# On the Equation $x^k = z_1^{k_1} z_2^{k_2} \cdots z_n^{k_n}$ in a Free Semigroup

**Tero Harju**
**Dirk Nowotka**

Turku Centre for Computer Science, TUCS,
Department of Mathematics, University of Turku

**Turku Centre for Computer Science**
**TUCS Technical Report No 602**
**April 2004**
**ISBN 952-12-1342-6**
**ISSN 1239-1891**

**Abstract**

Word equations of the form $x^k = z_1^{k_1} z_2^{k_2} \cdots z_n^{k_n}$ are considered in this paper. In particular, we investigate the case where $x$ is of different length than $z_i$, for any $i$, and $k$ and $k_i$ are at least 3, for all $1 \le i \le n$, and $n \le k$. We prove that for those equations all solutions are of rank 1, that is, $x$ and $z_i$ are powers of the same word for all $1 \le i \le n$. It is also shown that this result implies a well-known result by K. I. Appel and F. M. Djorup about the more special case where $k_i = k_j$ for all $1 \le i < j \le n$.

**Keywords:** combinatorics on words, word equations

**TUCS Laboratory**
Discrete Mathematics for Information Technology

# 1 Introduction

Word equations of the form

$$x^k = z_1^{k_1} z_2^{k_2} \cdots z_n^{k_n} \tag{1}$$

have long been of interest, see for example [7, 5, 1]. Originally motivated from questions concerning equations in free groups special cases of (1) in free semigroups were investigated. For example

$$x^k = z_1^{k_1} z_2^{k_2}$$

is of rank 1 which was shown by Lyndon and Schützenberger [7], and Lentin [5] investigated the solutions of

$$x^k = z_1^{k_1} z_2^{k_2} z_3^{k_3}$$

which has solutions of higher rank, see Example 6, and Appel and Djorup [1] investigated

$$x^k = z_1^k z_2^k \cdots z_n^k .$$

We show in Theorem 5 of this paper that equations of the form (1) are of rank 1, if all exponents are larger than 2 and $n \leq k$ and $x$ is not a conjugate of $z_i$ for any $1 \leq i \leq n$. This result straightforwardly implies Theorem 7 by Appel and Djorup [1].

We continue with fixing some notation. More basic definitions can be found in [6]. Let $A$ be a finite set and $A^*$ be the free monoid generated by $A$. We call $A$ *alphabet* and the elements of $A^*$ *words*. Let $w = w_{(1)} w_{(2)} \cdots w_{(n)}$ where $w_{(i)}$ is a letter, for every $1 \leq i \leq n$. We denote the length $n$ of $w$ by $|w|$. An integer $1 \leq p \leq n$ is a *period* of $w$, if $w_{(i)} = w_{(i+p)}$ for all $1 \leq i \leq n - p$. A nonempty word $u$ is called a *border* of a word $w$, if $w = uv = v'u$ for some suitable words $v$ and $v'$. We call $w$ *bordered*, if it has a border that is shorter than $w$, otherwise $w$ is called *unbordered*. A word $w$ is called *primitive* if $w = u^k$ implies that $k = 1$. We call two words $u$ and $v$ *conjugates*, denoted by $u \sim v$, if $u = xy$ and $v = yx$ for some words $x$ and $y$. Let $[u] = \{v \mid u \sim v\}$ and $w^* = \{w^i \mid i \geq 0\}$.

Let $\Sigma$ be an alphabet. A tuple $(u, v) \in \Sigma^* \times \Sigma^*$ is called *word equation* in $\Sigma$, usually denoted by $u = v$. Let $u, v \in \Sigma^*$ be such that every letter of $\Sigma$ occurs in $u$ or $v$. A morphism $\varphi\colon \Sigma^* \to A^*$ is called a *solution* of $u = v$, if $\varphi(u) = \varphi(v)$. The *rank of a solution* $\varphi$ of an equation $u = v$ is the minimum rank of a free subsemigroup that contains $\varphi(\Sigma)$. The *rank of an equation* is the maximum rank of all its solutions.

# 2 Some Known Results

The following theorem was shown by Fine and Wilf [2]. As usual, gcd denotes the greatest common devisor.

**Theorem 1.** *Let $w \in A^*$, and $p$ and $q$ be periods of $w$. If we have that $|w| \geq p + q - \gcd\{p, q\}$ then $\gcd\{p, q\}$ is a period of $w$.*

The following lemma is a consequence of Theorem 1; see [3].

**Lemma 2.** *Let $w \in A^*$ and $p$ be the smallest period of $w$. Then, for any period $q$ of $w$, with $q \leq |w| - p$, we have that $q$ is a multiple of $p$.*

The following theorem follows Lyndon and Schützenberger's proof [7] for free groups. See also [4] for a short direct proof and the following Lemma 4.

**Theorem 3.** *Let $x, y, z \in A^*$ and $i, j, k \geq 2$. If $x^i = y^j z^k$ then $x, y, z \in w^*$ for some $w \in A^*$.*

**Lemma 4.** *Let $x, z \in A^*$ be primitive and nonempty words. If $z^m$ is a factor of $x^k$ for some $k, m \geq 2$, then either $(m-1)|z| < |x|$ or $z$ and $x$ are conjugates.*

*Proof.* Assume that $(m-1)|z| \geq |x|$. Then $z^m$ has two periods $|x|$ and $|z|$, and hence, a period $\gcd\{|x|, |z|\}$ by Theorem 1. Now, $|x| = |z|$ and $x$ and $z$ are conjugates. □

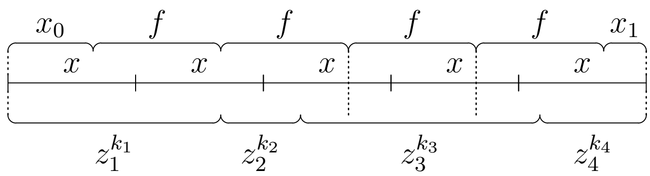
# 3 The Main Result

The following theorem is the main result of this paper. It shows that the solutions of a word equation of the form $x^k = z_1^{k_1} z_2^{k_2} \cdots z_n^{k_n}$ are necessarily of rank 1 under certain conditions.

**Theorem 5.** *Let $n \geq 2$ and $x, z_i \in A^*$ and $|x| \neq |z_i|$ and $k, k_i \geq 3$, for all $1 \leq i \leq n$. If $x^k = z_1^{k_1} z_2^{k_2} \cdots z_n^{k_n}$ and $n \leq k$ then $x, z_i \in w^*$, for some $w \in A^*$ and all $1 \leq i \leq n$.*

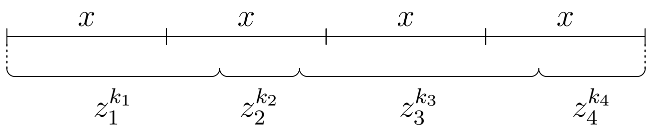
*Proof.* Assume w.l.o.g. that $x, z_i$, for all $1 \leq i \leq n$, are primitive words. Note, that $|z_i^{k_i - 1}| < |x|$ by Lemma 4, and therefore $|z_i| < |x|$ for all $i$.

If $n < k$ then let $f$ be an unbordered conjugate of $x$, and $x^k = x_0 f^{k-1} x_1$ with $x = x_0 x_1$. Let us illustrate this case with the following drawing.



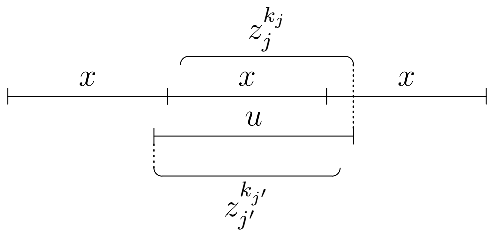
By the pigeon hole principle there exists an $i$ such that $f$ is a factor of $z_i^{k_i}$. But now, $f$ is bordered; a contradiction.

Assume $n = k$ in the following. Let us illustrate this case with the following drawing.



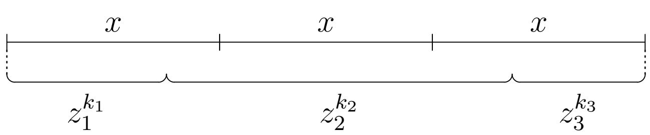

From $k_i \geq 3$, for all $1 \leq i \leq n$, follows that there exists a primitive word $z \in A^*$ such that for every $i$ with $|x| \leq |z_i^{k_i}|$ we have that $|z_i|$ is the smallest period of $x$ and $z_i \in [z]$ by Lemma 2.

There exists an $i$ such that $|x| \leq |z_i^{k_i}|$ by a length argument. We also have for all $1 \leq i < n$ that, if $|x| \leq |z_i^{k_i}|$ then $|z_{i+1}^{k_{i+1}}| < |x|$, otherwise either $z$ is not primitive or $x \in z_0^*$, with $z_0 \in [z]$, and $x$ is not primitive. Similarly for $z_{i-1}$. Moreover, we have that all factors $z_j^{k_j}$ with $|x| \leq |z_j^{k_j}|$ occur in a word $u$ which is a factor of $xxx$ and $|u| < |x| + |z|$ otherwise $z^{k_i+1}$, for some $1 \leq i \leq n$, and $xx$ have a common factor of length greater or equal to $|x| + |z|$ and either $x$ or $z$ is not primitive. Consider the following drawing.




Therefore, we have for every $i$ with $|x| \leq |z_i^{k_i}|$ that $|z_{i+1}^{k_{i+1}}| < |zz|$ because $|z_{i+1}| < |z|$ and otherwise $z$ is not primitive. This proves the case for $k > 3$ since then $|z_i^{k_i} z_{i+1}^{k_i}| < |xx|$ (for $k_i \geq 3$ for all $1 \leq i \leq n$ is required), for every $i$ such that $|x| \leq |z_i^{k_i}|$, and $|z_1^{k_1} z_2^{k_2} \cdots z_n^{k_n}| < |x^k|$; a contradiction.

The case $k = 3$ remains. Since we can construct from one equation a new one of the same rank by cyclic shifts, we can assume that $|x| \leq |z_2^{k_2}|$. Let us consider the following drawing for example.




By the arguments above, we have that $|z_1^{k_1}| < |x|$ and $|z_3^{k_3}| < |x|$. Now, $|z^{k_2-1}| < |x| < |z^{k_2}|$ and $|z^{k_2}| < |z_1^{k_1}| + |z_3^{k_3}|$. Let $x = z'^{k_2-1} z'_0$, where $z' \in [z]$ and $z'_0$ is a prefix of $z'$. Let $g$ be an unbordered conjugate of $z'$ such that $z'z' = g_1 g g_0$, where $g = g_0 g_1$ and $z' = g_1 g_0$. We get a contradiction, if

$|g_1 g| \leq |z_1^{k_1}|$ since then $z_1^{k_1}$ covers $g$, and hence, $g$ is bordered. So, assume $|g_1 g| > |z_1^{k_1}|$. But now, $|z_1^{k_1} z_2^{k_2}| < |xxg_1|$, because we have that $|g_0 z_0' x| < |z_2^{k_2}| < |x| + |z| < |g_0 z_0' x g_1|$, and $g$ is covered by $z_3^{k_3}$; a contradiction again. $\square$

The following example shows why the condition $|x| \neq |z_i|$ is needed in Theorem 5.

**Example 6.** *Consider $x^4 = z_1^3 z_2^3 z_3^3$. There exists a solution $\varphi$ of rank 2 with $\varphi(x) = \varphi(z_1) = a^3 b^3$ and $\varphi(z_2) = a^3$ and $\varphi(z_3) = b^3$.*

Theorem 5 implies the following result by Appel and Djorup [1].

**Theorem 7.** *Let $n \geq 2$ and $x, z_i \in A^*$, for all $1 \leq i \leq n$. If $x^k = z_1^k z_2^k \cdots z_n^k$ with $n \leq k$, then $x, z_i \in w^*$, for some $w \in A^*$ and all $1 \leq i \leq n$.*

*Proof.* If $n = 2$ the result follows from Theorem 3. Assume $n > 2$ in the following. Let $\bar{x}$ and $\bar{z}_i$ denote the primitive roots of $x = \bar{x}^\ell$ and $z_i = \bar{z}_i^{\ell_i}$, for all $1 \leq i \leq n$, respectively. Then we have

$$\bar{x}^{\ell k} = \bar{z}_1^{\ell_1 k} \bar{z}_2^{\ell_2 k} \cdots \bar{z}_n^{\ell_n k} . \qquad (2)$$

If there exists an $i$ such that $|\bar{z}_i| = |\bar{x}|$ then $\bar{z}_i \sim \bar{x}$ and we have the equation

$$\bar{x}^{(\ell - \ell_1)k} = \bar{z}_1^{\ell_1 k} \bar{z}_2^{\ell_2 k} \cdots \bar{z}_{i-1}^{\ell_{i-1} k} \bar{z}_{i+1}^{\ell_{i+1} k} \cdots \bar{z}_n^{\ell_n k} \qquad (3)$$

which has not a higher rank than (2). Since(3) meets our assumptions this reduction can be iterated until either $n = 2$ or $|\bar{z}_i| \neq |\bar{x}|$ for all $1 \leq i \leq n$. But, then Theorem 5 gives the result. $\square$

# References


[1] K. I. Appel and F. M. Djorup. On the equation $z_1^n z_2^n \cdots z_k^n = y^n$ in a free semigroup. *Trans. Amer. Math. Soc.*, 134:461–470, 1968.

[2] N. J. Fine and H. S. Wilf. Uniqueness theorem for periodic functions. *Proc. Amer. Math. Soc.*, 16:109–114, 1965.

[3] V. Halava, T. Harju, and L. Ilie. Periods and binary words. *J. Combin. Theory, Ser A*, 89(2):298–303, 2000.

[4] T. Harju and D. Nowotka. The equation $a^M = b^N c^P$ in a free semigroup. *Semigroup Forum*, 2004. to appear.

[5] A. Lentin. Sur l'équation $a^M = b^N c^P d^Q$ dans un monoïd libre. *C. R. Acad. Sci. Paris*, 260:3242–3244, 1965.

[6] M. Lothaire. *Combinatorics on Words*, volume 12 of *Encyclopedia of Mathematics and its Applications.* Addison-Wesley, Reading, MA, 1983.

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

**Turku Centre for Computer Science**
**Lemminkäisenkatu 14**
**FIN-20520 Turku**
**Finland**

http://www.tucs.fi

**University of Turku**
- **Department of Information Technology**
- **Department of Mathematics**

**Åbo Akademi University**
- **Department of Computer Science**
- **Institute for Advanced Management Systems Research**

**Turku School of Economics and Business Administration**
- **Institute of Information Systems Science**