A NEW PROOF OF HMELEVSKII’S THEOREM

Aleksi Saarela

Licentiate thesis
April 2009

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF TURKU
Contents

1 Introduction ........................................ 1
2 Definitions and basic results .................. 1
3 Parametric words .................................. 4
4 Remarks about parametric solutions ........ 6
5 Exponential equations ............................. 9
6 Basic equations .................................... 13
7 Images and \(\theta\)-images ......................... 15
8 Neighborhoods and trees ....................... 23
9 Supporting equations ............................. 27
10 Main theorem ..................................... 32
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 \( \theta \)-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 \( \Xi \) 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 \( xU \Rightarrow yV \).
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 \( w = a_1 \ldots a_n \). Its reverse is \( w^R = a_n \ldots a_1 \), and its length is \( |w| = n \).

The number of occurrences of a letter \( a \) in \( w \) is denoted by \( |w|_a \).

If \( \Sigma = \{ a_1, \ldots, a_n \} \), then \( U \in \Sigma^* \) can be denoted \( U(a_1, \ldots, a_n) \), and its image under a morphism \( h \) can be denoted \( h(U) = U(h(a_1), \ldots, h(a_n)) \).

If \( u \in \Sigma^* \), then the morphism \( a \mapsto u \) means the morphism, which maps \( a \mapsto a \), when \( i = 2, \ldots, n \).

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

\[ |u^nu'| = |v^nv'| \geq |u| + |v| - \gcd(|u|, |v|). \]

Now \( u^nu' = v^nv' \) 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 \( x \ldots = y \ldots \).

**Theorem 2.4** (Graph lemma). Let \( E \) be a system of equations and assume that its graph has \( c \) connected components. Let \( \Xi = \{ x_1, \ldots, x_n \} \) and let \( h : \Xi^* \to \Sigma^+ \) be a solution of \( E \). Now there exists a set \( F \subset \Sigma^+ \) with \( c \) elements such that \( h(x_1), \ldots, h(x_n) \in F^* \).
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 $x = (pq)^i p, y = (pq)^j q, z = (pq)^k p$, 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 $h(xyz) = h(zyx)$, so $h(xy) = t^n$ and $h(zy) = t^m$, where $t$ is primitive and $m, n > 0$. Now $h(y) = q(pq)^i$, 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 $x = (pq)^i p, y = (pq)^j q, z = (pq)^k p$, 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 $h(xyz) = h(zxy)$, so $h(xy) = t^n$ and $h(zy) = t^m$, where $m, n > 0$. 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 $i = m - j - 1$. 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 $x = (pq)^i p, y = (pq)^{i+1} p, z = q((pq)^{i+1} p)^{a-2} p q$, 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 $h(z) = q((pq)^{i+1} p)^{a-2} p q$. 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 $x = (pq)^i p, y = q, z = (pq)^j p$ or

\[
\begin{align*}
    x &= q(p(q)_{k+1} p)^{a-2} p q ((p(q)_{k+1} p)^{a-1} p q)^i, \\
    y &= (p(q)_{k+1} p, \\
    z &= q(p(q)_{k+1} p)^{a-2} p q ((p(q)_{k+1} p)^{a-1} p q)^j,
\end{align*}
\]

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, \( h(v) = (pq)^k p, h(y) = (pq)^k p \) and \( h(u) = qp((pq)^k p)^{a-2} pq. \) This gives a solution of the second form. If \( p \) and \( q \) would commute, the solution would be periodic. \( \square \)

Lemma 2.10. The nonperiodic solutions of the equation \( xyxxz \Rightarrow zx^2y \) are \( x = (pq)^j p, y = qp((pq)^l p)^j pq, z = pq, \) 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 \( h(x) = (pq)^l p, \) so \( y = qp((pq)^l p)^j pq. \) If \( p \) and \( q \) would commute, the solution would be periodic. \( \square \)

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

Proof. Assume that \( h(x) \leq h(y). \) Then \( h(y) = h(x)^c t, \) where \( h(x) \neq t. \) Because \( h(x)^a t \ldots = h(x)^{c+t} t \ldots, \) 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. \( \square \)

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 \( \Delta \) and the set of numerical parameters \( \Lambda. \) Now parametric words are defined inductively as follows:

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

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

(iii) if \( \alpha \) is a parametric word and \( i \in \Lambda, \) then \( (a^i) \) is a parametric word.
The set of parametric words is denoted by $P(\Delta, \Lambda)$. The sets of parameters are always denoted by $\Delta$ and $\Lambda$.

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 $\alpha$ and $\beta$ 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 $\alpha, \beta \in P(\Delta, \Lambda)$, then $f((\alpha \beta)) = f(\alpha)f(\beta)$; if $\alpha \in P(\Delta, \Lambda)$ and $i \in \Lambda$, then $f((\alpha^i)) = f(\alpha)^{f(i)}$. A parametric word is thus mapped by $f$ to a word of $\Delta^*$. This can be further mapped by a morphism $h : \Delta^* \to \Sigma^*$ to a word of $\Sigma^*$. The mapping $h \circ f$ is a valuation of a parametric word into $\Sigma^*$, and $f$ is its valuation to the set $\Delta^*$.

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 $\alpha, \beta \in P(\Delta, \Lambda)$, then the length of $\alpha \beta$ is the sum of lengths of $\alpha$ and $\beta$; if $\alpha \in P(\Delta, \Lambda) \setminus \{1\}$ and $i \in \Lambda$, then the length of $\alpha^i$ is the length of $\alpha$ 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 $\alpha, \beta \in P(\Delta, \Lambda)$, then the height of $\alpha \beta$ is the maximum of heights of $\alpha$ and $\beta$; if $\alpha \in P(\Delta, \Lambda) \setminus \{1\}$ and $i \in \Lambda$, then the height of $\alpha^i$ is the height of $\alpha$ plus one. Parametric words of height zero can be considered to be words of $\Delta^*$.

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

$$(x + y - z = 0) \land (x \geq 2) \lor ((x + y = 3) \land (x + z = 4))$$

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 $\Xi^*$ 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 $\Sigma^*$. 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 $x \in \Xi$. 

5
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 \( \Xi^* \) to \( P(\Xi, \Lambda) \) 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 parametrizability 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 \( S_{i1}, \ldots, S_{im} \), 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 \( xU \xrightarrow{R} yV \).

**Proof.** If the equation \( xh(U) = h(V) \) has a parametric solution \( \{ (h_j, R_j) : 1 \leq j \leq m \} \), then the equation \( xU \xrightarrow{R} yV \) has the parametric solution \( \{ (h_j \circ h, R_j) : 1 \leq j \leq m \} \).

| 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

\[
x = h_1(x), \ y = h_1(y), \ z = h_1(z), \ R_1 \quad \text{or} \\
\vdots \\
x = h_m(x), \ y = h_m(y), \ z = h_m(z), \ R_m,
\]
if the unknowns are $x, y, z$. Actually, only one pair $(h, R)$ is needed. For example, if we have a parametric solution

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

we can replace it with

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

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 $x^n = y z$. They are

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

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

$$x = t^{j' + k'}, \quad y = t^{n j'}, \quad z = t^{n k'}$$

\[\text{or} \quad x = t^{j' + k' + 1}, \quad y = t^{n j' + 1}, \quad z = t^{n k' + n - 1} \]

\[\text{or} \quad x = t^{j' + k' + 2}, \quad y = t^{n j' + 2}, \quad z = t^{n k' + n - 2} \]

\[\vdots \]

\[x = t^{j' + k' + n - 1}, \quad y = t^{n j' + n - 1}, \quad z = t^{n k' + n - 1}, \]

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

$$p = b j_0 + c k_0 + \sum_{n=1}^{N} \frac{b b_n + c c_n}{a} i_n,$$

$$q = a j_0 + \sum_{n=1}^{N} b_n i_n,$$

$$r = a k_0 + \sum_{n=1}^{N} c_n i_n,$$

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 $uvwv$ in a nontrivial way, which contradicts the primitivity of $uv$. If $h(x) = v$, then $h(y) = v(uv)^j$ 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 $\alpha$ and $\beta$ are parametric words, then $|(\alpha\beta)|_a = |\alpha|_a + |\beta|_a$,

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

For example, $|((p^i)q^{ij})|_a = p_a^i q_a^j + p_a$. If $\varphi$ 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 $x = \alpha_1$, $y = \beta_1$, $z = \gamma_1$ or $x = \alpha_2$, $y = \beta_2$, $z = \gamma_2$.

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

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

We will show that if $\alpha, \beta, \gamma$ 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 $\varphi$, 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 $|\alpha|_a|\beta|_b - |\alpha|_a|\beta|_a$. 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).

\[\square\]

5 Exponential equations

Let $\alpha$ and $\beta$ be parametric words. The pair $(\alpha, \beta)$ 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 :
\[ \Lambda \to \mathbb{N}_0 \text{ that satisfy } f(\alpha) = f(\beta). \] 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 \( \Xi \) with \( k \) letters can be thought to be the set \( \{1, \ldots, k\} \). Then we can define the functions \( \lambda, \mu : \Xi^* \to \mathbb{Z}[X] \):

\[
\lambda(w) = X^{m+1}, \quad \mu(w) = a_mX^m + \cdots + a_1X + a_0
\]

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

\[
\alpha = s_0t_1^{i_1}s_1 \ldots t_m^{i_m}s_m, \quad \beta = u_0v_1^{j_1}u_1 \ldots v_n^{j_n}u_n,
\]

\( s_0, \ldots, s_m, t_1, \ldots, t_m, u_0, \ldots, u_n, v_1, \ldots, v_n \in \Delta^* \) 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

\[
\mu(s_0)\lambda(t_1)^{f(i_1)}\lambda(s_1) \ldots \lambda(t_m)^{f(i_m)}\lambda(s_m)
\]

\[
+ \frac{\mu(t_1)(\lambda(t_1)^{f(i_1)} - 1)}{\lambda(t_1) - 1} \cdot \lambda(s_1) \ldots \lambda(t_m)^{f(i_m)}\lambda(s_m)
\]

\[
+ \cdots + \frac{\mu(t_m)(\lambda(t_m)^{f(i_m)} - 1)}{\lambda(t_m) - 1} \cdot \lambda(s_m) + \mu(s_m),
\]

which can be rewritten as

\[
\left( \mu(s_0) + \frac{\mu(t_1)}{\lambda(t_1) - 1} \right) \lambda(s_1 \ldots s_m)\lambda(t_1^{f(i_1)} \ldots t_m^{f(i_m)})
\]

\[
+ \sum_{k=2}^{m} \left( \mu(s_{k-1}) + \frac{\mu(t_k)}{\lambda(t_k) - 1} - \frac{\mu(t_{k-1})\lambda(s_{k-1})}{\lambda(t_{k-1}) - 1} \right) \lambda(s_k \ldots s_m)\lambda(t_k^{f(i_k)} \ldots t_m^{f(i_m)})
\]

\[+ \mu(s_m), \]

10
and \( \mu(f(\beta)) \) is of the corresponding form. Thus the equation
\[
(\lambda(t_1) - 1) \ldots (\lambda(t_m) - 1)(\lambda(v_1) - 1) \ldots (\lambda(v_n) - 1)\mu(f(\alpha)) = (\lambda(t_1) - 1) \ldots (\lambda(t_m) - 1)(\lambda(v_1) - 1) \ldots (\lambda(v_n) - 1)\mu(f(\beta))
\]
can be rewritten as
\[
X^{P_1} + \ldots + X^{P_m} = X^{Q_1} + \ldots + X^{Q_N},
\]
where every \( P_k \) and \( Q_k \) is a linear polynomial with unknowns \( f(i), f(j) \). Equation (4) can be satisfied only if \( M = N \). Then it is equivalent with the formula
\[
\bigvee_\pi \left( (P_1 = Q_{\pi(1)}) \land \ldots \land (P_N = Q_{\pi(N)}) \right),
\]
where \( \pi \) runs over all permutations of \( N \) elements. Hence the claim follows. \( \square \)

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

**Theorem 5.2.** Let \( \Lambda = \{i, j\} \). Let \( s_0, \ldots, s_m, t_1, \ldots, t_m, u_0, \ldots, u_n \) and \( v_1, \ldots, v_n \) be parametric words of height at most one, with no occurrences of parameter \( j \). Assume that \( i \) occurs at least in the words \( t_1, \ldots, t_m \) and \( v_1, \ldots, v_n \). Let \( \alpha = s_0t_1^1s_1 \ldots t_m^1s_m \) and \( \beta = u_0v_1^1u_1 \ldots v_n^1u_n \). 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
\[
X^{P_1} + \ldots + X^{P_m} = X^{Q_1} + \ldots + X^{Q_N},
\]
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
\[
\bigvee_\pi \left( (P_1 = Q_{\pi(1)}) \land \ldots \land (P_N = Q_{\pi(N)}) \right),
\]
where \( \pi \) 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 \( a \neq 0 \), 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. \( \square \)
The parametric words in the next theorem come from Lemma 2.9. Ex-
ponential 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

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

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 \( y^aA = y^aB \). Let the maximal
prefixes of the left- and right-hand sides of the form \( y^at_1 \ldots y^at_n \), where
\( t_l \in \{ x, z \} \), be \( U \) and \( V \). Now the equation is \( UA_1 = VB_1 \). Let \( T =
qp(pq)^{k+1}p)^{a-1}pq \). 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

\[
P(f(i), f(j), f(k)) = Q(f(i), f(j), f(k)).
\]

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

\[
f(T^ch(A_1)) = f(h(B_1)),
\]

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 \( B_1 = y^aB_2 \). Now (8) can be reduced to \( f(T^{c-1}h(A_1)) =
f((pq)^{k+1}ph(B_2)) \), 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 \( y^ax \) or \( y^az \), 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 equa-
tions \( h(U) = h(V) \), \( h(A_1) = h(B_1) \). 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 $E : s_0 t^i s_1 \ldots t^i s_m = u_0 t^i u_1 \ldots t^i u_n$ be an exponential equation of height one, $s_0, \ldots, s_m, u_0, \ldots, u_n, t \in \Delta^*$ and

$$\left|s_0 \ldots s_m u_0 \ldots u_n\right| < S|t|.$$ 

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 $b \leq 2|s_0 \ldots s_m t|$. 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 $|B| \leq 2|s_0 \ldots s_m u_0 \ldots u_n t^2|$. 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. $\square$

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. $x^a y \ldots = y^b x \ldots$
B2. $x^2 \ldots \Rightarrow y^a x \ldots$
B3. $x y t \ldots \Rightarrow z x y \ldots$
B4. $x y t \ldots \Rightarrow z y x \ldots$
B5. $x y z \ldots = z y x \ldots$
B6. $x y z \ldots = z y x \ldots$
B7. $x y z \ldots = z y x \ldots$
B8. $x y t \ldots \Rightarrow z^a x y \ldots$
B9. $x y x z \ldots \Rightarrow z x^2 y \ldots$
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 \( \{(h_j, R_j) : j = 1, \ldots, m\} \), where \( \Delta = \{p, q\} \) and \( \Lambda = \{i_1, \ldots, i_k\} \). 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

\[
\{(h_j, R_j \cap R_j') : j = 1, \ldots, m\} \cup A,
\]

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 \( \square \)

**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 \( x \mapsto yz \) to the equation \( xyz \ldots = y^a x \ldots \), which is of the form B1. The equations B3 and B4 are reduced by the substitution \( x \mapsto zx \) to the equations \( xyz \ldots = zyx \ldots \) and \( xyz \ldots = yzx \ldots \), which are of the form B5. The equation B8 is reduced by the substitution \( x \mapsto zx \) to the equation \( xyzA = zyx^a xyB \) for some \( A, B \in \Xi^* \). By Lemma 2.11, this is equivalent with the equation \( xyzxyzA = zyx^{a} xyB \), 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 \( xy = yx, xyz = zxy, xyz = zyx, x y^2 z = z y^2 x \) and \( xyzz \Rightarrow z x^2 y \) 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.

\[\begin{array}{c}
7\quad \text{Images and } \theta\text{-images}
\end{array}\]

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

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

\[h(x) = h(V^k t_1 \ldots t_i)u\quad (9)\]

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

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

\[xf(U) \Leftrightarrow f(t_{i+1} \ldots t_n t_1 \ldots t_i)xf(W).\quad (10)\]

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

\[xU(V^k Px, y, z) \Leftrightarrow QPxW(V^k Px, y, z).\]

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 $E_1, \ldots, E_n$ by an $n$-tuple of substitu-
tions, if $E$ is of the form $xU(x, y, z) \Rightarrow t_1 \ldots t_k xV(x, y, z)$, where $1 \leq n \leq k$
and $t_1, \ldots, t_k \in \{y, z\}$, equation $E_i$ is

\[xU(t_1 \ldots t_i x, y, z) \Leftrightarrow t_{i+1} \ldots t_k t_1 \ldots t_i xV(t_1 \ldots t_i x, y, z),\]

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

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

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 $E_1, \ldots, E_m$ by an $m$-tuple of substitutions, and if $E_1, \ldots, E_m$ 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

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

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

$$xy^bU(x, y, z) \Rightarrow z^cV(x, z)yW(x, y, z),$$

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 $E : xU(x, y, z) \Rightarrow V(y, z)xW(x, y, z)$, where both $y, z$ occur in $V$, and its images

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

(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

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

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 $E_{P,T}, E_{P,T+1}, E_{P,T+2}$, \ldots 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 $x \mapsto V^iPx$, $g$ 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 $|V^iPx| = O(n^2)$, 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 $E_1, E_2, \ldots$, and if $E_m, E_{m+1}, \ldots$ are equivalent, then the solutions of $E$ can be parameterized in terms of the solutions of $E_1, \ldots, E_m$. 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 $\theta$-images, which are defined later.

Consider an equation of type II

$$xy^b A(x, y, z) \Rightarrow z^c x B(x, z) y C(x, y, z),$$

(12)

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

$$xy^b A(z^i x, y, z) \Leftarrow z^c x B(z^i x, z) y C(z^i x, y, z).$$

(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

$$y^b A((xz)^i x, y, xz) = (zx)^c(xz)^d y C((xz)^i x, y, xz).$$

(14)

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

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

(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 $h(xz) = t^{\alpha i}$ and $D = v^{\alpha j}$. 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

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

(16)
where \( s_0, \ldots, s_m, u_0, \ldots, u_n \in \Delta^* \), 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 \( t_k \not\in s_k t_{k+1} \) 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

\[
|s_0 \ldots s_m u_0 \ldots u_n (tv)^2| < S|t^a| \quad \text{and} \quad b < a_1 S \tag{17}
\]

when \( ai' + b \) is in \( \{p_1, \ldots, p_m, q_1, \ldots, q_n\} \). 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 \( |t_k f(p_k)| > |s_0 \ldots s_m u_0 \ldots u_n (tv)^2| \) 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 \( \theta \)-images.

A sequence of equations \( E_0, \ldots, E_n \) 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 \( \theta \)-images of equations of type I and II. For equations of type I all images are \( \theta \)-images. For equations of type II the degenerated images of order 2 and nondegenerated images of order 3 are \( \theta \)-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 \( O(n^2) \).

18
Thus the equations
\[ E_T = x, y, z \]
Assume that all letters \( h \) and is of size \( O \) of the third order of length \( P \) second order. So also the original equation (12). The equations of \( G \) images. These images are nondegenerated images of the third order of the \( \theta \)-images of length \( O(n^{18}) \).

**Proof.** Let these solutions be called \( \tau \)-solutions. Let \( E_i \) be the equation (13) and let \( h \) be its solution. Theorem 5.4 can be used for the exponential equation
\[ h(xy^bA(z^i)x, y, z)) = h(z^ixB(z^i)x, z)yC(z^i)x, y, z)), \]
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 \( \theta \)-images of length \( O(n^{18}) \).

**Proof.** Let these solutions be called \( \tau \)-solutions. Let \( E_i \) be the equation (13). By Lemma 7.4, the \( \tau \)-solutions can be parameterized in terms of the \( \tau \)-solutions of \( E_0, \ldots, E_T \) for some \( T \). Let \( P_i \) be the set of those \( \tau \)-solutions \( h \) of \( E_i \), for which \( |h(z)| \geq |h(xy)| \), and let \( Q_i \) be the set of those \( \tau \)-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 \( \theta \)-images of (12).

In this construction there are \( O(n) \) images of the first order of length \( O(n^2) \), \( O(n^3) \) 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 \( A \), \( y \not\subseteq A \), \( 0 < q \leq n \) and \( a_q + c + 2 \leq
\[ k \leq i - c - |A| \]. Let
\[
D_1(x, z) = (zx)^c((xz)^{i+a_1}x)\ldots((xz)^{i+a_q-1}x)xz,
\]
\[
D_2(x, z) = (xz)^{i-k+a_q}((xz)^{i+a_q+1}x)\ldots((xz)^{i+a_n}x)(xz)^p.
\]

Now the equations
\[
y(D_1B)^a A((xz)^{i}x, D_1B, xz) \iff zD_2D_1 C(x, y, z)
\]
\[
y(D_1B)^a A((xz)^{i}x, D_1B, xz) \iff D_2D_1 C(x, y, z)
\]

have only trivial solutions.

**Proof.** The first equation is reduced by the morphism \( z \mapsto yz \) to the equation
\[
(D_1(x, yz)B')^a A((xyz)^{i}x, D_1(x, yz)B', xyz) = zD_2(x, yz)D_1(x, yz)C'.
\]

If \( a > 0 \), then the equation is of the form
\[
(yzx)^c x \ldots = (zxy)^{i-k} \ldots.
\]
Because \( c > 0 \) and \( i - k \geq c + 1 \), this equation has only trivial solutions by Corollary 2.5. If \( a = 0 \) and \( z^m y \leq A, m > 0 \), then the equation is of the form
\[
(xyz)^m y \ldots = (zxy)^{i-k} \ldots.
\]
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
\[
(xyz)^{m+i} \ldots = (zxy)^{i-k+a_q} zxxz \ldots,
\]
except if \( n = q \) and \( p = 0 \), when it is of the form
\[
(xyz)^{m+i} \ldots = (zxy)^{i-k+a_q} zx(yzx)^c xyz \ldots.
\]
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.

The second equation is similar. It is reduced by the morphism \( x \mapsto yx \) to the equation
\[
(D_1(yx, z)B')^a A((yxz)^{i}yx, D_1(yx, z)B', yxz)
\]
\[
= x(yzx)^{i-k+a_q}((yxz)^{i+a_q+1}yx)\ldots((yxz)^{i+a_n}yx)(yxz)^p D_1(yx, z)C'.
\]

If \( a > 0 \), then the equation is of the form
\[
(yzx)^c y \ldots = (xzy)^{i-k} \ldots.
\]
Because \( c > 0 \) and \( i - k \geq c + 1 \), this equation has only trivial solutions by Corollary 2.5. If \( a = 0 \) and \( z^m y \leq A, m > 0 \), then the equation is of the form
\[
(yxz)^m z \ldots = (xzy)^{i-k} \ldots.
\]
Because \( i - k \geq m + 1 \), this equation has only trivial solutions by Corollary 2.5. If \( a = 0 \) and \( z^m \leq A, m \geq 0 \), then the equation is of the form

\[(yz)^m + \ldots = (xzy)^{i-k+a} xy \ldots,\]

except if \( n = q \) and \( p = 0 \), when it is of the form

\[(yz)^m + \ldots = (xzy)^{i-k+a} x(yz)^q yx \ldots.\]

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 \( O(n^\theta) \) of its \( \theta \)-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 \( z \mapsto xz \):

\[y^h A((xz)^i, y, xz) \Rightarrow (xz)^i B((xz)^i, xz)yC((xz)^i, y, xz).\]

(18)

The length constraint is now \( |h(y)| \geq |h(z)| \). Equation (18) is a nondegenerated image of the second order of (12). Let \( D = (xz)^k B((xz)^k, xz) \). 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

\[y(D^j D_1 y)^{k-1} A((xz)^i x, D^j D_1 y, xz)\]

\[\Leftrightarrow D_2 D_1 B((xz)^i, xz)yC((xz)^i, D^j D_1 y, xz),\]

(19)

where \( D_2 = D \).

We can write \( D = (xz)^c ((xz)^{i+a_1} x) \ldots ((xz)^{i+a_n} x)(xz)^p \), 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

\[D_1 = (xz)^c (xz)^{i+a_1} x \ldots ((xz)^{i+a_q} x)(xz)^k,\]

\[D_2 = (xz)^{i-k+a_q} x ((xz)^{i+a_q+1} x) \ldots ((xz)^{i+a_n} x)(xz)^p\]

or

\[D_1 = (xz)^c ((xz)^{i+a_1} x) \ldots ((xz)^{i+a_q} x)(xz)^k x,\]

\[D_2 = z((xz)^{i-k+a_q} x ((xz)^{i+a_q+1} x) \ldots ((xz)^{i+a_n} x)(xz)^p,\]

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 $U \equiv V$ 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 $(xz)^j$ with $(xz)^m(xz)^m$ 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 $\theta$-images of length $O(n^{18})$.

**Proof.** The required $\theta$-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 $\theta$-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 $O(n^8)$ 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 $\theta$-images.

We define a complete set of $\theta$-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 $\theta$-images consisting of $O(n^{26})$ equations of length $O(n^{27})$.

We assume that every complete set of $\theta$-images satisfies the conditions of Theorem 7.10.

**Theorem 7.11.** Let $E$ be a word equation of length $n$. If $\{E_1, \ldots, E_m\}$ is a complete set of $\theta$-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 $h(x) = h(z)^mu$ for some $m \geq 1$ and $u \leq h(z)$, $h(z) = uv$ for some $v$ and $y = vuv$ 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

$$yzx \ldots = (zx)^cy \ldots$$

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

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

then $uv = vu$. 

---

23
Proof. Let $u = wt$. From $wu^{c+1}v \ldots = u^{c+1}vu \ldots$ it follows that
\[(wt)^{c+1}v \cdots = t(wt)^{c}vwt \ldots \quad \text{and} \quad (wt)^{c+1}v = t(wt)^{c}vw.\]
From $w(uv)^{c}u^{2} \ldots = (uv)^{c}u^{2} \ldots$ it follows that
\[(wtv)^{c}wtv\cdots = tv(wtv)^{c-1}wtv\ldots \quad \text{and} \quad (wtv)^{c}wt = tv(wtv)^{c-1}wtv.\]
In both cases the beginnings and ends of the last equation give $wt = tw$ and $wtv = twv$. So $\rho(w) = \rho(t) = \rho(tv) = \rho(v) = \rho(u)$. \[\square\]

Lemma 8.2. Let $E_0$ be the equation $xy^{a}zy^{b}s \ldots \Rightarrow zy^{b}xy^{a}t \ldots$, 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 $xP \Rightarrow zQ$ and $E_0, \ldots, E_k$ be a degenerated chain. Now the solutions of $E_k$ satisfying $y \neq 1$ are also solutions of the equation $xy^{a}zy^{b} \Rightarrow zy^{b}xy^{a}$.

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 $xy^{a}zy^{b}r \ldots \Rightarrow zy^{b}xy^{a}r \ldots$, where
\[r = (f_k \circ \cdots \circ f_1)(z) = (f_k \circ \cdots \circ f_1)(((xy^{a})^{c_3}zy^{b})^{c_2}xy^{a})^{c_1}(xy^{a})^{c_1}.\]
Let $f = f_k \circ \cdots \circ f_1$. 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
\[
|h(xy^{a}zy^{b})| - |h(zy^{b}xy^{a})| \leq |a + p - b - q|h(y)|
\leq (a + b)|h(y)| + |p - q||h(y)| \leq (1 + |p - q|)|h(xy^{a}zy^{b})|
\leq (k - 7)|h(xy^{a}zy^{b})| \leq |h(f(xy^{a}))|.
\]
Thus
\[w((u^{c_3}v)^{c_2}u)^{c_1}u^{c_3} = ((u^{c_3}v)^{c_2}u)^{c_1}u^{c_3} \ldots ,\]
where $u = h(f(xy^{a}))$, $v = h(f(zy^{b}))$ and $|v| \leq |u|$. Now, by Lemma 8.1, either $w = 1$ or $uv = vu$. In other words, $h(xy^{a}zy^{b}) = h(zy^{b}xy^{a})$ 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 $a + p \neq b + q$. \[\square\]

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

N1. $E_1, \ldots, E_n$ form a complete set of $\theta$-images of $E$,

N2. $E$ reduces to $E_1, \ldots, E_n$ 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 $U \Rightarrow V$ and $V \Rightarrow U$,
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 \( xy^a zy^b = zy^b xy^a zQ \).

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 \( E_1, \ldots, E_m \) 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 \( E_1, \ldots, E_n \), 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 \( O(n^{27k}) \). If each leaf equation in this tree has a parametric solution of length at most \( c \), then \( E \) has a parametric solution of length \( O(n^{5227k}c) \).

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

\[
a(na)^{52} \cdot a((an)^{27})^{52} \cdot a((an)^{27^2})^{52} \cdots a((an)^{27^{k-1}})^{52} \cdot c < a^k(an)^{5227k}c = O(n)^{5227k}c.
\]
A tree in which all leaves are basic equations is a basic tree.

If every \( \theta \)-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 \( \theta \)-images. The rule N1 is used this way instead of explicitly selecting some complete set of \( \theta \)-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 \( xyz^2 A(x, y, z) = yz^2 x B(x, y, z) \) has a basic tree.

**Proof.** With N5 we get the equation \( Axyz^2 = Byz^2 x \), and then with N4 the equation \( z^2 y x A^R = x^2 y B^R \). With N3 we get \( z^2 y x A^R \Rightarrow x^2 y B^R \) and \( z^2 y x A^R \Leftarrow x^2 y B^R \). The former is basic of the form B2. The latter is reduced by the pair of substitutions \( x \mapsto zx \), \( x \mapsto z^2 x \) to the equations \( y z x \ldots \Rightarrow x^2 y \cdots \) and \( y z^2 x \ldots = x z^2 y \cdots \). These are basic of the form B9 or B7 and we get a basic tree. \( \square \)

**Lemma 8.6.** The equation \( x^2 y z \ldots \Rightarrow z y x \ldots \) has a basic tree.

**Proof.** This equation is reduced by the pair of substitutions \( x \mapsto zx \) and \( x \mapsto zy \) to the equations \( xzxy \ldots \Leftarrow yzx \ldots \) and \( xzxyz \ldots = zyx \ldots \). The latter is basic of the form B5 and the first is reduced by the substitution \( y \mapsto xy \) to the equation \( x^2 y z \ldots = y z x^2 y \ldots \), which has a basic tree by Lemma 8.5. \( \square \)

**Lemma 8.7.** Every nondegenerated \( \theta \)-image of \( xy^2 z \ldots \Rightarrow z y^2 x \ldots \) has a basic tree.

**Proof.** The equation is of type I, so its nondegenerated \( \theta \)-images are of the form \( xy^2 z \ldots \Leftarrow y^2 xz \ldots \) or of the form \( xy^2 z \ldots \Leftarrow zyx \ldots \). These are basic of the form B2 or B8. \( \square \)

**Lemma 8.8.** Every nondegenerated \( \theta \)-image of \( x y z t A(x, y, z) \Rightarrow z x^2 y B(x, y, z) \), where \( t \neq z \), has a basic tree.

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

\[
yxzg(h(tA)) \Rightarrow z((xy)^j xz)^i xyg(h(B)), \quad (21)
\]

where \( h \) is the morphism \( x \mapsto z^i x \) and \( g \) is the morphism \( z \mapsto (xy)^j xz \). The nondegenerated \( \theta \)-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

\[
yxzC((xz)^i x, D^k D_1 y, xz) \Leftarrow D_2 D_1 y B((xz)^i x, D^k D_1 y, xz), \quad (22)
\]
where $D = D_1D_2 = zx(xz)^i x$, $D \neq D_1$ and $D^kD_1 \neq 1$. If $D_2D_1$ begins with one of $x^2$, $xxz$, $zzz$, then (22) is a basic equation. Otherwise $D_2D_1$ begins with $zx^2$, $D_1 = 1$ and $k > 0$. Then (22) is

$$yzC((xz)^i x, D^k y, xz) \iff zx(xz)^i xyB((xz)^i x, D^k y, xz).$$

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

$$xyzC((xyz)^i x, E^k y, xyz) = zx(xyz)^i xyB((xyz)^i x, E^k y, xyz),$$

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

(a) $xyzx = zxx$ and $y \ldots = z \ldots$, if $t = x$,
(b) $xyzyxx = zxxzx$ and $y \ldots = z \ldots$, if $t = y$ and $i > 1$,
(c) $xyzyxx = zxxzx$ and $y \ldots = x \ldots$, if $t = y$, $i = 1$ and $y \nleq B$,
(d) $xyzyxx = zxxzx$ and $(yzx)y \ldots = (yzx)x \ldots$, if $t = y$, $i = 1$ and $y \nleq B$.

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

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

$$yzz((xy)^j xz)^i x g(h(A)) \Rightarrow zx((xy)^j xz)^i x g(h(B)).$$

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

$$yxxy \ldots \Rightarrow zxy(xy)^j xzxy \ldots.$$ 

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

$$yx \ldots \Rightarrow x^2 \ldots, \quad yzx \ldots \Rightarrow xxz \ldots, \quad yzxxs \ldots \Rightarrow x^2 yzxx \ldots,$$

where $s \neq x$. The two first equations are basic of the form $B_2$ and $B_3$. The third equation is equivalent with the pair of equations $yzzx^2 \Rightarrow zx^2 yzx$, $s \ldots = x \ldots$ and has only trivial solutions by Corollary 2.5. \hfill \Box

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

$$x^a y^b t \ldots \Rightarrow zyx \ldots \quad \text{or} \quad x^a y^b t \ldots \Rightarrow zxy \ldots,$$  \hfill (23)
or of the form
\[ x^a y^b t \ldots \Rightarrow z(yz)^d x \ldots \]  \tag{24}

A tree whose leaves are basic equations, supporting equations of the form (23) or equations \( x^2 y t \ldots \Rightarrow zyzxy \ldots \), 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
\[ E_0 : x y^a t A(x, y, z) \Rightarrow z^c x B(x, z) y C(x, y, z), \]
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 \( xy^a z \ldots \Rightarrow zz \ldots \);
2. if \( a = 2, c = 1, B = 1 \) and \( y \not\in C \), then \( E_2 \) is of the form \( xy^2 z \ldots \Rightarrow zyx \ldots \);
3. if \( a = 2, c = 1 \) and \( B = x \), then \( E_2 \) is of the form \( xy^2 z \ldots \Rightarrow zz^2 y \ldots \);
4. if \( a = 1 \), then \( E_2 \) is basic equation \( B3 \) or of the form \( xyzs \ldots \Rightarrow zz^2 y \ldots \), 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 \( y \not\in C \), then \( E_3 \) is a basic equation or of the form \( yxz \ldots \Rightarrow zxy \ldots \);
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 \( x^2 y s \ldots \Rightarrow zyzxy, \) 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
\[ x y^a z A_1(x, y, z) \Leftarrow z^c x B(z^i x, z) C(z^j x, y, z), \]
where \( i > 0 \) and \( A_1 \neq 1 \). Its image \( E_2 \) is of the form
\[ D_2 D_1 z A_2(x, y, z) \Rightarrow z h(z^{c-1} x B(z^i x, z) C(z^j x, y, z)), \]
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 \( z \not\in A_2 \neq 1 \).

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. \( \square \)
Lemma 9.2. Let \( s, t \neq y \). Every nondegenerated \( \theta \)-image of the equation \( xy^2s \ldots \Rightarrow zxyt \ldots \) has a basic tree. Every nondegenerated \( \theta \)-image of the equation \( xy^2z \ldots \Rightarrow zx^2y \ldots \) 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 \( yxzy \ldots \Rightarrow zxzy \ldots \) is reduced by the substitution \( y \leftrightarrow zy \) to the equation of Lemma 8.5. \( \square \)

Lemma 9.3. Let \( s \neq x \) and \( t \neq y \). Consider the equations

(a) \( xy^2z \ldots \Rightarrow zx^2y \ldots \),
(b) \( xyzs \ldots \Rightarrow zxy^2 \ldots \),
(c) \( xy^2z \ldots \Rightarrow zxyt \ldots \),
(d) \( xyzt \ldots \Rightarrow zy^2x \ldots \),
(e) \( xyz \ldots \Rightarrow zy^2x \ldots \).

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 \( xy^azy^bu \ldots \Rightarrow zy^bxu^v \ldots \), 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 \( \theta \)-images for \( E_0 \), a complete set of \( \theta \)-images for each of these, and so on \( l \) times. These \( \theta \)-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 \( \theta \)-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') \( xy^2z \ldots \Rightarrow zxy^2 \ldots \)
(b') \( xyz \ldots \Rightarrow zxy^2 \ldots \)
(c') \( xy^2z \ldots \Rightarrow zxyt \ldots \)
(d') \( xyz \ldots \Rightarrow zy^2x \ldots \)

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 \( \theta \)-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 $E_0, \ldots, E_{j-1}$ are of type I. Let $0 \leq i < j$. If $i$ is even, then $E_i$ is of the form $xyz \Rightarrow zy^2x \ldots$. If $i$ is odd, then $E_i$ is of the form $zy^2x \ldots \Rightarrow xyz \ldots$. Assume first that $j$ is even. Now $E_j$ is of the form $yzxz \Rightarrow zy^2x \ldots$. Let $r \neq z$. This is the equation (b). Assume then that $j$ is odd. Now $E_j$ is of the form $yz^2 \ldots \Rightarrow xy \ldots$ or $zy \ldots \Rightarrow xyz \ldots$. 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 $x^a y^b t \ldots \Rightarrow zyx \ldots$, 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 $zyx \ldots \Rightarrow xy^2z \ldots$ or $yzzx \ldots \Rightarrow xy^2z \ldots$, 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 $xzxy \ldots \Leftrightarrow yzxs \ldots$ and $xzy \ldots = zyx \ldots$, 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 $yzxz \ldots \Leftrightarrow Dy$, where $D$ is a conjugate of $zxz$. If $D = xzx$, then this image is basic of the form B4. If $D = z^2$, then it is the equation (c) of Lemma 9.3. If $D = x^2 z$, then it is the equation of Lemma 8.6.

Second, consider the equation $x^a y^b t \ldots \Rightarrow zxy \ldots$, 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 $\theta$-images of the equation are, by 2 of Lemma 9.1, basic equations or of the form $xy^2z \ldots \Rightarrow zyxz \ldots$ or $yzzx \ldots \Rightarrow zyxz \ldots$. 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 $x^a y^b t \ldots \Rightarrow zyxz \ldots$, 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 $x \mapsto zx$:

$$xzxyz \ldots \Leftrightarrow yz^2xy \ldots.$$  

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

The images of the equation

$$zx^2yz \ldots \Rightarrow yz^2x^2 \ldots$$  

(25)
are of the form $zx^2yy'z\ldots \rightleftharpoons yzy'zx^2\ldots$, and the images of this under the morphisms $y \mapsto zy$, $y \mapsto zxy$, $y \mapsto z^2y$ and under other morphisms are

\begin{align*}
  x^2(zy)^{i+1}\ldots \rightleftharpoons yz(zy)^i zx^2\ldots, \\
xzz\ldots \rightleftharpoons yz^2x\ldots, \\
zx^2yzx\ldots \rightleftharpoons yz^2x^2y\ldots, \\
Dyzx\ldots \rightleftharpoons yz^2x^2z\ldots,
\end{align*}

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

\[ xyx(zy)^{i+1}\ldots \rightleftharpoons z^2(yz)^i(yx)^2\ldots. \]

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

\[ yx(xzy)^{i+1}\ldots \rightleftharpoons zxz(yxz)^i(yx)^2\ldots. \]

This is reduced to the equation

\[ yx(xz^2y)^{i+1}\ldots = xz(zyxz)^i(yzx)^2\ldots, \]

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. So (25) has a basic tree.

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

\begin{align*}
  x^2zxy\ldots \rightleftharpoons yz^2x^2\ldots, \\
xzx\ldots \rightleftharpoons yz^2x^2\ldots, \\
zx^2yz\ldots \rightleftharpoons yz^2x^2\ldots.
\end{align*}

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 $x \mapsto yx$:

\[ xyxyz\ldots \rightleftharpoons z^2(yx)^2\ldots. \]

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

\[ yx^2zyxz\ldots \rightleftharpoons zxz(yx)^2\ldots. \]
This is reduced to the equation
\[yx^2z^2yz \ldots = xz(zyx)^2 \ldots,\]
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 \(xyt \ldots \Rightarrow z(yz)^d x \ldots.\) Every image of
this equation has a basic tree by Lemma 9.4.

If \(a = 1\) and \(b = 2,\) then the equation is \(xy^2t \ldots \Rightarrow z(yz)^d x \ldots.\) Its
images are of the forms
\[xy^2z \ldots \Leftrightarrow zyz \ldots,\]  
\[xy^2z \ldots \Leftrightarrow yzy \ldots,\]  
\[xy^2z \ldots \Leftrightarrow yz^2s \ldots,\]  
\[xy^2z \ldots \Leftrightarrow z^2yt \ldots,\]  
where \(s \neq z, t \neq y.\) All images of (33) are of the form (23). All \(\theta\)-images
of (34) are, by 4 of Lemma 9.1, basic equations, supporting equations (23),
or equations (b) of Lemma 9.3. All \(\theta\)-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 \(x^2y^bt \ldots \Rightarrow z(yz)^d x \ldots.\) Its images are
supporting equations (23), except for the image under the morphism \(x \mapsto zx:\)
\[xzxy \ldots \Rightarrow (yz)^d zx \ldots.\]

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 \(xy^a zy^b s \ldots \Rightarrow zy^b xy^qt \ldots,\) 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 \(x \mapsto zy^c x\)
\((c = 0, \ldots, b)\) to the equations
\[xy^a z \ldots \Leftrightarrow y^{b-c} zy^c x \ldots \quad (c = 0, \ldots, b - 1),\]  
\[xy^a zy^b sP = zy^b xy^qtQ.\]
When $b-c > 1$, the equation (37) is basic of the form B2. When $b-c = 1$, its $\theta$-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 $y^d z y^a x \ldots = x y^b z \ldots$, where $d = b-a \geq 1$. Split this into one-sided equations

\begin{align}
y^d z y^a x \ldots &\Rightarrow x y^b z \ldots , \quad (39) \\
y^d z y^a x \ldots &\Leftarrow x y^b z \ldots . \quad (40)
\end{align}

If $d > 1$, then (39) is basic of the form B2. If $d = 1$, then its $\theta$-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

\begin{align}
y^{d-c} z y^{a+c} x \ldots &\Rightarrow x y^b z \ldots \quad \text{and} \quad z y^{a+d} x \ldots = x y^b z \ldots .
\end{align}

Latter is basic of the form B6 or B7, former is of the form (39). \hfill \square

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

*Proof.* The equation can be written in the form $x y^a z y^p u \ldots \Rightarrow z y^b x y^q v \ldots$, 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 $\theta$-images of $E_0$, a complete set of $\theta$-images of these, and so on $l$ times. These $\theta$-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 $\theta$-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 $x y^a z y^b x P \Rightarrow z y^b x y^a z Q$, 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 $\theta$-image of $E_{j-1}$. If $b = 0$, the equation $E_0$ is of the form $x y^a z \ldots \Rightarrow z x \ldots$, 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 $x y^a z \ldots \Rightarrow z y^b x \ldots$. Equation $E_{j-1}$ is of the same form. Now $E_j$ is of the form $y^c z y^d x \ldots \Rightarrow x y^a z \ldots$, 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. \hfill \square

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

*Proof.* By 1 of Lemma 9.1, all $\theta$-images of this equation are supporting equations or equations of Lemma 10.2. \hfill \square
Lemma 10.4. The equation $x^ny^mt \ldots \Rightarrow zyA(y,z)x \ldots$, 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

$$xy^mz \ldots \Rightarrow Dx \ldots,$$

(41)

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

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

(42)

and all the other images are of the form

$$xzy \ldots \Rightarrow Dx \ldots,$$

(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 $y \leq D$, then this is the equation of Lemma 10.3. If $z \leq D$, then this is of the form

$$x^ay^b \ldots \Rightarrow zy^dx \ldots,$$

(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

$$x^ay^b \ldots \Rightarrow z(yz)^dx \ldots,$$

(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 $xy^bz \ldots \Rightarrow Dx$, 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 $x(zx)^{a-1}y \ldots \Rightarrow y^dzx \ldots$, and all other images are of the form $xzy \ldots \Rightarrow Dx \ldots$, where $D$ is a conjugate of $zy^d$. First of these goes back to the case $a = 1$. The latter has a basic tree by Theorem 9.6.

Consider equation (45). Assume first that $a = 1$. Now every image of this equation is of the form $xy^bz \ldots \Rightarrow Dx$, where $D$ is a conjugate of $z(yz)^d$. If $yz \leq D$, this is the equation of Lemma 10.3. Otherwise $Dx = zczys$, 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 $x(zx)^{a-1}y \ldots \Rightarrow (yz)^dzx \ldots$, and all other images are of the form $xzy \ldots \Rightarrow Dx \ldots$, 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. \qed
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

\[
\begin{align*}
x^2 \ldots & \Rightarrow y^c x \ldots \quad (46) \\
x y \ldots & \Rightarrow y^c x \ldots \\
xyz^a t \ldots & \Rightarrow y^c x B(x, y) z \ldots \quad (48) \\
x^a y^b s \ldots & \Rightarrow y^c z B(y, z) x \ldots \quad (49) \\
x^a z^b t \ldots & \Rightarrow y z B(y, z) x \ldots \quad (50) \\
x^a z^b t \ldots & \Rightarrow y^d z B(y, z) x \ldots \\
\end{align*}
\]

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 $xy \ldots \Leftarrow Dx \ldots$, 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 $x(y \ldots)^{a-1} z^b y \ldots \Leftarrow Dx \ldots$, 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

\[
xy^a zy^p \ldots \Rightarrow zy^b xy^q \ldots \\
\]

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 $xU(x, y, z) \Rightarrow y^b x V(x, y, z)$ can be turned into $xU(y^i x, y, z) \Leftarrow y^b x V(y^i x, y, z)$ 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**


