

An Improved Version of Hmelevskii's Theorem on Three-Variable Word Equations

Aleksi Saarela  

Department of Mathematics and Statistics, University of Turku, Finland

Abstract

Hmelevskii proved in 1971 that every constant-free three-variable word equation has a parametric solution. We prove an improved version of this result by showing that every such equation has a parametric solution using only three numerical parameters and with only two levels of nesting. This means that the structure of the solution sets of these equations is considerably simpler than has been known before.

2012 ACM Subject Classification Mathematics of computing → Combinatorics on words

Keywords and phrases Combinatorics on words, word equation, parametric word

Digital Object Identifier 10.4230/LIPIcs.STACS.2026.77

Funding Supported by the Research Council of Finland under grant 339311.

1 Introduction

The study of word equations is interesting from the point of view of algebra and combinatorics, and also from the point of view of several more applied topics, such as string solvers [3] and document spanners [7]. Two very common (and closely related) research questions about word equations are studying the complexity of the satisfiability problem, that is, the problem of determining whether a given equation has a solution, and studying the structure of solution sets. These questions can be studied for different restricted subfamilies or for various generalizations of word equations. We give here some examples of existing results.

The satisfiability problem of word equations is known to be in $\text{NSPACE}(n)$ [12]. It is also known to be NP-hard, but it is an open question whether it is in NP. There are many generalized versions of word equations for which the satisfiability problem is undecidable, see, for example, [4]. An interesting open question is the decidability of the satisfiability of word equations with length constraints. On the other hand, many easier variants can be solved in polynomial time, e.g., [11, 6, 5].

Strong results about the structure of solution sets exist for many subfamilies of word equations. It is a folklore result that constant-free equations on one or two variables have only periodic solutions. Constant-free equations on three variables are much more complicated, but they always have a so-called parametric solution, as proved by Hmelevskii [10]. Constant-free equations on four variables, on the other hand, do not always have parametric solutions; this was also proved in [10]. For one-variable equations with constants, it is known that if the solution set is infinite, then the possible values for the variable are exactly the words in a language of the form $(uv)^*u$ [14], and if the solution set is finite, there are at most three solutions [16]. There are also results about the solution sets of arbitrary word equations or some of their generalizations, such as [2].

In this article, we concentrate on constant-free equations on three variables, with the goal of giving an improved, more precise version of the above-mentioned result of Hmelevskii. Although the statement of the old result is strong and elegant, there are a couple of weaknesses: First, the original proof, and even the simpler version of that proof in [13, 18], is very long



© Aleksi Saarela;

licensed under Creative Commons License CC-BY 4.0

43rd International Symposium on Theoretical Aspects of Computer Science (STACS 2026).

Editors: Meena Mahajan, Florin Manea, Annabelle McIver, and Nguyễn Kim Thăng

Article No. 77; pp. 77:1–77:14



Leibniz International Proceedings in Informatics

LIPICs Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany



and hard to read. Second, the parametric words that arise from the proof can be very complicated. For example, the number of numerical parameters and the nesting level can be estimated to be logarithmic with respect to the length of the equation, see [17, 18].

We prove as our main result that every constant-free equation on three variables has a parametric solution using only three numerical parameters and with nesting level at most two. This result was essentially conjectured in [19], and a similar result was proved for the subfamily of so-called unbalanced equations.

Our approach is very different from the one used by Hmelevskii, and it is not reliant on the results in [10]. On the other hand, we make extensive use of some other existing results, both old and recent, like the ones in [1, 19].

The structure of the article is as follows. In Section 2, we give many necessary definitions and state some existing results. In Section 3, we define a particular free group morphism and prove several lemmas related to it. This morphism then allows us to reformulate a result that was proved in [19]. The reformulation essentially combines six cases into one, making the result much easier to apply. On the other hand, the fact that the morphism is a free group morphism instead of a free monoid morphism leads to some complications. In Section 4, we give modified versions of some earlier results. The results are very close to the original ones, and large parts of the proofs are the same as in the original articles, but some changes are necessary to make the results work for our purposes. Section 5 contains the most important part of the proof of the main theorem. In this section, we find simple parametric representations for certain sets, and these can then be used as building blocks for a parametric solution of an arbitrary three-variable equation, as is finally done in Section 6.

2 Preliminaries

Let \mathbb{N} denote the set of nonnegative integers.

The set of all words over an alphabet Σ is denoted by Σ^* . This set, together with the concatenation operation, is a free monoid. The empty word, denoted by ε , is the neutral element of this monoid.

A word u is a *factor* of a word w if there exist words s, t such that $w = sut$. Words u and v are *conjugates* if there exist words s, t such that $u = st$ and $v = ts$.

The free monoid Σ^* can be extended to a free group, which we denote by $(\Sigma^{\pm 1})^*$. We are mostly interested in free monoids, but occasionally we have to refer to free groups. Morphisms over free groups, in particular, are a useful tool in certain parts of this article.

A mapping $h : (\Sigma_1^{\pm 1})^* \rightarrow (\Sigma_2^{\pm 1})^*$ is a *G-morphism* if $h(uv) = h(u)h(v)$ for all $u, v \in (\Sigma_1^{\pm 1})^*$. The morphism h is uniquely defined by the values $h(c)$ for $c \in \Sigma_1$. The set of all G-morphisms $(\Sigma_1^{\pm 1})^* \rightarrow (\Sigma_2^{\pm 1})^*$ is denoted by $\text{GM}(\Sigma_1, \Sigma_2)$.

If $h \in \text{GM}(\Sigma_1, \Sigma_2)$ and $h(c) \in \Sigma_2^*$ for all $c \in \Sigma_1$ (and, consequently, $h(u) \in \Sigma_2^*$ for all $u \in \Sigma_1^*$), then h is called an *M-morphism*. The set of all M-morphisms $(\Sigma_1^{\pm 1})^* \rightarrow (\Sigma_2^{\pm 1})^*$ is denoted by $\text{MM}(\Sigma_1, \Sigma_2)$.

A morphism $h \in \text{MM}(\Sigma_1, \Sigma_2)$ is *periodic* if there exists $w \in \Sigma_2^*$ such that $h(c) \in w^*$ for all $c \in \Sigma_1$, and *nonperiodic* otherwise.

► **Remark 1.** Usually when studying words, morphisms are defined as mappings $h : \Sigma_1^* \rightarrow \Sigma_2^*$ such that $h(uv) = h(u)h(v)$ for all $u, v \in \Sigma_1^*$. Every such mapping can be extended to an M-morphism in a unique way, and conversely, every M-morphism can be restricted to such a mapping. We use M-morphism so that we do not have to talk about extensions and restrictions.

2.1 Equations

Let Ξ be an alphabet of variables and let Σ be an alphabet of constants. A *constant-free word equation* on Ξ is a pair $E = (u, v)$, where $u, v \in \Xi^*$, and a *solution* of E is an M-morphism $h \in \text{MM}(\Xi, \Sigma)$ such that $h(u) = h(v)$. The equation E is *nontrivial* if $u \neq v$.

A *system of equations* is a set of equations. A *solution* of a system is an M-morphism that satisfies all equations in the system.

The set of all solutions of an equation or system E is denoted by $\text{Sol}(E)$, and the set of all equations satisfied by a morphism h is denoted by $\text{Eq}(h)$. Equations or systems E_1, E_2 are *equivalent* if $\text{Sol}(E_1) = \text{Sol}(E_2)$, and morphisms h_1, h_2 are *equivalent* if $\text{Eq}(h_1) = \text{Eq}(h_2)$.

In this article, we are interested in the three-variable case. From now on, let $\{x, y, z\}$ be an alphabet of three variables, let Σ be a nonunary alphabet of constants and let $a, b \in \Sigma$ be two distinct letters.

We use the shorthand notation $[u, v, w]$, where $u, v, w \in (\Sigma^{\pm 1})^*$, for the morphism $h \in \text{GM}(\{x, y, z\}, \Sigma)$ defined by $h(x) = u, h(y) = v, h(z) = w$.

► **Example 2.** Consider the equation $E = (xy, yz)$. For all $u, v \in \Sigma^*$ and $j \in \mathbb{N}$, the morphism $h = [uv, (uv)^j u, vu]$ is a solution of E :

$$h(xy) = uv(uv)^j u = (uv)^j uvu = h(yz).$$

Similarly, $[\varepsilon, u, \varepsilon]$ is a solution for all $u \in \Sigma^*$. It would be quite easy to show that there are no other solutions, so

$$\begin{aligned} \text{Sol}(E) &= \{[uv, (uv)^j u, vu] \mid u, v \in \Sigma^*, j \in \mathbb{N}\} \cup \{[\varepsilon, u, \varepsilon] \mid u \in \Sigma^*, j \in \mathbb{N}\} \\ &= \text{MM}(\{a, b\}, \Sigma) \circ (\{[ab, (ab)^j a, ba] \mid j \in \mathbb{N}\} \cup \{[\varepsilon, a, \varepsilon] \mid j \in \mathbb{N}\}). \end{aligned}$$

Here we are using the notation $G \circ H = \{g \circ h \mid g \in G, h \in H\}$. We frequently write solution sets or other sets of morphisms in this kind of form.

2.2 Parametric Words

Let $\mathcal{P}_0(p, q)$ be the set of functions of the form

$$\alpha : (\Sigma^*)^p \times \mathbb{N}^q \rightarrow \Sigma^*, \alpha(u_1, \dots, u_p; j_1, \dots, j_q) = u_{i_1} \cdots u_{i_n},$$

where $n \in \mathbb{N}$ and $i_1, \dots, i_n \in \{1, \dots, p\}$. For $d \geq 1$, let $\mathcal{P}_d(p, q)$ be the set of functions of the form

$$\alpha : (\Sigma^*)^p \times \mathbb{N}^q \rightarrow \Sigma^*, \alpha(X) = \alpha_0(X) \beta_1(X)^{j_{i_1}} \alpha_1(X) \cdots \beta_n(X)^{j_{i_n}} \alpha_n(X),$$

where $X = (u_1, \dots, u_p; j_1, \dots, j_q)$, $n \in \mathbb{N}$, $i_1, \dots, i_n \in \{1, \dots, q\}$ and $\alpha_i, \beta_i \in \mathcal{P}_{d-1}(p, q)$ for all i .

The elements of

$$\bigcup_{i=0}^{\infty} \mathcal{P}_i(p, q).$$

are called *parametric words with p word parameters and q numerical parameters*. For a parametric word α , the smallest d such that $\alpha \in \mathcal{P}_d(p, q)$ is called the *nesting level* of α . We have $\mathcal{P}_{d-1}(p, q) \subseteq \mathcal{P}_d(p, q)$, so $\mathcal{P}_d(p, q)$ is the set of parametric words with nesting level at most d .

► **Example 3.** The function defined by $\alpha(u, v; i, j, k) = u^i(u^j v)^k uv^k$ is a parametric word in $\mathcal{P}_2(2, 3)$.

Next we define parametric representations and solutions. To simplify notation, we concentrate on the three-variable case. A finite set

$$\{(\alpha_i, \beta_i, \gamma_i) \mid i \in \{1, \dots, k\}\}$$

of triples of parametric words in $\mathcal{P}_d(p, q)$ is a *parametric representation* of the set of morphisms

$$\{[\alpha_i(X), \beta_i(X), \gamma_i(X)] \mid i \in \{1, \dots, k\}, X \in (\Sigma^*)^p \times \mathbb{N}^q\}.$$

The family of all such sets of triples is denoted by $\mathcal{R}_d(p, q)$. For a three-variable equation E , a parametric representation of $\text{Sol}(E)$ is called a *parametric solution* of E .

► **Example 4.** The equation (xy, yz) in Example 2 has a parametric solution

$$\{(\alpha_1, \alpha_2, \alpha_3), (\beta_1, \beta_2, \beta_1)\},$$

where

$$\begin{aligned} \alpha_1(u, v; j) &= uv, & \alpha_2(u, v; j) &= (uv)^j u, & \alpha_3(u, v; j) &= vu, \\ \beta_1(u, v; j) &= \varepsilon, & \beta_2(u, v; j) &= u. \end{aligned}$$

Here $\alpha_2 \in \mathcal{P}_1(2, 1)$ and the other parametric words are in $\mathcal{P}_0(2, 1)$, so the parametric solution is in $\mathcal{R}_1(2, 1)$.

It is usually not necessary to explicitly define the parametric words, since they can be directly seen from expressions like $[uv, (uv)^j u, vu]$ or $[ab, (ab)^j a, ba]$.

Hmelevskii [10] proved that every constant-free three-variable word equation has a parametric solution. These parametric solutions use two word parameters, except that trivial equations have a parametric solution in $\mathcal{R}_0(3, 0)$. This is connected to the famous defect theorem, according to which n words satisfying a nontrivial relation can be expressed as products of $n - 1$ words (see [8] for more on the defect theorem and its variations). The number of numerical parameters and nesting level were not analyzed in [10], but a logarithmic upper bound follows from the proofs in [17, 18], leading to the next theorem.

► **Theorem 5.** *For every nontrivial constant-free three-variable word equation E , there exist q, d such that E has a parametric solution in $\mathcal{R}_d(2, q)$. Moreover, q and d are logarithmic with respect to the length of E .*

The following lemma is well-known, see Example 5.1.2 and the proof of Theorem 5.1.3 in [18] for an explanation.

► **Lemma 6.** *The set of periodic solutions of a constant-free three-variable equation has a parametric representation in $\mathcal{R}_1(1, 3)$.*

2.3 Classification of Morphisms

Budkina and Markov [1] classified all three-generator subsemigroups of a free semigroup. This result has been used in many places, often reformulated in terms of morphisms and equations. We copy here the formulation that was used in [19]. An essentially equivalent result was proved independently by Spehner [20, 21], see [9] for a good comparison of these results.

► **Theorem 7** (Budkina and Markov [1]). *Every nonperiodic morphism in $\text{MM}(\{x, y, z\}, \Sigma)$ that satisfies a nontrivial equation is equivalent, up to a permutation of the variables, to a morphism of one of the following types:*

BM1. $[a, b, a^{k_0} \prod_{i=1}^n ba^{k_i}]$, where $n, k_0, \dots, k_n \in \mathbb{N}$.

BM2. $[a, b^m, b^n]$, where $m, n \in \mathbb{N}$ and $m, n \geq 1$ and $\gcd(m, n) = 1$.

BM3. $[a, a^p b a^q, a^{p'} b \prod_{i=1}^n (a^{k_i} b) a^{q'}]$, where $p, q, p', q', n, k_1, \dots, k_n \in \mathbb{N}$ and $pp' = qq' = 0$ and $1 \leq p + q \leq k_1, \dots, k_n$.

BM4. $[a, a^p b (a^k b)^m, b (a^k b)^n a^q]$, where $p, q, k, m, n \in \mathbb{N}$ and $k, m, n \geq 1$ and $p, q \leq k$ and $\gcd(m + 1, n + 1) = 1$.

BM5. $[a, a^p b (a^k b)^m a^q, b (a^k b)^n]$, where $p, q, k, m, n \in \mathbb{N}$ and $p, q, k, m, n \geq 1$ and $p, q \leq k$ and $\gcd(m + 1, n + 1) = 1$.

BM6. $[a, a^p b a^q, b \prod_{i=1}^n (a^{k_i} b) (a^k b \prod_{i=1}^n (a^{k_i} b))^m]$, where $p, q, k, m, n, k_1, \dots, k_n \in \mathbb{N}$ and $m \geq 1$ and $1 \leq p, q \leq k < p + q \leq k_1, \dots, k_n$.

The labels BM1–BM6 are the same as were used in [19], which makes it easier for the reader to refer to [19]. The morphisms BM1, BM3 and BM6 share some similarities and can often be handled together. Similarly, BM2, BM4 and BM5 are often grouped together.

3 The Morphism ϕ

Let $\phi \in \text{GM}(\{a, b\}, \Sigma)$ be defined by

$$\phi(a) = aba, \quad \phi(b) = a^{-1}.$$

This particular morphism happens to be very useful for us. Specifically, it allows us to combine several lemmas that were proved in [19] into a single theorem (Theorem 12) that looks simpler and, crucially, is much easier to use in the later parts of the article.

First, we need some definitions and lemmas related to the behaviour of ϕ . These are important when formulating, proving and using Theorem 12. In particular, for a word w , we want to characterize the integers j such that $\phi^j(w)$ is a word. This characterization is provided in Lemma 11.

► **Lemma 8.** *The morphism ϕ has the following properties:*

■ ϕ has an inverse morphism defined by

$$\phi^{-1}(a) = b^{-1}, \quad \phi^{-1}(b) = bab.$$

■ For all $i, j \in \mathbb{Z}$,

$$\phi^j((ab)^i) = (ab)^i, \quad \phi^j((ba)^i) = (ba)^i.$$

■ For all $i, j \in \mathbb{Z}$,

$$\phi^j((ab)^i a) = (ab)^{i+j} a, \quad \phi^j(b(ab)^i) = b(ab)^{i-j}.$$

In particular,

$$\phi^j(a) = (ab)^j a, \quad \phi^j(b) = b(ab)^{-j}.$$

Proof. Straightforward computation. ◀

We need to study the question of when $\phi^j(w)$ is a word, or when $\phi^j \circ h$ is an M-morphism. For that purpose, we give some additional definitions.

A word $w \in \{a, b\}^+$ is called an *alternating block*, or just *block* for short, if neither aa nor bb is a factor of w . In other words, w is an alternating block if and only if it is a nonempty factor of some word in $(ab)^*$.

An *alternating block decomposition* (ABD) of $w \in \{a, b\}^*$ is a sequence (u_1, \dots, u_n) of alternating blocks such that $w = u_1 \cdots u_n$ and for all $i \in \{1, \dots, n-1\}$, the last letter of u_i is the same as the first letter of u_{i+1} .

► **Lemma 9.** *Every word $w \in \{a, b\}^*$ has a unique ABD.*

Proof. We split w in the middle of every occurrence of the factors aa and bb . This gives an ABD, and no other way of splitting w into factors can give an ABD. ◀

For a word $w \in \{a, b\}^*$ with an ABD (u_1, \dots, u_n) , we define its *a-degree*

$$\deg_a(w) = \inf\{k \in \mathbb{Z}_+ \mid \exists i : u_i = (ab)^{k-1}a\}.$$

and *b-degree*

$$\deg_b(w) = \inf\{k \in \mathbb{Z}_+ \mid \exists i : u_i = b(ab)^{k-1}\}.$$

For $c \in \{a, b\}$ and for $h \in \text{MM}(\{x, y, z\}, \Sigma)$ such that $h(x), h(y), h(z) \in \{a, b\}^*$, we define

$$\deg_c(h) = \inf\{\deg_c(h(x)), \deg_c(h(y)), \deg_c(h(z))\}.$$

► **Example 10.** The word $w = ababaabaabbaba$ has the ABD $(ababa, aba, ab, baba)$. We have $\deg_a(w) = 2$ and $\deg_b(w) = \infty$.

► **Lemma 11.** *For all $w \in \{a, b\}^*$ and $j \in \mathbb{Z}$, the following equivalence holds:*

$$\phi^j(w) \in \{a, b\}^* \iff -\deg_a(w) < j < \deg_b(w).$$

Proof. Let the ABD of w be (u_1, \dots, u_n) . By Lemma 8, every block u_i that is not of the form $b(ab)^k$ with $k < j$ or of the form $(ab)^k a$ with $k < -j$ is mapped to a word that begins and ends with the same letter as u_i . In particular, if $-\deg_a(w) < j < \deg_b(w)$, then $\phi^j(u_i) \in \{a, b\}^*$ for all i and therefore $\phi^j(w) \in \{a, b\}^*$.

If $j \geq \deg_b(w)$, then there is at least one i such that $u_i = b(ab)^k$ with $k < j$. For all such i , $\phi^j(u_i) = b(ab)^{k-j} = (a^{-1}b^{-1})^{j-k-1}a^{-1}$. If $i \geq 2$, then u_{i-1} ends with b and thus $\phi^j(u_{i-1})$ ends with either b or a^{-1} . Similarly, if $i \leq n-1$, then $\phi^j(u_{i+1})$ begins with either b or a^{-1} . This means that when we calculate $\phi^j(w)$ as the product of the images of the blocks, no cancellation can happen. Therefore, the reduced form of $\phi^j(w)$ still has a^{-1} in it, and $\phi^j(w)$ is not in $\{a, b\}^*$.

The case $j \leq -\deg_a(w)$ is analogous to the case $j \geq \deg_b(w)$. ◀

The next theorem shows why we are interested in the morphism ϕ : It allows us to give a greatly simplified formulation of certain old results. This is then useful when applying the theorem.

► **Theorem 12.** *Let h be a morphism of one of the types BM1–BM6. Let P be the set of periodic solutions of $\text{Eq}(h)$. Then*

$$\text{Sol}(\text{Eq}(h)) = \text{MM}(\{a, b\}, \Sigma) \circ \{\phi^j \circ h \mid 0 \leq j < \deg_b(h)\} \cup P. \tag{1}$$

Proof. Let $0 \leq j < \deg_b(h)$ and $f \in \text{MM}(\{a, b\}, \Sigma)$. First, we check that $f \circ \phi^j \circ h$ is an M-morphism (instead of being just a G-morphism): $0 \leq j < \deg_b(h)$ implies $-\deg_a(h(t)) < j < \deg_b(h(t))$ for all $t \in \{x, y, z\}$, so we can use Lemma 11 to see that $\phi^j(h(t)) \in \{a, b\}^*$ for all $t \in \{x, y, z\}$, and it follows that $f \circ \phi^j \circ h \in \text{MM}(\{x, y, z\}, \Sigma)$. If $(u, v) \in \text{Eq}(h)$, then $h(u) = h(v)$ and thus $(f \circ \phi^j \circ h)(u) = (f \circ \phi^j \circ h)(v)$. This shows that $f \circ \phi^j \circ h \in \text{Sol}(\text{Eq}(h))$ and that the right-hand side of (1) is a subset of the left-hand side.

The fact that every nonperiodic morphism in $\text{Sol}(\text{Eq}(h))$ is in

$$\text{MM}(\{a, b\}, \Sigma) \circ \{\phi^j \circ h \mid 0 \leq j < \deg_b(h)\}$$

follows from the results in [19]: Theorem 5.2 gives an equivalent equation for each $\text{Eq}(h)$, and Lemmas 6.1–6.6 then solve these equations. In each case, it can be easily checked that the formulas that give the nonperiodic solutions match $f \circ \phi^j \circ h$. This shows that the left-hand side of (1) is a subset of the right-hand side. ◀

It is an interesting question whether Theorem 12 could be proved in another way without having to use the rather large and cumbersome case analysis in [19].

4 Modified Versions of Previous Results

In [19], some ideas for proving a stronger version of Hmelevskii's theorem were discussed, and a couple of theorems were proved that could possibly point towards such a result. We were not able to use those theorems directly as they were stated. Instead, we prove here slightly modified versions of them. The changes to both the theorems and their proofs are mostly very small.

We also need a slightly modified version of Lemma 24 in [15]. We give this in the next lemma without proof, because the original proof in [15] works also for this modified statement.

► **Lemma 13.** *Let G be the set of morphisms in the classes $BM2, BM4, BM5$. Let E be a nontrivial constant-free equation on $\{x, y, z\}$. If $\text{Sol}(E) \cap G$ has more than one element, then there exist $m, p, q, r, s \in \mathbb{N}$ such that*

$$\text{Sol}(E) \cap G \subseteq \{[a, a^p b (a^m b)^i a^q, a^r b (a^m b)^j a^s] \mid i, j \in \mathbb{N}\} \subseteq \text{Sol}(E).$$

The next lemma is a modified version of Theorem 8.1 in [19].

► **Lemma 14.** *Let $G \subseteq \text{MM}(\{x, y, z\}, \Sigma)$ contain a representative of every equivalence class of nonperiodic morphisms that satisfy a nontrivial equation. Let E be a nontrivial constant-free equation on $\{x, y, z\}$. Let H be such that*

$$\text{Sol}(E) \cap G \subseteq H \subseteq \text{Sol}(E).$$

Let P be the set of periodic solutions of E . Then

$$\text{Sol}(E) = \bigcup_{h \in H} \text{Sol}(\text{Eq}(h)) \cup P.$$

Proof. Every nonperiodic $g \in \text{Sol}(E)$ is equivalent to some $h \in H$, and then $g \in \text{Sol}(\text{Eq}(g)) = \text{Sol}(\text{Eq}(h))$.

On the other hand, if $f \in \text{Sol}(\text{Eq}(h))$ for some $h \in H \subseteq \text{Sol}(E)$, then $E \in \text{Eq}(h)$ and thus $f \in \text{Sol}(\text{Eq}(h)) \subseteq \text{Sol}(E)$. ◀

The next lemma is a modified version of Theorem 8.2 in [19].

► **Lemma 15.** *Let E be a nontrivial constant-free equation on $\{x, y, z\}$. Let G be the set of morphisms that are, up to a permutation of the variables, of one of the types BM1–BM6. Then there exist sets H_1, \dots, H_9 such that*

$$\text{Sol}(E) \cap G \subseteq \bigcup_{k=1}^9 H_k \subseteq \text{Sol}(E) \tag{2}$$

and every H_k is either a finite set or, up to a permutation of the variables, of one of the following forms:

$$\{[a, a^p b a^q, (uv)^i u] \mid i \in \mathbb{N}\} \quad \text{for some } p, q \in \mathbb{N} \text{ and } u, v \in \Sigma^*, \tag{3}$$

$$\{[a, a^p b (a^m b)^i a^q, a^r b (a^m b)^j a^s] \mid i, j \in \mathbb{N}\} \quad \text{for some } m, p, q, r, s \in \mathbb{N}. \tag{4}$$

Proof. Let G_1 be the set of morphisms of the types BM1, BM3, BM6. Let G_2, \dots, G_6 be similar sets for the different permutations of the variables. Let G_7 be the set of morphisms of the types BM2, BM4, BM5. Let G_8, G_9 be similar sets for the different permutations of the variables (we need only three permutations instead of six because of symmetry). Then $G = \bigcup_{k=1}^9 G_k$. If we can find suitable sets H_k such that

$$\text{Sol}(E) \cap G_k \subseteq H_k \subseteq \text{Sol}(E), \tag{5}$$

then (2) follows.

Morphisms in G_1 can be written as $[a, a^p b a^q, w]$ for some $w \in \{a, b\}^*$. It was proved in [15] that E can have such a solution for at most one pair (p, q) . If we fix p and q and replace x by a and y by $a^p b a^q$ in E , we get a nontrivial one-variable equation with constants, and solving this one-variable equation gives us the possible values for w . It is known that if such an equation has infinitely many solutions, then there are u, v such that for each k , the morphism that maps the remaining variable z to $(uv)^i u$ is a solution, and there are no other solutions, see [14]. Thus we get a set H_1 that is either finite or of the form (3) and satisfies (5). Similarly, we can find sets H_2, \dots, H_6 .

For morphisms in G_7 , we can use Lemma 13 to find a set H_7 that is either finite or of the form (4) and satisfies (5). Similarly, we can find sets H_8 and H_9 . ◀

5 Parametric Representations for Certain Sets

Our intention is to use the set $\bigcup_{k=1}^9 H_k$ from Lemma 15 as the set H in Lemma 14. This leads us to study the sets $\bigcup_{h \in H_k} \text{Sol}(\text{Eq}(h))$ with the help of Theorem 12. The purpose of Lemma 16 is to handle the case where H_k is a finite set. Similarly, Lemma 17 is used for the case where H_k is of the form (3), and Lemma 19 is used for the case where H_k is of the form (4). After proving these three lemmas, we put all the pieces together in Theorem 20 in the next section.

► **Lemma 16.** *Let $h \in \text{MM}(\{x, y, z\}, \Sigma)$. The set*

$$\text{MM}(\{a, b\}, \Sigma) \circ \{\phi^j \circ h \mid 0 \leq j < \deg_b(h)\}$$

has a parametric representation in $\mathcal{R}_1(2, 1)$.

Proof. For a fixed j , the set

$$\text{MM}(\{a, b\}, \Sigma) \circ \{\phi^j \circ h\}$$

clearly has a parametric representation in $\mathcal{R}_0(2, 0)$, and the same is then true for a finite union of such sets. This takes care of the case where $\deg_b(h)$ is finite. If $\deg_b(h)$ is infinite and $h = [u, v, w]$, then the ABDs of u, v, w do not contain blocks of the form $b(ab)^i$, and therefore ϕ^j maps every block either to itself, or, in the case of blocks of the form $(ab)^i a$, to $(ab)^{i+j} a$. This means that $\phi^j(u)$ can be written in the form

$$u_0(ab)^j u_1(ab)^j \cdots u_{n-1}(ab)^j u_n, \quad (6)$$

where $u_0, \dots, u_n \in \{a, b\}^*$ do not depend on j , and $\phi^j(v)$ and $\phi^j(w)$ can be written in a similar form. Thus we get a parametric representation in $\mathcal{R}_1(2, 1)$. \blacktriangleleft

The following idea that was used in the proof of Lemma 16 is useful also later: If $\deg_b(u) = \infty$, that is, the ABD of u does not contain blocks of the form $b(ab)^i$, then $\phi^j(u)$ can be written in the form (6), and it essentially corresponds to a parametric word in $\mathcal{P}_1(2, 1)$. We use this kind of reasoning in the following lemmas without explaining it in detail like above.

► **Lemma 17.** *Let $u, v \in \{a, b\}^*$, $p, q \in \mathbb{N}$ and $h_i = [a, a^p b a^q, (uv)^i u]$. The set*

$$\text{MM}(\{a, b\}, \Sigma) \circ \{\phi^j \circ h_i \mid i \in \mathbb{N}, 0 \leq j < \deg_b(h_i)\} \quad (7)$$

has a parametric representation in $\mathcal{R}_2(2, 2)$.

Proof. If $p = q = 0$, then $\deg_b(h_i) = 1$ for all i and the set (7) is

$$\text{MM}(\{a, b\}, \Sigma) \circ \{[a, b, (uv)^i u] \mid i \in \mathbb{N}\},$$

which has a parametric representation in $\mathcal{R}_1(2, 1)$. For the rest of the proof, assume that $p \geq 1$ or $q \geq 1$. Then $\deg_b(h_i) = \deg_b((uv)^i u)$ for all i .

Let us first assume that some conjugate of uv begins and ends with the same letter c . Let this conjugate be ts , where $uv = st$. We can write (7) as

$$\begin{aligned} & \text{MM}(\{a, b\}, \Sigma) \circ \{\phi^j \circ h_0 \mid 0 \leq j < \deg_b(h_0)\} \\ & \cup \text{MM}(\{a, b\}, \Sigma) \circ \{\phi^j \circ h_1 \mid 0 \leq j < \deg_b(h_1)\} \\ & \cup \text{MM}(\{a, b\}, \Sigma) \circ \{\phi^j \circ h_i \mid i \geq 2, 0 \leq j < \deg_b(h_i)\}. \end{aligned}$$

Here, we can use Lemma 16 for the first two sets, so it is enough to consider the third set. For $i \geq 2$, $(uv)^i u = s(ts)^{i-1} tu$. Here ts begins and ends with c , s is either empty or ends with c , and tu is either empty or begins with c . Therefore, the ABD of $s(ts)^{i-1} tu$ consists of the ABD of s followed by $i-1$ copies of the ABD of ts followed by the ABD of tu . For all $i \geq 2$, $\deg_b(h_i) = \inf(\deg_b(s), \deg_b(ts), \deg_b(tu))$, which does not depend on i . If $\deg_b(h_i)$ is finite, then we have a finite union of sets of the form

$$\text{MM}(\{a, b\}, \Sigma) \circ \{[\phi^j(a), \phi^j(a^p b a^q), \phi^j(s)(\phi^j(ts))^{i-1} \phi^j(tu)] \mid i \geq 2\}.$$

In each set, j is a constant. We can write $i' = i - 2$ and $(\phi^j(ts))^{i-1} = (\phi^j(ts))^{i'} \phi^j(ts)$. Then i' runs through all natural numbers and we can think of it as a numerical parameter. Thus we get a parametric representation in $\mathcal{R}_1(2, 1)$. If $\deg_b(h_i)$ is infinite, then we have

$$\text{MM}(\{a, b\}, \Sigma) \circ \{[\phi^j(a), \phi^j(a^p b a^q), \phi^j(s)(\phi^j(ts))^{i-1} \phi^j(tu)] \mid i \geq 2, j \geq 0\},$$

where $\phi^j(a) = (ab)^j a$ and $\phi^j(a^p b a^q) = ((ab)^j a)^{p-1} ab((ab)^j a)^q$ if $p \geq 1$ and $\phi^j(a^p b a^q) = ((ab)^j a)^p b a((ab)^j a)^{q-1}$ if $q \geq 1$. Thus we can think of j and $i-2$ as numerical parameters, and we get a parametric representation in $\mathcal{R}_2(2, 2)$.

Let us then consider the case where no conjugate of uv begins and ends with the same letter. This means that $uv \in (ab)^* \cup (ba)^*$. There are four subcases:

77:10 An Improved Version of Hmelevskii's Theorem on Three-Variable Word Equations

- $u, v \in (ab)^*$,
- $u, v \in (ba)^*$,
- $u \in (ab)^*a, v \in b(ab)^*$,
- $u \in b(ab)^*, v \in (ab)^*a$.

The first three are simple: In all these subcases, $\deg_b(h_i) = \deg_b(uv) = \deg_b(u) = \infty$, and (7) can be written simply as

$$\text{MM}(\{a, b\}, \Sigma) \circ \{[\phi^j(a), \phi^j(a^pba^q), (\phi^j(uv))^i \phi^j(u)] \mid i, j \in \mathbb{N}\},$$

which has a parametric representation in $\mathcal{R}_2(2, 2)$.

The fourth subcase is the most complicated one. Example 18 illustrates this case for some particular values of u and v . It might be easier to get the basic idea from that example than from the general proof below.

Let $u = (ba)^r b$ and $v = (ab)^s a$. Then $(uv)^i u = (ba)^{(r+s+1)i+r} b$. Let $t = r + s + 1$. Let k, l be such that $j = tk + l$ and $0 \leq l < t$. Let m, n be such that $r - l = tm + n$ and $0 \leq n < t$. Then $(uv)^i u = (ba)^{ti+r} b$ and

$$\phi^j((uv)^i u) = (ba)^{ti+r-j} b = (ba)^{ti+r-tk-l} b = (ba)^{t(i-k)+tm+n} b = (ba)^{t(i-k+m)+n} b.$$

We have $\deg_b(h_i) = \deg_b((uv)^i u) = ti + r + 1$ and therefore we can rewrite the condition $j < \deg_b(h_i)$ using the following sequence of equivalences:

$$\begin{aligned} j < \deg_b(h_i) &\iff j < ti + r + 1 \iff tk + l < ti + r + 1 \\ &\iff t(i - k) + tm + n + 1 > 0 \iff t(i - k + m) + n + 1 > 0 \\ &\iff i - k + m \geq 0 \end{aligned}$$

At this point, r, s, t are fixed, while k, l, m, n depend on j . However, since there are only finitely many possible values for l , we can consider these separately. If we fix l , then m and n are also fixed. The part of (7) corresponding to a particular value of l is

$$\begin{aligned} &\text{MM}(\{a, b\}, \Sigma) \circ \{[\phi^{tk+l}(a), \phi^{tk+l}(a^pba^q), (ba)^{t(i-k+m)+n} b] \mid i, k \geq 0, i - k + m \geq 0\} \\ &= \text{MM}(\{a, b\}, \Sigma) \circ \{[\phi^{tk+l}(a), \phi^{tk+l}(a^pba^q), (ba)^{t(i-k+m)+n} b] \mid i \geq 0, 0 \leq k < m\} \\ &\cup \text{MM}(\{a, b\}, \Sigma) \circ \{[\phi^{tk+l}(a), \phi^{tk+l}(a^pba^q), (ba)^{t(i-k+m)+n} b] \mid i \geq k - m, k \geq m\}. \end{aligned}$$

Here, the first set of the union is a finite union of sets, one for each value of k . We can think of i as the only numerical parameter and write $(ba)^{t(i-k+m)+n} b = ((ba)^t)^i (ba)^{t(m-k)+n} b$, and we get a parametric representation in $\mathcal{R}_1(2, 1)$. In the second set of the union, on the other hand, we can write $k' = k - m$ and $i' = i - k + m$, and then k' and i' run through all natural numbers independently of each other, so we can think of them as numerical parameters. Thus we get a parametric representation in $\mathcal{R}_1(2, 2)$. Combining all these parametric representations for all values of l gives a parametric representation for (7). ◀

► **Example 18.** Consider Lemma 17 with $p = 1$, $q = 0$, $u = b$, $v = aba$. We have

$$\begin{aligned}
& \{\phi^j \circ h_i \mid i \in \mathbb{N}, 0 \leq j < \deg_b(h_i)\} \\
&= \{\phi^j \circ [a, ab, (baba)^i b] \mid i \in \mathbb{N}, 0 \leq j \leq 2i\} \\
&= \{[(ab)^j a, ab, (ba)^{2i-j} b] \mid i \in \mathbb{N}, 0 \leq j \leq 2i\} \\
&= \{[(ab)^{2k} a, ab, (ba)^{2i-2k} b] \mid i \in \mathbb{N}, 0 \leq 2k \leq 2i\} \\
&\quad \cup \{[(ab)^{2k+1} a, ab, (ba)^{2i-2k-1} b] \mid i \in \mathbb{N}, 0 \leq 2k+1 \leq 2i\} \\
&= \{[(abab)^k a, ab, (baba)^{i-k} b] \mid i, k \in \mathbb{N}, i-k \geq 0\} \\
&\quad \cup \{[(abab)^k aba, ab, (baba)^{i-k-1} bab] \mid i, k \in \mathbb{N}, i-k-1 \geq 0\} \\
&= \{[(abab)^k a, ab, (baba)^{i'} b] \mid i', k \in \mathbb{N}\} \\
&\quad \cup \{[(abab)^k aba, ab, (baba)^{i'} bab] \mid i', k \in \mathbb{N}\}.
\end{aligned}$$

Here we have split the set in two parts corresponding to even $j = 2k$ and odd $j = 2k + 1$. Then, in the end, we have replaced $i - k$ with i' in the first part, noticing that for all $i', k \in \mathbb{N}$, there exists $i \in \mathbb{N}$ such that $i' = i - k$. Similarly, we have replaced $i - k - 1$ by i' in the second part. We can think of i' and k as numerical parameters, and we get a parametric representation in $\mathcal{R}_1(2, 2)$.

► **Lemma 19.** Let $m, p, q, r, s \in \mathbb{N}$ and $h_{i,j} = [a, a^p b (a^m b)^i a^q, a^r b (a^m b)^j a^s]$. The set

$$\text{MM}(\{a, b\}, \Sigma) \circ \{\phi^k \circ h_{i,j} \mid i, j \in \mathbb{N}, 0 \leq k < \deg_b(h_{i,j})\} \quad (8)$$

has a parametric representation in $\mathcal{R}_2(2, 3)$.

Proof. First, let $m = 0$. If $\max(i, j) \geq 2$, then $\deg_b(h_{i,j}) = 1$, so we can write (8) as

$$\begin{aligned}
& \bigcup_{i,j \in \{0,1\}} \text{MM}(\{a, b\}, \Sigma) \circ \{\phi^k \circ h_{i,j} \mid 0 \leq k < \deg_b(h_{i,j})\} \\
& \cup \text{MM}(\{a, b\}, \Sigma) \circ \{h_{i,j} \mid i, j \in \mathbb{N}\}
\end{aligned}$$

The four sets corresponding to $i, j \in \{0, 1\}$ have parametric representations in $\mathcal{R}_1(2, 1)$ by Lemma 16, and the last set has a parametric representation in $\mathcal{R}_1(2, 2)$.

Then, let $m = 1$. For each of p, q, r, s , there are two cases depending on whether it is zero or positive. While this technically leads to a total of 16 cases, these are all quite similar, so we give here only the case $p = q = r = s = 0$: We can write

$$\phi^k \circ h_{i,j} = [(ab)^k a, b(ab)^{i-k}, b(ab)^{j-k}],$$

where k , $i - k$ and $j - k$ run through all natural numbers independently of each other, so we can think of them as three numerical parameters, and we get a parametric representation in $\mathcal{R}_1(2, 3)$.

Finally, let $m \geq 2$. We can write (8) as

$$\begin{aligned}
& \text{MM}(\{a, b\}, \Sigma) \circ \{\phi^k \circ h_{0,0} \mid 0 \leq k < \deg_b(h_{0,0})\} \\
& \cup \text{MM}(\{a, b\}, \Sigma) \circ \{\phi^k \circ h_{0,j} \mid j \geq 1, 0 \leq k < \deg_b(h_{0,j})\} \\
& \cup \text{MM}(\{a, b\}, \Sigma) \circ \{\phi^k \circ h_{i,0} \mid i \geq 1, 0 \leq k < \deg_b(h_{i,0})\} \\
& \cup \text{MM}(\{a, b\}, \Sigma) \circ \{\phi^k \circ h_{i,j} \mid i, j \geq 1, 0 \leq k < \deg_b(h_{i,j})\}.
\end{aligned}$$

We explain here how to get a parametric representation for the last of these four sets; the first three can be handled in a similar way. For $i, j \geq 1$, we can write

$$\begin{aligned}\phi^k \circ h_{i,j} &= \phi^k \circ [a, a^p b a^m b (a^m b)^{i-1} a^q, a^r b a^m b (a^m b)^{j-1} a^s] \\ &= [\phi^k(a), \phi^k(a^p b a^m b) (\phi^k(a^m b))^{i-1} \phi^k(a^q), \phi^k(a^r b a^m b) (\phi^k(a^m b))^{j-1} \phi^k(a^s)].\end{aligned}$$

Every word that is being mapped by ϕ^k here has infinite b -degree. We can think of $i - 1$, $j - 1$ and k as numerical parameters, and we get a parametric representation in $\mathcal{R}_2(2, 3)$. ◀

6 Main Result

We are now ready to prove our main result.

► **Theorem 20.** *Every nontrivial constant-free word equation E on $\{x, y, z\}$ has a parametric solution in $\mathcal{R}_2(2, 3)$.*

Proof. Let P be the set of periodic solutions of E . Let G and H_1, \dots, H_9 be as in Lemma 15. We can then use Lemma 14 with $H = \bigcup_{k=1}^9 H_k$. This, together with Theorem 12, gives

$$\begin{aligned}\text{Sol}(E) &= \bigcup_{h \in H} \text{Sol}(\text{Eq}(h)) \cup P \\ &= \bigcup_{k=1}^9 \bigcup_{h \in H_k} \text{Sol}(\text{Eq}(h)) \cup P \\ &= \bigcup_{k=1}^9 \bigcup_{h \in H_k} \text{MM}(\{a, b\}, \Sigma) \circ \{\phi^i \circ h \mid 0 \leq i < \deg_b(h)\} \cup P \\ &= \bigcup_{k=1}^9 \text{MM}(\{a, b\}, \Sigma) \circ \{\phi^i \circ h \mid h \in H_k, 0 \leq i < \deg_b(h)\} \cup P.\end{aligned}$$

Note that the sets P in Theorem 12 are subsets of the set P in this proof, so they can be ignored here.

The set P has a parametric representation in $\mathcal{R}_1(1, 3)$ by Lemma 6. To complete the proof of the theorem, it suffices to show that each of the sets

$$\text{MM}(\{a, b\}, \Sigma) \circ \{\phi^i \circ h \mid h \in H_k, 0 \leq i < \deg_b(h)\}$$

has a parametric representation in $\mathcal{R}_2(2, 3)$. If H_k is a finite set, this follows from Lemma 16, if H_k is of the form (3), this follows from Lemma 17, and if H_k is of the form (4), this follows from Lemma 19. ◀

7 Conclusion

In this article, we have proved that every nontrivial constant-free word equation on three variables has a parametric solution with at most three numerical parameters and with nesting level at most two. This is a much more exact version of the old result of Hmelevskii. Several interesting questions remain:

- Is the result optimal, that is, does there exist a constant-free word equation on three variables that does not have a parametric solution with less than three numerical parameters or with nesting level less than two?

- A parametric solution was defined as a set of triples. How large does this set need to be, that is, how many triples do we need, at most? Can we give a fixed finite bound, or does this depend on the length of the equation?
- What is the complexity of finding a parametric solution for a given constant-free equation on three variables?

References

- 1 L. G. Budkina and Al. A. Markov. F -semigroups with three generators. *Akademiya Nauk SSSR. Matematicheskie Zametki*, 14:267–277, 1973.
- 2 Laura Ciobanu, Volker Diekert, and Murray Elder. Solution sets for equations over free groups are EDT0L languages. *International Journal of Algebra and Computation*, 26(5):843–886, 2016. doi:10.1142/S0218196716500363.
- 3 Joel D. Day. Word equations in the context of string solving. In *Proceeding of the 26th DLT*, volume 13257 of *LNCS*, pages 13–32. Springer, 2022. doi:10.1007/978-3-031-05578-2_2.
- 4 Joel D. Day, Vijay Ganesh, Paul He, Florin Manea, and Dirk Nowotka. The satisfiability of word equations: decidable and undecidable theories. In *Reachability problems*, volume 11123 of *LNCS*, pages 15–29. Springer, 2018. doi:10.1007/978-3-030-00250-3_2.
- 5 Joel D. Day, Florin Manea, and Dirk Nowotka. The hardness of solving simple word equations. In *Proceedings of the 42nd MFCS*, volume 83 of *LIPICs*, pages 18:1–14. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2017. doi:10.4230/LIPICs.MFCS.2017.18.
- 6 Robert Dąbrowski and Wojtek Plandowski. Solving two-variable word equations (extended abstract). In *Proceedings of the 31st ICALP*, volume 3142 of *LNCS*, pages 408–419. Springer, 2004. doi:10.1007/978-3-540-27836-8_36.
- 7 Dominik D. Freydenberger and Mario Holldack. Document spanners: from expressive power to decision problems. *Theory of Computing Systems*, 62:854–898, 2017. doi:10.1007/s00224-017-9770-0.
- 8 Tero Harju and Juhani Karhumäki. Many aspects of defect theorems. *Theoretical Computer Science*, 324(1):35–54, 2004. doi:10.1016/j.tcs.2004.03.051.
- 9 Tero Harju and Dirk Nowotka. On the independence of equations in three variables. *Theoretical Computer Science*, 307(1):139–172, 2003. doi:10.1016/S0304-3975(03)00098-7.
- 10 Ju. I. Hmelevskii. *Equations in free semigroups*. American Mathematical Society, 1976. Translated by G. A. Kandall from the Russian original: Trudy Mat. Inst. Steklov. 107 (1971).
- 11 Artur Jež. One-variable word equations in linear time. *Algorithmica*, 74(1):1–48, 2016. doi:10.1007/s00453-014-9931-3.
- 12 Artur Jež. Word equations in non-deterministic linear space. *Journal of Computer and System Sciences*, 123:122–142, 2022. doi:10.1016/j.jcss.2021.08.001.
- 13 Juhani Karhumäki and Alekski Saarela. An analysis and a reproof of Hmelevskii’s theorem. In *Proceedings of the 12th DLT*, volume 5257 of *LNCS*, pages 467–478. Springer, 2008. doi:10.1007/978-3-540-85780-8_37.
- 14 Markku Laine and Wojciech Plandowski. Word equations with one unknown. *International Journal of Foundations of Computer Science*, 22(2):345–375, 2011. doi:10.1142/S0129054111008088.
- 15 Dirk Nowotka and Alekski Saarela. One-variable word equations and three-variable constant-free word equations. *International Journal of Foundations of Computer Science*, 29(5):935–950, 2018. doi:10.1142/S0129054118420121.
- 16 Dirk Nowotka and Alekski Saarela. An optimal bound on the solution sets of one-variable word equations and its consequences. *SIAM Journal on Computing*, 51(1):1–18, 2022. doi:10.1137/20M1310448.
- 17 Alekski Saarela. On the complexity of Hmelevskii’s theorem and satisfiability of three unknown equations. In *Proceedings of the 13th DLT*, volume 5583 of *LNCS*, pages 443–453. Springer, 2009. doi:10.1007/978-3-642-02737-6_36.

- 18 Aleksi Saarela. *Word equations and related topics: independence, decidability and characterizations*. PhD thesis, University of Turku, 2012. URL: <http://urn.fi/URN:ISBN:978-952-12-2737-0>.
- 19 Aleksi Saarela. On the solution sets of three-variable word equations. *Theory of Computing Systems*, 68:1556–1571, 2024. doi:10.1007/s00224-024-10193-9.
- 20 Jean-Claude Spohner. *Quelques problèmes d'extension, de conjugaison et de présentation des sous-monoïdes d'un monoïde libre*. PhD thesis, Univ. Paris, 1976.
- 21 Jean-Claude Spohner. Les systemes entiers d'équations sur un alphabet de 3 variables. In *Semigroups Theory and Applications*, volume 1320 of *LNM*, pages 342–357. Springer, 1988. doi:10.1007/BFb0083443.