On the Solution Sets of Three-Variable Word Equations

Aleksi Saarela*

Department of Mathematics and Statistics, University of Turku, Turku, Finland.

Corresponding author(s). E-mail(s): amsaar@utu.fi;

Abstract

It is known that the set of solutions of any constant-free three-variable word equation can be represented using parametric words, and the number of numerical parameters and the level of nesting in these parametric words is at most logarithmic with respect to the length of the equation. We show that this result can be significantly improved in the case of unbalanced equations, that is, equations where at least one variable has a different number of occurrences on the left-hand side and on the right-hand side. More specifically, it is sufficient to have two numerical parameters and one level of nesting in this case. We also discuss the possibility of proving a similar result for balanced equations in the future.

Keywords: combinatorics on words, word equation, entire system, unbalanced equation, parametric solution

1 Introduction

Word equations have been studied both from an algorithmic and algebraic point of view. Some well-known results are that the complexity of the satisfiability problem of word equations can be solved in nondeterministic linear space [1], and that every system of word equations is equivalent to a finite subsystem [2, 3].

In this article, we concentrate on constant-free equations, and all equations are assumed to be constant-free from now on. For some relations between constant-free equations and equations with constants, see [4].

*Supported by the Academy of Finland under grant 339311

Equations with one or two variables have only periodic solutions, and are therefore not interesting. The three-variable case, on the other hand, is highly nontrivial, while simultaneously being much simpler than the four-variable case. Some examples of difficult results about three-variable equations are Hmelevskii's theorem that every three-variable equation has a parametric solution [5] (this does not hold for equations with four or more variables), and a bound of 18 for the size of independent systems [6] (no finite bound is known for equations with four or more variables).

Hmelevskii's theorem, in particular, is relevant for this article. The original proof, and even the simpler modern version of that proof in [7, 8], is very long. Also, while the basic concept of parametric solutions is simple, the actual parametric formulas that arise from the proof can be very complicated. They were analyzed in [8, 9], and it was proved, for example, that the number of numerical parameters needed in these formulas is at most logarithmic with respect to the length of the equation, and the total length of the formulas is at most exponential.

In this article, we find out that for certain families of three-variable equations and systems of equations, namely, for so-called unbalanced equations and entire systems, the set of solutions can be described using explicitly given formulas that are quite simple. In particular, only two numerical parameters are needed to represent all solutions, and only one numerical parameter is needed if we disregard periodic solutions. We also outline a strategy to possibly extend our result to all three-variable equations, although one or two numerical parameters will probably no longer be sufficient in that case. This can potentially lead to a much stronger and more explicit version of Hmelevskii's theorem in the future.

This article is an extended version of the conference paper [10]. The most important differences are the following: We have added Section 3 about parametric words. In the conference version, parametric words were mentioned but not defined formally. We have added Theorem 5.2 and Corollary 5.3. These are essentially direct consequences of results in [10], but the relevant parts were split and hidden inside many lemmas. We have added Theorem 7.2. The idea behind this theorem was briefly discussed in [10], but there was no formal statement or proof. Finally, we have added Theorem 8.2.

2 Preliminaries

First, we go through some basic definitions and lemmas abouts words. For more, see [11, 12].

Let $\mathbb{N}$ denote the set of nonnegative integers. Throughout the article, let Σ be an alphabet that contains at least two letters a and b. Let ε denote the empty word.

A word u is a *factor* (*prefix*, *suffix*) of a word w if there exist words x, y such that $w = xuy$ ($w = uy$, $w = xu$, respectively). If one of the words u, v is a prefix (suffix) of the other, we use the notation $u \sim_{\mathrm{p}} v$ ($u \sim_{\mathrm{s}} v$, respectively).

If $w \in \Sigma^*$ and $n \in \mathbb{N}$, then w^n is called a *power* of w, or more specifically, an *n-power* of w. If u is a prefix of w, then $w^n u$ is a called a *fractional power* of w. We also use negative powers as follows: If $w = uv$, then $u^{-1}w = v$ and $wv^{-1} = u$. If x is not a prefix (suffix) of w, then $x^{-1}w$ (wx^{-1}, respectively) is not defined, so whenever we use expressions like these, we have to make sure that they represent well-defined words.

Words u and v are *conjugates* if there exist words x, y such that $u = xy$ and $v = yx$. If a word is an n-power, then all of its conjugates are also n-powers.

Let Ξ be another alphabet. A mapping $h : \Xi^* \to \Sigma^*$ is a *morphism* if $h(uv) = h(u)h(v)$ for all $u, v \in \Xi^*$. The morphism h is *periodic* if there exists $w \in \Sigma^*$ such that $h(u) \in w^*$ for all $u \in \Xi^*$, and *nonperiodic* otherwise.

Next, we state some well-known results that are needed later. These can be considered folklore results, and Lemmas 2.1 and 2.3 can be found, for example, in [11, Corollary 1.2.6, Proposition 1.3.4].

Lemma 2.1. *Let $x, y \in \Sigma^*$. The following are equivalent:*

1. *x and y are powers of a common word.*
2. *$xy = yx$.*
3. *x and y satisfy a nontrivial relation, that is, there exist $x_1, \ldots, x_m, y_1, \ldots, y_n \in \{x, y\}$ such that $(x_1, \ldots, x_m) \neq (y_1, \ldots, y_n)$ but $x_1 \cdots x_m = y_1 \cdots y_n$.*

Lemma 2.2. *Let $x, y \in \Sigma^*$. If y is a fractional power of x and x is a suffix of y, then x and y are powers of a common word.*

Proof. Because y is a fractional power of x, we can write $x = pq$ and $y = (pq)^n p$ for some words p, q and integer $n \geq 0$. Because x is a suffix of y, $x = qp$. It follows that $pq = qp$ and, by Lemma 2.1, $p, q \in r^*$ for some word r. Then also $x, y \in r^*$. □

Lemma 2.3. *Let $x, y, z \in \Sigma^*$ and let $xy = yz$. Then $x = z = \varepsilon$ or*

$$x = uv, \qquad y = (uv)^j u, \qquad z = vu$$

for some $u, v \in \Sigma^*$ and $j \in \mathbb{N}$.

The next result is one of the equivalent formulations of the periodicity theorem of Fine and Wilf.

Theorem 2.4 (Fine and Wilf [13])**.** *Let $x, y \in \Sigma^*$. If a power of x and a power of y have a common prefix of length $|xy| - \gcd(|x|, |y|)$, then x and y are powers of a common word.*

Let us fix an alphabet of variables Ξ and an alphabet of constants Σ. A *word equation* is a pair $E = (L, R)$, where $L, R \in \Xi^*$, and a *solution* of E is a morphism $h : \Xi^* \to \Sigma^*$ such that $h(L) = h(R)$. The equation E is *nontrivial* if $L \neq R$.

A *system of equations* is a set of equations. A *solution* of a system is a morphism that satisfies all equations in the system. A system is *nontrivial* if it contains at least one nontrivial equation.

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

We are particularly interested in the three-variable case $\Xi = \{X, Y, Z\}$. Throughout the article, we let X, Y, Z be distinct variables, and we use the shorthand notation $[x, y, z]$, where $x, y, z \in \Sigma^*$, for the morphism $h : \{X, Y, Z\}^* \to \Sigma^*$ defined by $h(X) = x$, $h(Y) = y$, $h(Z) = z$.

Example 2.5. Consider the equation $E = (XY, YZ)$. We can easily check that the morphism $h = [uv, (uv)^j u, vu]$, where $u, v \in \Sigma^*$ and $j \in \mathbb{N}$, is a solution of E:

$$h(XY) = uv(uv)^j u = (uv)^j uvu = h(YZ).$$

It follows from Lemma 2.3 that all solutions of E are of this form or of the form $[\varepsilon, u, \varepsilon]$.

An equation (L, R) is *balanced* if every variable has as many occurrences in L as in R, and *unbalanced* otherwise. Results related to balanced equations can be found, for example, in [14, 15]. We need the following two theorems.

Theorem 2.6 (Harju and Nowotka [14])**.** *Let $g, h : \{X, Y, Z\}^* \to \Sigma^*$ be nonperiodic morphisms such that $\mathrm{Eq}(g) \neq \mathrm{Eq}(h)$. Then $\mathrm{Eq}(g) \cap \mathrm{Eq}(h)$ does not contain any unbalanced equations.*

Theorem 2.7 (Harju and Nowotka [14])**.** *If two unbalanced equations have a common nonperiodic solution, then they have the same set of periodic solutions.*

3 Parametric Words

Parametric words can be formalized in a couple of different ways. In this section, we define them as certain kinds of functions.

First, let us consider functions $(\Sigma^*)^p \times \mathbb{N}^q \to \Sigma^*$. Here $(\Sigma^*)^p$ means a cartesian product rather than a concatenation of languages, so these are functions with p word parameters and q numerical parameters. For $i \in \{1, \ldots, p\}$, let U_i be the function defined by

$$U_i(u_1, \ldots, u_p; j_1, \ldots, j_q) = u_i.$$

We can use $\mathcal{E}$ to mean the function that maps everything to the empty word. If α, β are functions, then their product (or concatenation), denoted by $\alpha\beta$, is the function

$$(\alpha\beta)(u_1, \ldots, u_p; j_1, \ldots, j_q) = \alpha(u_1, \ldots, u_p; j_1, \ldots, j_q)\beta(u_1, \ldots, u_p; j_1, \ldots, j_q).$$

For all $i \in \{1, \ldots, q\}$, we also define a formal power of α, denoted by α^{J_i}, as the function

$$\alpha^{J_i}(u_1, \ldots, u_p; j_1, \ldots, j_q) = \alpha(u_1, \ldots, u_p; j_1, \ldots, j_q)^{j_i}.$$

Parametric words can now be defined as the functions we get by starting with the functions $\mathcal{E}, U_1, \ldots, U_p$ and repeatedly applying the above-mentioned operations. Formally, let

$$\mathcal{P}_0(p, q) = \{U_{k_1} \cdots U_{k_n} \mid n \in \mathbb{N}, k_i \in \{1, \ldots, p\}\},$$

where the case $n = 0$ gives $\mathcal{E}$. For $d \geq 1$, let

$$\mathcal{P}_d(p, q) = \{\alpha_0 \beta_1^{J_{k_1}} \alpha_1 \cdots \beta_n^{J_{k_n}} \alpha_n \mid n \in \mathbb{N}, k_i \in \{1, \ldots, q\}, \alpha_i, \beta_i \in \mathcal{P}_{d-1}(p, q)\}.$$

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. Note that $\mathcal{P}_{d-1}(p,q) \subseteq \mathcal{P}_d(p,q)$. This means that $\mathcal{P}_d(p,q)$ is the set of parametric words with nesting level at most d.

We can naturally use shorthand notation such as $\alpha^{J_1}\alpha = \alpha^{J_1+1}$, $\alpha^{J_1}\alpha^{J_1} = \alpha^{2J_1}$, and $\alpha^{J_1}\alpha^{J_2} = \alpha^{J_1+J_2}$. We are mostly interested in the case $p = 2$, and then we use the notation $U = U_1$ and $V = U_2$. We can also let $J = J_1$ and $K = J_2$.

Example 3.1. The parametric word $\alpha = U(V^J U)^K U V^J \in \mathcal{P}_2(2,2)$ is the function defined by $\alpha(u, v; j, k) = u(v^j u)^k u v^j$.

Next we define parametric representations and solutions. To simplify notation, we concentrate on the three-variable case, which is the only one needed in this article. Generalizing the definitions for more variables would be straightforward.

A finite set

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

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

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

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

Example 3.2. By Lemma 2.5, the equation (XY, YZ) has a parametric solution

$$\{(UV, (UV)^J U, VU), (\mathcal{E}, U, \mathcal{E})\} \in \mathcal{R}_1(2,1).$$

Hmelevskii [5] proved that every three-variable equation has a parametric solution. These parametric solutions use two word parameters, except that trivial equations have the parametric solution $\{(U_1, U_2, U_3)\} \in \mathcal{R}_0(3,0)$. The number of numerical parameters and nesting level were not analyzed in [5], but a logarithmic upper bound follows from the proofs in [8, 9], leading to the next theorem.

Theorem 3.3. *For every nontrivial three-variable equation E, there exist q, d such that E has a parametric solution in $\mathcal{R}_d(2,q)$. Moreover, $q, d \in O(\log |E|)$.*

The process of solving a word equation is often divided into two parts: Finding all periodic solutions (which is straightforward), and finding all nonperiodic solutions (which is much more difficult). To make it easier to talk about these situations, we give the following definition: A parametric representation for a set $S \subseteq \mathrm{Sol}(E)$ such that every nonperiodic solution of E is in S is called a *parametric NonPer-solution* of E.

Lemma 3.4. *If a three-variable equation E has a parametric NonPer-solution in $\mathcal{R}_d(2,q)$, then it has a parametric solution in $\mathcal{R}_{\max(d,1)}(2, \max(q,3))$. Moreover, if E is unbalanced, then it has a parametric solution in $\mathcal{R}_{\max(d,1)}(2, \max(q,2))$.*

Proof. It is well-known that the set of periodic solutions has the parametric representation $\{(U^{J_1}, U^{J_2}, U^{J_3})\} \in \mathcal{R}_1(1,3)$ if the equation is balanced, and it has a parametric representation in $\mathcal{R}_1(1,2)$ if the equation is unbalanced (see, for instance, Example 5.1.2 and the proof of Theorem 5.1.3 in [8] for an explanation). This parametric representation together with the NonPer-solution gives a parametric solution of E. The claim follows. □

4 Lemmas

Before moving to the classification of entire systems and unbalanced equations in Section 5 and to the solution sets of these in Section 6, we prove some (mostly technical) lemmas that are needed in those sections.

Lemma 4.1. *Let $x, y \in \Sigma^*$ and $m, n, p, q \in \mathbb{N}$ and $m, n, p+q \geq 1$. Let $x^p \sim_{\mathrm{p}} y^m x$ and $x^q \sim_{\mathrm{s}} xy^n$. Then x and y are powers of a common word or*

$$x = (uv)^j u, \qquad y = x^{p-1}uvx^q = x^p vux^{q-1}$$

for some $u, v \in \Sigma^*$ and $j \in \mathbb{N}$.

Proof. Throughout the proof, we assume that $p \geq q$ and, consequently, $p \geq 1$. The case $p < q$ is symmetric and can be handled in the same way by reversing all the words.

First, let $|y| \geq |x^{p+q-1}|$. Then $y = x^{p-1}wx^q$ for some word w. From $x^p \sim_{\mathrm{p}} y^m x$ it follows that $x \sim_{\mathrm{p}} wx^q(x^{p-1}wx^q)^{m-1}x$. Clearly, $wx^q(x^{p-1}wx^q)^{m-1}x$ has a prefix $w^k x$ for some $k \geq 1$ (if $q+p-1 \geq 1$, then $k = 1$, otherwise $k = m$), and then x is a prefix of $w^k x$. Let $j \geq 0$ be the largest integer such that w^j is a prefix of x and let u be such that $x = w^j u$. Then u is a prefix of $w^k u$ and, by the maximality of j, u is shorter than w and thus a prefix of w, so we can write $w = uv$ for some word v, and then $x = (uv)^j u$.

Next, let $|y| < |x^{p+q-1}|$ and $q = 0$. Then $|x^p| \geq |xy|$ and $|y^m x| \geq |xy|$. From $x^p \sim_{\mathrm{p}} y^m x$ it follows that x is a fractional power of y, and then from the theorem of Fine and Wilf it follows that x and y are powers of a common word.

Next, let $|y| < |x^{p+q-1}|$ and $q \geq 1$ and $|x^p| < |y|$. Then y has a prefix x^p and a suffix x^q. Let $y = zx^q$. We have $|zx| < |x^p|$, so zx is a prefix of x^p and therefore a fractional power of x. By Lemma 2.2, x and zx are powers of a common word, and then also y is a power of that same word.

Next, let $|y| < |x^{p+q-1}|$ and $q \geq 1$ and $|x| < |y| \leq |x^p|$. Then y is a fractional power of x and ends in x. By Lemma 2.2, x and y are powers of a common word.

Finally, let $|y| < |x^{p+q-1}|$ and $q \geq 1$ and $|y| \leq |x|$. Let $k \geq 0$ be the largest integer such that y^k is a prefix of x and let z be such that $x = y^k z$. From x being a prefix of $y^m x$ it follows that z is a prefix of $y^m z$, and by the maximality of k, z is shorter than y and thus a prefix of y. This means that x is a fractional power of y. Also, x ends in y. By Lemma 2.2, x and y are powers of a common word. □

Lemma 4.2. *Let $x, y \in \Sigma^*$ and $m, n, \in \mathbb{N}$ and $\gcd(m, n) = 1$. Let $x^m y = yz^n$. Then x, y, z are powers of a common word or*

$$x = (st)^n, \qquad y = (st)^i s, \qquad z = (ts)^m$$

for some $s, t \in \Sigma^*$ and $i \in \mathbb{N}$.

Proof. By Lemma 2.3, $x^m = uv$, $y = (uv)^j u$, $z^n = vu$ for some $u, v \in \Sigma^*$ and $j \in \mathbb{N}$. Then uv is an m-power, and because its conjugate vu is an n-power, uv is also an n-power, say, $uv = r^n$. From $x^m = r^n$ and Lemma 2.1 it follows that x and r are powers of a common word p, and then $uv = p^l$ for some positive integer l, and l is divisible by both m and n. By $\gcd(m, n) = 1$, l is divisible by mn, and $uv = w^{mn}$ for some

$w \in p^*$. We can write $w = st$, $u = (st)^k s$, $v = t(st)^{mn-k-1}$ for some $s, t \in \Sigma^*$ and $k \in \mathbb{N}$, $k \leq mn-1$. Then $x = (st)^n$ and $z = (ts)^m$ and $y = (st)^{mnj+k}s$. □

Lemma 4.3. *Let $x, y, z \in \Sigma^*$ and $i, k \in \mathbb{N}$ and $i \geq 1$ and $k \geq 2$. Let $(xz)^i x = y^k$. Then x, y, z are powers of a common word or*

$$x = (uv)^j u, \qquad y = (uv)^{j+1}u, \qquad z = vu((uv)^{j+1}u)^{k-2}uv$$

for some $u, v \in \Sigma^*$ and $j \geq 0$.

Proof. If $i \geq 2$ or $|x| \geq |y|$, then $|(xz)^i x| = |y^k| \geq |xzy|$, so xz and y are powers of a common word by the theorem of Fine and Wilf, and then x, y, z are powers of a common word.

If $i = 1$ and $|x| < |y|$, then $y = sx = xt$ and $z = ty^{k-2}s$ for some $s, t \in \Sigma^+$. By Lemma 2.3, $s = uv$, $t = vu$, $x = (uv)^j u$ for some $u, v \in \Sigma^*$ and $j \in \mathbb{N}$, and then $y = (uv)^{j+1}u$ and $z = vu((uv)^{j+1}u)^{k-2}uv$. □

Lemma 4.4. *Let $h : \{X, Y, Z\}^* \to \Sigma^*$ be a nonperiodic morphism. If $E \in \mathrm{Eq}(h)$ is unbalanced, then E is equivalent to $\mathrm{Eq}(h)$.*

Proof. Every solution of $\mathrm{Eq}(h)$ is a solution of E. Every periodic solution of E is a solution of all balanced equations in $\mathrm{Eq}(h)$, because periodic morphisms satisfy all balanced equations, and also a solution of all unbalanced equations in $\mathrm{Eq}(h)$ by Theorem 2.7. If g is a nonperiodic solution of E, then $E \in \mathrm{Eq}(g) \cap \mathrm{Eq}(h)$, so it must be $\mathrm{Eq}(g) = \mathrm{Eq}(h)$ by Theorem 2.6. This means that g is a solution of $\mathrm{Eq}(h)$. We have shown that E and $\mathrm{Eq}(h)$ have the same solutions. □

5 Classification of Entire Systems

Budkina and Markov [16] classified all three-generator subsemigroups of a free semigroup. In the next theorem, we give a reformulation of this theorem in terms of morphisms and equations. An essentially equivalent result was proved independently by Spehner [17, 18]. These results have been used to study three-variable word equations in [14] and [19], for example. In [14], there is also a good comparison of these results.

Theorem 5.1 (Budkina and Markov [16])**.** *Every nonperiodic morphism $\{X, Y, Z\}^* \to \Sigma^*$ 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* $n, k_0, \ldots, k_n \in \mathbb{N}$.

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* $p, q, p', q', n, k_1, \ldots, k_n \in \mathbb{N}$ *and* $pp' = qq' = 0$ *and* $1 \leq p + q \leq k_1, \ldots, k_n$.

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* $p, q, k, m, n, k_1, \ldots, k_n \in \mathbb{N}$ *and* $m, p, q \geq 1$ *and* $p, q \leq k < p + q \leq k_1, \ldots, k_n$.

With the help of Theorem 5.1, we can prove a similar classification result for entire systems (Theorem 5.2) and for unbalanced equations (Corollary 5.3).

Theorem 5.2. *For every nonperiodic morphism $h : \{X, Y, Z\}^* \to \Sigma^*$ that satisfies a nontrivial equation,* $\mathrm{Eq}(h)$ *is equivalent, up to a permutation of the variables, to an unbalanced equation of one of the following types:*

BME1. $(X^{k_0} \prod_{i=1}^{n} Y X^{k_i}, Z)$, *where* $n, k_0, \ldots, k_n \in \mathbb{N}$.

BME2. (Y^n, Z^m), *where* $m, n \in \mathbb{N}$ *and* $m, n \geq 1$ *and* $\gcd(m, n) = 1$.

BME3. $(X^p Z X^q, X^{p'} Y \prod_{i=1}^{n} (X^{k_i - p - q} Y) X^{q'})$, *where* $p, q, p', q', n, k_1, \ldots, k_n \in \mathbb{N}$ *and* $pp' = qq' = 0$ *and* $1 \leq p + q \leq k_1, \ldots, k_n$.

BME4. $((X^{k-p}Y)^{n+1} X^k, X^k (Z X^{k-q})^{m+1})$, *where* $p, q, k, m, n \in \mathbb{N}$ *and* $k, m, n \geq 1$ *and* $p, q \leq k$ *and* $\gcd(m + 1, n + 1) = 1$.

BME5. $((X^{k-p} Y X^{k-q} Z)^{n+1}, (X^k Z)^{m+n+2})$, *where* $p, q, k, m, n \in \mathbb{N}$ *and* $p, q, k, m, n \geq 1$ *and* $p, q \leq k$ *and* $\gcd(m + 1, n + 1) = 1$.

BME6. $((X^k Z)^{m+2}, (X^{k-p} Y \prod_{i=1}^{n} (X^{k_i - p - q} Y) X^{k-q} Z)^{m+1})$, *where* $p, q, k, m, n, k_1, \ldots, k_n \in \mathbb{N}$ *and* $m, p, q \geq 1$ *and* $p, q \leq k < p + q \leq k_1, \ldots, k_n$.

Proof. By Theorem 5.1, h is equivalent, up to a permutation of the variables, to one of the morphisms BM1–BM6. It can be verified by a straightforward computation that each of these morphisms satisfies the corresponding equation BME1–BME6, and these equations are unbalanced. Thus there exists an unbalanced equation $E \in \mathrm{Eq}(h)$ that is equal, up to a permutation of the variables, to one of the equations BME1–BME6. By Lemma 4.4, $\mathrm{Eq}(h)$ is equivalent to E. □

Corollary 5.3. *Every unbalanced three-variable equation E with a nonperiodic solution h is equivalent, up to a permutation of the variables, to one of the equations BME1–BME6.*

Proof. By Lemma 4.4, E is equivalent to $\mathrm{Eq}(h)$, so the claim follows from Theorem 5.2. □

6 Solutions of Entire Systems

In this section, we solve the equations BME1–BME6. By Theorem 5.2 and Corollary 5.3, this essentially solves all entire systems and all unbalanced equations in the three-variable case. For each equation, we find an explicit description of all nonperiodic solutions of that equation using two word parameters, denoted by u and v, and possibly one numerical parameter, denoted by j. Each of the results could be formulated in terms of parametric solutions, but we return to this in Section 7.

Lemma 6.1. *Let E be the equation BME1. Then $[x, y, z]$ is a solution of E if and only if*

$$x = u, \qquad y = v, \qquad z = u^{k_0} \prod_{i=1}^{n} v u^{k_i} \tag{1}$$

for some $u, v \in \Sigma^*$.

Proof. Let $g = [x, y, z]$ be a solution of E. We can let x and y be arbitrary words u and v, and then g is a solution if and only if $z = u^{k_0} \prod_{i=1}^{n} v u^{k_i}$. □

Lemma 6.2. *Let E be the equation BME2. Then $[x, y, z]$ is a solution of E if and only if*

$$x = u, \qquad y = v^m, \qquad z = v^n \tag{2}$$

for some $u, v \in \Sigma^*$.

Proof. Let $g = [x, y, z]$ be a solution of E. Then $y^n = z^m$ is both an n-power and an m-power, so it is also an mn-power of some word v because $\gcd(m, n) = 1$. This means that $y = v^m$ and $z = v^n$. Then x can be an arbitrary word u and this always gives a solution g. □

Lemma 6.3. *Let E be the equation BME3. If $[x, y, z]$ is a nonperiodic solution of E, then*

$$x = (uv)^j u, \qquad y = x^{p-1}uvx^q, \qquad z = x^{p'-1}uv\prod_{i=1}^{n}(x^{k_i-1}uv)x^{q'} \tag{3}$$

for some $u, v \in \Sigma^*$ and $j \geq 0$. Moreover, every morphism defined by these formulas is a solution of E, except that if $p' = q' = 0$ and $k_i = 1$ for all i, then we must require that $j \leq n$.

Proof. Let $g = [x, y, z]$ be a nonperiodic solution of E. We have

$$x^p z x^q = x^{p'} y \prod_{i=1}^{n}(x^{k_i-p-q}y)x^{q'}.$$

We show that there exists $m \geq 1$ such that $x^p \sim_{\mathrm{p}} y^m x$. First, if $p = 0$, this is trivial. Second, if $p > 0$ and $k_i > p + q$ for some i, then $p' = 0$ and we can let m be the smallest number i such that $k_i > p + q$. Finally, if $p > 0$ and $k_i = p + q$ for all i, then $p' = 0$ and x^p is a prefix of $y^{n+1}x^{q'}$, which either has a prefix $y^{n+1}x$ (if $q' \geq 1$) or is a prefix of $y^{n+1}x$ (if $q' = 0$), and in either case we can let $m = n + 1$. We have shown that $x^p \sim_{\mathrm{p}} y^m x$. Similarly, $x^q \sim_{\mathrm{s}} xy^{m'}$ for some $m' \geq 1$.

If x and y are powers of a common word, then g is periodic, so it follows from Lemma 4.1 that x and y are of the claimed form. Now g is a solution of E if and only if

$$\begin{aligned} z &= x^{-p+p'} y \prod_{i=1}^{n}(x^{k_i-p-q}y)x^{q'-q} \\ &= x^{-p+p'} x^{p-1}uvx^q \prod_{i=1}^{n}(x^{k_i-p-q}x^{p-1}uvx^q)x^{q'-q} \\ &= x^{p'-1}uv\prod_{i=1}^{n}(x^{k_i-1}uv)x^{q'} \end{aligned}$$

and if this is a well-defined word, despite $p' - 1$ being negative in the case $p' = 0$. If $k_i \geq 2$ for some i or if $q' \geq 1$, then $x^{p'-1}$ is followed by $(uv)^r x = x(vu)^r$ for some

$r \geq 1$, making z a well-defined word. If $k_i = 1$ for all i and $p' = q' = 0$, then

$$z = x^{-1}uv \prod_{i=1}^{n} (uv) = ((uv)^j u)^{-1}(uv)^{n+1} = v(uv)^{n-j}$$

which is a well-defined word if and only if $j \leq n$ (or if $u = \varepsilon$ and $v^{n-j+1} = \varepsilon$, but that only gives periodic solutions). □

Lemma 6.4. *Let E be the equation BME4. If $[x, y, z]$ is a nonperiodic solution of E, then*

$$x = (uv)^j u, \qquad y = x^{p-1}uv(x^{k-1}uv)^m, \qquad z = (vux^{k-1})^n vux^{q-1} \tag{4}$$

for some $u, v \in \Sigma^*$ and $j \geq 0$. Moreover, every morphism defined by these formulas is a solution of E, except that if $k = 1$ and $p = 0$, then we must require $j \leq m$, and if $k = 1$ and $q = 0$, then we must require $j \leq n$.

Proof. Let $g = [x, y, z]$ be a nonperiodic solution of E. We have

$$(x^{k-p}y)^{n+1}x^k = x^k(zx^{k-q})^{m+1},$$

so Lemma 4.2 gives

$$x^{k-p}y = (st)^{m+1}, \qquad zx^{k-q} = (ts)^{n+1}, \qquad x^k = (st)^i s$$

for some $s, t \in \Sigma^*$ and $i \in \mathbb{N}$.

If $i = 0$, then $s = x^k$ and

$$y = x^{p-k}(st)^{m+1} = x^{p-k}(x^k t)^{m+1} = x^p t(x^k t)^m,$$
$$z = (ts)^{n+1}x^{q-k} = (tx^k)^{n+1}x^{q-k} = (tx^k)^n tx^q.$$

If we let $u = x$ and $v = t$, then this matches (4) with $j = 0$.

If $k \geq 2$ and $i \geq 1$, then by Lemma 4.3, either x, s, t are powers of a common word, making g periodic, or $s = (uv)^j u$, $x = (uv)^{j+1}u$, $t = vux^{k-2}uv$ for some $u, v \in \Sigma^*$ and $j \in \mathbb{N}$. We get

$$y = x^{p-k}(st)^{m+1} = x^{p-k}((uv)^j uvux^{k-2}uv)^{m+1} = x^{p-1}uv(x^{k-1}uv)^m$$
$$z = (ts)^{n+1}x^{q-k} = (vux^{k-2}uv(uv)^j u)^{n+1}x^{q-k} = (vux^{k-1})^n vux^{q-1}.$$

This matches (4) with $j \geq 1$. Because $uv(x^{k-1}uv)^m$ always begins with $uvx = xvu$, y is a well-defined word even if $p = 0$. Similarly, z is a well-defined word even if $q = 0$.

If $k = 1$ and $i \geq 1$, then

$$x = (st)^i s, \qquad y = x^{p-1}(st)^{m+1}, \qquad z = (ts)^{n+1}x^{q-1}.$$

If we let $u = s$ and $v = t$ and $j = i$, then this matches (4) with $j \geq 1$. Finally, we have to make sure that y and z are well-defined words even if $p = 0$ or $q = 0$. If $p = 0$, then we must require $i \leq m$, and if $q = 0$, then we must require $i \leq n$. □

Lemma 6.5. *Let E be the equation BME5. If $[x, y, z]$ is a nonperiodic solution of E, then*

$$x = (uv)^j u, \qquad y = x^{p-1}uv(x^{k-1}uv)^m x^q, \qquad z = x^{-1}uv(x^{k-1}uv)^n \tag{5}$$

for some $u, v \in \Sigma^*$ and $j \geq 0$. Moreover, every morphism defined by these formulas is a solution of E, except that if $k = 1$, then we must require that $j \leq n$.

Proof. Let $g = [x, y, z]$ be a nonperiodic solution of E. We have

$$(x^{k-p}yx^{k-q}z)^{n+1} = (x^k z)^{m+n+2},$$

and $\gcd(n+1, m+n+2) = 1$, so

$$x^{k-p}yx^{k-q}z = w^{m+n+2}, \qquad x^k z = w^{n+1}$$

for some $w \in \Sigma^*$. We get

$$w^{m+1} = w^{m+n+2}w^{-n-1} = x^{k-p}yx^{k-q}z(x^k z)^{-1} = x^{k-p}yx^{-q}.$$

If $k = 1$, then from $xz = w^{n+1}$ it follows that $w = uv$ and $x = (uv)^j u$ for some $u, v \in \Sigma^*$ and $j \in \mathbb{N}$, $j \leq n$. Then

$$y = x^{p-1}w^{m+1}x^q = x^{p-1}uv(uv)^m x^q, \qquad z = x^{-1}w^{n+1} = x^{-1}uv(uv)^n.$$

This matches (5).

If $k \geq 2$ and $|x^{k-1}| \leq |w|$, then from $x^k z = w^{n+1}$ it follows that $w = x^{k-1}t$ for some $t \in \Sigma^*$, and that x^k is a prefix of $x^{k-1}tx$, so x is a prefix of tx. This means that $t = uv$ and $x = (uv)^j u$ for some $u, v \in \Sigma^*$ and $j \in \mathbb{N}$. Then

$$y = x^{p-k}w^{m+1}x^q = x^{p-1}uv(x^{k-1}uv)^m x^q, \qquad z = x^{-k}w^{n+1} = x^{-1}uv(x^{k-1}uv)^n.$$

This matches (5). Because $uv(x^{k-1}uv)^n$ always begins with $uvx = xvu$, z is a well-defined word.

If $k \geq 2$ and $|w| < |x^{k-1}|$, then from $x^k z = w^{n+1}$ it follows that x^k and w^{n+1} have a common prefix of length $|x^k| > |xw|$. By the theorem of Fine and Wilf, x and w are powers of a common word, and this leads to g being periodic. □

Lemma 6.6. *Let E be the equation BME6. If $[x, y, z]$ is a nonperiodic solution of E, then*

$$x = (uv)^j u, \qquad y = x^{p-1}uvx^q, \qquad z = x^{-k}\Big(x^{k-1}uv\prod_{i=1}^{n}(x^{k_i-1}uv)\Big)^{m+1} \tag{6}$$

for some $u, v \in \Sigma^*$ and $j \geq 0$. Moreover, every morphism defined by these formulas is a solution of E, except that if $k = 1$ and $n = 0$, then we must require that $j \leq m$.

Proof. Let $g = [x, y, z]$ be a nonperiodic solution of E. We have

$$(x^k z)^{m+2} = \Big(x^{k-p} y \prod_{i=1}^{n} (x^{k_i-p-q} y) x^{k-q} z\Big)^{m+1}, \tag{7}$$

and therefore,

$$|x^k z| \le |x^{k-p} y \prod_{i=1}^{n} (x^{k_i-p-q} y) x^{k-q} z|.$$

Thus x^k is a prefix of $x^{k-p} y \prod_{i=1}^{n} (x^{k_i-p-q} y) x^{k-q}$, and consequently, x^p is a prefix of $y \prod_{i=1}^{n} (x^{k_i-p-q} y) x^{k-q}$. It follows that $x^p \sim_{\mathrm{p}} y^{m'} x$ for some $m' \ge 1$. Similarly, we see that $x^q \sim_{\mathrm{s}} x y^{m''}$ for some $m'' \ge 1$. If x and y are powers of a common word, then g is periodic, so it follows from Lemma 4.1 that x and y are of the claimed form.

The left-hand side and right-hand side of (7) is both an $(m+2)$-power and an $(m+1)$-power, so it is an $(m+2)(m+1)$-power of some word w. Now g is a solution of E if and only if

$$x^k z = w^{m+1}, \qquad x^{k-p} y \prod_{i=1}^{n} (x^{k_i-p-q} y) x^{k-q} z = w^{m+2},$$

so

$$w = w^{m+2} w^{-m-1} = x^{k-p} y \prod_{i=1}^{n} (x^{k_i-p-q} y) x^{-q}$$

and

$$\begin{aligned} z = x^{-k} w^{m+1} &= x^{-k} \Big(x^{k-p} y \prod_{i=1}^{n} (x^{k_i-p-q} y) x^{-q}\Big)^{m+1} \\ &= x^{-k} \Big(x^{k-p} x^{p-1} u v x^q \prod_{i=1}^{n} (x^{k_i-p-q} x^{p-1} u v x^q) x^{-q}\Big)^{m+1} \\ &= x^{-k} \Big(x^{k-1} u v \prod_{i=1}^{n} (x^{k_i-1} u v)\Big)^{m+1}. \end{aligned}$$

This is always a well-defined word, except that in the case $k = 1$ and $n = 0$, we get $z = x^{-1}(uv)^{m+1}$, and we must additionally require that $j \le m$. □

7 Main Result

Let us take a closer look at the lemmas proved in the previous section. We see that the formulas (1)–(6) that describe the nonperiodic solutions contain at most one free numerical parameter j. The other numbers in these formulas, denoted by symbols such as k_i, p, q and so on, are actually constants defined by the morphism h. The next example illustrates this in the case of the last lemma. In the following theorem, we formulate this precisely in terms of parametric solutions.

Example 7.1. Consider Lemma 6.6 and equation BME6. If $p = q = m = 1$ and $k = 2$ and $n = 0$, then the equation has a parametric NonPer-solution

$$\{((UV)^J U, UV(UV)^J U, VUUV)\} \in \mathcal{R}_1(2, 1).$$

If $p = q = k = m = 1$ and $n = 0$, then the equation has a parametric NonPer-solution

$$\{(U, UVU, VUV), (UVU, UVUVU, V)\} \in \mathcal{R}_0(2, 0).$$

Theorem 7.2. *Every nontrivial entire system* $\mathrm{Eq}(h)$*, where* h *is nonperiodic, and every unbalanced equation* E *on three variables has a parametric NonPer-solution in* $\mathcal{R}_1(2, 1)$ *and a parametric solution in* $\mathcal{R}_1(2, 2)$*.*

Proof. By Theorem 5.2, the entire system $\mathrm{Eq}(h)$ is equivalent, up to a permutation of the variables, to one of the equations BME1–BME6, and by Corollary 5.3, the same is true for E if it has a nonperiodic solution. By the lemmas of Section 6, each of the equations BME1–BME6 has a parametric NonPer-solution in $\mathcal{R}_1(2, 1)$ and, by Lemma 3.4, a parametric solution in $\mathcal{R}_1(2, 2)$.

If E has only periodic solutions, then the empty set is a parametric NonPer-solution of E, and E has a parametric solution in $\mathcal{R}_1(2, 2)$ by Lemma 3.4. □

8 Towards a Characterization for Balanced Equations

We would like to prove a result similar to Theorem 7.2 for balanced three-variable equations. The next theorem points towards such a result.

Theorem 8.1. *Let* E *be a three-variable equation. Let* H *be a set of representatives of all equivalence classes of morphisms* $\{X, Y, Z\}^* \to \Sigma^*$*. Then*

$$\mathrm{Sol}(E) = \bigcup_{h \in \mathrm{Sol}(E) \cap H} \mathrm{Sol}(\mathrm{Eq}(h)).$$

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

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

If the set $\mathrm{Sol}(E) \cap H$ is finite, then this theorem, together with the results proved in this article, leads to a simple parametric solution for E. Unfortunately, the set $\mathrm{Sol}(E) \cap H$ can be infinite, but the results in [19] give some restrictions on how complex this set can be. This could allow us to prove a stronger version of Hmelevskii's theorem.

Theorem 8.2. *Let* E *be a three-variable equation. Let* H *be the set of morphisms of the form BM1–BM6. Then* $\mathrm{Sol}(E) \cap H = (A \cap H) \cup (B \cap H)$*, where* A *is either a finite set or the set*

$$\{[a, a^i b a^j, (uv)^k u] \mid k \in \mathbb{N}\}$$

for some $i, j \in \mathbb{N}$ and $u, v \in \Sigma^*$, and B is either a finite set or the set

$$\{[a, a^i b(a^m b)^p a^j, a^k b(a^m b)^q a^l] \mid p, q \geq 1, \gcd(p+1, q+1) = 1\}$$

for some $i, j, k, l, m \in \mathbb{N}$.

Proof. Each of the morphisms in H is either of the form $[a, a^i b a^j, w]$ or of the form $[a, a^i b(a^m b)^p a^j, a^k b(a^m b)^q a^l]$.

For morphisms of the form $[a, a^i b a^j, w]$, it was proved in [19] that E can have such a solution for at most one pair (i, j). If we fix i and j and replace X by a and Y by $a^i b a^j$ 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 $(uv)^k u$ is a solution, and there are no other solutions, see [20].

For morphisms of the form $[a, a^i b(a^m b)^p a^j, a^k b(a^m b)^q a^l]$, it was proved in [19] that if E has infinitely many such solutions, then the set of such solutions in $\mathrm{Sol}(E)$ is

$$\{[a, a^i b(a^m b)^p a^j, a^k b(a^m b)^q a^l] \mid p, q \geq 1, \gcd(p+1, q+1) = 1\}$$

for some $i, j, k, l, m \in \mathbb{N}$. □

We expect that every nontrivial three-variable equation has a parametric solution in $\mathcal{R}_d(2, q)$ for some fixed numbers d, q, perhaps even for $d = 2$ and $q = 3$. However, proving this kind of a result requires additional work in the future.

References

[1] A. Jeż, Word equations in non-deterministic linear space. Journal of Computer and System Sciences **123**, 122–142 (2022). https://doi.org/10.1016/j.jcss.2021.08.001

[2] M.H. Albert, J. Lawrence, A proof of Ehrenfeucht's conjecture. Theoretical Computer Science **41**(1), 121–123 (1985). https://doi.org/10.1016/0304-3975(85)90066-0

[3] V.S. Guba, Equivalence of infinite systems of equations in free groups and semigroups to finite subsystems. Matematicheskie Zametki **40**(3), 321–324 (1986). https://doi.org/10.1007/BF01142470

[4] A. Saarela, *Hardness results for constant-free pattern languages and word equations*, in *Proceedings of the 47th ICALP*, *LIPIcs*, vol. 168 (Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 2020), pp. 140:1–140:15. https://doi.org/10.4230/LIPIcs.ICALP.2020.140

[5] J.I. Hmelevskiĭ, *Equations in free semigroups* (American Mathematical Society, 1976). Translated by G. A. Kandall from the Russian original: Trudy Mat. Inst. Steklov. 107 (1971)

[6] D. Nowotka, A. 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). https://doi.org/10.1137/20M1310448

[7] J. Karhumäki, A. Saarela, *An analysis and a reproof of Hmelevskii's theorem*, in *Proceedings of the 12th DLT*, *LNCS*, vol. 5257 (Springer, 2008), pp. 467–478. https://doi.org/10.1007/978-3-540-85780-8_37

[8] A. Saarela. Word equations and related topics: independence, decidability and characterizations (2012). URL http://urn.fi/URN:ISBN:978-952-12-2737-0. Doctoral dissertation, University of Turku

[9] A. Saarela, *On the complexity of Hmelevskii's theorem and satisfiability of three unknown equations*, in *Proceedings of the 13th DLT*, *LNCS*, vol. 5583 (Springer, 2009), pp. 443–453. https://doi.org/10.1007/978-3-642-02737-6_36

[10] A. Saarela, *On the Solution Sets of Entire Systems of Word Equations*, in *Proceedings of the 14th WORDS*, *LNCS*, vol. 13899 (Springer, 2023), pp. 261–273. https://doi.org/https://doi.org/10.1007/978-3-031-33180-0_20

[11] M. Lothaire, *Combinatorics on Words* (Addison-Wesley, 1983)

[12] M. Lothaire, *Algebraic Combinatorics on Words* (Cambridge University Press, 2002). URL http://www-igm.univ-mlv.fr/~berstel/Lothaire/AlgCWContents.html

[13] N.J. Fine, H.S. Wilf, Uniqueness theorems for periodic functions. Proceedings of the American Mathematical Society **16**, 109–114 (1965). https://doi.org/10.1090/S0002-9939-1965-0174934-9

[14] T. Harju, D. Nowotka, On the independence of equations in three variables. Theoretical Computer Science **307**(1), 139–172 (2003). https://doi.org/10.1016/S0304-3975(03)00098-7

[15] A. Saarela, Systems of word equations, polynomials and linear algebra: A new approach. European Journal of Combinatorics **47**, 1–14 (2015). https://doi.org/10.1016/j.ejc.2015.01.005

[16] L.G. Budkina, A.A. Markov, F-semigroups with three generators. Akademiya Nauk SSSR. Matematicheskie Zametki **14**, 267–277 (1973)

[17] J.C. Spehner, Quelques problémes d'extension, de conjugaison et de présentation des sous-monoïdes d'un monoïde libre. Ph.D. thesis, Univ. Paris (1976)

[18] J.C. Spehner, *Les systemes entiers d'équations sur un alphabet de 3 variables*, in *Semigroups Theory and Applications*, *LNM*, vol. 1320 (Springer, 1988), pp. 342–357. https://doi.org/10.1007/BFb0083443

[19] D. Nowotka, A. Saarela, One-variable word equations and three-variable constant-free word equations. International Journal of Foundations of Computer Science **29**(5), 935–950 (2018). https://doi.org/10.1142/S0129054118420121

[20] M. Laine, W. Plandowski, Word equations with one unknown. International Journal of Foundations of Computer Science **22**(2), 345–375 (2011). https://doi.org/10.1142/S0129054111008088