International Journal of Foundations of Computer Science
Vol. 18, No. 6 (2007) 1167–1175


World Scientific
www.worldscientific.com

# INTRICACIES OF SIMPLE WORD EQUATIONS: AN EXAMPLE

ELENA CZEIZLER

*Department of Mathematics and Turku Centre for Computer Science, University of Turku, Joukahaisenkatu 3–5 B, 6th floor, Turku, 20520, Finland*
*elenac@it.utu.fi*

ŠTĚPÁN HOLUB

*Department of Algebra, Charles University in Prague*
*Sokolovska 83, Praha 8, 186 75, Czech Republic*
*holub@karlin.mff.cuni.cz*

JUHANI KARHUMÄKI

*Department of Mathematics and Turku Centre for Computer Science, University of Turku, Turku, 20014, Finland*
*juhani.karhumaki@utu.fi*

MARKKU LAINE

*Department of Mathematics and Turku Centre for Computer Science, University of Turku, Turku, 20014, Finland*
*majlain@utu.fi*

Received 24 January 2007
Accepted 16 May 2007
Communicated by R. Stiebe

As is well known, simple word equations can be very tedious to solve, often requiring specific ad hoc methods. We illustrate this by giving an example of an equation over four unknowns, having only periodic solutions, but for which showing this is not at all obvious.

*Keywords*: Word equations; solutions of instances of PCP.

## 1. Introduction

The theory of word equations is fundamental for many areas of mathematics and computing. Despite of that, many fragments of this theory are quite poorly understood. In fact, the whole theory is full of amazingly simple open problems.

After the discovery of the algorithmic undecidability, it was thought by A. Markov in late 1950's, that maybe word equations could be used to solve negatively Hilbert's 10th Problem, see [3]. This hope was motivated by at that time discovered undecidable word problems for semigroups. However, this turned out not to be the case: Hilbert's 10th Problem is undecidable, as shown by Matiyasevich [10], while

the satisfiability problem for word equations is decidable, as shown by Makanin [9]. Moreover, the possibility to express inequality as a finite disjunction of finite systems of equalities allows to show that the question whether a given word is a solution of a nontrivial instance of the Post Correspondence Problem is decidable as well, see [2]. Here, nontrivial means that the lists are not equal and that not all words of the lists of PCP are powers of a common word, or equivalently, that the corresponding morphisms are nonperiodic.

It follows that, in principle, we can decide whether a given equation has a solution, or even a nonperiodic solution. In practice, the situation is completely different. To emphasize this we recall that no characterization is known of those words which can be solutions of nontrivial instances of a binary PCP, that is of those $w \in \{a, b\}^*$, which for some $h, g : \{a, b\}^* \to \{a, b\}^*$ satisfy the equality $h(w) = g(w)$, with $h$ and/or $g$ being nonperiodic and $h \neq g$. More amazingly, it is not difficult to give a concrete $w_0$ for which the reader could have difficulties to answer the above question. On the other hand, a nontrivial partial characterization of all possible sets of solutions of binary PCP was achieved in [5, 6], the first result being conjectured in [2].

The goal of this note is to emphasize the above intriguing property of word equations. We choose $w_0 = a^2b^3a^2$ and show that according to our intuition, of all morphisms $h, g : \{a, b\}^* \to \{a, b\}^*$, with $h \neq g$, only the periodic ones can satisfy $h(w_0) = g(w_0)$. However, to our surprise, no standard methods, as described e. g. in [7, 1], seem to give an obvious solution to this claim. Only a more complicated analysis allows us to formulate the result:

**Theorem 1.** *The equation $x^2y^3x^2 = u^2v^3u^2$ has only periodic solutions, provided $x \neq u$.*

As we see this, the value of this note is given by the observation, that a statement of the solution set of this simple looking word equation can be rather difficult to prove. In order to illustrate this, we note that any standard application of the length argument does not seem to help. Also attempts to cancel unknowns from the left or from the right lead to more complicated equations. The most promising idea is to write

$$x^2 = u^2t \qquad \text{and} \qquad x^2 = t'u^2,$$

and substitute it to the equation. This leads to the equation

$$pqy^3qp = v^3,$$

which, although in some sense a simpler equation than the original one, seems to resist the standard attempts as well.

To conclude this section we describe the structure of this note. After preliminaries in Section 2, we introduce a few auxiliary lemmas and solutions of some special cases of our theorem in Section 3. Section 4 is devoted to the proof of the problem.

## 2. Preliminaries

We need just the basic terminology of combinatorics on words. Let us recall that a word $u$ is a *factor* (resp. *prefix*, *suffix*) of $w$ if there exist words $x, y$ such that $w = xuy$ (resp. $w = uy$, $w = xu$). A factor (resp. prefix, suffix) $u$ of a word $w$ is called *proper* if $u \neq 1$ and $u \neq w$. Words $u$ and $v$ are *prefix* (resp. *suffix*) *comparable* if one of them is a prefix (resp. suffix) of the other. If $w = uv$, we also write $v = u^{-1}w$ (resp. $u = wv^{-1}$). For a word $w \in \Sigma^*$ we denote by $|w|$ its *length*. We say that a word $w$ is *covered* by the sequence $u_1u_2 \dots u_k$ if $w$ is a factor of $u_1u_2 \dots u_k$. A word $w \in \Sigma^+$ is called *primitive* if it cannot be written as a proper integer power of another word $u \in \Sigma^*$. For a given word $w$, the unique primitive word $u$ such that $w = u^n$ for some $n \geq 1$ is called the *primitive root* of $w$. The following result illustrates a fundamental property of primitive words.

**Lemma 2.** *Let $p \in \Sigma^+$ be a primitive word. If we can write $p^2 = upv$ for some words $u, v \in \Sigma^*$, then necessarily either $u = 1$ or $v = 1$.*

We say that two words $u$ and $v$ *commute* if $uv = vu$. The following well-known result characterizes the commutation of two words in terms of primitive roots.

**Lemma 3.** *Let $u, v \in \Sigma^*$. Then, the following conditions are equivalent:*

- *$u$ and $v$ commute;*
- *$u$ and $v$ satisfy a nontrivial relation;*
- *either $u$ and $v$ have the same primitive root or at least one of them is empty.*

We say that two words $u$ and $v$ are *conjugates* if there exist some words $p$ and $q$ such that $u = pq$ and $v = qp$. The next result characterizes the conjugacy of two words.

**Lemma 4.** *Let $u, v \in \Sigma^+$. Then, the following conditions are equivalent:*

- *$u$ and $v$ are conjugates;*
- *there exists a word $z$ such that $uz = zv$;*
- *the primitive roots of $u$ and $v$ are conjugates.*

**Lemma 5.** *Let $u, v, z \in \Sigma^*$. Then, the following conditions are equivalent:*

- *$uz = zv$;*
- *there exist words $p, q$ and a nonnegative integer $i$ such that $u = pq$, $v = qp$, and $z = (pq)^i p = p(qp)^i$.*

The conjugates of a primitive word have the following property.

**Lemma 6.** *Let $p = p_1p_2$ be primitive. Then $p_2p_1$ is also primitive. Moreover, if both $p_1$ and $p_2$ are nonempty then $p \neq p_2p_1$.*

Next, we recall a fundamental periodicity property of words, also known as Fine and Wilf theorem. As usual, $gcd(n, m)$ denotes the *greatest common divisor of integers $n$ and $m$.*

*Let $u, v \in \Sigma^*$, $n = |u|$, $m = |v|$, and $d = gcd(n, m)$. If two powers $u^p$ and $v^q$ of $u$ and $v$ have a common prefix of length at least $n + m - d$, then $u$ and $v$ are powers of a common word.*

Another important periodicity result was proved by Lyndon and Schützenberger in [8], see also [4] for a short proof.

**Lemma 8.** *If words $x, y$ and $z$ satisfy the relation $x^m y^n = z^p$ for some integers $m, n, p \geq 2$, then they all are powers of a common word.*

Next, let $\Sigma$ be a finite alphabet and $X = \{x_1, \ldots, x_n\}$ a set of unknowns, with $\Sigma \cap X = \emptyset$. An *equation* over the alphabet $\Sigma$, with $X$ as the set of unknowns is a pair $(u, v) \in (\Sigma \cup X)^* \times (\Sigma \cup X)^*$, usually written as $u = v$. A *solution* of an equation $u = v$ is a morphism $\varphi : (X \cup \Sigma)^* \to \Sigma^*$ such that $\varphi(u) = \varphi(v)$ and $\varphi(a) = a$ for every $a \in \Sigma$. We say that a solution $\varphi$ is *periodic* if there exists some word $u \in \Sigma^*$ such that $\varphi(x) \in u^*$ for any $x \in X$.

## 3. Auxiliary Results

In this section we present some preliminary lemmas which prove to be useful in our future considerations.

The first result is an immediate consequence of Lemma 8.

**Lemma 9.** *If $u^i v^j u^k = z^l$, for some words $u, v, z \in \Sigma^*$, and positive integers $i, j, k, l$ such that $j > 1$, $i + k > 1$, and $l > 1$, then $u$, $v$, and $z$ are powers of a common word.*

**Proof.** First, by circular shifting of both sides of the equation $u^i v^j u^k = z^l$ we derive $v^j u^{k+i} = z_1^l$, where $z_1$ is a conjugate of $z$. Since $j > 1$, $i + k > 1$, and $l > 1$, Lemma 8 implies that $u, v$, and $z_1$ are all powers of a common word. Then, since $z^l = u^i v^j u^k$, we immediately obtain that also $z$ is a power of the same word. □

**Lemma 10.** *Let $u$ and $v$ be two words such that $|u| \geq |v|$. If $z_1 u$ is a prefix of $v^i$ and $u z_2$ is a suffix of $v^j$ for some $i, j \geq 2$, then $z_1 u z_2$ and $v$ commute.*

**Proof.** We can suppose without loss of generality that $v$ is primitive. Let $v'$ be the prefix of $u$ of length $|v|$. Lemma 2 implies that the position of $v'$ in a power of $v$ is given uniquely, which yields the claim. □

**Lemma 11.** *Let $u$ and $v$ be two words such that $|u| \geq |v|$. If, for some $k \geq 1$, $v^k$ is both prefix and suffix comparable with $u$ and, moreover, $(2k - 1)|v| \geq |u|$, then $u$ and $v$ commute.*

**Proof.** As in the previous proof, we can again assume that $v$ is primitive. Since $|v| \leq |u| \leq (2k - 1)|v|$, if $v^k$ is both a prefix and a suffix of $u$, then $u = v^l$, for some $k \leq l \leq 2k - 1$, i. e., $u$ and $v$ commute. Otherwise, $u$ is both a prefix and a suffix

of $v^k$, and the claim follows from the previous lemma, when we choose $z_1$ and $z_2$ to be empty words. □

Next, we investigate the word equation $x^2y^3x^2 = u^2v^3u^2$, in particular whether it admits nontrivial, nonperiodic solutions. In order to simplify the notations, we use $x$, $y$, $u$, and $v$ also as a shorthand for an arbitrary solution $\varphi(x)$, $\varphi(y)$, $\varphi(u)$, and $\varphi(v)$ of the equation. By nontrivial we mean a solution with $x \neq u$.

First, if $|x| = |u|$, then $x = u$ and $y = v$, i. e., the solution is trivial. Hence, since the equation is symmetric, we can suppose henceforth, without loss of generality, that $|x| > |u|$, and thus $|y| < |v|$. Using the above considerations, we can already settle some specific cases of our problem. First, if either one of $y$ or $u$ is the empty word, then we immediately obtain, due to Lemma 9, that $x, y, u$, and $v$ are all powers of a common word, i. e., the solution is periodic. Also, due to Lemma 9, if $x$ and $y$ (or symmetrically $u$ and $v$) commute, then the solution is again periodic.

**Lemma 12.** *The equation $x^2y^3x^2 = u^2v^3u^2$ has only periodic solutions, provided $x$ and $u$ commute.*

**Proof.** Let $p$ be the common primitive root of $x$ and $u$. Then, from the equation $x^2y^3x^2 = u^2v^3u^2$ we derive $p^iy^3p^i = v^3$, where $p^i = u^{-2}x^2 = x^2u^{-2}$. Thus, Lemma 9 implies that also $y$ and $v$ are powers of $p$, i. e., the solution is periodic. □

**Corollary 13.** *Let $p$ be the primitive root of $x$. If $x$ and $u$ do not commute, then $u^2$ is both a prefix and a suffix of $p$ and, moreover, $3|u| < |p|$.*

**Proof.** Since $x^2y^3x^2 = u^2v^3u^2$ and $|u| < |x|$, $u^2$ is both a prefix and a suffix of $p^i$, with $i \geq 0$. If $u^2$ would be longer than $p$, then we would get a contradiction by Lemma 11. Thus, the first part of the claim follows.

If $3|u| \geq |p|$, then, by Lemma 11, $u$ commutes with $p$, and thus also with $x$. But this is a contradiction. Thus, we must have $3|u| < |p|$. □

**Lemma 14.** *The equation $x^2y^3x^2 = u^2v^3u^2$ has only periodic solutions, provided the primitive roots of the words $y$ and $v$ are conjugates*

**Proof.** Let $p = p_1p_2$ be the primitive root of $v$ and $p_2p_1$ be the primitive root of $y$. Then, $x^2(p_2p_1)^{3i}x^2 = u^2p^{3j}u^2$, for some $i, j \geq 1$. Since $|x| > |u|$, we deduce that $x^4 = u^2p^{3(j-i)}u^2$. Then, Lemma 9 implies that $u$ and $x$ are powers of $p$, and thus, due to Lemma 12, the equation $x^2y^3x^2 = u^2v^3u^2$ admits only periodic solutions. □

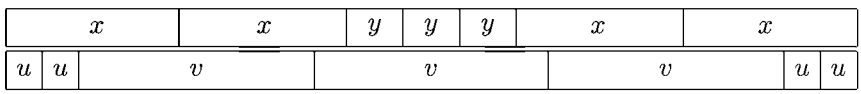
## 4. Proof of the Main Result

Now we are finally ready to prove the main result.

**Proof of Theorem 1.** Assume that $x$, $y$, $u$ and $v$ are some words satisfying the equation $x^2y^3x^2 = u^2v^3u^2$, i. e., using the shorthand notation introduced earlier,

they represent an arbitrary solution of this equation. Since we look only for nontrivial solutions, we can suppose, without loss of generality, that $|x| > |u|$, and $|y| < |v|$. Also, since Lemmas 12 and 14 already solved some specific cases of our theorem, we may assume that $x$ and $u$ do not commute and the primitive roots of the words $y$ and $v$ are not conjugates. Let $p_x, p_y, q_u$, and $q_v$ be the primitive roots of $x, y, u$, and $v$, respectively. First, we note that if $3|y| = |v|$, then $p_y$ and $q_v$ are conjugates, which is a contradiction. Thus, we can divide our analysis in two cases depending on whether $3|y| < |v|$ or $3|y| > |v|$.

**Case 1:** Suppose first that $3|y| < |v|$. Then, due to the length restrictions, we have the following situation:




In other words, the first $v$ has to end somewhere inside the second $x$ and, symmetrically, the third $v$ has to start somewhere inside the third $x$. So, we can again divide our analysis in two cases depending on the lengths of $x$ and $v$.

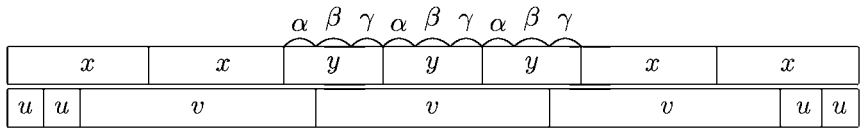
**Case 1.1:** Assume first that $|x| \leq |v|$. Then, since $u^2v$ is a prefix and $vu^2$ is a suffix of $x^2$, we obtain, due to Lemma 10, that $u^2vu^2 = p_x^i$, for some positive integer $i \geq 0$. Moreover, $|x| \leq |v|$ and $u \neq 1$ imply that $i \geq 2$. Due to Corollary 13, we know that $u^2 = p_1$ and $v = p_2 p_x^{i-2} p_3$, where $i \geq 2$ and $p_x = p_1p_2 = p_3p_1$. Lemma 5 now implies that there exist some words $\alpha, \beta \in \Sigma^*$ and some positive integer $k \geq 0$ such that $p_3 = \alpha\beta$, $p_2 = \beta\alpha$, $p_1 = (\alpha\beta)^k\alpha$, and $p_x = (\alpha\beta)^{k+1}\alpha$. Note that both $\alpha$ and $\beta$ are nonempty, since $p_x$ is primitive and $p_1$ is not empty. Since $x^2y^3x^2 = u^2v^3u^2$, we also obtain that $v = p_1p_x^n y^3 p_x^n p_1$ for some $n \geq 0$. This means that $p_2p_x^{i-2}p_3 = p_1p_x^n y^3 p_x^n p_1$, or equivalently,

$$\beta\alpha((\alpha\beta)^{k+1}\alpha)^{i-2}\alpha\beta = (\alpha\beta)^k\alpha((\alpha\beta)^{k+1}\alpha)^n y^3((\alpha\beta)^{k+1}\alpha)^n(\alpha\beta)^k\alpha. \tag{3}$$

If $k \geq 1$, then the two sides of equation (3) start with $\alpha\beta$ and $\beta\alpha$, respectively. Thus, $\alpha$ and $\beta$ commute, which contradicts the primitivity of $p_x = (\alpha\beta)^{k+1}\alpha$. Hence, we must have $k = 0$. If $n \geq 1$, then we obtain that $\beta\alpha^2 = \alpha^2\beta$, which, again, contradicts the primitivity of $p_x$. So, also $n$ equals 0, implying that $v = p_1y^3p_1 = p_2p_x^{i-2}p_3$, where $p_x = p_1p_2 = p_3p_1$. But this is equivalent with $(p_1)^2y^3(p_1)^2 = p_x^i$, for some $i \geq 2$, which, due to Lemma 9, implies that $p_1$, $y$, and $p_x$ are all powers of a common word. Thus, $p_x$ is not primitive, which is a contradiction.

**Case 1.2:** Consider now the case when $|x| > |v|$. From the situation illustrated by the above picture we notice that the second and the third occurrences of $x$ are covered by $v^2$. More precisely, $\left((u^2)^{-1}x\right)x$ is a prefix and $x\left(x(u^2)^{-1}\right)$ is a suffix of $v^2$. Therefore, by Lemma 10, $v$ and $(u^2)^{-1}x^3(u^2)^{-1}$ commute. This implies, that $x^3 = u^2q_v^k u^2$, where $k \geq 2$ and $q_v$ is the primitive root of $v$. But, due to Lemma 9, this implies that $x$ and $u$ commute, and thus we have a contradiction again.

**Case 2:** Suppose now that $3|y| > |v|$. If $3|y| \geq |v| + |p_y|$, then by Lemma 7, $p_y$ and $q_v$ are conjugates, which is a contradiction. Thus, we have that $3|y| < |v| + |p_y|$. This implies the existence of nonempty words $\alpha$, $\beta$ and $\gamma$ for which $y = \alpha\beta\gamma$ and $v = (\beta\gamma)(\alpha\beta\gamma)(\alpha\beta)$, with $|\alpha| = |\gamma| < \frac{1}{2}|p_y|$. So, we have the following situation



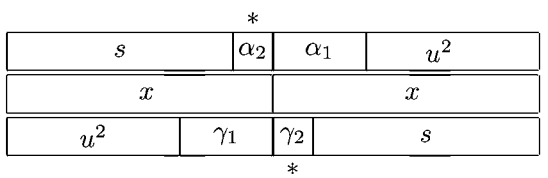

illustrating that $u^2v = x^2\alpha$ and $vu^2 = \gamma x^2$.

Since $\gamma$ is a prefix and $\alpha$ is a suffix of $v$, we have $\beta\gamma = \gamma\beta'$ and $\alpha\beta = \beta''\alpha$ for some words $\beta'$ and $\beta''$, with $|\beta'| = |\beta| = |\beta''|$. Let $s = \gamma^{-1}v\alpha^{-1} = \beta'\alpha\beta\gamma\beta''$. From $v = \gamma s\alpha$, $u^2v = x^2\alpha$, and $vu^2 = \gamma x^2$ we deduce

$$x^2 = u^2\gamma s = s\alpha u^2. \tag{4}$$

Now we have two cases depending on whether $p_x$ is longer or shorter than $s$.

**Case 2.1:** Assume first that $|p_x| \geq |s|$. By Corollary 13, we know that $u^2$ is strictly shorter than $x$. Therefore, by (4), we have factorizations $\gamma = \gamma_1\gamma_2$ and $\alpha = \alpha_2\alpha_1$, with $|\alpha_1| = |\gamma_1| > 0$, such that $x = u^2\gamma_1 = \gamma_2 s$ and $x = s\alpha_2 = \alpha_1 u^2$. The situation is illustrated by the following picture, in which the symbols $*$ remind that $\alpha_2$ and $\gamma_2$ can be empty:




If we compute

$$|x| \geq |p_x| \geq |s| > |\alpha| + |\gamma| \geq |\alpha_1| + |\gamma_1| = 2\big(|x| - 2|u|\big),$$

we see that $|x| < 4|u|$, which means that the two $u$'s in the beginning and the end of $x$ overlap inside $x$. In other words, if $t$ is this overlap, we have $x = \left(u^2t^{-1}\right)t\left(t^{-1}u^2\right)$, $\gamma_1 = t^{-1}u^2$ and $\alpha_1 = u^2t^{-1}$.

From Lemma 11 we get that the length of $t$ has to be less than the length of the primitive root $q_u$ of $u$, since $x$ and $u$ do not commute. Now, we observe that the word $\gamma_2\beta'\alpha_2$, which is a prefix of $x$, has length

$$\begin{aligned} |\gamma_2\beta'\alpha_2| &< |\gamma_2\beta'\alpha_2\beta\gamma_2\beta''| = |\gamma_2\beta'\alpha\beta\gamma\beta''| - |\alpha_1\gamma_1| \\ &= |x| - |\alpha_1\gamma_1| = |t| < |q_u|\,. \end{aligned}$$

Then, the word $\gamma_2\beta'\alpha_2 q_u$ is a proper prefix of $q_u q_u$, since $q_u$ is a prefix of $\alpha_1$ and both $\gamma_2\beta'\alpha_2\alpha_1$ and $q_u q_u$ are prefixes of $x$. But this is impossible, because $q_u$ is supposed to be primitive, see Lemma 2.

**Case 2.2:** We are left with the case $|p_x| < |s|$. In this case, $s \in p_x^+ p_x$, by Lemma 11, since $s$ is a prefix and a suffix of $x^2$. Therefore, by equation (4),

$$u^2\gamma, \alpha u^2 \in p_x^+. \tag{6}$$

Then $v$ is a factor of $p_x^\omega$, since $v = \gamma s \alpha$. Also, $v$ is a factor of $p_y^\omega$, where $p_y$ is the primitive root of $y$, since $y^3$ covers $v$. We observe that

$$|v| = |\gamma s \alpha| > |s| \geq 2\,|p_x|$$

and

$$|v| = |(\beta\gamma)(\alpha\beta\gamma)(\alpha\beta)| > 2\,|\alpha\beta\gamma| = 2\,|y| \geq 2\,|p_y|\,.$$

It follows, by Lemma 7, that $p_x$ and $p_y$ are conjugates.

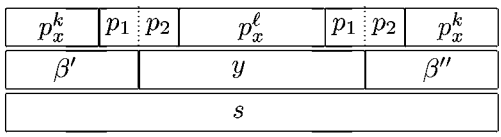
Since $|\alpha| = |\gamma| < \frac{1}{2}\,|p_y| = \frac{1}{2}\,|p_x|$, $\alpha$ is a proper prefix and $\gamma$ is a proper suffix of $p_x$. By Corollary 13, the length of $p_x$ is strictly larger than $3\,|u|$, and then, by (6), $u^2\gamma = \alpha u^2 = p_x$. Therefore

$$|\alpha| = |p_x| - 2\,|u| > |p_x| - 2\frac{|p_x|}{3} = \frac{1}{3}\,|p_x|\,.$$

Thus the length of $\alpha$ is in the range

$$\frac{1}{3}\,|p_x| < |\alpha| < \frac{1}{2}\,|p_x|\,. \tag{8}$$

Since $s = \beta' y \beta''$, $|p_x|$ divides $|y|$, and $x$ and $y$ do not commute, there is a factorization $p_x = p_1 p_2$ such that $|p_1| = |p_2|$, $\beta' = p_x^k p_1$, $y = p_2 p_x^\ell p_1$, and $\beta'' = p_2 p_x^k$, with $k, \ell \geq 0$.




Now,

$$\begin{aligned}|\alpha| &= \frac{1}{2}\,|\alpha\gamma| = \frac{1}{2}\big(\,|\alpha\beta\gamma| - |\beta|\,\big) = \frac{1}{2}\big(\,|y| - |\beta|\,\big) \\ &= \frac{1}{2}\Big(l + 1 - \big(k + \tfrac{1}{2}\big)\Big)\,|p_x| \in \big\{\big(n + \tfrac{1}{4}\big)\,|p_x|\,, \big(n + \tfrac{3}{4}\big)\,|p_x|\big\}\,,\end{aligned}$$

where $n = \left\lfloor \frac{1}{2}(l-k) \right\rfloor$. But then $|\alpha|$ is not in the interval (8) as required above, which is a contradiction. □

**Acknowledgments**

This research was supported by the Academy of Finland under the grants 203354 and 110650. The research of the first author was partially supported by a Turun Yliopistosäätiön grant. The second author was supported by the research project MSM 0021620839 financed by MSMT, and by the Grant Agency of Charles University, grant 444/2004.

## References

[1] C. Choffrut, J. Karhumäki, Combinatorics on Words. In: G. Rozenberg, A. Salomaa (eds.), *Handbook of Formal Languages* **1**, Chapter 6, 329–438, Springer 1997.

[2] K. Culik II, J. Karhumäki, On the equality sets for homomorphisms on free monoids with two generators. *RAIRO Theor. Informatics* **14** (1980), 349–369.

[3] V. Diekert, Makanin's Algorithm. In M. Lothaire (ed.), *Algebraic Combinatorics on Words*, Chapter 12, 387–442, Cambridge University Press, 2002.

[4] T. Harju, D. Nowotka, The equation $x^i = y^j z^k$ in a free semigroup. *Semigroup Forum* **68** (2004), 488–490.

[5] S. Holub, Binary equality sets are generated by two words. *Journal of Algebra* **259** (2003), 1–42.

[6] S. Holub, A unique structure of two-generated binary equality sets. In M. Ito, M. Toyama (eds.), *Developments in Language Theory.* Lecture Notes in Computer Science **2450**, 245–257, Springer, 2003.

[7] A. Lentin, Equations in free monoids. In M. Nivat (ed.), *Automata, languages and programming*, 67–85, 1972.

[8] R. C. Lyndon, M. P. Schützenberger, The equation $a^M = b^N c^P$ in a free group. *Michigan Math. J.* **9** (1962), 289–298.

[9] G. S. Makanin, The problem of solvability of equations in a free semigroup. *Mat. Sb. (NS)* **103** (1977) 2, 147–236. In Russian. English translation: *Math. USSR-Sb.* **32** (1977), 129–198.

[10] Y. Matiyasevich, Enumerable sets are diophantine. *Soviet Math. Doklady* **11** (1970), 354–357. In Russian. English translation: *Dokl. Akad. Nauk. SSSR* **191** (1971), 279–282.