFA, has a solution that satisfies all regular constraints.

Finally, we recall the 3-Partition problem (see [10]). This problem is NP-complete in the strong sense, i.e., it remains NP-hard even when the input numbers are given in unary.

- Problem 3 (3-Partition - 3-PAR).

Instance: $3 m$ nonnegative integers (given in unary) $A=\left(k_{1}, \ldots, k_{3 m}\right)$, whose sum is $m s$ Question: Is there a partition of $A$ into $m$ disjoint groups of three elements, such that each group sums exactly to $s$.

## 3 Lower bounds

In this section, we show that the highly restricted class of regular-ordered word equations is NP-hard, and, thus, that even when the order in which the variables occur in an equation is fixed, and each variable may only repeat once - and never on the same side of the equation satisfiability remains intractable. As mentioned in the introduction, our result shows the intractability of the satisfiability problem for a class of equations considerably simpler than the simplest intractable classes of equations known so far. Our result seems also particularly interesting since we are able to provide a corresponding upper bound in the next section, and even show that the minimal solutions of regular-ordered equations are "optimally short".

- Theorem 4. The satisfiability problem for regular-ordered word equations is NP-hard.

In order to show NP-hardness, we shall provide a reduction from a reachability problem for a simple type of regulated string-rewriting system. Essentially, given two words - a starting point, and a target - and an ordered series of $n$ rewriting rules (a rewriting program, in a sense), the problem asks whether this series of rules may be applied consecutively (in the predefined order) to the starting word such that the result matches the target. We stress that the order of the rules is predefined, but the place where a rule is to be applied within the sentential form is non-deterministically chosen.

Problem 5 (Rewriting with Programmed Rules - REP).
Instance: Words $u_{\text {start }}, u_{\text {end }} \in \Sigma^{*}$ and an ordered series of $n$ substitution rules $w_{i} \rightarrow w_{i}^{\prime}$, with $w_{i}, w_{i}^{\prime} \in \Sigma^{*}$, for $1 \leq i \leq n$.

Question: Can $u_{\text {end }}$ be obtained from $u_{\text {start }}$ by applying each rule (i.e., replacing an occurrence of $w_{i}$ with $w_{i}^{\prime}$ ), in order, to $u_{\text {start }}$.

- Example 6. Let $u_{\text {start }}=b^{5}$ and $u_{\text {end }}=\left(a^{11} b c^{2}\right)^{5}$; for $1 \leq i \leq 10$, consider the rules $w_{i} \rightarrow w_{i}^{\prime}$ with $w_{i}=b$ and $w_{i}^{\prime}=a^{i} b c$. We can obtain $u_{\text {end }}$ from $u_{\text {start }}$ by first applying $w_{1} \rightarrow w_{1}^{\prime}$ to the first $b$, then $w_{2} \rightarrow w_{2}^{\prime}$ to the second $b$, and further, in order for $3 \leq i \leq 5$, by applying $w_{i} \rightarrow w_{i}^{\prime}$ to the $i^{t h} b$. Then, we apply $w_{6}$ to the fifth $b$ (counting from left to right). Further we apply in order, for $7 \leq i \leq 10, w_{i} \rightarrow w_{i}^{\prime}$ to the $(11-i)^{t h}$ occurrence of $b$.

It is not so hard to see that REP is NP-complete (the size of the input is the sum of the lengths of $u_{\text {start }}, u_{\text {end }}, w_{i}$ and $\left.w_{i}^{\prime}\right)$. A reduction can be given from 3-PAR, in a manner similar to the construction in the example above. Importantly for our proof, 3-PAR is strongly NP-complete, so it is simpler to reduce it to a problem whose input consists of words.

- Lemma 7. REP is NP-complete.

Our reduction centres on the construction, for any instance $\mu$ of REP, of a regular-ordered word equation $\alpha_{\mu}=\beta_{\mu}$ which possesses a specific form of solution - which we shall call overlapping - if and only if the instance of REP has a solution. By restricting the form of solutions in this way, the exposition of the rest of the reduction is simplified considerably. The main idea is that the applications of the rewriting rules are encoded in the periods of each variable in the solution.

- Definition 8. Let $n \in \mathbb{N}, \mu$ be an instance of REP with $u_{\text {start }}$, $u_{\text {end }}$ and rules $w_{i} \rightarrow w_{i}^{\prime}$ for $1 \leq i \leq n$. Let \# be a 'new' letter not occurring in any component of REP. We define the regular-ordered equation $\alpha_{\mu}=\beta_{\mu}$ such that:
$\alpha_{\mu}:=x_{1} w_{1} x_{2} w_{2} \cdots x_{n} w_{n} x_{n+1} \# u_{\text {end }}, \beta_{\mu}:=\# u_{\text {start }} x_{1} w_{1}^{\prime} x_{2} w_{2}^{\prime} \cdots x_{n} w_{n}^{\prime} x_{n+1}$. A solution $h:(X \cup \Sigma)^{*} \rightarrow \Sigma^{*}$ is called overlapping if, for every $1 \leq i \leq n$, there exists $z_{i} \in \Sigma^{*}$ such that $w_{i} z_{i}$ is a suffix of $h\left(x_{i}\right)$ and $h\left(\# u_{\text {start }} x_{1} \cdots w_{i-1}^{\prime} x_{i}\right)=h\left(x_{1} w_{1} \cdots x_{i} w_{i}\right) z_{i}$.

Of course, satisfiability of a class of word equations asks whether any solution exists, rather than just overlapping solutions. Hence, before we prove our claim that $\alpha_{\mu}=\beta_{\mu}$ has an overlapping solution if and only if $\mu$ satisfies REP, we present a construction of an equation $\alpha=\beta$ which has a solution if and only if $\alpha_{\mu}=\beta_{\mu}$ has an overlapping solution. Essentially, this shows that solving the satisfiability of regular-ordered equations is as hard as solving the satisfiability of word equations when we restrict our search to overlapping solutions.

- Lemma 9. Let $\mu$ be an instance of REP. There exists a regular-ordered equation $\alpha=\beta$ of size $O\left(\left|\alpha_{\mu} \beta_{\mu}\right|\right)$ such that $\alpha=\beta$ is satisfiable if and only if $\alpha_{\mu}=\beta_{\mu}$ has an overlapping solution.

The rest of the proof relies on the following technical characterisation of overlapping solutions to $\alpha_{\mu}=\beta_{\mu}$ in terms of periods $v_{i}$ of the images $h\left(x_{i}\right)$. The $y_{i}$ factors will correspond to the $z_{i}$ factors discussed in the definition of overlapping solutions (see also Figure 1).

- Lemma 10. Let $\mu$ be a an instance of REP with $u_{\text {start }}, u_{\text {end }}$ and rules $w_{i} \rightarrow w_{i}^{\prime}$ for $1 \leq i \leq n$. A substitution $h:(X \cup \Sigma)^{*} \rightarrow \Sigma^{*}$ is an overlapping solution to $\alpha_{\mu}=\beta_{\mu}$ if and only if there exist prefixes $v_{1}, v_{2}, \ldots, v_{n}$ of $h\left(x_{1}\right), h\left(x_{2}\right), \ldots, h\left(x_{n}\right)$ such that:

1. $h\left(x_{i}\right) w_{i}$ is a prefix of $v_{i}^{\omega}$ for $1 \leq i \leq n$, and
2. $v_{1}=\# u_{\text {start }}$, and for $2 \leq i \leq n, v_{i}=y_{i-1} w_{i-1}^{\prime}$, and
3. $y_{n} w_{n}^{\prime} h\left(x_{n+1}\right)=h\left(x_{n+1}\right) \# u_{\text {end }}$,
where for $1 \leq i \leq n, y_{i}$ is the suffix of $h\left(x_{i}\right)$ of length $\left|v_{i}\right|-\left|w_{i}\right|$.


Figure 1 The period of $h\left(x_{i}\right)$ is $v_{i}$, and since $w_{i} y_{i}$ is a suffix of $h\left(x_{i}\right)$ and $\left|w_{i} y_{i}\right|=\left|v_{i}\right|$, we have that $w_{i} y_{i}$ is a cyclic shift of $v_{i}$ (i.e., they are conjugate) - so $v_{i}=s w_{i} t$ and $w_{i} y_{i}=w_{i} t s$ for some $s, t$. $v_{i+1}$ is conjugate to $s w_{i}^{\prime} t$ since $v_{i+1}=y_{i} w_{i}^{\prime}=t s w_{i}^{\prime}$. Thus $v_{i+1}$ is obtained from $v_{i}$ by "applying" the rule $w_{i} \rightarrow w_{i}^{\prime}$ (and conjugating, but we can keep track of this due to the unique occurrence of \#).

We shall now take advantage of Lemma 10 in order to demonstrate the correctness of our construction of $\alpha_{\mu}=\beta_{\mu}$ - i.e., that it has an overlapping solution if and only if $\mu$ satisfies REP. In particular, the periods $v_{i}$ of the images $h\left(x_{i}\right)$ of the variables - which are obtained as the 'overlap' between the two occurrences of $h\left(x_{i}\right)$ - store the $i^{t h}$ stage of a rewriting $u_{\text {start }} \rightarrow \ldots \rightarrow u_{\text {end }}$. In fact, this is obtained as the conjugate of $v_{i}$ starting with \#. Thus the solution-word, when it exists, stores a sort-of rolling computation history.

- Lemma 11. Let $\mu$ be a an instance of REP with $u_{\text {start }}, u_{\text {end }}$ and rules $w_{i} \rightarrow w_{i}^{\prime}$ for $1 \leq i \leq n$. There exists an overlapping solution $h:(X \cup \Sigma)^{*} \rightarrow \Sigma^{*}$ to the equation $\alpha_{\mu}=\beta_{\mu}$ if and only if $\mu$ satisfies REP.

Proof. Suppose firstly that $\mu$ satisfies REP. Then there exist $s_{1}, s_{2}, \ldots, s_{n}, t_{1}, t_{2}, \ldots, t_{n}$ such that $u_{\text {start }}=s_{1} w_{1} t_{1}$, for $1 \leq i \leq n-1, s_{i} w_{i}^{\prime} t_{i}=s_{i+1} w_{i+1} t_{i+1}$ and $s_{n} w_{n}^{\prime} t_{n}=u_{\text {end }}$. Let $h:(X \cup \Sigma)^{*} \rightarrow \Sigma^{*}$ be the substitution such that $h\left(x_{1}\right)=\# s_{1} w_{1} t_{1} \# s_{1}, h\left(x_{n+1}\right)=$ $t_{n} \# s_{n} w_{n}^{\prime} t_{n} \# s_{n} w_{n}^{\prime} t_{n}$, and for $2 \leq i \leq n, h\left(x_{i}\right)=t_{i-1} \# s_{i-1} w_{i-1}^{\prime} t_{i-1} \# s_{i}$. We shall now show that $h$ satisfies Lemma 10, and hence that $h$ is an overlapping solution to $\alpha_{\mu}=\beta_{\mu}$.

Let $v_{1}=\# s_{1} w_{1} t_{1}$, let $y_{1}:=t_{1} \# s_{1}$, and for $2 \leq i \leq n$, let $v_{i}:=t_{i-1} \# s_{i-1} w_{i-1}^{\prime}$ and let $y_{i}:=t_{i} \# s_{i}$. Note that for $1 \leq i \leq n, v_{i}$ is a prefix of $h\left(x_{i}\right)$, and moreover, since $s_{i-1} w_{i-1}^{\prime} t_{i-1}=s_{i} w_{i} t_{i}, y_{i}$ is the suffix of $h\left(x_{i}\right)$ of length $\left|v_{i}\right|-\left|w_{i}\right|$.

It is clear that $h$ satisfies Condition (1) of Lemma 10 for $i=1$. For $2 \leq i \leq n$, we have $h\left(x_{i}\right) w_{i} t_{i}=t_{i-1} \# s_{i-1} w_{i-1} t_{i-1} \# s_{i} w_{i} t_{i}=t_{i-1} \# s_{i-1} w_{i-1} t_{i-1} \# s_{i-1} w_{i-1} t_{i-1}$, which is a prefix of $v_{i}^{\omega}$, and hence $h\left(x_{i}\right) w_{i}$ is also a prefix of $v_{i}^{\omega}$. Thus $h$ satisfies Condition (1) for all $i$. Moreover, $v_{1}=\# u_{\text {start }}$, and for $2 \leq i \leq n, y_{i-1} w_{i-1}^{\prime}=t_{i-1} \# s_{i-1} w_{i-1}^{\prime}=v_{i}$, so $h$ satisfies Condition (2). Finally, $y_{n} w_{n}^{\prime} h\left(x_{n+1}\right)=t_{n} \# s_{n} w_{n}^{\prime} t_{n} \# s_{n} w_{n}^{\prime} t_{n} \# s_{n} w_{n}^{\prime} t_{n}=h\left(x_{n+1}\right) \# u_{\text {end }}$ so $h$ also satisfies Condition (3).

Now suppose that $h$ is an overlapping solution to $\alpha_{\mu}=\beta_{\mu}$. Then $h$ satisfies Conditions (1), (2) and (3) of Lemma 10. Let $v_{i}, y_{i}$ be defined according to the lemma for $1 \leq i \leq n$, and let $v_{n+1}=y_{n} w_{n}^{\prime}$. We shall show that $\mu$ satisfies REP as follows. We begin with the following observations, whose proofs are omitted due to space constraints.

- Claim 12. For $1 \leq i \leq n, y_{i} w_{i}$ and $v_{i}$ are conjugate. Hence, for $1 \leq i \leq n+1,\left|v_{i}\right|_{\#}=1$.

Let $\tilde{v}_{i}$ be the (unique) conjugate of $v_{i}$ which has $\#$ as a prefix. Then we have the following:

- Claim 13. For $1 \leq i \leq n$, there exist $s_{i}, t_{i}$ such that $\tilde{v}_{i}=\# s_{i} w_{i} t_{i}$ and $\tilde{v}_{i+1}=\# s_{i} w_{i}^{\prime} t_{i}$.

Recall from Condition (3) of Lemma 10 that $v_{n+1} h\left(x_{n+1}\right)=y_{n} w_{n}^{\prime} h\left(x_{n+1}\right)=$ $h\left(x_{n+1}\right) \# u_{\text {end }}$. Consequently, $v_{n+1}$ and $\# u_{\text {end }}$ are conjugate, so $\tilde{v}_{n+1}=\# u_{\text {end }}$. Moreover, by Condition (2) of Lemma 10, $v_{1}=\tilde{v}_{1}=\# u_{\text {start }}$. Thus, it follows from Claim 13 that $\mu$ satisfies REP.


Figure 2 Fixing positions: since an occurrence of the $i^{\text {th }}$ letter of $h(x)$ corresponds to an occurrence of the $(|h(y)|-j)^{t h}$ letter of $y$, whose other occurrences correspond to the $k^{t h}$ letter of $h(z)$ and first letter of $h(w)$, all these positions are equivalent and contain the same letter, e.g., a.

It is clear that the equation $\alpha_{\mu}=\beta_{\mu}$ (and hence also the equation $\alpha=\beta$ given in Lemma 9) may be constructed in polynomial time, therefore our reduction from REP is complete. So, by Lemmas 7 and 11, we have shown Theorem 4.

## 4 NP-upper bound

In this section, we discuss a series of results related to the satisfiability of regular-ordered word equations. To this end, we extend the classical approach of filling the positions (see e.g., [15] and the references therein). This method essentially comprises of assuming that for a given equation $\alpha=\beta$, we have a solution $h$ with specified lengths $|h(x)|$ for each variable $x$. The assumption that $h$ satisfies the equation induces an equivalence relation on the positions of each $h(x)$ : if a certain position in the solution-word is produced by an occurrence of the $i^{\text {th }}$ letter of $h(x)$ on the RHS and an occurrence of the $j^{t h}$ letter of $h(y)$ on the LHS, then these two positions must obviously have the same value/letter and we shall say that these occurrences correspond. These individual equivalences can be combined to form equivalence classes, and if no contradictions occur (i.e., two different terminal symbols a and b do not belong to the same class), a valid solution can be derived.

Such an approach already allows for some straightforward observations regarding the (non-)minimality of a solution $h$. In particular, if an equivalence class of positions is not associated with any terminal symbol, then all positions in this class can be mapped to $\varepsilon$, resulting in a strictly shorter solution. On the other hand, even for our restricted setting, this observation is insufficient to provide a bound on the length of minimal solutions. In fact, in the construction of the equivalence classes we ignore, or at least hide, some of the structural information about the solution. In what follows, we shall see that by considering the exact 'order' in which positions are equated, we are able to give some more general conditions under which a solution is not minimal.

For our approach, rather than just constructing these equivalence classes, we shall construct sequences of equivalent positions, and then analyse "similar" sequences. For example, one occurrence of a position $i$ in $h(x)$ might correspond to an occurrence of position $j$ in $h(y)$, while another occurrence of position $j$ in $h(y)$ might correspond to position $k$ in $h(z)$, and so on, in which case we would consider the sequence: $\ldots \rightarrow(x, i) \rightarrow(y, j) \rightarrow(z, k) \rightarrow \ldots$

The sequence terminates when either a variable which occurs only once or a terminal symbol is reached. For general equations, considering all such sequences leads naturally to a graph structure where the nodes are positions $(x, i) \in X \times \mathbb{N}$, and number of edges from each node is determined by the number of occurrences of the associated variable. Each connected component of such a graph corresponds to an equivalence class of positions as before. In the case of quadratic (and therefore also regular) equations, where each variable occurs at most twice, each 'node' $(x, i)$ has at most two edges, and hence our graph is simply a set of disjoint chains, without any loops. As before, each chain (called in the following sequence) must be


Figure 3 Illustration of Lemma 14 in the case of a short subsequence $\ldots,\left(x, 1, d_{1}\right),\left(y, 2, d_{2}\right),\left(x, 1, d_{3}\right),\left(y, 2, d_{4}\right), \ldots:$ since the two sequences starting at $\left(x, 1, d_{1}\right)$ and $\left(x, 1, d_{3}\right)$ are similar, they define a common region $w$ (shaded). Since they are consecutive, the first and last occurrences of $w$ are adjacent, and on opposite sides of the equation. Thus, removing the region $w$ from $h(x)$ and $h(y)$ does not alter the fact that $h$ satisfies the equation.
associated with some occurrence of a terminal symbol, which must occur either at the start or the end. Hence we have $k<n$ sequences, where $n$ is the length of the equation, such that every position $(x, i)$, where $x$ is a variable and $1 \leq i \leq|h(x)|$, occurs in exactly one sequence. It is also not hard to see that the total length of the sequences is upper bounded by $2|h(\alpha)|$.

In order to be fully precise, we will distinguish between different occurrences of a variable/terminal symbol by associating each with an index $z \in \mathbb{N}$ by enumerating occurrences from left to right in $\alpha \beta$. When considering quadratic equations, $z \in\{1,2\}$ for each variable $x$.

Formally, we define our sequences for a given solution $h$ to a quadratic equation $\alpha=\beta$ as follows: a position is a tuple $(x, z, d)$ such that $x$ is a variable or terminal symbol occurring in $\alpha \beta, 1 \leq z \leq|\alpha \beta|_{x}$, and $1 \leq d \leq|h(x)|$. Two positions $(x, z, d)$ and ( $y, z^{\prime}, d^{\prime}$ ) correspond if they generate the same position in the solution-word. The positions are similar if they belong to the same occurrence of the same variable (i.e., $x=y$ and $z=z^{\prime}$ ). For each position $p$ associated with either a terminal symbol or a variable occurring only once in $\alpha \beta$, we construct a sequence $S_{p}=p_{1}, p_{2}, \ldots$ such that

- $p_{1}=p$ and $p_{2}$ is the (unique) position corresponding with $p_{1}$, and
- for $i \geq 2$, if $p_{i}=(x, z, d)$ such that $x$ is a terminal symbol or occurs only once in $\alpha \beta$, then the sequence terminates, and
- for $i \geq 2$, if $p_{i}=(x, z, d)$, such that $x$ is a variable occurring twice, then $p_{i+1}$ is the position corresponding to the (unique) position $\left(x, z^{\prime}, d\right)$ with $z^{\prime} \neq z$ (i.e., the 'other' occurrence of the $i^{t h}$ letter in $h(x)$ ).
We extend the idea of similarity from positions to sequences of positions in the natural way: two sequences $p_{1}, p_{2}, \ldots, p_{i}$ and $q_{1}, q_{2}, \ldots, q_{i}$ are similar whenever $p_{j}$ and $q_{j}$ are similar for all $j \in\{1,2, \ldots, i\}$. Our main tool is the following lemma, which essentially shows that if a sequence contains two similar consecutive subsequences, then the solution defining that sequence is not minimal.

Lemma 14. Let $h$ be a solution to a quadratic equation $\alpha=\beta$, and let $p$ be a position associated with a single-occurring variable or terminal symbol. If the sequence $S_{p}$ has a subsequence $p_{1}, p_{2}, \ldots, p_{t}, p_{t+1}, p_{t+2}, \ldots, p_{2 t}$ such that $p_{1}, p_{2}, \ldots, p_{t}$ and $p_{t+1}, p_{t+2}, \ldots, p_{2 t}$ are similar, then $h$ is not minimal.

Proof. Assume that $S_{p}$ has such a subsequence and assume w.l.o.g. that it is length-minimal (so $t$ is chosen to be as small as possible). For $1 \leq i \leq 2 t$, let $p_{i}=\left(x_{i}, z_{i}, d_{i}\right)$ and note that by definition of similarity, for $1 \leq i \leq t, x_{i}=x_{i+t}$ and $z_{i}=z_{i+t}$. Assume that $d_{1}<d_{t+1}$ (the case where $d_{1}>d_{t+1}$ may be treated identically). We need the following two claims, whose proofs are omitted due to space constraints.

- Claim 15. Suppose that $(x, z, d),\left(x, z, d^{\prime}\right),\left(x, z, d^{\prime \prime}\right)$ are positions with $d \leq d^{\prime}<d^{\prime \prime}$ such that $(x, z, d)$ and $\left(x, z, d^{\prime \prime}\right)$ correspond to $\left(y, z^{\prime}, e\right)$ and $\left(y, z^{\prime}, e^{\prime \prime}\right)$ respectively. Then $e^{\prime \prime}-e=d^{\prime \prime}-d$, and there exists $e^{\prime}$ with $e^{\prime}-e=d^{\prime}-d$ such that $\left(x, z, d^{\prime}\right)$ and $\left(y, z^{\prime}, e^{\prime}\right)$ correspond.

A straightforward consequence of Claim 1 is that there exists a constant $C \in \mathbb{N}$ such that for all $i \in\{1,2, \ldots, t\}, d_{i+t}-d_{i}=C$. Intuitively, each pair of similar positions $p_{i}=\left(x_{i}, z_{i}, d_{i}\right)$ and $p_{i+t}=\left(x_{i}, z_{i}, d_{i}+C\right)$ are the first and last positions of a factor $h\left(x_{i}\right)\left[d_{i} . . d_{i}+C-1\right]$, which as we shall see later on in the proof, can be removed to produce a shorter solution $g$.

It also follows from Claim 1, along with the fact that we chose $t$ to be minimal, that there does not exist a position $p_{i}=\left(x_{1}, z_{1}, k\right)$ in the chain such that $d_{1}<k<d_{1}+C$. Symmetrically, there does not exist a position $p_{i}=\left(x_{t}, z_{t}, k\right)$ such that $d_{t}<k<d_{t}+C$ :

- Claim 16. Let $j \in\{2, \ldots, t, t+2, \ldots, 2 t\}$ such that $x_{j}=x_{1}\left(=x_{t+1}\right)$ and $z_{j}=z_{1}\left(=z_{t+1}\right)$. Then $d_{j} \notin\left\{d_{1}, \ldots, d_{t+1}\left(=d_{1}+C\right)\right\}$. Likewise, if $j \in\{1, \ldots, t-1, t+1, \ldots, 2 t-1\}$ such that $x_{j}=x_{t}$ and $z_{j}=z_{t}$, then $d_{j} \notin\left\{d_{t}, \ldots, d_{2 t}\right\}$.

Using the observations above, we shall remove parts of the solution $h$ to obtain a new, strictly shorter solution and thus show that $h$ is not minimal as required.

To do this, we shall define a new equation $\alpha^{\prime}=\beta^{\prime}$ obtained by replacing the second occurrence of each variable $x$ (when it exists) with a new variable $x^{\prime}$. The reason is so we may delete factors independently from different occurrences of $h\left(x_{i}\right)$, and more easily keep track of the equivalence of the left and right hand side of the equation. Note that we can derive a solution $h^{\prime}$ to $\alpha^{\prime}=\beta^{\prime}$ from the solution $h$ to our original equation by simply setting $h^{\prime}(x)=h^{\prime}\left(x^{\prime}\right)=h(x)$ for all $x \in \operatorname{var}(\alpha \beta)$. Likewise, any solution to $\alpha^{\prime}=\beta^{\prime}$ for which this condition holds (i.e., $h^{\prime}(x)=h^{\prime}\left(x^{\prime}\right)$ for all $x \in \operatorname{var}(\alpha \beta)$ ) induces a solution $g$ to our original equation $\alpha=\beta$ given by $g(x)=h^{\prime}(x)\left(=h^{\prime}\left(x^{\prime}\right)\right)$. Finally, for each position $(x, z, d)$ in the original solution $h$, there exists a unique "associated position" in $h^{\prime}$ given by $h(x)[d]$ if $z=1$ and $h\left(x^{\prime}\right)[d]$ if $z=2$. Furthermore, it follows from the definitions that for any pair of positions $p, q$ which correspond (in terms of $h$ ), we can remove the associated positions from $h^{\prime}$ and the result will still be a valid solution to our modified equation $\alpha^{\prime}=\beta^{\prime}$ (although such a solution may no longer induce a valid solution to our original equation, since it is no longer necessarily the case where $h^{\prime}(x)=h^{\prime}\left(x^{\prime}\right)$ for all $\left.x\right)$.

We construct our shorter solution $g$ to $\alpha=\beta$ as follows. Let $h^{\prime}$ be the solution to $\alpha^{\prime}=\beta^{\prime}$ derived directly from $h$. Recall from the definition of $S_{p}$ that, for $1 \leq i<t$, the positions $\left(x_{i}, \bar{z}_{i}, d_{i}\right)$ and $\left(x_{i+1}, z_{i+1}, d_{i+1}\right)$ correspond, where $\bar{z}=(z+1) \bmod 2$ (i.e., so that $\bar{z} \neq z)$. Moreover, $\left(x_{i}, \bar{z}_{i}, d_{i}+C\right)$ and $\left(x_{i+1}, z_{i+1}, d_{i+1}+C\right)$ correspond, and thus by Claim 1, $\left(x_{i}, \bar{z}_{i}, d_{i}+k\right)$ and $\left(x_{i+1}, z_{i+1}, d_{i+1}+k\right)$ correspond for $0 \leq k \leq C-1$. Since corresponding positions must have the same value/letter, it follows that there exists a factor $w \in \Sigma^{+}$such that $w=h\left(x_{i}\right)\left[d_{i} . . d_{i}+C-1\right]\left(=h^{\prime}(x)\left[d_{i} . . d_{i}+C-1\right]=h^{\prime}\left(x^{\prime}\right)\left[d_{i} . . d_{i}+C-1\right]\right)$ for $1 \leq i \leq t$.

We now produce a new solution, $h^{\prime \prime}$ to $\alpha^{\prime}=\beta^{\prime}$ as follows. For each $i$ such that $1 \leq i \leq t-1$ and for each $k$ such that $d_{i} \leq k \leq d_{i}+C-1$, delete from $h^{\prime}$ the pair of positions associated with $\left(x_{i}, \bar{z}_{i}, d_{i}+k\right)$ and $\left(x_{i+1}, z_{i+1}, d_{i+1}+k\right)$. Note that since these positions correspond, in deleting them, we continue to have a valid solution to $\alpha^{\prime}=\beta^{\prime}$. Notice also that for every position associated with $\left(x_{i}, \bar{z}_{i}, d_{i}+k\right)$ such that $1<i \leq t$, we also delete the position associated with $\left(x_{i}, z_{i}, d_{i}+k\right)$. Hence, for all $x \notin\left\{x_{1}, x_{t}\right\}, h^{\prime \prime}(x)=h^{\prime \prime}\left(x^{\prime}\right)$. The same does not necessarily hold for $x_{1}$ and $x_{t}$, however. In particular, we deleted positions associated with $\left(x_{1}, \overline{z_{1}}, d_{1}+k\right)$ and $\left(x_{t}, z_{t}, d_{t}+k\right)$ for $0 \leq k \leq C-1$, but not their counterparts $\left(x_{1}, z_{1}, d_{1}+k\right)$ and ( $\left.x_{t}, \bar{z}_{t}, d_{t}+k\right)$. Hence, to derive a valid solution $g$, we must also delete these positions. To see that, in doing so, we still have a valid solution to $\alpha^{\prime}=\beta^{\prime}$, note firstly that, by Claim 2, we have not deleted any of these positions already. Moreover, it
follows from the sequence $S_{p}$ that $\left(x_{t}, \bar{z}_{t}, d_{t}\right)$ corresponds to $\left(x_{1}, z_{1}, d_{1}+C\right)$. Assume $z_{1}=1$ (the case $z_{1}=2$ is symmetric). It follows that $z_{t}=1$ (since $\bar{z}_{t} \neq z_{1}$ ). Thus there exists an index $m$ such that $h^{\prime \prime}\left(x_{1}\right)\left[d_{1} . . d_{1}+C-1\right]$ generates the factor $w$ starting at position $m$ in $h^{\prime \prime}\left(\alpha^{\prime}\right)$ and $h^{\prime \prime}\left(x_{t}\right)\left[d_{t} . . d_{t}+C-1\right]$ generates the (same) factor $w$ starting at position $m+|w|$ in $h^{\prime \prime}(\beta)$. It is straightforward to see that removing these factors (i.e., deleting the positions associated with $\left(x_{1}, z_{1}, d_{1}+k\right)$ and $\left(x_{t}, \bar{z}_{t}, d_{t}+k\right)$ for $\left.0 \leq k \leq C-1\right)$ does not affect the agreement of the two sides of the equation. Thus we obtain a shorter solution $h^{\prime \prime}$ to $\alpha^{\prime}=\beta^{\prime}$ such that $h(x)=h\left(x^{\prime}\right)$ for all variables $x$, hence a shorter solution $g$ given by $g(x)=h^{\prime \prime}(x)$ to $\alpha=\beta$.

An important fact related to the representation of the minimal solutions of quadratic equations as oriented sequences of positions, that start or end with a terminal symbol, is that the number of such sequences is linear in the size of the equation. Also, for variables that occur only once in a quadratic equation (so, only in one side), each of their positions is the start or end of a chain, so their length can be at most linear in the size of the equation. Thus, when interested in showing that a certain class of quadratic equation is in NP, we can assume that these equations do not contain variables occurring only once. Such variables could be non-deterministically replaced by words of at most linear size, and we would have to solve a new equation, whose size is at most quadratic in the size of the original one.

Further, using Lemma 14 and the observations above, we obtain immediately that minimal solutions to regular-ordered equations are at most linear in the length of the equation.

- Proposition 17. Let $E$ be a regular-ordered word equation with length $n$, and let $h$ be a minimal solution to $E$. Then $|h(x)|<n$ for each variable $x$ occurring in $E$.

Proof. Every position of a minimal solution $h$ to $E$ occurs somewhere in one of the associated sequences $S_{p}$, and there are no more than $n$ such sequences. So, it is sufficient to show that each one contains at most one position $(x, z, d)$ for each variable $x$. This follows easily from the fact that $E$ is regular and ordered and $h$ is minimal, so it fulfils the restrictions of Lemma 14.

We can see that, in terms of restricting the lengths of individual variables, the result in Proposition 17 is optimal. For instance, in a minimal solution $h$ to the equation $w \mathrm{c} x_{1}=x_{1} \mathrm{c} w$, with $w \in\{a, b\}^{*}$, the variable $x_{1}$ is mapped to $w$, so $|h(x)|=|E|-2 \in O(|E|)$. Furthermore, Theorem 18 follows now as a direct consequence of Proposition 17 and Lemma 1, as the length of a minimal solution to a regular-ordered equation $\alpha=\beta$ is $O\left(|\alpha \beta|^{2}\right)$.

- Theorem 18. The satisfiability problem for regular-ordered equations is in NP.

It is a simple consequence of Proposition 17 that the satisfiability of a regular-ordered equation $E$ with a constant number $k$ of variables can be checked in P-time.

We now consider the satisfiability problem for regular equations with regular constraints, where we can make further use of the ideas presented so far in this section. Firstly, we observe that the problem is, in general, PSPACE-complete, even for regular-ordered equations (the proof given in [21] that the problem is PSPACE-complete for regular equations is also sufficient for the regular-ordered case).

- Proposition 19. The satisfiability of regular-ordered equations with regular constraints is PSPACE-complete

However, when considering regular equations whose sides contain exactly the same variables, and, moreover, in the same order, we get the following result, which shows an
important difference between the unrestricted regular-ordered equations, where the variables occurring only on one side do not affect the complexity of the satisfiability problem, and the same type of equations subject to regular constraints.

- Theorem 20. The satisfiability of regular-ordered equations whose sides contain exactly the same variables, with regular constraints, is in NP.

The same upper bound holds also for regular-ordered equations with regular constraints, when the regular constraints are regular languages accepted by NFAs with at most $c$ states, where $c$ is a constant (called constant regular constraints in the following).

- Theorem 21. The satisfiability problem for regular-ordered equations with constant regular constraints is in NP.

The proofs of the last two results rely also on the approach outlined in Lemma 14, but they are more involved. We first define the sequences of positions fixed by the terminals in a minimal solution of an equation. While this time the sequences may contain repetitions, we show that they cannot contain repetitions of non-constant exponent (where the constant, however, depends exponentially on $c$ ). This provides, again, a polynomial upper bound on the length of minimal solutions of such equations.

## 5 Tractable equations

Finally, we discuss a class of equations for which satisfiability is in P. Tractability was obtained so far from two sources: bound the number of variables by a constant (e.g., one or two-variable equations $[13,1]$ ), or heavily restrict their structure (e.g., regular equations whose sides do not have common variable, or equations that only have one repeated variable, but at least one non-repeated variable on each side [21]). The class we consider slightly relaxes the previous restrictions. As the satisfiability of quadratic or even regular-ordered equations is NP-hard it seems reasonable to consider here patterns where the number of repeated variables is bounded by a constant (but may have an arbitrary number of non-repeated variables). More precisely, we consider here non-cross equations with only one repeated variable. This class generalises naturally the class of one-repeated variables.

- Theorem 22. Let $x \in X$ be a variable and $\mathcal{D}$ be the class of word equations $\alpha=\beta$ such that $\alpha, \beta \in(\Sigma \cup X)^{*}$ are non-cross and each variable of $X$ other than $x$ occurs at most once in $\alpha \beta$. Then the satisfiability problem for $\mathcal{D}$ is in P .

In the light of the results from [21], it follows that the interesting case of the above theorem is when the equation $\alpha=\beta$ is such that $\alpha=x u_{1} x u_{2} \cdots u_{k} x$ and $\beta=\beta^{\prime} v_{0} x v_{1} x v_{2} \cdots x v_{k} \beta^{\prime \prime}$ where $v_{0}, v_{1}, \ldots, v_{k}, u_{1}, u_{2}, \ldots, u_{k} \in \Sigma^{*}$ and $\beta^{\prime}, \beta^{\prime \prime}$ are regular patterns that do not contain $x$ and are variable disjoint. Essentially, this is a matching problem in which we try to align two non-cross patterns, one that only contains a repeated variable and constants, while the other contains the repeated variable, constants, and some wild-cards that can match any factor. As the proofs of [21] used essentially the non-repeated variables occurring in each of the sides, a novel and much more involved approach was needed here. The idea of our proof is to first show that such equations have minimal solutions of polynomial length. Further, we note that if we know the length of $\beta^{\prime}$ (w.r.t. the length of $\alpha$ ) then we can determine the position where the factor $v_{0} x v_{1} x v_{2} \cdots x v_{k}$ occurs in $\alpha$, so the problem boils down to seeing how the positions of $x$ are fixed by the constant factors $v_{i}$. Once this is done, we check if there exists an assignment of the variables of $\beta^{\prime}$ and $\beta^{\prime \prime}$ such that the constant factors of these patterns fit correctly to the corresponding prefix, respectively, suffix of $\alpha$.

## 6 Conclusions and Prospects

The main result of this paper is the NP-completeness of the satisfiability problem for regularordered equations. While the lower bound seems remarkable to us because it shows that solving very simple equations, which also always have short solutions, is NP-hard, the upper bound seems more interesting from the point of view of the tools we developed to show it. We expect the combinatorial analysis of sequences of equivalent positions in a minimal solution to an equation (which culminated here in Lemma 14) can be applied to obtain upper bounds on the length of the minimal solutions to more general equations than just the regular-ordered ones. It would be interesting to see whether this type of reasoning leads to polynomial upper bounds on the length of minimal solutions to regular (not ordered) or quadratic equations, or to exponential upper bounds on the length of minimal solutions of non-cross or cubic equations. In the latter cases, a more general approach should be used, as the equivalent positions can no longer be represented as linear sequences, but rather as directed graphs.

Regarding the final section our paper, it seems interesting to us to see whether deciding the satisfiability of word equations with one repeated variable (so without the non-cross sides restriction) is still tractable. Also, it seems interesting to analyse the complexity of word equations where the number of repeated variables is bounded by a constant.

## References

1 R. Da̧browski and W. Plandowski. Solving two-variable word equations. In Proc. 31th International Colloquium on Automata, Languages and Programming, ICALP 2004, volume 3142 of Lecture Notes in Computer Science, pages 408-419, 2004.
2 V. Diekert, A. Jez, and M. Kufleitner. Solutions of word equations over partially commutative structures. In Proc. 43 rd International Colloquium on Automata, Languages, and Programming, ICALP 2016, volume 55 of Leibniz International Proceedings in Informatics (LIPIcs), pages 127:1-127:14, 2016.
3 V. Diekert and J. M. Robson. On quadratic word equations. In Proc. 16th Annual Symposium on Theoretical Aspects of Computer Science, STACS 1999, volume 1563 of Lecture Notes in Computer Science, pages 217-226, 1999.
4 A. Ehrenfeucht and G. Rozenberg. Finding a homomorphism between two words is NPcomplete. Information Processing Letters, 9:86-88, 1979.
5 H. Fernau, F. Manea, R. Mercaş, and M.L. Schmid. Pattern matching with variables: Fast algorithms and new hardness results. In Proc. 32nd Symposium on Theoretical Aspects of Computer Science, STACS 2015, volume 30 of Leibniz International Proceedings in Informatics (LIPIcs), pages 302-315, 2015.
6 H. Fernau and M. L. Schmid. Pattern matching with variables: A multivariate complexity analysis. Information and Computation, 242:287-305, 2015.
7 H. Fernau, M. L. Schmid, and Y. Villanger. On the parameterised complexity of string morphism problems. Theory of Computing Systems, 2015. http://dx.doi.org/10.1007/s00224-015-9635-3.
8 D. D. Freydenberger. A logic for document spanners. In Proc. 20th International Conference on Database Theory, ICDT 2017, Leibniz International Proceedings in Informatics (LIPIcs), 2017. To appear.

9 D. D. Freydenberger and M. Holldack. Document spanners: From expressive power to decision problems. In Proc. 19th International Conference on Database Theory, ICDT 2016, volume 48 of Leibniz International Proceedings in Informatics (LIPIcs), pages 17:117:17, 2016.

10 M. R. Garey and D. S. Johnson. Computers And Intractability. W. H. Freeman and Company, 1979.
11 J. Jaffar. Minimal and complete word unification. Journal of the ACM, 37(1):47-85, 1990.
12 A. Jez. Context unification is in PSPACE. In Proc. 41st International Colloquium on Automata, Languages, and Programming, ICALP 2014, volume 8573 of Lecture Notes in Computer Science, pages 244-255. Springer, 2014.
13 A. Jeż. One-variable word equations in linear time. Algorithmica, 74:1-48, 2016.
14 A. Jeż. Recompression: A simple and powerful technique for word equations. Journal of the $A C M, 63,2016$.
15 J. Karhumäki, F. Mignosi, and W. Plandowski. The expressibility of languages and relations by word equations. Journal of the ACM, 47:483-505, 2000.
16 A. Koscielski and L. Pacholski. Complexity of Makanin's algorithm. Journal of the ACM, 43(4):670-684, 1996.
17 M. Lothaire. Algebraic Combinatorics on Words. Cambridge University Press, Cambridge, New York, 2002.
18 R. C. Lyndon. Equations in free groups. Transactions of the American Mathematical Society, 96:445-457, 1960.
19 R. C. Lyndon and P. E. Schupp. Combinatorial Group Theory. Springer, 1977.
20 G. S. Makanin. The problem of solvability of equations in a free semigroup. Matematicheskii Sbornik, 103:147-236, 1977.
21 F. Manea, D. Nowotka, and M. L. Schmid. On the solvability problem for restricted classes of word equations. In Proc. 20th International Conference on Developments in Language Theory, DLT 2016, volume 9840 of Lecture Notes in Computer Science, pages 306-318. Springer, 2016.
22 W. Plandowski. An efficient algorithm for solving word equations. In Proceedings of the 38th Annual ACM Symposium on Theory of Computing, STOC 2006, pages 467-476, 2006.
23 W. Plandowski and W. Rytter. Application of Lempel-Ziv encodings to the solution of words equations. In Proc. 25th International Colloquium on Automata, Languages and Programming, ICALP'g8, volume 1443 of Lecture Notes in Computer Science, pages 731742. Springer, 1998.

24 D. Reidenbach and M. L. Schmid. Patterns with bounded treewidth. Information and Computation, 239:87-99, 2014.
25 K. U. Schulz. Word unification and transformation of generalized equations. Journal of Automated Reasoning, 11:149-184, 1995.

