On the Solution Sets of Entire Systems of Word Equations*

Aleksi Saarela[0000−0002−6636−2317]

Department of Mathematics and Statistics, University of Turku, Finland
amsaar@utu.fi

Abstract. The set of all constant-free word equations satisfied by a given morphism is called an entire system of equations. We show that in the three-variable case, the set of nonperiodic solutions of any entire system can be described using parametric formulas with just one numerical parameter. We also show how the solution set of any equation can be represented as a union of solution sets of entire systems. Even though an infinite union is needed in some cases, this still points towards a stronger version of Hmelevskii's theorem about parametric solutions of three-variable word equations.

Keywords: Combinatorics on words · Word equation · Entire system · 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 [7], and that every system of word equations is equivalent to a finite subsystem [1, 4].

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 [16].

Equations with one or two variables are trivial. 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 [6] (this does not hold for equations with four or more variables), and a bound 18 for the size of independent systems [12] (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 modernized version of that proof in [8, 14], 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 [13, 14], and it was proved, for example, that the number of

* Supported by the Academy of Finland under grant 339311

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 a large number of three-variable equations and systems of equations, namely, for so-called entire systems and unbalanced equations, the set of solutions can be described using explicitly given formulas that are quite simple. In particular, only one numerical parameter is needed to represent nonperiodic solutions. We also outline a strategy to extend our result to all three-variable equations, although one numerical parameter will 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.

2 Preliminaries

First, we go through some basic definitions and lemmas abouts words. For more, see [9, 10].

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 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.

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.

Lemma 1. *Let $x, y \in \Sigma^*$. The following are equivalent:*

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

Lemma 2. *Let $x, y \in \Sigma^*$. If y is a fractional power of x and ends in x, then x and y are powers of a common word.*

Lemma 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 4 (Fine and Wilf [3]). *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 $E = (U, V)$, where $U, V \in \Xi^*$, and a *solution* of E is a morphism $h : \Xi^* \to \Sigma^*$ 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 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 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 3 that all solutions of E are of this form or of the form $[\varepsilon, u, \varepsilon]$.

An equation (U, V) is *balanced* if every variable has as many occurrences in U as in V, and *unbalanced* otherwise. Results related to balanced equations can be found, for example, in [5] and [15]. We need the following two theorems.

Theorem 6 (Harju and Nowotka [5]). *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 7 (Harju and Nowotka [5]). *If two unbalanced equations have a common nonperiodic solution, then they have the same set of periodic solutions.*

Budkina and Markov [2] 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 [5] and [11], for example. In [5], there is also a good comparison of these results.

Theorem 8 (Budkina and Markov [2]). *Every nonperiodic morphism from $\{X, Y, Z\}^*$ to Σ^* that satisfies a nontrivial equation is equivalent, up to a permutation of the variables, to a morphism of one of the following types:*

1. $[a, b, w]$, *where* $w \in \{a, b\}^*$.
2. $[a, b^m, b^n]$, *where* $m, n \in \mathbb{N}$ *and* $m, n \geq 1$ *and* $\gcd(m, n) = 1$.
3. $[a, a^p b a^q, a^{p'} b \prod_{i=1}^{n} (a^{k_i} b) a^{q'}]$, *where* $p, q, p', q', n, k_1, \ldots, k_n \in \mathbb{N}$ *and* $pp' = qq' = 0$ *and* $1 \leq p + q \leq k_1, \ldots, k_n$.
4. $[a, a^p b (a^k b)^m, b (a^k b)^n a^q]$, *where* $p, q, k, m, n \in \mathbb{N}$ *and* $k, m, n \geq 1$ *and* $p, q \leq k$ *and* $\gcd(m + 1, n + 1) = 1$.
5. $[a, a^p b (a^k b)^m a^q, b (a^k b)^n]$, *where* $p, q, k, m, n \in \mathbb{N}$ *and* $p, q, k, m, n \geq 1$ *and* $p, q \leq k$ *and* $\gcd(m + 1, n + 1) = 1$.
6. $[a, a^p b a^q, b \prod_{i=1}^{n} (a^{k_i} b) (a^k b \prod_{i=1}^{n} (a^{k_i} b))^m]$, *where* $p, q, k, m, n, k_1, \ldots, k_n \in \mathbb{N}$ *and* $m, p, q \geq 1$ *and* $p, q \leq k < p + q \leq k_1, \ldots, k_n$.

3 Lemmas

In this section, we prove some lemmas that are needed later.

Lemma 9. *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 $x^q \sim_{\mathrm{s}} x y^n$. 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 a similar way.

First, let $|y| \geq |x^{p+q-1}|$. Then $y = x^{p-1} w x^q$ for some word w. From $x^p \sim_{\mathrm{p}} y^m x$ it follows that $x \sim_{\mathrm{p}} w x^q (x^{p-1} w x^q)^{m-1} x$. Therefore, x is a prefix of $w^k x$ for some $k \geq 1$. It follows that $w = uv$ and $x = (uv)^j u$ for some $u, v \in \Sigma^*$ and $j \geq 0$.

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 begins and ends with powers of x that overlap by a factor of length at least $|x|$. By Lemma 2, x and y are powers of a common 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, x and y are powers of a common word.

Finally, let $|y| < |x^{p+q-1}|$ and $q \geq 1$ and $|y| \leq |x|$. Then x is a fractional power of y and ends in y. By Lemma 2, x and y are powers of a common word. □

Lemma 10. *Let $x, y \in \Sigma^*$ and $m, n, \in \mathbb{N}$ and $\gcd(m, n) = 1$. Let $x^m y = y z^n$. 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 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. By $\gcd(m, n) = 1$, $uv = w^{mn}$ for some $w \in \Sigma^*$. 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 11. *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 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 12. *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 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 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. □

4 Solutions of Entire Systems

In this section, we go through all entire systems $\mathrm{Eq}(h)$, where $h : \{X, Y, Z\}^* \to \Sigma^*$ is a nonperiodic morphism that satisfies a nontrivial equation. By Theorem 8, we can concentrate on the morphisms specified in that theorem.

In each case, with the help of Lemma 12, we find that the entire system is equivalent to a relatively simple unbalanced equation. Then we proceed to find an explicit description of all nonperiodic solutions of that equation. In each such description, there are two word parameters, denoted by u and v, and possibly one numerical parameter, denoted by j.

The formulas that describe the nonperiodic solutions also give some periodic solutions when u and v are powers of a common word. In some cases, all periodic solutions are obtained this way, but in other cases, some periodic solutions are missing. If we want to represent the set of all solutions, both the nonperiodic and periodic ones, we can always do that by adding separate formulas that give all the periodic solutions, although then we need two numerical variables.

Lemma 13. *Let $n, k_0, \ldots, k_n \in \mathbb{N}$. Let*

$$h = [a, b, a^{k_0} \prod_{i=1}^{n} ba^{k_i}].$$

Then $\mathrm{Eq}(h)$ *is equivalent to the equation*

$$E = (X^{k_0} \prod_{i=1}^{n} YX^{k_i}, Z)$$

and $[x, y, z]$ is a solution of E if and only if

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

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

Proof. It is easy to check that h is a solution of E. Thus $E \in \mathrm{Eq}(h)$, and E is unbalanced, so E and $\mathrm{Eq}(h)$ are equivalent by Lemma 12.

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 $z = u^{k_0} \prod_{i=1}^{n} vu^{k_i}$. □

Lemma 14. *Let $m, n \in \mathbb{N}$ and $m, n \geq 1$ and $\gcd(m, n) = 1$. Let*

$$h = [a, b^m, b^n].$$

Then $\mathrm{Eq}(h)$ *is equivalent to the equation*

$$E = (Y^n, Z^m)$$

and $[x, y, z]$ 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. It is easy to check that h is a solution of E. Thus $E \in \mathrm{Eq}(h)$, and E is unbalanced, so E and $\mathrm{Eq}(h)$ are equivalent by Lemma 12.

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

$$h = \Big[a, a^p b a^q, a^{p'} b \prod_{i=1}^{n} (a^{k_i} b) a^{q'}\Big].$$

Then $\mathrm{Eq}(h)$ *is equivalent to the equation*

$$E = \Big(X^p Z X^q, X^{p'} Y \prod_{i=1}^{n} (X^{k_i - p - q} Y) X^{q'}\Big).$$

If $[x, y, z]$ *is a nonperiodic solution of* E*, then*

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

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. It is easy to check that h is a solution of E. Thus $E \in \mathrm{Eq}(h)$, and E is unbalanced, so E and $\mathrm{Eq}(h)$ are equivalent by Lemma 12.

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

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

so $x^p \sim_{\mathrm{p}} y^m x$ for some $m \geq 1$. If $p = 0$, this is trivial, and if $p > 0$, then $p' = 0$ and m is the smallest number i such that $k_i > p - q$, or $m = n + 1$ if such i does not exist. Similarly, $x^q \sim_{\mathrm{s}} x y^{m'}$ for some $m' \geq 1$. If x and y are powers of a common word, then g is periodic, so it follows from Lemma 9 that x and y are of the claimed form. Now g is a solution of E if and only if

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

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 16. *Let $p, q, k, m, n \in \mathbb{N}$ and $k, m, n \geq 1$ and $p, q \leq k$ and* $\gcd(m + 1, n + 1) = 1$. *Let*

$$h = [a, a^p b(a^k b)^m, b(a^k b)^n a^q].$$

Then $\mathrm{Eq}(h)$ *is equivalent to the equation*

$$E = ((X^{k-p}Y)^{n+1}X^k, X^k(ZX^{k-q})^{m+1}).$$

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. It is easy to check that h is a solution of E. Thus $E \in \mathrm{Eq}(h)$, and E is unbalanced, so E and $\mathrm{Eq}(h)$ are equivalent by Lemma 12.

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 10 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 11, 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 17. *Let $p, q, k, m, n \in \mathbb{N}$ and $p, q, k, m, n \geq 1$ and $p, q \leq k$ and* $\gcd(m+1, n+1) = 1$. *Let*

$$h = [a, a^p b (a^k b)^m a^q, b(a^k b)^n].$$

Then $\mathrm{Eq}(h)$ *is equivalent to the equation*

$$E = ((X^{k-p} Y X^{k-q} Z)^{n+1}, (X^k Z)^{m+n+2}).$$

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. It is easy to check that h is a solution of E. Thus $E \in \mathrm{Eq}(h)$, and E is unbalanced, so E and $\mathrm{Eq}(h)$ are equivalent by Lemma 12.

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

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

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

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

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

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

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

$$h = \Big[a, a^p b a^q, b \prod_{i=1}^{n} (a^{k_i} b) \Big(a^k b \prod_{i=1}^{n} (a^{k_i} b) \Big)^m \Big].$$

Then Eq(h) *is equivalent to the equation*

$$E = \Big((X^kZ)^{m+2}, \Big(X^{k-p}Y\prod_{i=1}^{n}(X^{k_i-p-q}Y)X^{k-q}Z\Big)^{m+1}\Big).$$

If $[x, y, z]$ *is a nonperiodic solution of* E*, then*

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

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. It is easy to check that h is a solution of E. Thus $E \in$ Eq(h), and E is unbalanced, so E and Eq(h) are equivalent by Lemma 12.

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

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

and therefore,

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

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 $m' \geq 1$. Similarly, we see that $x^q \sim_{\mathrm{s}} xy^{m''}$ for some $m'' \geq 1$. If x and y are powers of a common word, then g is periodic, so it follows from Lemma 9 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

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

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

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

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 $j \le m$. □

Let us take a closer look at the lemmas proved in this section. We see that the formulas (1)–(6) that describe the nonperiodic solutions contain at most one free numerical variable 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.

Example 19. Consider Lemma 18.

If $p = q = m = 1$ and $k = 2$ and $n = 0$, then a nonperiodic solution $[x, y, z]$ of E is of the form

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

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

If $p = q = k = m = 1$ and $n = 0$, then a nonperiodic solution $[x, y, z]$ of E is of the form

$$x = (uv)^j u, \qquad y = uv(uv)^j u, \qquad z = v(uv)^{1-j}$$

for some $u, v \in \Sigma^*$ and $j \in \{0, 1\}$.

5 Connections to Hmelevskii's Theorem and Future Work

In Section 4, we found an explicit representation for the nonperiodic solutions of every nontrivial entire system of three-variable equations. By the next theorem, this also gives a representation for the nonperiodic solutions of every unbalanced three-variable equation.

Theorem 20. *The family of the sets* $\mathrm{Sol}(\mathrm{Eq}(h))$*, where* $h : \{X, Y, Z\}^* \to \Sigma^*$ *is a nonperiodic morphism that satisfies a nontrivial equation, is the same as the family of the sets* $\mathrm{Sol}(E)$*, where* E *is an unbalanced three-variable equation with a nonperiodic solution.*

Proof. In Section 4, we proved that every such entire system $\mathrm{Eq}(h)$ is equivalent to an unbalanced equation. On the other hand, every unbalanced equation E with a nonperiodic solution h is equivalent to $\mathrm{Eq}(h)$ by Lemma 12. □

As was mentioned in the introduction, Hmelevskii proved that every three-variable equation has a parametric solution (for a precise definition of parametric words and parametric solutions, see, for example, [6] or [14]). The representations we found for entire systems are much simpler than the ones guaranteed by Hmelevskii's theorem. In particular, the best known upper bound for the number of numerical parameters in parametric solutions of three-variable equations is logarithmic with respect to the length of the equation. The formulas we found in the previous section, on the other hand, use at most one numerical parameter (although if we want to represent also periodic solutions, we need two numerical parameters).

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

Theorem 21. *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 in Section 4, gives a simple parametric solution for E. Unfortunately, the set $\mathrm{Sol}(E) \cap H$ can be infinite, but the results in [11] give some restrictions on how complicated this set can be. This could allow us to prove a stronger version of Hmelevskii's theorem.

In particular, we expect that every three-variable equation has a parametric solution that uses only three numerical parameters, instead of a logarithmic number. However, proving this kind of result requires additional work in the future.

References

1. Albert, M.H., Lawrence, J.: A proof of Ehrenfeucht's conjecture. Theoretical Computer Science **41**(1), 121–123 (1985). https://doi.org/10.1016/0304-3975(85)90066-0
2. Budkina, L.G., Markov, A.A.: F-semigroups with three generators. Akademiya Nauk SSSR. Matematicheskie Zametki **14**, 267–277 (1973)
3. Fine, N.J., Wilf, H.S.: 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
4. Guba, V.S.: 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

5. Harju, T., Nowotka, D.: 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
6. Hmelevskiĭ, J.I.: Equations in free semigroups. American Mathematical Society (1976), translated by G. A. Kandall from the Russian original: Trudy Mat. Inst. Steklov. 107 (1971)
7. Jeż, A.: 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
8. Karhumäki, J., Saarela, A.: An analysis and a reproof of Hmelevskii's theorem. In: Proceedings of the 12th DLT. LNCS, vol. 5257, pp. 467–478. Springer (2008)
9. Lothaire, M.: Combinatorics on Words. Addison-Wesley (1983)
10. Lothaire, M.: Algebraic Combinatorics on Words. Cambridge University Press (2002), http://www-igm.univ-mlv.fr/ berstel/Lothaire/AlgCWContents.html
11. Nowotka, D., Saarela, A.: 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
12. Nowotka, D., Saarela, A.: 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
13. Saarela, A.: On the complexity of Hmelevskii's theorem and satisfiability of three unknown equations. In: Proceedings of the 13th DLT. LNCS, vol. 5583, pp. 443–453. Springer (2009)
14. Saarela, A.: Word equations and related topics: independence, decidability and characterizations (2012), http://urn.fi/URN:ISBN:978-952-12-2737-0, doctoral dissertation, University of Turku
15. Saarela, A.: 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. Saarela, A.: Hardness results for constant-free pattern languages and word equations. In: Proceedings of the 47th ICALP. LIPIcs, vol. 168, pp. 140:1–140:15. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik (2020). https://doi.org/10.4230/LIPIcs.ICALP.2020.140
17. Spehner, J.C.: Quelques problémes d'extension, de conjugaison et de présentation des sous-monoïdes d'un monoïde libre. Ph.D. thesis, Univ. Paris (1976)
18. Spehner, J.C.: Les systemes entiers d'équations sur un alphabet de 3 variables. In: Semigroups Theory and Applications. LNCS, vol. 1320, pp. 342–357. Springer (1988). https://doi.org/10.1007/BFb0083443