A NEW PROOF OF HMELEVSKII'S THEOREM

Aleksi Saarela

Licentiate thesis
April 2009

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF TURKU

Contents

1 Introduction

This work concerns combinatorics on words, or more precisely the theory of word equations. Fundamental results of this topic include the decidability of the satisfiability problem for word equations, see [9], and the compactness result of systems of word equations, see [1] and [5]. The first result was improved to a PSPACE algorithm in [10].

In the case of constant-free word equations with only three unknowns fundamental results have also been achieved. Hmelevskii [7] proved in 1970 that the general solution of any such equation can be expressed as a finite formula on word and numerical parameters. On other direction Spehner [11, 12] classified all sets of relations a given solution, that is a triple of words, can satisfy. Both of these results have only very complicated proofs. Another example of a challenging nature of word problems is that the question of finding any upper bound for the maximal size of independent system of word equations on three unknowns is still open, see [6] and [3].

The result of Hmelevskii is well known, see e.g. [8], but a readable presentation seems to be lacking. This work attempts to give a simplified proof using modern tools of combinatorics on words. As a new result, we get an upper bound of the size of the formula giving the general solution. This bound is double exponential in terms of the length of the equation, and thus very probably far from optimal.

This work begins in section 2 with some definitions and well-known theorems. Then some simple equations, which will be used later, are solved. In section 3 we define parametric words and parametric solutions formally and present some very basic properties of them, and in section 4 we take a closer look at the form of parametric solutions. Section 5 deals with exponential equations, which are an important tool used in our proof. In section 6 we are able to prove Hmelevskii's theorem for a large class of equations. All other equations will be reduced to these equations later on. The main tools in this process are images and θ-images, which are the topic of section 7. Finally, in the last three sections a so called basic tree is constructed for an arbitrary equation, and this completes the proof of Hmelevskii's theorem. An upper bound for the height of such a tree gives an upper bound for the length of the parametric solution.

2 Definitions and basic results

In this section we fix the terminology and state the basic auxiliary results needed, for more see [2].

We consider word equations $U = V$, where $U, V \in \Xi^*$ and Ξ is the alphabet of unknowns. A morphism $h : \Xi^* \to \Sigma^*$ is a solution of this equation, if $h(U) = h(V)$. We also consider *one-sided* equations $xU \rightrightarrows yV$.

A morphism $h : \Xi^* \to \Sigma^*$ is a solution of this equation, if $h(xU) = h(yV)$ and $|h(x)| \geq |h(y)|$.

A solution h is *periodic*, if there exists such $t \in \Sigma^*$ that every $h(x)$, where $x \in \Xi$, is a power of t. Otherwise h is *nonperiodic*. Periodic solutions are easy to find and represent, so in many cases it is enough to consider nonperiodic solutions.

A word w is *primitive*, if it is not of the form t^n, where $t \neq w$ and $n \geq 2$. Every word w can be represented uniquely as t^n with t primitive; then t is the *primitive root* of w and the notation $t = \rho(w)$ is used.

If a word u is a *prefix* of a word v, that is $v = uw$ for some w, the notation $u \leq v$ is used. If also $u \neq v$, then u is a *proper prefix* and the notation $u < v$ is used.

Let $w = a_1 \dots a_n$. Its *reverse* is $w^R = a_n \dots a_1$, and its *length* is $|w| = n$. The number of occurrences of a letter a in w is denoted by $|w|_a$.

If $\Sigma = \{a_1, \dots, a_n\}$, then $U \in \Sigma^*$ can be denoted $U(a_1, \dots, a_n)$, and its image under a morphism h can be denoted $h(U) = U(h(a_1), \dots, h(a_n))$. If $u \in \Sigma^*$, then the morphism $a_1 \mapsto u$ means the morphism, which maps $a_1 \mapsto u$ and $a_i \mapsto a_i$, when $i = 2, \dots, n$.

The following theorems and lemmas give solutions to some simple equations. These solutions will be the basis of parametric solutions of all equations with three unknowns. We start with the well known lemmata, see [2].

Theorem 2.1 (Commutation). *Let $U, V \in \{x, y\}^*$ and $U \neq V$. Assume that $|U|_x = a$, $|U|_y = b$, $|V|_x = c$ and $|V|_y = d$. The solutions of the equation $U = V$ are $x = t^i$, $y = t^j$, where $t \in \Sigma^*$, $ai + bj = ci + dj$ and $i, j \geq 0$.*

Theorem 2.2 (Conjugation). *The solutions of the equation $xz = zy$ are $x = pq$, $y = qp$, $z = p(qp)^i$ or $x = y = 1$, $z = p$, where $p, q \in \Sigma^*$ and $i \geq 0$.*

Theorem 2.3 (Fine and Wilf). *Let $u, v \in \Sigma^+$, $u' < u$, $v' < v$ and*

$$|u^m u'| = |v^n v'| \geq |u| + |v| - \gcd(|u|, |v|).$$

Now $u^m u' = v^n v'$ if and only if $uv = vu$.

For the next theorem we define the *graph* of a system of equations. It is a graph, whose vertices are the unknowns of the system, and where two vertices x and y are connected by an edge, if the system contains an equation of the form $x \dots = y \dots$.

Theorem 2.4 (Graph lemma). *Let E be a system of equations and assume that its graph has c connected components. Let $\Xi = \{x_1, \dots, x_n\}$ and let $h : \Xi^* \to \Sigma^+$ be a solution of E. Now there exists a set $F \subset \Sigma^+$ with c elements such that $h(x_1), \dots, h(x_n) \in F^*$.*

The above theorem has the following corollary, which suits particularly well to our considerations.

Corollary 2.5. *Let $A, B, C, D \in \{x, y, z\}^*$. Each solution h of the system of equations $xA = yB, xC = zD$, for which $h(x), h(y), h(z) \neq 1$, is periodic.*

We continue by solving a few examples of word equations needed in our presentation.

Lemma 2.6. *The nonperiodic solutions of the equation $xyz = zyx$ are $x = (pq)^i p$, $y = q(pq)^j$, $z = (pq)^k p$, where $p, q \in \Sigma^*$, $i, j, k \geq 0$, $pq \neq qp$ and pq can be assumed to be primitive.*

Proof. The claimed solutions satisfy the equation and are nonperiodic. If h is a nonperiodic solution, then $h(xyzy) = h(zyxy)$, so $h(xy) = t^m$ and $h(zy) = t^n$, where t is primitive and $m, n > 0$. Now $h(y) = q(pq)^j$, where $pq = t$ and $0 \leq j < m, n$, so $h(x) = (pq)^i p$ and $h(z) = (pq)^k p$, where $i = m - j - 1$ and $k = n - j - 1$. If p and q would commute, the solution would be periodic. □

Lemma 2.7. *The nonperiodic solutions of the equation $xyz = zxy$ are $x = (pq)^i p$, $y = q(pq)^j$, $z = (pq)^k$, where $p, q \in \Sigma^*$, $i, j, k \geq 0$ and $pq \neq qp$.*

Proof. The claimed solutions satisfy the equation and are nonperiodic. If h is a nonperiodic solution, then $h(xy) = t^m$ and $h(z) = t^k$, where $m > 0, k \geq 0$. Now $h(y) = q(pq)^j$, where $pq = t$ and $0 \leq j < m$, so $h(x) = (pq)^i p$ and $h(z) = (pq)^k$, where $i = m - j - 1$. If p and q would commute, the solution would be periodic. □

Lemma 2.8. *Let $a \geq 2$. The nonperiodic solutions of the equation $xzx = y^a$ are $x = (pq)^i p$, $y = (pq)^{i+1} p$, $z = qp((pq)^{i+1} p)^{a-2} pq$, where $p, q \in \Sigma^*$, $i \geq 0$ and $pq \neq qp$.*

Proof. The claimed solutions satisfy the equation and are nonperiodic. Let h be a nonperiodic solution. If it would be $|h(x)| \geq |h(y)|$, then $h(xz)$ and $h(y)$ would be powers of a common word by Theorem 2.3, and h would be periodic. Thus $|h(x)| < |h(y)|$. Now $h(y) = uh(x) = h(x)v$, where $u, v \neq 1$, and $h(z) = vh(y)^{a-2}u$. By Theorem 2.2, $u = pq$, $v = qp$, $h(x) = (pq)^i p$, $h(y) = (pq)^{i+1} p$ and $h(z) = qp((pq)^{i+1} p)^{a-2} pq$. If p and q would commute, the solution would be periodic. □

Lemma 2.9. *Let $a \geq 2$. The nonperiodic solutions of the equation $xy^a z = zy^a x$ are $x = (pq^a)^i p$, $y = q$, $z = (pq^a)^j p$ or*

$$\begin{cases} x &= qp((pq)^{k+1} p)^{a-2} pq(((pq)^{k+1} p)^{a-1} pq)^i, \\ y &= (pq)^{k+1} p, \\ z &= qp((pq)^{k+1} p)^{a-2} pq(((pq)^{k+1} p)^{a-1} pq)^j, \end{cases}$$

where $p, q \in \Sigma^*$, $i, j, k \geq 0$ and $pq \neq qp$.

Proof. The claimed solutions satisfy the equation and are nonperiodic. If h is a nonperiodic solution, then, by Lemma 2.6,

$$h(x) = u(vu)^i,\ h(y^a) = v(uv)^b,\ h(z) = u(vu)^j,$$

where uv is primitive. If $b = 0$, this gives a solution of the first form. If $b > 1$, then, by Theorem 2.3, hy and vu commute. Then $u = 1$ or $v = 1$ and $h(x), h(y), h(z) \in (uv)^*$, which is a contradiction. If $b = 1$, then, by Lemma 2.8, $h(v) = (pq)^k p$, $h(y) = (pq)^{k+1}p$ and $h(u) = qp((pq)^{k+1}p)^{a-2}pq$. This gives a solution of the second form. If p and q would commute, the solution would be periodic. □

Lemma 2.10. *The nonperiodic solutions of the equation $xyxz \rightrightarrows zx^2y$ are $x = (pq)^i p$, $y = qp((pq)^{i+1}p)^j pq$, $z = pq$, where $p, q \in \Sigma^*$, $i \geq 1$, $j \geq 0$ and $pq \neq qp$.*

Proof. The claimed solutions satisfy the equation and are nonperiodic. If h is a nonperiodic solution, then, by Lemma 2.6,

$$h(xy) = (uv)^b u,\ h(x) = v(uv)^c,\ h(z) = (uv)^d u.$$

Because $h(z) \leq h(x) \leq h(xy)$ and $uv \neq vu$, it must be $h(z) = u \leq h(x) = v \leq uv$. Now $h(z) = pq$ and $h(x) = (pq)^i p$, so $y = qp((pq)^{i+1}p)^j pq$. If p and q would commute, the solution would be periodic. □

Lemma 2.11. *Let $a, b \geq 1$ and $U, V \in \Xi^*$. If h is a solution of the equation $x^a yU = y^b xV$, then $h(x)$ and $h(y)$ commute.*

Proof. Assume that $h(x) \leq h(y)$. Then $h(y) = h(x)^c t$, where $h(x) \not\leq t$. Because $h(x)^{a+c} \ldots = h(x)^c t \ldots$, it must be $t \leq h(x)$. Now $h(x)^{a+c} t \ldots = h(y)^b h(x) \ldots$ and $|h(x)^{a+c} t|, |h(y)^b h(x)| \geq |h(x)h(y)|$. The claim follows by Theorem 2.3. □

3 Parametric words

In this section, we define the central notions of this presentation, namely parametric words, parameterizability and parametric solutions.

Fix the alphabet of *word parameters* Δ and the set of *numerical parameters* Λ. Now *parametric words* are defined inductively as follows:

(i) if $a \in \Delta \cup \{1\}$, then (a) is a parametric word,

(ii) if α and β are parametric words, then so is $(\alpha\beta)$,

(iii) if α is a parametric word and $i \in \Lambda$, then (α^i) is a parametric word.

The set of parametric words is denoted by $\mathcal{P}(\Delta, \Lambda)$. The sets of parameters are always denoted by Δ and Λ.

When there is no danger of confusion, unnecessary parenthesis can be omitted and notations like $\alpha^i \alpha^j = \alpha^{i+j}$ and $(\alpha^i)^j = \alpha^{ij}$ can be used. Then parametric words form a monoid, if the product of α and β is defined to be $\alpha\beta$.

If f is a function $\Lambda \to \mathbb{N}_0$, we can abuse the notation and use the same symbol for the function, which maps parametric words by giving values for the numerical parameters with f: if $a \in \Delta \cup \{1\}$, then $f((a)) = a$; if $\alpha, \beta \in \mathcal{P}(\Delta, \Lambda)$, then $f((\alpha\beta)) = f(\alpha)f(\beta)$; if $\alpha \in \mathcal{P}(\Delta, \Lambda)$ and $i \in \Lambda$, then $f((\alpha^i)) = f(\alpha)^{f(i)}$. A parametric word is thus mapped by f to a word of Δ^*. This can be further mapped by a morphism $h : \Delta^* \to \Sigma^*$ to a word of Σ^*. The mapping $h \circ f$ is a *valuation* of a parametric word into Σ^*, and f is its valuation to the set Δ^*.

We define the *length* of a parametric word: the length of 1 is zero; if $a \in \Delta$, then the length of a is one; if $\alpha, \beta \in \mathcal{P}(\Delta, \Lambda)$, then the length of $\alpha\beta$ is the sum of lengths of α and β; if $\alpha \in \mathcal{P}(\Delta, \Lambda) \smallsetminus \{1\}$ and $i \in \Lambda$, then the length of α^i is the length of α plus one.

Next we define the *height* of a parametric word: if $a \in \Delta \cup \{1\}$, then the height of a is zero; if $\alpha, \beta \in \mathcal{P}(\Delta, \Lambda)$, then the height of $\alpha\beta$ is the maximum of heights of α and β; if $\alpha \in \mathcal{P}(\Delta, \Lambda) \smallsetminus \{1\}$ and $i \in \Lambda$, then the height of α^i is the height of α plus one. Parametric words of height zero can be considered to be words of Δ^*.

A *linear Diophantine relation* R is a disjunction of systems of linear Diophantine equations with lower bounds for the unknowns. For example,

$$((x + y - z = 0) \wedge (x \geq 2)) \vee ((x + y = 3) \wedge (x + z = 4))$$

is a linear Diophantine relation over the unknowns x, y and z. We are only interested in the nonnegative values of the unknowns. If $\Lambda = \{i_1, \ldots, i_k\}$, f is a function $\Lambda \to \mathbb{N}_0$, and $f(i_1), \ldots, f(i_k)$ satisfy R, then the notation $f \in R$ can be used.

Let S be a set of morphisms $\Xi^* \to \Sigma^*$, $\Lambda = \{i_1, \ldots, i_k\}$, h_j a morphism from the monoid Ξ^* to parametric words and R_j a linear Diophantine relation, when $j = 1, \ldots, m$. The set $\{(h_j, R_j) : 1 \leq j \leq m\}$ is a *parametric representation* of S, if

$$S = \{h \circ f \circ h_j : 1 \leq j \leq m, f \in R_j\},$$

where $h \circ f$ runs over all valuations to Σ^*. The linear Diophantine relations are not strictly necessary, but they make some proofs easier. A set can be *parameterized*, if it has a parametric representation. The *length* of the parametric representation is the sum of the lengths of all $h_j(x)$, where $j = 1, \ldots, m$ and $x \in \Xi$.

It follows immediately that if two sets can be parameterized, then also their union can be parameterized.

Let $S, S_1, \ldots, S_n$ be sets of morphisms $\Xi^* \to \Sigma^*$. The set S can be *parameterized in terms of the sets* $S_1, \ldots, S_n$, if there exists such morphisms $h_1, \ldots, h_n$ from Ξ^* to $\mathcal{P}(\Xi, \Lambda)$ that

$$S = \{g \circ f \circ h_j : 1 \leq j \leq n, g \in S_j\},$$

where f runs over functions $\Lambda \to \mathbb{N}_0$.

Again it is a direct consequence of the definitions that the parameterizability is preserved in compositions. Namely, if S can be parameterized in terms of the sets $S_1, \ldots, S_n$ and every S_i can be parameterized in terms of the sets $S_{i1}, \ldots, S_{in_i}$, then S can be parameterized in terms of the sets S_{ij}.

We conclude these definitions by saying that solutions of an equation can be *parameterized*, if the set of its all solutions can be parameterized. A parametric representation of this set is a *parametric solution* of the equation.

These definitions can be generalized in an obvious way for systems of equations. Theorems 2.1 and 2.2 and Lemmas 2.6 – 2.10 give parametric solutions for some equations. For example, the conjugate equation $xz = zy$ has a parametric solution $\{(h_1, R), (h_2, R)\}$, where $\Delta = \{p, q\}$, $\Lambda = \{i\}$, $h_1(x) = pq$, $h_1(y) = qp$, $h_1(z) = p(qp)^i$, $h_2(x) = h_2(y) = 1$, $h_2(z) = p$ and R is the trivial relation satisfied by all functions $f : \Lambda \to \mathbb{N}_0$.

The following theorem states that the basic tool in solving equations, namely the cancellation of the first variable, preserves the parameterizability of solutions.

Theorem 3.1. *Let $U, V \in \Xi^*$, $x, y \in \Xi$ and $x \neq y$. Let $h : \Xi^* \to \Xi^*$ be the morphism $x \mapsto yx$. If the equation $xh(U) = h(V)$ has a parametric solution, then so does the equation $xU \rightrightarrows yV$.*

Proof. If the equation $xh(U) = h(V)$ has a parametric solution

$$\{(h_j, R_j) : 1 \leq j \leq m\},$$

then the equation $xU \rightrightarrows yV$ has the parametric solution

$$\{(h_j \circ h, R_j) : 1 \leq j \leq m\}. \qquad \square$$

4 Remarks about parametric solutions

A parametric solution was defined as a set $\{(h_j, R_j) : 1 \leq j \leq m\}$. This solution can be written less formally as

$$\begin{aligned} &x = h_1(x), \;\; y = h_1(y), \;\; z = h_1(z), \;\; R_1 \;\; \text{or} \\ &\;\vdots \\ &x = h_m(x), \; y = h_m(y), \; z = h_m(z), \; R_m, \end{aligned}$$

if the unknowns are x, y, z. Actually, only one pair (h, R) is needed. For example, if we have a parametric solution

$$x = \alpha_1,\ y = \beta_1,\ z = \gamma_1 \qquad \text{or} \qquad x = \alpha_2,\ y = \beta_2,\ z = \gamma_2,$$

we can replace it with

$$x = \alpha_1^i \alpha_2^j,\ y = \beta_1^i \beta_2^j,\ z = \gamma_1^i \gamma_2^j, \quad i + j = 1,$$

where i and j are new parameters.

On the other hand, the linear Diophantine relations are not necessary either, if we again allow many morphisms. We can get rid of the relations by replacing every pair (h, R) with several morphisms h. This follows from article [4]. We will not give the proof here, but present an example.

Example 4.1. Consider the periodic solutions of the equation $x^n = yz$. They are

$$x = t^i,\ y = t^j,\ z = t^k, \quad ni = j + k.$$

We can replace j with $nj' + b$ and k with $nk' + c$, where $0 \leq b, c < n$. Then $i = j' + k' + (b + c)/n$. Only those pairs (b, c) for which $b + c$ is divisible by n are possible. Thus we get a representation

$$\begin{array}{llll}
x = t^{j'+k'}, & y = t^{nj'}, & z = t^{nk'} & \text{or} \\
x = t^{j'+k'+1}, & y = t^{nj'+1}, & z = t^{nk'+n-1} & \text{or} \\
x = t^{j'+k'+1}, & y = t^{nj'+2}, & z = t^{nk'+n-2} & \text{or} \\
\vdots & & & \\
x = t^{j'+k'+1}, & y = t^{nj'+n-1}, & z = t^{nk'+1}, &
\end{array}$$

where the parameters j', k' can now have any nonnegative values.

The periodic solutions of an equation on three unknowns can be represented with just one morphism and without any Diophantine relations.

Theorem 4.2. *The periodic solutions of an equation $U = V$ have a representation*

$$x = t^p,\ y = t^q,\ z = t^r,$$

where p, q, r are polynomials of numerical parameters

Proof. All periodic solutions of an equation $U = V$ are of the form $x = t^i, y = t^j, z = t^k$, and the exponents i, j, k must satisfy the constraint $|U|_x i + |U|_y j + |U|_z k = |V|_x i + |V|_y j + |V|_z k$. By permuting the unknowns we can assume that this can be written as $ai = bj + ck$, where a, b, c are nonnegative integers and $a > 0$ (except for some trivial cases). Let $(b_n, c_n)_{n=1}^N$ be a sequence of all solutions $(u, v) \in \{0, \ldots, a-1\}^2$ of the congruence $bu + cv \equiv 0$

(mod a). For each pair (b_n, c_n), we could define a corresponding morphism, and these would together form a parametric representation. This was done in Example 4.1. However, we can also replace the exponents i, j, k with the polynomials

$$p = bj_0 + ck_0 + \sum_{n=1}^{N} \frac{bb_n + cc_n}{a} i_n,$$

$$q = aj_0 + \sum_{n=1}^{N} b_n i_n,$$

$$r = ak_0 + \sum_{n=1}^{N} c_n i_n,$$

where $j_0, k_0, i_1, \ldots, i_n$ are new parameters, which can now have any values. Thus the solutions can be represented with one parametric word for each unknown. The parametric representation has at most quadratic length with respect to the length of the equation. □

Theorem 4.2 does not hold, if instead of periodic solutions we consider all solutions. Indeed, we will show that a parametric solution for the equation $xyxzyz = zxzyxy$ consists of at least three morphisms, if linear Diophantine relations are not allowed. First we determine the solutions of this equation.

Lemma 4.3. *The nonperiodic solutions of the equation $xyxzyz = zxzyxy$ are $x = p, y = q, z = 1$ or $x = p, y = q, z = pq$, where $p, q \in \Sigma^*$ and $pq \neq qp$.*

Proof. The claimed solutions satisfy the equation and are nonperiodic. If h is a nonperiodic solution, then, by Lemma 2.6,

$$h(xy) = (uv)^i u,\ h(xzy) = v(uv)^j,\ h(z) = (uv)^k u,$$

where uv is primitive. If $|h(x)| \geq |uv|$, then uv and vu are both prefixes of $h(x)$, $uv = vu$, and the solution is periodic. Thus $|h(x)| < |uv|$. Symmetrically $|h(y)| < |uv|$, so $i = 0$ or $i = 1$. If $k > 0$ and $h(x) \neq v$, then uv is a factor of $uvuv$ in a nontrivial way, which contradicts the primitivity of uv. If $h(x) = v$, then $h(y) = v(uv)^l$ for some l, u and v satisfy a nontrivial relation and the solutions is periodic. Thus $k = 0$ and $h(z) = u$. If $i = 0$, then $h(xy) = h(z)$. If $i = 1$, then either $h(z) = 1$ or $j = 1$ or $j = 2$ or $v = 1$. If $j = 1$, then $|v| = 2|u|$, u is a prefix and a suffix of v, and u and v commute. If $j = 2$, then $|u| = 2|v|$, v is a prefix and a suffix of u, and u and v commute. If $v = 1$, then $|h(x)|, |h(y)| < |uv|$ is not possible. This proves that the claimed solutions are all nonperiodic solutions. If p and q would commute, the solution would be periodic. □

The number of occurrences of a letter $a \in \Sigma$ in a parametric word after giving values for the parameters can be viewed as a polynomial, where the variables are the numerical parameters $i \in \Lambda$ and new variables p_a for every $p \in \Delta$ and $a \in \Sigma$. Formally, we define the polynomial $|\alpha|_a$ as follows:

(i) if $p \in \Delta$, then $|(p)|_a = p_a$,

(ii) if α and β are parametric words, then $|(\alpha\beta)|_a = |\alpha|_a + |\beta|_a$,

(iii) if α is a parametric word and $i \in \Lambda$, then $|(\alpha^i)|_a = |\alpha|_a i$.

For example, $|(p^i q)^j p|_a = p_a ij + q_a j + p_a$. If φ is a valuation, then $|\varphi(\alpha)|_a$ is the value taken by the polynomial $|\alpha|_a$, when i is given the value $\varphi(i)$ (for all $i \in \Lambda$) and p_a is given the value $|\varphi(p)|_a$ (for all $p \in \Delta$).

Theorem 4.4. *The equation $xyxzyz = zxzyxy$ does not have a parametric solution of the form*

$$x = \alpha_1,\ y = \beta_1,\ z = \gamma_1 \qquad \textit{or} \qquad x = \alpha_2,\ y = \beta_2,\ z = \gamma_2.$$

Proof. The following are examples of the solutions of the equation:

$$x = a, y = b, z = 1;\ x = a, y = b, z = ab;\ x = a, y = a, z = a. \tag{1}$$

We will show that if α, β, γ are parametric words such that

$$x = \varphi(\alpha),\ y = \varphi(\beta),\ z = \varphi(\gamma) \tag{2}$$

is a solution of the equation for all valuations φ, then we can get at most one of the three above-mentioned solutions from these parametric words.

Consider the three polynomials $|\gamma|_a$, $|\alpha\beta|_a - |\gamma|_a$, and $|\alpha|_a|\beta|_b - |\alpha|_b|\beta|_a$. The values taken by them are

$$|z|_a,\ |xy|_a - |z|_a,\ |x|_a|y|_b - |x|_b|y|_a, \tag{3}$$

where (x, y, z) can be any solution of the equation $xyxzyz = zxzyxy$. If $z = 1$, the first value is zero, if $xy = z$, the second value is zero, and if x and y are powers of a common word, the third value is zero. By Lemma (4.3), one of these holds for any solution, so the product of the three polynomials is zero. But this means that one of the polynomials must be zero. For the first solution in (1) only the first value in (3) is zero, for the second solution only the second value is zero, and for the third solution only the third value is zero. Thus only one of these solutions can be obtained from (2). □

5 Exponential equations

Let α and β be parametric words. The pair (α, β) can be viewed as an equation, referred to as an *exponential equation.* The *height* of this equation is the height of $\alpha\beta$. The solutions of this equation are the functions f :

$\Lambda \to \mathbb{N}_0$ that satisfy $f(\alpha) = f(\beta)$. If the numerical parameters are in order $i_1, \ldots, i_n$, then we can talk of the solution $(f(i_1), \ldots, f(i_n))$ or of the solution $i_1 = f(i_1), \ldots, i_n = f(i_n)$.

If we know some parametric words, which give all solutions of an equation, but which also give some extra solutions, then often the right solutions can be picked by adding some constraints for the numerical parameters. These constraints can be found by exponential equations, and the following theorems prove that they are in our cases equivalent with linear Diophantine relations.

We will transform words into polynomials when studying exponential equations. Alphabet Ξ with k letters can be thought to be the set $\{1, \ldots, k\}$. Then we can define the functions $\lambda, \mu : \Xi^* \to \mathbb{Z}[X]$:

$$\lambda(w) = X^{m+1}, \qquad \mu(w) = a_m X^m + \cdots + a_1 X + a_0$$

for all $w = a_m \ldots a_0 \in \Xi^*$. This corresponds to the n-adic representation of a number when $n > k$: the word w represents the number obtained by giving the value n for X in the polynomial $\mu(w)$. In particular, if $u, v \in \Xi^*$, then

$$\mu(uv) = \mu(u)\lambda(v) + \mu(v).$$

Theorem 5.1. *Let E be an exponential equation of height one. There exists a linear Diophantine relation R such that a function $f : \Lambda \to \mathbb{N}_0$ is a solution of E if and only if $f \in R$.*

Proof. Let E be the equation $\alpha = \beta$, where

$$\alpha = s_0 t_1^{i_1} s_1 \ldots t_m^{i_m} s_m, \qquad \beta = u_0 v_1^{j_1} u_1 \ldots v_n^{j_n} u_n,$$

$s_0, \ldots, s_m$, $t_1, \ldots, t_m$, $u_0, \ldots, u_n$, $v_1, \ldots, v_n \in \Delta^*$ and $i_1, \ldots, i_m, j_1, \ldots, j_n \in \Lambda$. Function f is a solution if and only if $\mu(f(\alpha)) = \mu(f(\beta))$. Now $\mu(f(\alpha))$ is

$$\begin{aligned}
&\mu(s_0)\lambda(t_1)^{f(i_1)}\lambda(s_1) \ldots \lambda(t_m)^{f(i_m)}\lambda(s_m) \\
&+\frac{\mu(t_1)(\lambda(t_1)^{f(i_1)} - 1)}{\lambda(t_1) - 1} \cdot \lambda(s_1) \ldots \lambda(t_m)^{f(i_m)}\lambda(s_m) \\
&+\cdots+ \frac{\mu(t_m)(\lambda(t_m)^{f(i_m)} - 1)}{\lambda(t_m) - 1} \cdot \lambda(s_m) + \mu(s_m),
\end{aligned}$$

which can be rewritten as

$$\begin{aligned}
&\left(\mu(s_0) + \frac{\mu(t_1)}{\lambda(t_1) - 1}\right) \lambda(s_1 \ldots s_m)\lambda(t_1^{f(i_1)} \ldots t_m^{f(i_m)}) \\
&+\sum_{k=2}^{m} \left(\mu(s_{k-1}) + \frac{\mu(t_k)}{\lambda(t_k) - 1} - \frac{\mu(t_{k-1})\lambda(s_{k-1})}{\lambda(t_{k-1}) - 1}\right) \lambda(s_k \ldots s_m)\lambda(t_k^{f(i_k)} \ldots t_m^{f(i_m)}) \\
&+\mu(s_m),
\end{aligned}$$

and $\mu(f(\beta))$ is of the corresponding form. Thus the equation

$$\begin{aligned}&(\lambda(t_1)-1)\dots(\lambda(t_m)-1)(\lambda(v_1)-1)\dots(\lambda(v_n)-1)\mu(f(\alpha))\\=&(\lambda(t_1)-1)\dots(\lambda(t_m)-1)(\lambda(v_1)-1)\dots(\lambda(v_n)-1)\mu(f(\beta))\end{aligned}$$

can be rewritten as

$$X^{P_1}+\dots+X^{P_M}=X^{Q_1}+\dots+X^{Q_N}, \tag{4}$$

where every P_k and Q_k is a linear polynomial with unknowns $f(i_l)$, $f(j_l)$. Equation (4) can be satisfied only if $M=N$. Then it is equivalent with the formula

$$\bigvee_{\pi}\left((P_1=Q_{\pi(1)})\wedge\dots\wedge(P_N=Q_{\pi(N)})\right),$$

where π runs over all permutations of N elements. Hence the claim follows. □

In some cases Theorem 5.1 can be generalized for exponential equations of height two.

Theorem 5.2. *Let $\Lambda=\{i,j\}$. Let $s_0,\dots,s_m$, $t_1,\dots,t_m$, $u_0,\dots,u_n$ and $v_1,\dots,v_n$ be parametric words of height at most one, with no occurrences of parameter j. Assume that i occurs at least in the words $t_1,\dots,t_m$ and $v_1,\dots,v_n$. Let $\alpha=s_0t_1^js_1\dots t_m^js_m$ and $\beta=u_0v_1^ju_1\dots v_n^ju_n$. Now there exists a linear Diophantine relation R such that a function $f:\Lambda\to\mathbb{N}_0$ is a solution of the exponential equations $E:\alpha=\beta$ if and only if $f\in R$.*

Proof. Like in the proof of Theorem 5.1, the equation $\mu(f(\alpha))=\mu(f(\beta))$ can be turned into the equation

$$X^{P_1}+\dots+X^{P_M}=X^{Q_1}+\dots+X^{Q_N}, \tag{5}$$

where every P_k and Q_k is of the form $af(i)f(j)+bf(i)+cf(j)+d$ for some integers a,b,c,d. Equation (5) can be satisfied only if $M=N$. Then it is equivalent with the formula

$$\bigvee_{\pi}\left((P_1=Q_{\pi(1)})\wedge\dots\wedge(P_N=Q_{\pi(N)})\right), \tag{6}$$

where π runs over all permutations of N elements.

Consider now the equations $P_k=Q_{\pi(k)}$. They are of the form $af(i)f(j)+bf(i)+cf(j)+d=0$. If $a=0$, this is a linear equation. If $a\neq0$, then $f(i)\leq|b+c+d|$ or $f(j)\leq|b+c+d|$, because otherwise $|af(i)f(j)|>|bf(i)+cf(j)+d|$. If $f(i)$ or $f(j)$ is fixed, the equation turns into a linear equation. Hence the claim follows. □

The parametric words in the next theorem come from Lemma 2.9. Exponential equations formed by the parametric words in the other Lemmas 2.6 – 2.10 are handled by Theorems 5.1 and 5.2, but Lemma 2.9 requires this special treatment.

Theorem 5.3. *Let $\Delta = \{p, q\}$, $\Lambda = \{i, j, k\}$ and $a \geq 2$. Let $\alpha = (pq^a)^i p$, $\beta = q$, $\gamma = (pq^a)^j p$, or*

$$\begin{cases} \alpha &= qp((pq)^{k+1}p)^{a-2}pq(((pq)^{k+1}p)^{a-1}pq)^i, \\ \beta &= (pq)^{k+1}p, \\ \gamma &= qp((pq)^{k+1}p)^{a-2}pq(((pq)^{k+1}p)^{a-1}pq)^j. \end{cases}$$

Let $A, B \in \{x, y, z\}^*$ and let h be the morphism mapping $x \mapsto \alpha, y \mapsto \beta, z \mapsto \gamma$. Now there exists a linear Diophantine relation R such that a function $f : \Lambda \to \mathbb{N}_0$ is a solution of the exponential equation $E : h(A) = h(B)$ if and only if $f \in R$.

Proof. In the first case E is of height one and the claim follows from Theorem 5.1. Consider the second case. It can be assumed that A and B begin with x and z. Consider the equivalent equation $y^a A = y^a B$. Let the maximal prefixes of the left- and right-hand sides of the form $y^a t_1 \dots y^a t_n$, where $t_l \in \{x, z\}$, be U and V. Now the equation is $UA_1 = VB_1$. Let $T = ((pq)^{k+1}p)^{a-1}pq$. Now the parametric words $h(U)$ and $h(V)$ are of the form $T^{P(i,j,k)}$ and $T^{Q(i,j,k)}$, where P and Q are linear polynomials.

We show that if f is a solution of $h(A) = h(B)$, then

$$P(f(i), f(j), f(k)) = Q(f(i), f(j), f(k)). \tag{7}$$

Assume that $P(f(i), f(j), f(k)) > Q(f(i), f(j), f(k))$ (the other direction is symmetric). Then

$$f(T^c h(A_1)) = f(h(B_1)), \tag{8}$$

where $c \geq 1$. Because $\beta^{a-1}pq \leq T$, it must be $\beta^{a-1}pq \leq h(B_1)$. It follows that $B_1 = y^a B_2$. Now (8) can be reduced to $f(T^{c-1}h(A_1)) = f((pq)^k ph(B_2))$, and either $c > 1$ or $y \leq A_1$. In both cases $(pq)^{k+1}p \leq T^{c-1}h(A_1)$, and thus $pq \leq h(B_2)$, which is possible only if B_2 begins with x or z. But then B_1 begins with $y^a x$ or $y^a z$, which is against the maximality assumption of V. Equation (7) has been shown.

Now the equation $h(UA_1) = h(VB_1)$ is equivalent with the pair of equations $h(U) = h(V)$, $h(A_1) = h(B_1)$. The former is equivalent with the linear Diophantine equation (7). The latter is shorter than the original equation and the theorem can be proved inductively. □

We must examine some exponential equations of height one more closely.

Theorem 5.4. *Let $\Lambda = \{i\}$. Let $E : s_0 t^i s_1 \dots t^i s_m = u_0 t^i u_1 \dots t^i u_n$ be an exponential equation of height one, $s_0, \dots, s_m$, $u_0, \dots, u_n$, $t \in \Delta^*$ and*

$$|s_0 \dots s_m u_0 \dots u_n| < S|t|.$$

There exists a number $T = O(S)$ such that f is a solution of E for every $f(i) \geq T$, or f is not a solution for any $f(i) \geq T$.

Proof. Like in the proof of Theorem 5.1, we get the equation (4). The polynomials P_j are of the form $af(i) + b$. On the other hand, they are exponents of terms of products of $\lambda(s_k)$, $\mu(s_k)$, $\lambda(t)$, $\lambda(t)^{f(i)}$, $\mu(t)$. Each of these polynomials can occur in the products at most once. Thus $|t|$ divides a and $b \leq 2|s_0 \dots s_m t|$. Similar conditions hold for coefficients of Q_j. The equation $P_j = Q_{\pi(j)}$ can be written as $Af(i) = B$, where $A = 0$ or $|A| \geq |t|$ and $|B| \leq 2|s_0 \dots s_m u_0 \dots u_n t^2|$. Now there exists the required number T such that the equations $P_j = Q_{\pi(j)}$ have no solutions $f(i) \geq T$, unless the equations are trivial. This proves the claim. □

6 Basic equations

From now on we only consider equations with three unknowns. The alphabet of unknowns is $\Xi = \{x, y, z\}$. The left-hand side of an equation can be assumed to begin with x. We can also assume that x occurs on the right-hand side, but not as the first letter.

Periodic solutions and solutions, where some unknown has the value 1, are called *trivial*. These are easy to parameterize by Theorem 2.1.

An equation is a *basic equation*, if it is a trivial equation $U = U$, where $U \in \Xi^*$, if it has only trivial solutions, or if it is of one of the following forms, where $a, b \geq 1$, $c \geq 2$ and $t \in \{x, z\}$:

B1. $x^a y \dots = y^b x \dots$

B2. $x^2 \dots \rightrightarrows y^a x \dots$

B3. $xyt \dots \rightrightarrows zxy \dots$

B4. $xyt \dots \rightrightarrows zyx \dots$

B5. $xyz \dots = zxy \dots$

B6. $xyz \dots = zyx \dots$

B7. $xy^c z \dots = zy^c x \dots$

B8. $xyt \dots \rightrightarrows z^a xy \dots$

B9. $xyxz \dots \rightrightarrows zx^2 y \dots$

The parameterizability of basic equations is easy to prove with the help of previous lemmas and theorems.

Lemma 6.1. *Let $S, T, U, V \in \Xi^*$. Assume that the equation $S = T$ has a parametric solution $\{(h_j, R_j) : j = 1, \dots, m\}$, where $\Delta = \{p, q\}$ and $\Lambda = \{i_1, \dots, i_k\}$. Assume that the exponential equations $h_j(U) = h_j(V)$ are equivalent with linear Diophantine relations. Then the pair of equations $S = T, U = V$ has a parametric solution.*

Proof. Let $h_j(U) = h_j(V)$ be equivalent with the linear Diophantine relation R'_j. We show that the solutions of the equation have a parametric representation

$$\{(h_j, R_j \cap R'_j) : j = 1, \dots, m\} \cup A,$$

where A is a parametric representation of the periodic solutions

If $\varphi = h \circ f$ is a valuation in $R_j \cap R'_j$, then $\varphi \circ h_j$ is a solution of $S = T$ and f is a solution of $h_j(U) = h_j(V)$. Now $\varphi \circ h_j$ is also a solution of $U = V$.

If g is a nonperiodic solution of the pair of equations $S = T, U = V$, then $g = \varphi \circ h_j$ for some number j and valuation $\varphi = h \circ f$ satisfying $f \in R_j$. It needs to be shown that f is a solution of $h_j(U) = h_j(V)$. The morphism h is a solution of the equation $f(h_j(U)) = f(h_j(V))$, which has two unknowns. But h cannot be periodic, because g is not periodic. Thus $f(h_j(U))$ and $f(h_j(V))$ must be the same word □

Theorem 6.2. *Every basic equation has a parametric solution of bounded length.*

Proof. For equations $U = U$ and for equations with only trivial solutions the claim is clear. We prove it for equations B1 − B9. First we reduce equations to other equations by Theorem 3.1. The equation B2 is reduced by the substitution $x \mapsto yx$ to the equation $xyx \dots = y^a x \dots$, which is of the form B1. The equations B3 and B4 are reduced by the substitution $x \mapsto zx$ to the equations $xyz \dots = zxy \dots$ and $xyz \dots = yzx \dots$, which are of the form B5. The equation B8 is reduced by the substitution $x \mapsto zx$ to the equation $xyzA = z^a xyB$ for some $A, B \in \Xi^*$. By Lemma 2.11, this is equivalent with the equation $xyzxyzA = zxyz^a xyB$, which is of the form B5. Therefore only the cases B1, B5, B6, B7 and B9 have to be considered.

Consider the equations B1, B5, B6, B7 and B9 as the equation $U = V$ of Lemma 6.1, and the equations $xy = yx$, $xyz = zxy$, $xyz = zyx$, $xy^c z = zy^c x$ and $xyxz \rightrightarrows zx^2 y$ as the equation $S = T$. For B1 this can be done by Lemma 2.11, otherwise by a length argument. By Lemmas 2.7, 2.9 and 2.10, the solutions of these equations are obtained from certain parametric words over word parameters p, q and numerical parameters i, j, k. For equations B1, B5 and B6, the exponential equation of Lemma 6.1 will be of height one and Theorem 5.1 can be used. For B9, Theorem 5.2 can be used, and for B7, Theorem 5.3 can be used. So the exponential equation is in all cases equivalent with a linear Diophantine relation and the claim follows from Lemma 6.1. □

7 Images and θ-images

In this section we define images and θ-images of equations and prove some results about them. If h is a solution of the equation $xU \rightrightarrows yV$, then $h(y) \leq h(x)$. This fact was already behind Theorem 3.1. This will be generalized.

Let $t_1, \dots, t_n \in \{y, z\}$ and $V = t_1 \dots t_n$. Let $t_{n+1} = t_1$. If a morphism h is a solution of the equation $E : xU \rightrightarrows VxW$, then

$$h(x) = h(V^k t_1 \dots t_i)u \tag{9}$$

for some numbers k, i and word u satisfying $k \geq 0$, $0 < i \leq n$ and $h(t_{i+1}) \not\leq u$.

On the other hand, a morphism h satisfying (9) is a solution of E if and only if $uh(U) = h(t_{i+1} \dots t_n t_1 \dots t_i)uh(W)$. We can write $h = g \circ f$, where f is the morphism $x \mapsto V^k t_1 \dots t_i x$ and g is the morphism for which $g(x) = u$, $g(y) = h(y)$ and $g(z) = h(z)$. Now h is a solution of E if and only if g is a solution of

$$xf(U) \leftleftarrows f(t_{i+1} \dots t_n t_1 \dots t_i)xf(W). \tag{10}$$

An *image* of an equation $xU(x, y, z) \rightrightarrows V(y, z)xW(x, y, z)$ under the morphism $x \mapsto V^k Px$, where $k \geq 0$, $V = PQ$ and $Q \neq 1$, is

$$xU(V^k Px, y, z) \leftleftarrows QPxW(V^k Px, y, z).$$

If V contains only one of y, z or if $P = 1$, the image is *degenerated*.

The m first images of an equation of length n are of length $O(mn)$. Images are needed in the most important reduction steps used in the proof of parameterizability of equations with three unknowns. The solutions of an equation are easily obtained from the solutions of its images, so it is enough to consider them. There are infinitely many images, but a finite number is enough, if one of them is turned from a one-sided equation to an ordinary equation.

Equation E is *reduced to the equations* $E_1, \dots, E_n$ *by an n-tuple of substitutions*, if E is of the form $xU(x, y, z) \rightrightarrows t_1 \dots t_k xV(x, y, z)$, where $1 \leq n \leq k$ and $t_1, \dots, t_k \in \{y, z\}$, equation E_i is

$$xU(t_1 \dots t_i x, y, z) \leftleftarrows t_{i+1} \dots t_k t_1 \dots t_i xV(t_1 \dots t_i x, y, z),$$

when $1 \leq i < n$, and equation E_n is

$$xU(t_1 \dots t_n x, y, z) = t_{n+1} \dots t_k t_1 \dots t_n xV(t_1 \dots t_n x, y, z).$$

By the above, Theorem 3.1 can be generalized.

Theorem 7.1. *Let E be an equation of length n. If E is reduced to the equations $E_1, \dots, E_m$ by an m-tuple of substitutions, and if $E_1, \dots, E_m$ have parametric solutions of length at most c, then E has a parametric solution of length $O(mn)c$.*

Reductions with n-tuples of substitutions are not sufficient. Other ways to restrict the considerations to a finite number of images are needed.

Equation

$$xU(x, y, z) \rightrightarrows V(y, z)xW(x, y, z)$$

is of *type I*, if both unknowns y, z occur in V. Equation

$$xy^bU(x, y, z) \rightrightarrows z^cxV(x, z)yW(x, y, z),$$

where $b, c \geq 1$, is of *type II*, if $b > 1$ or $V \neq 1$.

Theorem 7.2. *The solutions of an equation of type I of length n can be parameterized in terms of the solutions of $O(n^2)$ of its images of length $O(n^3)$.*

Proof. Consider the equation $E : xU(x, y, z) \rightrightarrows V(y, z)xW(x, y, z)$, where both y and z occur in V, and its images

$$E_{P,i} : xU(V^iPx, y, z) \leftleftarrows QPxW(V^iPx, y, z), \tag{11}$$

where $i \geq 0$, $V = PQ$ and $Q \neq 1$. We show that there exists a number T such that if P and Q are fixed, then the equations (11) are equivalent for all $i \geq T$.

Let h be a solution of $E_{P,i}$. Then theorem 5.4 can be used for the exponential equation

$$h(x)U(h(V)^ih(Px), h(y), h(z)) = h(QPx)W(h(V)^ih(Px), h(y), h(z)),$$

where i is considered to be unknown. The bound S in the theorem does not depend on h and is of size $O(n)$, because both y and z occur in V and $h(x) \leq h(y)$ or $h(x) \leq h(z)$. So there exists a number $T = O(n)$ such that h is a solution for all $i \geq T$ or for no $i \geq T$. Thus the equations $E_{P,T}, E_{P,T+1}, E_{P,T+2}, \dots$ are equivalent if P is fixed.

Now the images of this theorem can be taken to be $E_{P,j}$, where $P < V$ and $j \leq T$. The solutions of E are $g \circ f \circ h'$, where either h' is the morphism $x \mapsto V^jPx$, g runs over the solutions of the corresponding image $E_{P,j}$, f does nothing and $j < T$, or h' is the morphism $x \mapsto V^{T+i}Px$, i is a numerical parameter, g runs over the solutions of $E_{P,T}$ and f gives values for i. Because $T = O(n)$ and $|V| = O(n)$, there are $O(n^2)$ of these images, and because $|V^jPx| = O(n^2)$, they are of length $O(n^3)$. □

Like in the proof of Theorem 7.2, we will often use a variation of the following reasoning: if the images of E are $E_1, E_2, \dots,$ and if $E_m, E_{m+1}, \dots$ are equivalent, then the solutions of E can be parameterized in terms of the solutions of $E_1, \dots, E_m$. It is also easy to see that if each of these images has a parametric solution of length at most c, then E has a parametric solution of length $O(m^2)c$. This also holds for θ-images, which are defined later.

Consider an equation of type II

$$xy^b A(x,y,z) \rightrightarrows z^c x B(x,z) y C(x,y,z), \tag{12}$$

where $b, c \geq 1$ and $b > 1$ or $B \neq 1$. Its images are degenerated and of the form

$$xy^b A(z^i x,y,z) \leftleftarrows z^c x B(z^i x,z) y C(z^i x,y,z). \tag{13}$$

Theorem 7.2 holds for some of the equations (12).

Theorem 7.3. *If $B = z^d$, $d \geq 1$, then the solutions of* (12) *can be parameterized in terms of the solutions of $O(n^2)$ of its images of length $O(n^3)$.*

Proof. Equation (13) is reduced by the mapping $z \mapsto xz$ to the equation

$$y^b A((xz)^i x, y, xz) = (zx)^c (xz)^d y C((xz)^i x, y, xz). \tag{14}$$

Let h be its solution. Let $D = h((zx)^c(xz)^d)$ and $h(y) = D^j Y$, where $Y < D$. Then we get the equality

$$Y(D^jY)^{b-1} A(h((xz)^i x), D^j Y, h(xz)) = DYC(h((xz)^i x), D^j Y, h(xz)). \tag{15}$$

On the other hand, if (15) holds, then h is a solution of (14) and it gives a solution of (13). It needs to be shown that there exists a bound $T = O(n^2)$, which does not depend on h, such that if (15) holds for some $i \geq T$, then it holds for all $i \geq T$. Then the images (13) with $i \leq T$ are sufficient, like in the proof of Theorem 7.2.

If $j < c + d + 1 = O(n)$ is fixed, then (15) can be considered to be an exponential equation with unknown i, and Theorem 5.4 can be used. The bound $S = O(n^2)$ not depending on h exists, because $|Y| < (d + c)|h(xz)|$.

For the rest of the proof we consider the case $j \geq c+d+1$. Let t and v be the primitive roots of $h(xz) = t^{a_1}$ and $D = v^{a_2}$. If these have equal length, then $t = v$ and $h(xz) = h(zx)$, which leads to a periodic solution. Assume that $|t| \neq |v|$. In (15), starting from the left, move the powers of t and v as far to the left as possible by changing them to their suitable conjugates, and then combine as much as possible from the right to these powers. This may require replacing i and j with $i' = i - b_1$ and $j' = j - b_2$ for some b_1, b_2. By Theorem 2.3, powers of conjugates of $h(xz)$ and D can overlap for at most $|h(xz)D|$ letters, so we can select $b_1, b_2 \leq c+d+1$, and i' and j' can be used if i and j are large enough. This way (15) can be written as

$$s_0 t_1^{p_1} s_1 \dots t_m^{p_m} s_m = u_0 v_1^{q_1} u_1 \dots v_n^{q_n} u_n, \tag{16}$$

where $s_0, \dots, s_m$, $u_0, \dots, u_n \in \Delta^*$, every t_k and v_k is either a conjugate of t or a conjugate of v, and every p_k and q_k is a polynomial of first degree with unknowns i', j'. The coefficients in these polynomials cannot be negative. Also the last letter of t_k is different from the last letter of s_{k-1}, and $t_k \not\leq s_k t_{k+1}^a$ for all a. The same holds for words u_k and v_k and for polynomials q_k. Because the words $h(xz)$ and D consist of $h(x)$ and $h(z)$ and $Y < D$, there exists a bound $S = O(n^2)$ such that

$$|s_0 \dots s_m u_0 \dots u_n (tv)^2| < S|t^a| \qquad \text{and} \qquad b < a_1 S \tag{17}$$

when $ai' + b$ is in $\{p_1, \dots, p_m, q_1, \dots, q_n\}$. The same holds with v in place of t, j' in place of i', and a_2 in place of a_1.

We prove by induction with respect to $m + n$ that if (16) has a solution f with $f(i'), f(j') \geq S + 2$, then $s_k = u_k$, $t_k = v_k$ and $f(p_k) = f(q_k)$ for all k. If $m + n = 0$, then the claim is clear (although the equation is of height zero). If $m = 0, n > 0$, or other way around, then the exponent occurring in the equation can get only small values. Assume that $m, n > 0$. From (17) it follows that $|t_k^{f(p_k)}| > |s_0 \dots s_m u_0 \dots u_n (tv)^2|$ for all k, and similarly for v_k. It can be assumed that $u_0 \leq s_0$, so $v_1 = BA$ and $s_0 = u_0 (BA)^k B$ for some A, B. Now $|v_1^{f(q_1)}| \geq |s_0| + |t_1^2|$ and $|t_1^{f(p_1)}| \geq |(AB)^2|$. Thus the powers of t_1 and AB have a common prefix of length $|t_1 AB|$ and, by Theorem 2.3, $t_1 = AB$. Now $t_1 = v_1$, $B = 1$, $k = 0$ and $s_0 = u_0$. We prove that $f(p_1) = f(q_1)$. From $f(p_1) > f(q_1)$ it would follow that $v_1 = t_1 \leq u_1 v_2^{f(q_2)}$ (or $v_1 = t_1 \leq u_1$, if $n = 1$), which is a contradiction. The case $f(p_1) < f(q_1)$ is symmetric. It follows inductively that $s_k = u_k$, $t_k = v_k$ and $f(p_k) = f(q_k)$ for all k.

Now it can be seen that $p_k - q_k$ contains only one of i' and j', because $t_k = v_k$, and the coefficient of i' or j' is divisible by a_1 or a_2. So if $f(p_k) = f(q_k)$ and $f(i'), f(j') \geq S$, then it must be $p_k = q_k$ because of (17). The claim follows. □

Theorem 7.2 can be generalized by defining θ-images.

A sequence of equations $E_0, \dots, E_n$ is a *chain*, if E_i is an image of E_{i-1} for all i, $1 \leq i \leq n$. Then E_n is an *image of order* n of E_0. If every E_i is a degenerated image, then the chain is degenerated and E_n is a degenerated image of order n.

We define *θ-images* of equations of type I and II. For equations of type I all images are θ-images. For equations of type II the degenerated images of order 2 and nondegenerated images of order 3 are θ-images.

Lemma 7.4. *The solutions h of equation* (12) *satisfying* $|h(y)| \leq |h(z)|$ *can be parameterized in terms of the solutions of $O(n)$ of its images of length $O(n^2)$.*

Proof. This is proved like Theorem 7.2. Let E_i be the equation (13) and let h be its solution. Theorem 5.4 can be used for the exponential equation

$$h(xy^b A(z^i x, y, z)) = h(z^c x B(z^i x, z) y C(z^i x, y, z)),$$

where i is considered to be the unknown. The bound S does not depend on h and is of size $O(n)$, because $h(x), h(y) \leq h(z)$. So there exists a number $T = O(n)$ such that either h is a solution for all $i \geq T$ or for no $i \geq T$. Thus the equations $E_T, E_{T+1}, E_{T+2}, \ldots$ are equivalent. Like in the proof of Theorem 7.2, the images E_j, where $j \leq T$, are sufficient. □

Lemma 7.5. *The solutions h of (12) satisfying $|h(y)| \leq |h(z)|$ can be parameterized in terms of the solutions of $O(n^{17})$ of its θ-images of length $O(n^{18})$.*

Proof. Let these solutions be called τ-solutions. Let E_i be the equation (13). By Lemma 7.4, the τ-solutions can be parameterized in terms of the τ-solutions of $E_0, \ldots, E_T$ for some T. Let P_i be the set of those τ-solutions h of E_i, for which $|h(z)| \geq |h(xy)|$, and let Q_i be the set of those τ-solutions h of E_i, for which $|h(y)| \leq |h(z)| \leq |h(xy)|$.

Let E_i' be the image of E_i under the morphism $z \mapsto xz$, and let E_i'' be the image of E_i' under the morphism $y \mapsto zy$. From the length constraint $|h(y)| \leq |h(z)| \leq |h(xy)|$ it follows that the set Q_i can be parameterized in terms of the solutions of E_i'', which is a nondegenerated image of the third order of (12).

Consider the set P_i. The equation (13) is of type I, so its solutions can be parameterized in terms of the solutions of a finite number of its images. Because of the condition $|h(z)| \geq |h(xy)|$ in the definition of P_i, the image under the morphism $z \mapsto xz$ can be omitted. Let the set thus obtained be F_i. The set P_i can be parameterized in terms of the solutions of equations of F_i. Partition F_i into the sets G_i and H_i of degenerated and nondegenerated images. The equations of H_i are of type I, so their equations can be parameterized in terms of the solutions of a finite number of their images. These images are nondegenerated images of the third order of the original equation (12). The equations of G_i are degenerated images of the second order. So also P_i can be parameterized in terms of the solutions of a finite number of θ-images of (12).

In this construction there are $O(n)$ images of the first order of length $O(n^2)$, $O(n^5)$ images of the second order of length $O(n^6)$, and $O(n^{17})$ images of the third order of length $O(n^{18})$. The claim follows. □

Lemma 7.6. *Let $A, B, C \in \Xi^*$ and $i, k, a, p, a_1, \ldots, a_n \geq 0$ and $c, q > 0$. Assume that all letters x, y, z occur in A, $y \not\leq A$, $0 < q \leq n$ and $a_q + c + 2 \leq$*

$k \le i - c - |A|$. Let

$$\begin{aligned}D_1(x,z) &= (zx)^c((xz)^{i+a_1}x)\dots((xz)^{i+a_{q-1}}x)xz,\\ D_2(x,z) &= (xz)^{i-k+a_q}x((xz)^{i+a_{q+1}}x)\dots((xz)^{i+a_n}x)(xz)^p.\end{aligned}$$

Now the equations

$$\begin{aligned}y(D_1B)^aA((xz)^ix, D_1B, xz) &\leftleftarrows zD_2D_1C(x,y,z)\\ y(D_1B)^aA((xz)^ix, D_1B, xz) &\leftleftarrows D_2D_1C(x,y,z)\end{aligned}$$

have only trivial solutions.

Proof. The first equation is reduced by the morphism $z \mapsto yz$ to the equation

$$(D_1(x,yz)B')^aA((xyz)^ix, D_1(x,yz)B', xyz) = zD_2(x,yz)D_1(x,yz)C'.$$

If $a > 0$, then the equation is of the form

$$(yzx)^cx\dots = (zxy)^{i-k}\dots.$$

Because $c > 0$ and $i - k \ge c + 1$, this equation has only trivial solutions by Corollary 2.5. If $a = 0$ and $z^my \le A$, $m > 0$, then the equation is of the form

$$(xyz)^my\dots = (zxy)^{i-k}\dots.$$

Because $i - k \ge m + 1$, this equation has only trivial solutions by Corollary 2.5. If $a = 0$ and $z^mx \le A$, $m \ge 0$, then the equation is of the form

$$(xyz)^{m+i}\dots = (zxy)^{i-k+a_q}zxxyz\dots,$$

except if $n = q$ and $p = 0$, when it is of the form

$$(xyz)^{m+i}\dots = (zxy)^{i-k+a_q}zx(yzx)^cxyz\dots.$$

Because $i - k + a_q > 0$ and $i > i - k + a_q + c + 1$, this equation has in both cases only trivial solutions by Corollary 2.5.

The second equation is similar. It is reduced by the morphism $x \mapsto yx$ to the equation

$$\begin{aligned}&(D_1(yx,z)B')^aA((yxz)^iyx, D_1(yx,z)B', yxz)\\ =&x(zyx)^{i-k+a_q}((yxz)^{i+a_{q+1}}yx)\dots((yxz)^{i+a_n}yx)(yxz)^pD_1(yx,z)C'.\end{aligned}$$

If $a > 0$, then the equation is of the form

$$(zyx)^cy\dots = (xzy)^{i-k}\dots.$$

Because $c > 0$ and $i - k \ge c + 1$, this equation has only trivial solutions by Corollary 2.5. If $a = 0$ and $z^my \le A$, $m > 0$, then the equation is of the form

$$(yxz)^mz\dots = (xzy)^{i-k}\dots.$$

Because $i-k \geq m+1$, this equation has only trivial solutions by Corollary 2.5. If $a=0$ and $z^m x \leq A$, $m \geq 0$, then the equation is of the form

$$(yxz)^{m+i} \ldots = (xzy)^{i-k+a_q} xyx \ldots,$$

except if $n=q$ and $p=0$, when it is of the form

$$(yxz)^{m+i} \ldots = (xzy)^{i-k+a_q} x(zyx)^c yx \ldots.$$

Because $i-k+a_q > 0$ and $i > i-k+a_q+c+1$, this equation has in both cases only trivial solutions by Corollary 2.5. □

Lemma 7.7. *If x occurs in B, then the nonperiodic solutions h of* (12) *satisfying $|h(y)| \geq |h(z)|$, and some periodic solutions, can be parameterized in terms of the solutions of $O(n^5)$ of its θ-images of length $O(n^6)$.*

Proof. The images of (12) are the equations (13). Because of the condition $|h(y)| \geq |h(z)|$, it is enough to consider the image of this under the morphism $z \mapsto xz$:

$$y^b A((xz)^i x, y, xz) \rightrightarrows (zx)^c B((xz)^i x, xz) y C((xz)^i x, y, xz). \tag{18}$$

The length constraint is now $|h(y)| \geq |h(xz)|$. Equation (18) is a nondegenerated image of the second order of (12). Let $D = (zx)^c B((xz)^i x, xz)$. Now the image of (18) under the morphism $y \mapsto D^j D_1 y$, where $j \geq 0$, $D_1 < D$ and $D^j D_1 \neq 1$, is

$$\begin{aligned} &y(D^j D_1 y)^{b-1} A((xz)^i x, D^j D_1 y, xz) \\ \leftleftarrows &D_2 D_1 B((xz)^i x, xz) y C((xz)^i x, D^j D_1 y, xz), \end{aligned} \tag{19}$$

where $D_1 D_2 = D$.

We can write $D = (zx)^c((xz)^{i+a_1}x)\ldots((xz)^{i+a_n}x)(xz)^p$, where $n \geq 1$, $p \geq 0$ and $a_1, \ldots, a_n \geq 0$. Let $M = \max\{a_l + c + 1 + |A| : 1 \leq l \leq n\}$. If D_1 "cuts" the factor $(xz)^i$ in D, then

$$\begin{aligned} D_1 &= (zx)^c((xz)^{i+a_1}x)\ldots((xz)^{i+a_{q-1}}x)(xz)^k, \\ D_2 &= (xz)^{i-k+a_q} x((xz)^{i+a_{q+1}}x)\ldots((xz)^{i+a_n}x)(xz)^p \end{aligned}$$

or

$$\begin{aligned} D_1 &= (zx)^c((xz)^{i+a_1}x)\ldots((xz)^{i+a_{q-1}}x)(xz)^{k-1}x, \\ D_2 &= z(xz)^{i-k+a_q} x((xz)^{i+a_{q+1}}x)\ldots((xz)^{i+a_n}x)(xz)^p, \end{aligned}$$

where $0 < k \leq t$ and $0 < q \leq n$. If $M \leq k \leq t-M$, then, by Lemma 7.6, equation (19) has only trivial solutions.

All nonperiodic solutions h of (12), for which $|h(y)| \geq |h(z)|$, are obtained from the solutions of (19). Divide the solutions of the original equation into sets P and Q depending on whether they are obtained from (19) when $i \leq 2M$ or when $i \geq 2M$. It needs to be shown that these sets, and some periodic solutions, can be parameterized in terms of the solutions of a finite number of equations (19).

Let $U \leftleftarrows V$ be the equation (19) and let h be its solution. If $i \leq 2M$ is fixed, then $h(U) = h(V)$ can be viewed as an exponential equation with j as the unknown. We use Theorem 5.4. It gives a $T = O(n^2)$ such that h is a solution for all $j \geq T$ or for no $j \geq T$. It can be assumed that the same T is valid for all $i \leq 2M$. Like in the proof of Theorem 7.2, the set P, and some periodic solutions, can be parameterized in terms of the equations (19) with $i \leq 2M$ and $j \leq T$. There are $O(n^3)$ of those.

Consider the set Q. We can write $i = 2M + m$. Replace $(xz)^i$ with $(xz)^M(xz)^m(xz)^M$ in (19). Now D_1 can no longer "cut" $(xz)^m$, if we are interested only in equations with nonperiodic solutions. So there are only $O(n^2)$ possibilities for D_1. Fix D_1 and a solution h. Now $h(U) = h(V)$ can be viewed as an exponential equation with j and m as the unknowns. Fix m so that Theorem 5.4 can be used. There exists a bound $L = O(n)$ not depending on m such that either h is a solution for all $j \geq L$ or for no $j \geq L$. Next, fix j and view $h(U) = h(V)$ as an exponential equation with m as the unknown. Now, by Theorem 5.4, there exists a bound $N_j = O(nj)$ such that either h is a solution for all $m \geq N_j$ or for no $m \geq N_j$. The bound N_j can be assumed to be increasing with respect to j. By combining these considerations it can be seen that either h is a solution for all $j \geq L$, $m \geq N_L$ or for no $j \geq L$, $m \geq N_L$. The set Q, and some periodic solutions, can be parameterized in terms of the equations (19) with $i \leq 2M + N_L$ and $j \leq L$. There are $O(n^3)$ of those for every D_1. This proves the theorem. □

Lemma 7.8. *If x occurs in B, then the nonperiodic solutions of* (12)*, and some periodic solutions, can be parameterized in terms of the solutions of $O(n^{17})$ of its θ-images of length $O(n^{18})$.*

Proof. The required θ-images are obtained by combining the sets of Lemmas 7.5 and 7.7. □

Lemma 7.9. *If $B = z^d$, where $d \geq 1$, then the solutions of* (12) *can be parameterized in terms of the solutions of $O(n^{26})$ of its θ-images of length $O(n^{27})$.*

Proof. All images of the equation are degenerate; $O(n^2)$ of these of length $O(n^3)$ can be chosen by Theorem 7.3. These images are of type I, so $O(n^6)$ of their images of length $O(n^9)$ can be chosen by Theorem 7.2. Of these images of the second order, the nondegenerated images are of type I, so $O(n^{18})$ of their images of length $O(n^{27})$ can be chosen. These nondegenerated images of the third order with the degenerated images of the second order give the set of required θ-images. □

We define a *complete set of θ-images* of an equation of type I or II. For equations of type I it is the set of Theorem 7.2. For equations of the form (12) it is the set of Lemma 7.5, if $B = 1$, the set of Lemma 7.8, if x occurs in B, and the set of Lemma 7.9, if $B = z^d$, $d \geq 1$. The next theorem follows immediately from this definition.

Theorem 7.10. *Every equation of type I or II of length n has a complete set of θ-images consisting of $O(n^{26})$ equations of length $O(n^{27})$.*

We assume that every complete set of θ-images satisfies the conditions of Theorem 7.10.

Theorem 7.11. *Let E be a word equation of length n. If $\{E_1, \dots, E_m\}$ is a complete set of θ-images of E and every E_i has a parametric solution of length at most c, then E has a parametric solution of length $O(mn^{26})c$.*

Proof. For equations of type I this follows from Theorem 7.2. Consider the type II equation (12). If $B \neq 1$, then the claim follows from Lemmas 7.8 and 7.9. Assume that $B = 1$. By Lemma 7.5, it suffices to show that those solutions h of (12), for which $|h(y)| \geq |h(z)|$, can be parameterized. Let h be such a solution. Then $h(x) = h(z)^m u$ for some $m \geq 1$ and $u \leq h(z)$, $h(z) = uv$ for some v and $y = vuw$ for some w. Now $h = g \circ f$, where f and g are morphisms, $f(x) = (xz)^m x$, $f(y) = zxy$, $f(z) = xz$ and g is a solution of

$$yzx \ldots = (zx)^c y \ldots . \tag{20}$$

On the other hand, all such morphisms h are solutions of (12). By Lemma 2.11, g is also a solutions of $yzx = zxy$. Now, by Lemmas 2.7 and 6.1, the solutions g of (20) can be parameterized. This gives a parametric representation for the required solutions h, if the exponent m in the morphism f is considered to be a numerical parameter. □

8 Neighborhoods and trees

The proof of the parameterizability of equations with three unknowns consists mainly of reducing equations to other equations. This forms a tree-like structure. The intention is to make all leaf equations in this tree to be basic equations. The possible reduction steps are given in the definition of a neighborhood, which is preceded by two lemmas.

Lemma 8.1. *Let $u, v, w \in \Sigma^*$, $0 < |w| \leq |u|$ and $c \geq 1$. If*

$$wu^{c+1}v \ldots = u^{c+1}vu \ldots \qquad \text{or} \qquad w(uv)^c u^2 \ldots = (uv)^c u^2 \ldots,$$

then $uv = vu$.

Proof. Let $u = wt$. From $wu^{c+1}v \dots = u^{c+1}vu \dots$ it follows that

$$(wt)^{c+1}v \cdots = t(wt)^c vwt \dots \quad \text{and} \quad (wt)^{c+1}v = t(wt)^c vw.$$

From $w(uv)^c u^2 \dots = (uv)^c u^2 \dots$ it follows that

$$(wtv)^c wtwt \cdots = tv(wtv)^{c-1} wtwt \dots \quad \text{and} \quad (wtv)^c wt = tv(wtv)^{c-1} wtw.$$

In both cases the beginnings and ends of the last equation give $wt = tw$ and $wtv = tvw$. So $\rho(w) = \rho(t) = \rho(tv) = \rho(v) = \rho(u)$. □

Lemma 8.2. *Let E_0 be the equation $xy^a zy^p s \dots \rightrightarrows zy^b xy^q t \dots$, where $s, t \in \{x, z\}$ and $a + p \neq b + q$. Let $k \geq 8 + |p - q|$ be even, E_k be the equation $xP \rightrightarrows zQ$ and $E_0, \dots, E_k$ be a degenerated chain. Now the solutions of E_k satisfying $y \neq 1$ are also solutions of the equation $xy^a zy^b \rightrightarrows zy^b xy^a$.*

Proof. Assume that E_{i+1} is the image of E_i under the morphism $f_i : x \mapsto (zy^b)^{c_i} x$, when i is even, and under the morphism $f_i : z \mapsto (xy^a)^{c_i} z$, when i is odd. Because $f_0(x)$ and $f_0(z)$ and thus $f_0(s)$ and $f_0(t)$ begin with z, the equation E_k is of the form $xy^a zy^p r \dots \rightrightarrows zy^b xy^q r \dots$, where

$$r = (f_k \circ \cdots \circ f_1)(z) = (f_k \circ \cdots \circ f_4)((((xy^a)^{c_3} zy^b)^{c_2} xy^a)^{c_1} (xy^a)^{c_3}).$$

Let $f = f_k \circ \cdots \circ f_4$. The words xy^a and zy^b occur as factors of $f(xy^a)$ at least $k - 4$ times. If h is a solution of E_k, then

$$\begin{aligned} ||h(xy^a zy^p)| - |h(zy^b xy^q)|| &\leq |a + p - b - q||h(y)| \\ \leq (a + b)|h(y)| + |p - q||h(y)| &\leq (1 + |p - q|)|h(xy^a zy^b)| \\ \leq (k - 7)|h(xy^a zy^b)| &\leq |h(f(xy^a))|. \end{aligned}$$

Thus

$$w((u^{c_3} v)^{c_2} u)^{c_1} u^{c_3} \dots = ((u^{c_3} v)^{c_2} u)^{c_1} u^{c_3} \dots,$$

where $u = h(f(xy^a))$, $v = h(f(zy^b))$ and $|w| \leq |u|$. Now, by Lemma 8.1, either $w = 1$ or $uv = vu$. In other words, $h(xy^a zy^p) = h(zy^b xy^q)$ or $h(xy^a zy^b) = h(zy^b xy^a)$. The first case is not possible by the assumptions $h(y) \neq 1$ and $a + p \neq b + q$. □

The equations $E_1, \dots, E_n$ form a *neighborhood* of an equation E, if one of the following conditions holds:

N1. $E_1, \dots, E_n$ form a complete set of θ-images of E,

N2. E reduces to $E_1, \dots, E_n$ with an n-tuple of substitutions,

N3. E is the equation $U = V$, U and V begin with different letters, $n = 2$, and E_1 and E_2 are equations $U \rightrightarrows V$ and $V \rightrightarrows U$, N4. $n = 1$ and E is the equation $U = V$ and E_1 is the equation $U^R = V^R$,

N5. E is the equation $SU = TV$, $|S|_t = |T|_t$ for all $t \in \Xi$, $n = 1$ and E_1 is the equation $US = VT$,

N6. $n = 1$ and E_1 is E reduced from the left or multiplied from the right,

N7. $n = 1$ and, with the assumptions of Lemma 8.2, E is the equation $xP \rightrightarrows zQ$ and E_1 the equation $xy^a zy^b xP \rightrightarrows zy^b xy^a zQ$.

The rules N1 and N2 will be the most important ones. The rule N3 makes it possible to consider one-sided equations. Because of the rule N6 it can be assumed that equations are reduced from the left and continue sufficiently far to right. The other rules are used in some special cases. Next theorem justifies the definition of a neighborhood.

Theorem 8.3. *Let E be a word equation of length n and let $E_1, \dots, E_m$ be its neighborhood. If each E_i has a parametric solution of length at most c, then E has a parametric solution of length $O(mn^{26})c$.*

Proof. For N1 this follows from Theorem 7.11, for N2 from Theorem 7.1 and for N7 from Lemma 8.2. The other cases are clear. □

Directed acyclic graph, whose vertices are equations, is a *tree* of E, if the following conditions hold:

(i) only vertex with no incoming edges is E,

(ii) all other vertices have exactly one incoming edge,

(iii) if there are edges from E_0 to exactly $E_1, \dots, E_n$, then these equations form a neighborhood of E.

Theorem 8.4. *Let E be a word equation of length n. If E has a tree of height k, then all equations in the tree are of length $O(n)^{27^k}$. If each leaf equation in this tree has a parametric solution of length at most c, then E has a parametric solution of length $O(n)^{52 \cdot 27^k} c$.*

Proof. In the case N1 the first claim follows directly from Theorem 7.10, and for the other cases the bound $O(n)^{27^k}$ is more than enough. Now, by Theorem 8.3, there exists a constant a such that E has a parametric solution of length

$$\begin{aligned} &a(an)^{52} \cdot a((an)^{27})^{52} \cdot a((an)^{27^2})^{52} \cdot \dots \cdot a((an)^{27^{k-1}})^{52} \cdot c \\ <&a^k (an)^{52 \cdot 27^k} c = O(n)^{52 \cdot 27^k} c. \square \end{aligned}$$

A tree in which all leaves are basic equations is a *basic tree.*

If every θ-image of an equation of type I or II has a basic tree, then the equation has a basic tree, because it has a complete set of θ-images. The rule N1 is used this way instead of explicitly selecting some complete set of θ-images.

The main theorem is proved by a sequence of lemmas. The lemmas are proved by using the rules of the definition of a neighborhood in various ways.

Lemma 8.5. *The equation $xyz^2A(x,y,z) = yz^2xB(x,y,z)$ has a basic tree.*

Proof. With N5 we get the equation $Axyz^2 = Byz^2x$, and then with N4 the equation $z^2yxA^R = xz^2yB^R$. With N3 we get $z^2yxA^R \rightrightarrows xz^2yB^R$ and $z^2yxA^R \leftleftarrows xz^2yB^R$. The former is basic of the form B2. The latter is reduced by the pair of substitutions $x \mapsto zx$, $x \mapsto z^2x$ to the equations $zyzx\ldots \rightrightarrows xz^2y\ldots$ and $yz^2x\ldots = xz^2y\ldots$. These are basic of the form B9 or B7 and we get a basic tree. □

Lemma 8.6. *The equation $x^2yz\ldots \rightrightarrows zyxy\ldots$ has a basic tree.*

Proof. This equation is reduced by the pair of substitutions $x \mapsto zx$ and $x \mapsto zyx$ to the equations $xzxyz\ldots \leftleftarrows yzxy\ldots$ and $xzyxyz\ldots = zyxy\ldots$. The latter is basic of the form B5 and the first is reduced by the substitution $y \mapsto xy$ to the equation $zx^2yz\ldots = yzx^2y\ldots$, which has a basic tree by Lemma 8.5. □

Lemma 8.7. *Every nondegenerated θ-image of $xy^2z\ldots \rightrightarrows zy^2x\ldots$ has a basic tree.*

Proof. The equation is of type I, so its nondegenerated θ-images are of the form $xy^2z\ldots \leftleftarrows y^2zx\ldots$ or of the form $xy^2z\ldots \leftleftarrows yzyx\ldots$. These are basic of the form B2 or B8. □

Lemma 8.8. *Every nondegenerated θ-image of $xyztA(x,y,z) \rightrightarrows zx^2yB(x,y,z)$, where $t \neq z$, has a basic tree.*

Proof. The equation is of type II. Its nondegenerated images of the second order are

$$yxzg(h(tA)) \rightrightarrows zx((xy)^jxz)^ixyg(h(B)), \tag{21}$$

where h is the morphism $x \mapsto z^ix$ and g is the morphism $z \mapsto (xy)^jxz$. The nondegenerated θ-images are the images of (21). Consider the cases $j = 0$ and $j > 0$ and let $C = tA$.

First, let $j = 0$. The images of (21) are

$$yxzC((xz)^ix, D^kD_1y, xz) \leftleftarrows D_2D_1yB((xz)^ix, D^kD_1y, xz), \tag{22}$$

where $D = D_1D_2 = zx(xz)^ix$, $D \neq D_1$ and $D^kD_1 \neq 1$. If D_2D_1 begins with one of x^2, xzx, zxz, then (22) is a basic equation. Otherwise D_2D_1 begins with zx^2, $D_1 = 1$ and $k > 0$. Then (22) is

$$yxzC((xz)^ix, D^ky, xz) \leftleftarrows zx(xz)^ixyB((xz)^ix, D^ky, xz).$$

This is reduced by the substitution $z \mapsto yz$ to the equation

$$xyzC((xyz)^ix, E^ky, xyz) = zx(xyz)^ixyB((xyz)^ix, E^ky, xyz),$$

where $E = yzx(xyz)^ix$. This is equivalent with one of the following pairs of equations:

(a) $xyzx = zxxy$ and $y \ldots = z \ldots$, if $t = x$,

(b) $xyzyzxx = zxxyzxy$ and $y \ldots = z \ldots$, if $t = y$ and $i > 1$,

(c) $xyzyzxx = zxxyzxy$ and $y \ldots = x \ldots$, if $t = y$, $i = 1$ and $y \not\leq B$,

(d) $xyzyzxx = zxxyzxy$ and $(yzx)y \ldots = (yzx)x \ldots$, if $t = y$, $i = 1$ and $y \leq B$.

By Corollary 2.5, there are only trivial solutions in all cases.

Next, let $j \geq 0$. If $t = x$, then (21) is

$$yxz((xy)^jxz)^ixg(h(A)) \rightrightarrows zx((xy)^jxz)^ixyg(h(B)).$$

This is equivalent with the pair of equations $yxzx \rightrightarrows zxxy$, $y \ldots = x \ldots$ and has only trivial solutions by Corollary 2.5. If $t = y$, then (21) is

$$yxzy \ldots \rightrightarrows zxxy(xy)^{j-1}xzxy \ldots.$$

Every image of this equation is of one of the following forms:

$$yx \ldots \leftleftarrows x^2 \ldots, \qquad yxz \ldots \leftleftarrows xzx \ldots, \qquad yxzzx^2s \ldots \leftleftarrows zx^2yxzx \ldots,$$

where $s \neq x$. The two first equations are basic of the form B2 and B3. The third equation is equivalent with the pair of equations $yxzzx^2 \leftleftarrows zx^2yxz$, $s \ldots = x \ldots$ and has only trivial solutions by Corollary 2.5. □

9 Supporting equations

We define supporting equations and prove as an intermediate result that they have basic trees.

Let $1 \leq a, b \leq 2$, $d \geq 1$ and $t \neq y$. A *supporting equation* is an equation of the form

$$x^ay^bt \ldots \rightrightarrows zyx \ldots \qquad \text{or} \qquad x^ay^bt \ldots \rightrightarrows zxy \ldots, \tag{23}$$

or of the form

$$x^a y^b t \ldots \rightrightarrows z(yz)^d x \ldots . \tag{24}$$

A tree whose leaves are basic equations, supporting equations of the form (23) or equations $x^2yt \ldots \rightrightarrows zyzxy \ldots$, where $t \neq y$, is a *supporting tree.*

Lemma 9.1. *Let $E_0, \ldots, E_3$ be a chain of images of the equation*

$$E_0 : xy^a tA(x, y, z) \rightrightarrows z^c xB(x, z)yC(x, y, z),$$

where $a, c \geq 1$, $A, C \neq 1$ and $t \neq y$. Assume first that E_2 is a degenerated image. Now

1. *E_2 is of the form $xy^a z \ldots \rightrightarrows zx \ldots$;*

2. *if $a = 2$, $c = 1$, $B = 1$ and $y \not\leq C$, then E_2 is of the form $xy^2z \ldots \rightrightarrows zxyx \ldots$;*

3. *if $a = 2$, $c = 1$ and $B = x$, then E_2 is of the form $xy^2z \ldots \rightrightarrows zx^2y \ldots$;*

4. *if $a = 1$, then E_2 is basic equation B3 or of the form $xyzs \ldots \rightrightarrows zx^2y \ldots$, where $s \neq z$.*

Assume then that E_2 is a nondegenerated image. Now

1. *E_3 is a supporting equation;*

2. *if $a = 2$, $c = 1$, $B = 1$ and $y \not\leq C$, then E_3 is a basic equation or of the form $yxzy \ldots \rightrightarrows zxzy \ldots$;*

3. *if $a = 2$, $c = 1$ and $B = x$, then E_3 is a supporting equation of the form* (23) *or an equation of the form $x^2ys \ldots \rightrightarrows zyzxy$, where $s \neq y$;*

4. *if $a = 1$, then E_3 is a supporting equation of the form* (23).

Proof. The equation E_1 is of the form

$$xy^a zA_1(x, y, z) \leftleftarrows z^c xB(z^i x, z)C(z^i x, y, z),$$

where $i > 0$ and $A_1 \neq 1$. Its image E_2 is of the form

$$D_2 D_1 zA_2(x, y, z) \rightrightarrows zh(z^{c-1} xB(z^i x, z)C(z^i x, y, z)),$$

where h is the morphism $z \mapsto (xy^a)^j D_1 z$, $j \geq 0$, $D_1 < xy^a$, $(xy^a)^j D_1 \neq 1$, $D_1 D_2 = xy^a$ and $z \not\leq A_2 \neq 1$.

The equation E_2 is a degenerated image if and only if $D_1 = 1$. Then the first four claims are correct. If $D_1 \neq 1$, then by writing E_3 separately in the three cases $t = 0$, $D_1 = x$, and $t > 0$, $D_1 = x$, and $t \geq 0$, $D_1 = xy^b$, $1 \leq b < a$, the last four claims can be seen to be correct. □

Lemma 9.2. *Let $s, t \neq y$. Every nondegenerated θ-image of the equation $xy^2s\ldots \rightrightarrows zxyt\ldots$ has a basic tree. Every nondegenerated θ-image of the equation $xy^2z\ldots \rightrightarrows zx^2y\ldots$ has a supporting tree.*

Proof. For the latter equation this follows from 3 of Lemma 9.1. For the former it follows from 2 of Lemma 9.1, because the equation $yxzy\ldots \rightrightarrows zxzy\ldots$ is reduced by the substitution $y \mapsto zy$ to the equation of Lemma 8.5. □

Lemma 9.3. *Let $s \neq x$ and $t \neq y$. Consider the equations*

(a) $xy^2z\ldots \rightrightarrows zx^2y\ldots$,

(b) $xyzs\ldots \rightrightarrows zx^2y\ldots$,

(c) $xy^2z\ldots \rightrightarrows zxyt\ldots$,

(d) $xyzt\ldots \rightrightarrows zy^2x\ldots$,

(e) $xyz\ldots \rightrightarrows zy^2x\ldots$.

the first has a supporting tree and the others have basic trees.

Proof. Let E_0 be one of (a)–(d). It can be written in the form $xy^azy^pu\ldots \rightrightarrows zy^bxy^qv\ldots$, where $u, v \neq y$. Here always $a+p \neq b+q$. Let $l \geq 8+|p-q|$ be even. Form a complete set of θ-images for E_0, a complete set of θ-images for each of these, and so on l times. These θ-images form chains $E_0, \ldots, E_l$. We show that each chain has an equation with the required tree. This proves the lemma.

First, consider chains of degenerated θ-images. There is a corresponding degenerated chain of ordinary images. Now, by N7, the equation E_l can be replaced by one of the following:

(a') $xy^2z\ldots \rightrightarrows zxy^2\ldots$

(b') $xyz\ldots \rightrightarrows zxy\ldots$

(c') $xy^2z\ldots \rightrightarrows zxy^2\ldots$

(d') $xyzy\ldots \rightrightarrows zy^2x\ldots$.

Equation (b') is basic of the form B3. Equations (a') and (c') are reduced by the substitution $x \mapsto zx$ to equations of Lemma 8.5. Equation (d') is reduced to the equation $xyzyP = y^2zxQ$, which can be transformed to $yzyx\ldots = xzy^2\ldots$ by N5 and N4. This has a basic tree by Lemma 8.5.

Second, consider nondegenerated chains. Assume that the part $E_0, \ldots, E_{j-1}$ of the chain is degenerated and that E_j is a nondegenerated θ-image of E_{j-1}. If E_0 is of the form (a) – (c), then E_{j-1} is of the same form and E_j has the required tree by Lemma 9.2 or Lemma 8.8. If E_0 is of the form (d), then all of $E_0, \dots, E_{j-1}$ are of type I. Let $0 \leq i < j$. If i is even, then E_i is of the form $xyz \dots \rightrightarrows zy^2x \dots$. If i is odd, then E_i is of the form $zy^2x \dots \rightrightarrows xyz \dots$. Assume first that j is even. Now E_j is of the form $yxzr \dots \rightrightarrows zy^2x \dots$, where $r \neq z$. This is the equation (b). Assume then that j is odd. Now E_j is of the form $y^2 \dots \rightrightarrows xy \dots$ or $yzy \dots \rightrightarrows xyz \dots$. These are basic of the form B2 and B3.

The lemma has been proved for equations (a) – (d). The equation (e) is of the form (d) or (d'), so it has a basic tree. □

Lemma 9.4. *Supporting equations of the form* (23) *have basic trees.*

Proof. First, consider the equation $x^a y^b t \dots \rightrightarrows zyx \dots$, where $1 \leq a, b \leq 2$ and $t \neq y$. If $a = b = 1$, then this is basic of the form B4. If $a = 1$ and $b = 2$, then this of type I and its images are of the form $zyx \dots \rightrightarrows xy^2z \dots$ or $yzxs \dots \rightrightarrows xy^2z \dots$, where $s \neq x$. These have basic trees by Lemma 9.3. Assume that $a = 2$. The equation is reduced by the substitutions $x \mapsto zx$, $x \mapsto zyx$ to the equations $xzxy \dots \leftleftarrows yzxs \dots$ and $xzy \dots = zyx \dots$, where $s \neq x$. The latter is basic of the form B5. If in the former $s = y$, then it is reduced by the substitution $y \mapsto xy$ to the equation of Lemma 8.5. If $s = z$, then the images of the equation are of the form $yzxz \dots \leftleftarrows Dy$, where D is a conjugate of xzx. If $D = xzx$, then this image is basic of the form B4. If $D = zx^2$, then it is the equation (c) of Lemma 9.3. If $D = x^2z$, then it is the equation of Lemma 8.6.

Second, consider the equation $x^a y^b t \dots \rightrightarrows zxy \dots$, where $1 \leq a, b \leq 2$ and $t \neq y$. If $a = 2$ or $a = b = 1$, then this is basic of the form B2 or B3. Assume that $a = 1$ and $b = 2$. If the fourth letter on the right is y, then the equation is reduced by the substitution $x \mapsto zx$ to the equation of Lemma 8.5. Otherwise, the θ-images of the equation are, by 2 of Lemma 9.1, basic equations or of the form $xy^2z \dots \rightrightarrows zxyx \dots$ or $yxzy \dots \rightrightarrows zxzy \dots$. The former has a basic tree by Lemma 9.3, the latter is reduced by the substitution $y \mapsto zy$ to the equation of Lemma 8.5. □

Lemma 9.5. *The equation $x^2yt \dots \rightrightarrows zyzxy \dots$, where $t \neq y$, has a basic tree.*

Proof. The images of this equation have basic trees by Lemma 9.4, except for the image under the morphism $x \mapsto zx$:

$$xzxyz \dots \leftleftarrows yz^2xy \dots.$$

This is reduced by the substitution $y \mapsto xy$ to the equation $zx^2yz \dots = yz^2x^2 \dots$. Consider the corresponding one-sided equations.

The images of the equation

$$zx^2yz \dots \rightrightarrows yz^2x^2 \dots \tag{25}$$

are of the form $zx^2yy^iz\dots \leftleftarrows yzy^izx^2\dots$, and the images of this under the morphisms $y \mapsto zy$, $y \mapsto zxy$, $y \mapsto zx^2y$ and under other morphisms are

$$x^2(zy)^{i+1}\dots \rightrightarrows yz(zy)^izx^2\dots, \tag{26}$$

$$xzx\dots \rightrightarrows yz^2x\dots, \tag{27}$$

$$zx^2yzx\dots \rightrightarrows yz^2x^2y\dots, \tag{28}$$

$$Dyzx\dots \rightrightarrows yz^2x^2z\dots, \tag{29}$$

where D is a conjugate of zx^2. The last two can be split into pairs of equations $zx^2yz \rightrightarrows yz^2x^2$, $x\dots = y\dots$ and $Dyz \rightrightarrows yz^2x^2$, $x\dots = z\dots$. These have only trivial solutions by Corollary 2.5. Consider the first two equations. They are nondegenerated images, so their images are θ-images of (25). These are equations of Lemma 9.4, except for the image of (26) under the morphism $x \mapsto yx$:

$$xyx(zy)^{i+1}\dots \leftleftarrows z^2(yz)^i(yx)^2\dots.$$

All images of this are again equations of Lemma 9.4, except for the image under the morphism $z \mapsto xz$:

$$yx(xzy)^{i+1}\dots \rightrightarrows zxz(yxz)^i(yx)^2\dots.$$

This is reduced to the equation

$$yx(xz^2y)^{i+1}\dots = xz(zyxz)^i(zyx)^2\dots,$$

which can be split into the pair of equations $yx^2z^2 = xz^2yx$, $y\dots = z\dots$, which has only trivial solutions by Corollary 2.5. So (25) has a basic tree.

The images of the equation $zx^2yz\dots \leftleftarrows yz^2x^2\dots$ are of the following forms:

$$x^2zyz\dots \rightrightarrows yz^2x^2\dots, \tag{30}$$

$$xzxyz\dots \rightrightarrows yz^2x^2\dots, \tag{31}$$

$$zx^2yz\dots \rightrightarrows yz^2x^2\dots. \tag{32}$$

The images of (31) are equations of Lemma 9.4. The equation (32) is of the form (25). The images of (30) are equations of Lemma 9.4, except for the image under the morphism $x \mapsto yx$:

$$xyxzyz\dots \leftleftarrows z^2(yx)^2\dots.$$

All images of this are again equations of Lemma 9.4, except for the image under the morphism $z \mapsto xz$:

$$yx^2zyxz\dots \rightrightarrows zxz(yx)^2\dots.$$

This is reduced to the equation

$$yx^2z^2yxz\ldots = xz(zyx)^2\ldots,$$

which can be split into the pair of equations $yx^2z^2 = xz^2yx$, $y\ldots = z\ldots$, which has only trivial solutions by Corollary 2.5. □

Lemmas 9.4 and 9.5 prove that if an equation has a supporting tree, then it has a basic tree.

Theorem 9.6. *Every supporting equation has a basic tree.*

Proof. By Lemma 9.4, it is enough to consider equations (24).

If $a = b = 1$, then the equation is $xyt\ldots \rightrightarrows z(yz)^dx\ldots$. Every image of this equation has a basic tree by Lemma 9.4.

If $a = 1$ and $b = 2$, then the equation is $xy^2t\ldots \rightrightarrows z(yz)^dx\ldots$. Its images are of the forms

$$xy^2z\ldots \leftleftarrows zyz\ldots, \tag{33}$$

$$xy^2z\ldots \leftleftarrows yzy\ldots, \tag{34}$$

$$xy^2z\ldots \leftleftarrows yz^2s\ldots, \tag{35}$$

$$xy^2z\ldots \leftleftarrows z^2yt\ldots, \tag{36}$$

where $s \neq z$, $t \neq y$. All images of (33) are of the form (23). All θ-images of (34) are, by 4 of Lemma 9.1, basic equations, supporting equations (23), or equations (b) of Lemma 9.3. All θ-images of (34) are, by 3 of Lemma 9.1, equations of Lemmas 9.3, 9.4 or 9.5. All images of (36) are supporting equations (23), except for the image under the morphism $z \mapsto xz$, which is the equation of Lemma 9.5.

If $a = 2$, then the equation is $x^2y^bt\ldots \rightrightarrows z(yz)^dx\ldots$. Its images are supporting equations (23), except for the image under the morphism $x \mapsto zx$:

$$xzxy\ldots \rightrightarrows (yz)^dzx\ldots.$$

If $d \geq 1$, then the images of this equation are supporting equations (23). If $d = 1$, then this is the equation (24) with $a = 1$ and $b = 2$. □

10 Main theorem

Lemma 10.1. *The equation $xy^azy^ps\ldots \rightrightarrows zy^bxy^qt\ldots$, where $a > 0$, $a+p = b+q$ and $s, t \neq y$, has a basic tree.*

Proof. If $a = 1$ and $b = 0$, then the equation is basic of the form B8. Consider other cases. The equation is reduced by the substitutions $x \mapsto zy^cx$ $(c = 0, \ldots, b)$ to the equations

$$xy^az\ldots \leftleftarrows y^{b-c}zy^cx\ldots \qquad (c = 0, \ldots, b-1), \tag{37}$$

$$xy^azy^psP = zy^bxy^qtQ. \tag{38}$$

When $b-c>1$, the equation (37) is basic of the form B2. When $b-c=1$, its θ-images have a basic tree by 4 of Lemma 9.1 and by Lemmas 9.3 and 9.4.

If $a=b$, the equation (38) is basic of the form B6 or B7. Assume that $a<b$; the case $a>b$ is similar. By using N5 and N4 we get the equation $y^d zy^a x\ldots = xy^b z\ldots$, where $d=b-a\geq 1$. Split this into one-sided equations

$$y^d zy^a x\ldots \rightrightarrows xy^b z\ldots, \tag{39}$$

$$y^d zy^a x\ldots \leftleftarrows xy^b z\ldots. \tag{40}$$

If $d>1$, then (39) is basic of the form B2. If $d=1$, then its θ-images have a basic tree by 4 of Lemma 9.1 and by Lemmas 9.3 and 9.4. The equation (40) is reduced by the substitutions $x\mapsto y^c x$ $(c=1,\ldots,d)$ to the equations

$$y^{d-c} zy^{a+c} x\ldots \rightrightarrows xy^b z\ldots \qquad \text{and} \qquad zy^{a+d}x\ldots = xy^b z\ldots.$$

Latter is basic of the form B6 or B7, former is of the form (39). □

Lemma 10.2. *The equation $E_0 : xy^a z\ldots \rightrightarrows zy^b x\ldots$, where $a>0$, has a basic tree.*

Proof. The equation can be written in the form $xy^a zy^p u\ldots \rightrightarrows zy^b xy^q v\ldots$, where $u,v\neq y$. If $a+p=b+q$, then the claim follows from Lemma 10.1. Assume that $a+p\neq b+q$. Let $l\geq 8+|p-q|$ be even. Like in Lemma 9.3, form a complete set of θ-images of E_0, a complete set of θ-images of these, and so on l times. These θ-images form chains $E_0,\ldots,E_l$. We show that each chain has an equation with a basic tree; this proves the claim.

First, consider chains of degenerated θ-images. There is a corresponding chain of ordinary images and we can use the rule N7. The equation E_l is replaced by the equation $xy^a zy^b xP \rightrightarrows zy^b xy^a zQ$, which has a basic tree by Lemma 10.1.

Second, consider nondegenerated chains. Assume that the part $E_0,\ldots,E_{j-1}$ of the chain is degenerated and that E_j is a nondegenerated θ-image of E_{j-1}. If $b=0$, the equation E_0 is of the form $xy^a z\ldots \rightrightarrows zx\ldots$, and E_{j-1} is of the same form. Now by 1 of Lemma 9.1, E_j is a supporting equation and thus has a basic tree. If $b>0$, then E_0 is of the form $xy^a z\ldots \rightrightarrows zy^b x\ldots$. Equation E_{j-1} is of the same form. Now E_j is of the form $y^c zy^d x\ldots \rightrightarrows xy^a z\ldots$, where $c+d=a$ and $c\geq 1$. If $c>1$, then E_j is basic of the form B2. If $c=1$, then E_j has a basic tree by 4 of Lemma 9.1 and by Lemmas 9.3 and 9.4. □

Lemma 10.3. *The equation $xy^a t\ldots \rightrightarrows z^c xB(x,z)y\ldots$, where $a,c\geq 1$ and $t\neq y$, has a basic tree.*

Proof. By 1 of Lemma 9.1, all θ-images of this equation are supporting equations or equations of Lemma 10.2. □

Lemma 10.4. *The equation $x^n y^m t \ldots \rightrightarrows zyA(y,z)x \ldots$, where $n, m \geq 1$ and $t \neq y$, has a basic tree.*

Proof. If $n = 1$, every image of the equation is of the form

$$xy^m z \ldots \leftleftarrows Dx \ldots, \tag{41}$$

where D is a conjugate of zyA. If $n > 1$, the image of the equation under the morphism $x \mapsto zx$ is

$$x(zx)^{n-1} y \ldots \leftleftarrows yAzx \ldots, \tag{42}$$

and all the other images are of the form

$$xzy \ldots \leftleftarrows Dx \ldots, \tag{43}$$

where D is a conjugate of zyA.

Consider equation (41). If $y^2 \leq D$, then this is basic of the form B2. If $yz \leq D$, then this is the equation of Lemma 10.3. If $z \leq D$, then this is of the form

$$x^a y^b s \ldots \rightrightarrows zy^d x \ldots, \tag{44}$$

where $a, b, d \geq 1$ and $s \neq y$. The case of equation (43) is similar. The equation (42) is of the form

$$x^a y^b s \ldots \rightrightarrows z(yz)^d x \ldots, \tag{45}$$

where $a, b, d \geq 1$ and $s \neq y$. It is enough to prove that equations (44) and (45) have basic trees.

Consider equation (44). Assume first that $a = 1$. Now every image of this equation is of the form $xy^b z \ldots \leftleftarrows Dx$, where D is a conjugate of zy^d. If $z \leq D$, then this is the equation of Lemma 10.2. If $y^2 \leq D$, this is basic of the form B2. If $yz \leq D$, then this is the equation of Lemma 10.3. Assume then that $a > 1$. Now the image of the equation under the morphism $x \mapsto zx$ is $x(zx)^{a-1} y \ldots \leftleftarrows y^d zx \ldots$, and all other images are of the form $xzy \ldots \leftleftarrows Dx \ldots$, where D is a conjugate of zy^d. First of these is of type I and its images have basic trees by Theorem 9.6. The latter is the equation of Lemma 10.3, if $zy \leq D$; otherwise its images have basic trees by Theorem 9.6.

Consider equation (45). Assume first that $a = 1$. Now every image of this equation is of the form $xy^b z \ldots \leftleftarrows Dx$, where D is a conjugate of $z(yz)^d$. If $yz \leq D$, this is the equation of Lemma 10.3. Otherwise $Dx = z^c ys$, where $1 \leq c \leq 2$ and $s \neq y$, and this image is of the form (44) and has a basic tree. Assume then that $a > 1$. Now the image of the equation under the morphism $x \mapsto zx$ is $x(zx)^{a-1} y \ldots \leftleftarrows (yz)^d zx \ldots$, and all other images are of the form $xzy \ldots \leftleftarrows Dx \ldots$, where D is a conjugate of $z(yz)^d$. First of these goes back to the case $a = 1$. The latter has a basic tree by Lemma 9.4. □

Theorem 10.5. *Every equation of length n with three unknowns has a basic tree of height $O(n)$.*

Proof. The trivial equation $U = U$ is a basic equation. All other equations can be reduced from the left and split into one-sided equations. By multiplication from the right, every one-sided equation can be turned into one of the equations

$$x^2 \ldots \rightrightarrows y^c x \ldots \tag{46}$$
$$xy \ldots \rightrightarrows y^c x \ldots \tag{47}$$
$$xz^a t \ldots \rightrightarrows y^c x B(x,y) z \ldots \tag{48}$$
$$x^a y^b s \ldots \rightrightarrows y^c z B(y,z) x \ldots \tag{49}$$
$$x^a z^b t \ldots \rightrightarrows yz B(y,z) x \ldots \tag{50}$$
$$x^a z^b t \ldots \rightrightarrows y^d z B(y,z) x \ldots, \tag{51}$$

where $a, b, c \geq 1$, $d > 1$, $t \neq z$ and $s \neq y$. We prove that all of these have basic trees.

Equation (46) is basic of the form B2. Equation (47) is reduced by the substitution $x \mapsto yx$ to the equation $xy \ldots = y^c x \ldots$, which is basic of the form B1. Equation (48) is the equation of Lemma 10.3. Equation (50) is the equation of Lemma 10.4.

The equation (49) is of type I and its images are of the form $xy \ldots \leftleftarrows Dx \ldots$, where D is a conjugate of $y^c z B$. If $y^2 \leq D$, then this is of the form (46), if $yz \leq D$, then of the form (48), and if $z \leq D$, then of the form (50). So every image of the equation (49) and thus the equation itself has a basic tree.

The equation (51) is of type I and its images are of the form $x(y \ldots)^{a-1} z^b y \ldots \leftleftarrows Dx \ldots$, where D is a conjugate of $y^d z B$. Again it is of the form (46), (48) or (50). So every image of the equation (49) and thus the equation itself has a basic tree.

The constructions of trees in the lemmas produce trees of bounded length with two exceptions: Lemmas 9.3 and 10.2, where a tree with height of order $|p - q|$ is constructed for the equation

$$xy^a zy^p \ldots \rightrightarrows zy^b xy^q \ldots . \tag{52}$$

We prove that the powers of y here cannot be more than n, which proves this theorem. In the definition of neighborhood, the rules N1, N2, N5 and N6 can produce higher powers than those in the initial equation. There is no need to use N6 to generate high powers and N5 is only used in Lemmas 8.5, 9.3 and 10.1, where it does not generate high powers. Consider N1 and N2. Here an equation $xU(x,y,z) \rightrightarrows y^a x V(x,y,z)$ can be turned into $xU(y^i x, y, z) \leftleftarrows y^a x V(y^i x, y, z)$ for high values of i. But in order for y to be in the position of (52), the rules N1 or N2 must be used again. Then y is replaced by xuy for some $u \in \{x, z\}^*$ and the powers of y disappear. The claim is proved. □

In the next theorem $\exp^2$ denotes the double exponential function $\exp \circ \exp$.

Theorem 10.6. *Every equation of length n with three unknowns has a parametric solution of length* $\exp^2(O(n))$.

Proof. By Theorem 10.5, every equation has a basic tree of height $O(n)$. By Theorem 6.2, the leaf equations have parametric solutions of bounded length. Now from Theorem 8.4 it follows that E has a parametric solution of length $O(n)^{52 \cdot 27^k}$, where $k = O(n)$, that is of length $\exp^2(O(n))$. □

References

[1] M.H. Albert, J. Lawrence: *A proof of Ehrenfeucht's conjecture*. Theoret. Comput. Sci. 41:121–123 (1985)

[2] C. Choffrut, J. Karhumäki: *Combinatorics of words*. In: G. Rozenberg, A. Salomaa (eds), Handbook of Formal Languages, Springer (1997)

[3] E. Czeizler, J. Karhumäki: *On non-periodic solutions of independent systems of word equations over three unknowns*. Internat. J. Found. Comput. Sci. 18:873–897 (2007)

[4] S. Eilenberg, M.P. Schützenberger: *Rational sets in commutative monoids*. J. Algebra 13:173-191 (1969)

[5] V. S. Guba: *Equivalence of infinite systems of equations in free groups and semigroups to finite subsystems*. Mat. Zametki 40:321–324 (1986)

[6] T. Harju, J. Karhumäki, W. Plandowski: *Independent systems of equations*. In: M. Lothaire (ed), Algebraic Combinatorics on Words, Cambridge University Press (2002)

[7] Y.I. Hmelevskii: *Equations in free semigroups*. Proc. Steklov Inst. of Math. 107 (1971); Amer. Math. Soc. Translations (1976)

[8] M. Lothaire: *Combinatorics on words*. Addison-Wesley (1983)

[9] G. S. Makanin: *The problem of solvability of equations in a free semigroup*. Mat. Sb. 103:147–236 (1977); English transl. in Math. USSR Sb. 32:129–198

[10] W. Plandowski: *Satisfiability of word equations with constants is in PSPACE*. J. ACM 51:483–496 (2004)

[11] J.-C. Spehner: *Quelques problemes d'extension, de conjugaison et de presentation des sous-monoides d'un monoide libre*. Ph.D. Thesis, Univ. Paris (1976)

[12] J.-C. Spehner: *Les presentations des sous-monoides de rang* 3 *d'un monoide libre*. Semigroups, Proc. Conf. Math. Res. Inst. 116–155 (1978)