Complexity of Makanin's Algorithm

ANTONI KOŚCIELSKI AND LESZEK PACHOLSKI

University of Wrocław, Wrocław, Poland

Abstract. The exponent of periodicity is an important factor in estimates of complexity of word-unification algorithms. We prove that the exponent of periodicity of a minimal solution of a word equation is of order $2^{1.07d}$, where d is the length of the equation. We also give a lower bound $2^{0.29d}$, so our upper bound is almost optimal and exponentially better than the original bound $(6d)^{2^{2d^4}} + 2$. Consequently, our result implies an exponential improvement of known upper bounds on complexity of word-unification algorithms.

Categories and Subject Descriptors: F.2.2 [**Analysis of Algorithms and Problem Complexity**]: Nonnumerical Algorithms and Problems—*computations on discrete structures*; I.1.2 [**Algebraic Manipulation**]: Algorithms—*algebraic algorithms*

General Terms: Algorithms, complexity, equations

Additional Key Words and Phrases: Diophantine equations, periodicity, semantic unification, semigroups, word equations

1. *Introduction*

The problem of whether the set of all equations that are satisfiable in some free group—or, equivalently, in all groups—is recursive (usually called the *satisfiability problem for group equations*), and the analogous problem for semigroups (usually called the *satisfiability problem for semigroup equations*) were first formulated by A. A. Markov in the early sixties (see Adyan and Makanin [1984/1986]). Special cases of the problem were solved affirmatively by A. A. Markov (see Adyan and Makanin [1984/1986]), Yu.I Khmelevskiĭ [1967], G. Plotkin [1972], and A. Lentin [1972]. But the full solution turned out to be extremely difficult and eluded researchers for many years.

The breakthrough came in a series of papers by Makanin [1977; 1982/1983; 1984/1985]. The first of these, which is long and very technical, gave a positive solution to the satisfiability problem for semigroup equations. The second, which

---

A preliminary version of this paper appeared in the *Proceedings of the 31st IEEE Symposium on Foundations of Computer Science*. IEEE, New York, 1990, pp. 824–829.

This research was partially supported by KBN grants 2 1197 91 01 and 8 S503 022 07.

Authors' address: Instytut Informatyki, Uniwersytet Wrocławski, Przesmyckiego 20, 51-151 Wrocław, Poland; e-mail: {kosciels, pacholsk}@tcs.uni.wroc.pl.

appeared a few years later, together with corrections published in the third paper, established the analogous and much more difficult result for groups.

Makanin's decision procedure for equational satisfiability in semigroups has received a lot of attention in the literature, mainly from computer scientists. Undoubtedly, this is because the notion of a free semigroup—in other words, of an algebra of words (or strings) with the operation of concatenation—is of fundamental importance in computer science: most algorithms and data structures refer to words. Thus, several improvements of Makanin's algorithm have been given,[1] and attempts have even been made to implement the algorithm (see Abdulrab [1987]). Moreover, related unification problems have been studied. In particular, Jaffar [1980] describes an algorithm for generating a minimal and complete set of unifiers for any satisfiable semigroup equation.

Despite the fact that Makanin's algorithm has been intensively studied, and despite its obvious potential for important applications, no systematic investigation of its complexity has yet been undertaken. A possible reason for this is the complicated nature of the algorithm itself. It consists of a series of involved transformations applied to complex data structures. At each step of the algorithm, the transformation to be applied is chosen from a set of several possible transformations, and depends on the form of the data structure to which it is to be applied. The data structures themselves are called *generalized equations.*

In this paper, we undertake the investigation of the complexity of Makanin's algorithm for semi-groups. To facilitate this, we give here a brief sketch of the structure of the algorithm. For simplicity, we refer only to equations and not to generalized equations.

The algorithm consists of the repeated application of certain basic procedures. The first of these determines whether or not an equation is simple. The second, a nondeterministic reduction procedure, when applied to a nonsimple equation, generates a member of a finite set of "reduced" equations such that the original equation is satisfiable if and only if one of its reduced equations is satisfiable. The third procedure, when applied to a simple equation, generates a solution of the equation or determines that it has no solution.

The search tree of the algorithm can now be described as follows. Starting with an equation $\mathscr{E}$, whose satisfiability we wish to determine, we first apply procedure 1. If $\mathscr{E}$ is not simple, then we apply procedure 2 and obtain a finite set of reduced equations. To each of the reduced equations $\mathscr{D}$, we again apply procedure 1. Whenever $\mathscr{D}$ is not simple, in the next round we apply procedure 2 to construct a new set of (still further) reduced equations that are equisatisfiable with $\mathscr{D}$. If $\mathscr{D}$ is simple, we apply procedure 3 to check whether or not it has a solution. Continuing in this fashion, we generate a possibly infinite tree. The root is labeled with $\mathscr{E}$, the internal nodes with reduced equations, and the leaves with simple equations. Each parent equation is satisfiable if and only if one of its children is.

In case the starting equation $\mathscr{E}$ is satisfiable, the algorithm is guaranteed to produce a leaf, that is, a simple equation, that has a solution. We can terminate the algorithm as soon as such a leaf is encountered. In case the equation is not satisfiable, the algorithm can run indefinitely, generating arbitrarily long equations. To handle this situation, a bound n is computed a priori such that, if a

[1] See, for example, Pecuchet [1984], Abdulrab and Pecuchet [1989], Jaffar [1990], and Schultz [1993].

solution to $\mathscr{E}$ exists at all, then a simple, satisfiable, reduced equation will be generated before the tree reaches the depth n. The bound n can be computed directly from the length of $\mathscr{E}$ and the "exponent of periodicity" of its "minimal" solution (see below for an explanation of these notions). In the semigroup case, this bound is of the order of the twice-iterated exponential function.[2] So, the problem of satisfiability of word equations is in NTIME($2^{2^{cp(d)}}$), where c is a constant and $p(d)$ is the bound on the exponent of periodicity of minimal solutions of equations of the length d. In fact, we conjecture that, using the ideas present in Makanin [1977], this bound can be improved to single exponential in the periodicity exponent.

The Makanin's algorithm for semigroups, and the unification algorithms based on it, use an important fact that the periodicity exponent of a minimal solution of a word equation can be bounded by a recursive function of the length of the equation. In fact, Makanin [1977] proved that if d is the length of an equation, then the exponent of periodicity of its minimal solutions (see below) does not exceed $(6d)^{2^{2d^4}} + 2$. This result was announced by Bulitko [1970], but the proof given there is not correct.

In Kościelski and Pacholski [1989], we forced this bound down to d^{2d^4}. Our improvement, based on Makanin's Reduction Lemma, was obtained by finding better bounds than did Makanin on the size of the minimal positive integer solutions of sets of linear Diophantine equations. In fact, the bounds we obtained were close to the almost optimal bounds recently obtained by Bombieri and Vaaler [1983]. We conjectured, however, that the exponent of periodicity could actually be bounded by an exponential function 2^{cd}, for some constant c. Thus, it was evident to us that an optimal bound could not be obtained by an analysis of the general linear Diophantine equations alone.

The principal goal of the present paper is to prove our conjecture. Namely, we show that the exponent of periodicity of a minimal solution of a word equation of the length d is bounded by the function of the order $2^{1.07d}$. It is known (see Benanav et al. [1985]) that the problem of deciding if a word equation has a solution is NP-hard.

The paper is divided into three parts. In the first, we study presentations of words in a special form, and prove the uniqueness of such presentations. Further, we describe a function that, when given the representations of two words, computes the representation of their concatenation. In the second part, we establish a Reduction Lemma. Given a word equation $\mathscr{E}$, we construct a set $\mathscr{M}$ of linear Diophantine equations whose minimal solutions describe the periodicity exponent of a minimal solution of $\mathscr{E}$. In the third part, we provide an upper bound on the size of minimal solutions of this set of linear Diophantine equations, thus giving the final result. Finally, we prove a lower bound of $2^{0.29d}$ for the exponent of periodicity of minimal solutions of a word equation of the length d.

By $\mathbb{Z}$, we denote the set of integers, and by $\mathbb{N}$, the set of nonnegative integers, $\mathbb{N}^+$ is the set of positive integers. Given any set Σ, by Σ^* we denote the set of all words in Σ. Σ^+ is the set of nonempty words in Σ. If W is a word, then $|W|$

[2] In some versions of the algorithm, the stopping mechanism is implemented into the data structure and the procedure. However, what actually happens during the execution of the algorithm is equivalent to using an a priori computed bound.

denotes the length of W. ε is the empty word. Let Σ, Ξ be two disjoint, finite alphabets. $\Sigma = \{a_1, \ldots, a_v\}$ is the set of (constant) letters and $\Xi = \{x_1, \ldots, x_\mu\}$ is the set of variables. A word equation in (Σ, Ξ) is a pair $\mathscr{E} = (W_1, W_2)$ of words in $(\Sigma \cup \Xi)^*$, also denoted by $W_1 = W_2$. $|W_1| + |W_2|$ is the length of $\mathscr{E}$ and is denoted by $|\mathscr{E}|$. We assume that each letter of $\Sigma \cup \Xi$ appears in W_1W_2. A solution of $\mathscr{E}$ is a function $S\colon \Xi \to \Sigma^*$ such that

$$W_1(S(x_1)/x_1, \ldots, S(x_\mu)/x_\mu)$$

$$= W_2(S(x_1)/x_1, \ldots, S(x_\mu)/x_\mu), \tag{1}$$

where $W(S(x_i)/x_i)$ denotes the word obtained from W by replacing each occurrence of x_i by $S(x_i)$. It is well known (see, e.g., Mackanin [1977]), and easy to check that in the study of upper bounds on the complexity of the satisfiability problem for word equations the assumption of the nonemptiness of all coordinates of a solution does not lead to any loss of generality. Therefore, to avoid cumbersome special cases, by a solution of a word equation we shall understand a solution whose all coordinates are nonempty. Given any function $S\colon \Xi \to \Sigma^*$, slightly abusing the notation, by the same letter S we shall denote the extension of S to the homomorphism $S\colon (\Sigma \cup \Xi)^* \to \Sigma^*$, which is the identity of Σ. Thus, (1) can be rephrased as $S(W_1) = S(W_2)$. Given a solution S, we put $|S| = \sum_{i=1}^{\mu} |S(x_i)|$, and we call $|S|$ the length of S. A solution is minimal if it has the minimal length. The periodicity exponent of a non-empty word W is the maximal integer p such that $W = U_1U^pU_2$, for some non-empty word U. The periodicity exponent of a solution S of a word equation $\mathscr{E}$ is the maximum of the periodicity exponents of the words $S(x_i)$, for $i = 1, 2, \ldots, \mu$.

2. *Presentation of Words*

We state here some facts necessary to obtain a reduction of a problem concerning word equations to a problem concerning linear diophantine equations. The first two lemmas are well known.

LEMMA 2.1. *For any words W_1, W_2, if $W_1W_2 = W_2W_1$, then $W_1 = U^m$, and $W_2 = U^n$, for some word U and integers m, n.*

Definition 2.2. A word U is primitive if $U \neq V^n$, for every word V and every integer $n \geq 2$.

LEMMA 2.3. *If U is primitive and $U^2 = U_1UU_2$, then either $U_1 = \varepsilon$ and $U_2 = U$, or $U_1 = U$ and $U_2 = \varepsilon$.*

Definition 2.4. Let P be a nonempty word. A sequence $(V_0, \ldots, V_v)$ is a P-partition of W if $W = V_0 \cdots V_v$ and

(i) for $i < v$, P is a suffix of V_i,
(ii) for $0 < i \leq v$, P is a prefix of V_i.

A P-partition $(V_0, \ldots, V_v)$ of W is finer than a P-partition $(U_0, \ldots, U_u)$ of W if $v > u$, and there exists a sequence $0 = j_{-1} < j_0 < j_1 < \cdots < j_u = v + 1$ such that, for each k, $(0 \leq k \leq u)$, $U_k = V_{j_{k-1}}V_{j_{k-1}+1} \cdots V_{j_k-1}$.

A P-partition $(V_0, \ldots, V_v)$ of W is maximal if there is no P-partition of W which is finer than $(V_0, \ldots, V_v)$. A P-partition of W is the greatest partition of W, if it is finer than any other P-partition of W.

It is not difficult to check, that a partition $(V_0, \ldots, V_v)$ is maximal if none of the words V_i, for $i \leq v$, contains P^2 as a subword.

LEMMA 2.5. *Let P be a primitive word.*

(*i*) *If $(V_0, \ldots, V_v)$ and $(U_0, \ldots, U_u)$ are maximal P-partitions of W, then $v = u$ and for each $i \leq v$, $V_i = U_i$.*

(*ii*) *If W is a prefix of T, $(V_0, \ldots, V_v)$ is a maximal P-partition of W and $(U_0, \ldots, U_u)$ is a maximal P-partition of T, then $v \leq u$ and for $i < v$, $U_i = V_i$.*

(*iii*) *If W is a suffix of T, $(V_v, \ldots, V_0)$ is a maximal P-partition of W, $(U_u, \ldots, U_0)$ is a maximal P-partition of T, then $v \leq u$, and for $i < v$, $U_i = V_i$.*

(*iv*) *For each W, there exists the greatest P-partition of W.*

PROOF. We shall prove only part (i) and part (iv). To prove (i) assume that P is a primitive word, and that $(V_0, \ldots, V_v)$, $(U_0, \ldots, U_u)$ are maximal P-partitions of W. The thesis is obvious if $v = 0$. Clearly, it suffices to prove, that if $u, v > 0$, then $|U_0| = |V_0|$. So, assume that $u, v > 0$, and suppose that $|U_0| \neq |V_0|$. By symmetry, we can assume that $|U_0| < |V_0|$. We have $U_0 = UP$ and $V_0 = VP$, for some words U, V. Since $u, v > 0$, VP^2 and UP^2 are subwords of W, so VP^2 has a prefix UP^2, and $|U| < |V|$. We also have $|V_0| < |U_0P|$. In fact, otherwise, $V_0 = U_0V'$, $|V'| \geq |P|$, and therefore V' has a prefix and a suffix P, which contradicts the assumption of maximality of $(V_0, \ldots, V_v)$. Consequently $V = UV''$, where $|V''| < |P|$. But $V''P^2$ has a prefix P^2, so P^2 has a prefix $V''P$. Now, by Lemma 2.3, either $V'' = \varepsilon$ or $V'' = P$, so, we have arrived at a contradiction.

To prove (iv) assume that P is a primitive word. Clearly, the one element sequence (W) is a P-partition, so the finite set of P-partitions is non empty. Therefore, it has a maximal element. By part (i), there is only one maximal P-partition. □

Definition 2.6. Let u be a nonnegative integer and let P be a nonempty word. A sequence $(U_0, \ldots, U_u)$ is P-stable if

(i) for $i \leq u$, P^2 is not a subword of U_i,

(ii) for $0 < i < u$, $U_i \neq P$,

(iii) for $i < u$, P is a suffix of U_i,

(iv) for $0 < i \leq u$, P is a prefix of U_i.

Assume that a sequence $(U_0, \ldots, U_u)$ is P-stable. Then clearly, any subsequence of it is P-stable. Moreover, $|U_i| > |P|$, for $0 < i < u$, and if $u > 0$, then $|U_0| \geq |P|$ and $|U_u| \geq |P|$.

Definition 2.7

(i) Let $w \in \mathbb{N}$, $W_0, \ldots, W_w, P \in \Sigma^*$. Then $[W_0, \ldots, W_w]_P$: $\mathbb{N}^w \to \Sigma^*$ is the function such that

$$[W_0, \ldots, W_w]_P(k_1, \ldots, k_w) = W_0P^{k_1}W_1P^{k_2} \cdots P^{k_{w-1}}W_{w-1}P^{k_w}W_w.$$

(ii) A P-presentation of a word W is a P-stable sequence $(U_0, \ldots, U_u)$ such that $W = [U_0, \ldots, U_u]_P(l_1, \ldots, l_u)$, for some $l_1, \ldots, l_u \in \mathbb{N}$.

(iii) The length of the P-presentation $(U_0, \ldots, U_u)$ is u. A word W is of P-order u if it has a P-presentation of the length u.

LEMMA 2.8. *Let $P \in \Sigma^*$ be a primitive word.*

(*i*) *Assume that $u, v \in \mathbb{N}$, $k_1, \ldots, k_u, l_1, \ldots, l_v \in \mathbb{N}$, and that sequences $\vec{U} = (U_0, \ldots, U_u)$ and $\vec{V} = (V_0, \ldots, V_v)$ are P-stable. If*

$$W = [U_0, \ldots, U_u]_P(k_1, \ldots, k_u) = [V_0, \ldots, V_v]_P(l_1, \ldots, l_v), \tag{2}$$

then $u = v$, $k_i = l_i$, for each $i = 1, 2, \ldots, u$, and $U_i = V_i$, for each $i = 0, 1, \ldots, u$.

(*ii*) *Each word W has the unique P-presentation.*

PROOF. Clearly (2) defines two P-partitions of W, which by the assumption of P-stability of $\vec{U}$ and $\vec{V}$ are maximal. Now, the conclusion of (i) easily follows from Lemma 2.5. To get (ii) notice that a P-presentation of W can easily be obtained from a maximal P-partition of W. □

Definition 2.9. If $(U_0, \ldots, U_u)$ is a P-presentation of W, then we write $(U_0, \ldots, U_u) = [W]_P^{-1}$.

From now on, we fix a primitive word $P \in \Sigma^+$. We sometimes omit the subscript P and write $[W_0, \ldots, W_w]$ instead of $[W_0, \ldots, W_w]_P$, and $[X]^{-1}$ instead of $[X]_P^{-1}$. Moreover, we write order and presentation for P-order and P-presentation respectively. By $ord(W)$ we denote the P-order of W.

LEMMA 2.10. *If X, Y are of order 0, then either*

(*i*) *XY has order 0, or*

(*ii*) *XY has order 1 and $XY = [[XY]^{-1}](c)$, for some $c \leq 1$, or*

(*iii*) *XY has order 2 and $XY = [[XY]^{-1}](0, 0)$.*

If moreover $|X| = 1$ or $|Y| = 1$, then XY has order 0, or has order 1 and $XY = [[XY]^{-1}](0)$.

PROOF. It can be easily checked that if none of conditions (i)–(iii) holds, then either P^2 is a subword of X or P^2 is a subword of Y, so either X or Y have order > 0. □

Below, we give an example that shows that case (iii) of Lemma 2.10 can happen.

Example 2.11. Let $P = aabaa$, $X = aabaaaaba = Paaba$, $Y = abaaaabaa = abaaP$. Then X, Y are of order 0 and $XY = PaabaabaaP$ has order 2, since $aabaabaa = Pbaa = aabP$.

LEMMA 2.12. *Suppose that $X \in \Sigma^*$ and $ord(X) = u$. Then*

(*i*) *If $a \in \Sigma$, then either*

$$[[X]^{-1}](g_1, \ldots, g_u)a = [[Xa]^{-1}](g_1, \ldots, g_u), \text{ or}$$

$$[[X]^{-1}](g_1, \ldots, g_u)a = [[Xa]^{-1}](g_1, \ldots, g_{u-1}, g_u + 1), \text{ or}$$

$$[[X]^{-1}](g_1, \ldots, g_u)a = [[Xa]^{-1}](g_1, \ldots, g_u, 0).$$

(*ii*) *If* $Y \in \Sigma^*$, *and* $ord(Y) = v$, *then* $[[X]^{-1}](g_1, \ldots, g_u)[[Y]^{-1}](h_1, \ldots, h_v)$ *equals to one of the following expressions*:

(1) $[[XY]^{-1}](g_1, \ldots, g_u + c + 2 + h_1, \ldots, h_v)$, *with* $c \leq 1$,
(2) $[[XY]^{-1}](g_1, \ldots, g_u + c, h_1 + c', \ldots, h_v)$, *with* $c + c' \leq 2$,
(3) $[[XY]^{-1}](g_1, \ldots, g_u + c, c', h_1 + c'', \ldots, h_v)$, *with* $c + c' + c'' \leq 1$,
(4) $[[XY]^{-1}](g_1, \ldots, g_{u-1}, g_u, 0, 0, h_1, \ldots, h_v)$.

PROOF. An easy proof of part (i) is omitted. To prove (ii) notice, that if $[X]^{-1} = (U_0, \ldots, U_u)$ and $[Y]^{-1} = (V_0, \ldots, V_v)$, then we have

$$[[X]^{-1}](g_1, \ldots, g_u)[[Y]^{-1}](h_1, \ldots, h_v) = U_0 P^{g_1} \cdots U_{u-1} P^{g_u} Z P^{h_1} V_1 \cdots P^{h_v} V_v,$$

for $Z = U_u V_0$. Since U_u, V_0 are of order 0, a P-presentation of Z is described by one of the cases (i)–(iii) of Lemma 2.10. So, we consider three cases.

Case 1. Z has order 0. Then clearly $(U_0, \ldots, U_{u-1}, U_u V_0, V_1, \ldots, V_v)$ is a stable sequence and the equality (2) with $c = c' = 0$ holds.

Case 2. Z has order 1. Then for $d \leq 1$, $Z = Z_0 P^d Z_1$, (Z_0, Z_1) is a P-presentation of Z and we have four cases, depending on whether or not $Z_i = P$. If $Z_0 = Z_1 = P$, then $(U_0, \ldots, U_{u-1}, V_1, \ldots, V_v)$ is a presentation of XY and the equality (1) holds with $c = d$. If $Z_0 \neq P \neq Z_1$, then $(U_0, \ldots, U_{u-1}, Z_0, Z_1, V_1, \ldots, V_v)$ is a presentation of XY and (3) with $c = c'' = 0$ and $c' = d$ holds. If $Z_0 = P \neq Z_1$, then $(U_0, \ldots, U_{u-1}, Z_1, V_1, \ldots, V_v)$ is a presentation of XY, and (2) with $c = d + 1$, $c' = 0$ holds. We get (2) with $c = 0$, $c' = d + 1$ in the symmetric case.

Case 3. Z has order 2. Then Z has a presentation (Z_0, Z_1, Z_2) with $Z_1 \neq P$. Again four subcases are possible depending on logical values of formulas $Z_0 = P$, $Z_2 = P$. If $Z_0 \neq P \neq Z_2$, then we get (4), if $Z_0 = P = Z_2$, then we get (2) with $c = c' = 1$, and if $Z_0 \neq P = Z_2$, then we get (3) with $c = c' = 0$, $c'' = 1$. Finally, we get (3) with $c = 1$, $c' = c'' = 0$ in the symmetric case. □

3. *Main Reduction*

In this chapter, we shall reduce the problem of finding upper bounds for the exponent of periodicity of a minimal solution of word equations to the problem of computing upper bounds on minimal positive integer solutions of systems of linear Diophantine equations.

Definition 3.1. Let $\vec{a}, \vec{b} \in \mathbb{N}^n$, and $\vec{a} = (a_1, \ldots, a_n)$, $\vec{b} = (b_1, \ldots, b_n)$. Then $\vec{a} \leq \vec{b}$ iff $a_i \leq b_i$, for each i such that $0 < i \leq n$. A solution $\vec{a} \in \mathbb{N}^n$ of a set $\mathcal{L}$ of linear Diophantine equations is minimal if $\vec{a}$ is a minimal element of the set of all nonzero solutions of $\mathcal{L}$ ordered by $\leq$.

We are now going to state the main result of this chapter.

THEOREM 3.2 (REDUCTION LEMMA). *Let $\mathscr{E}$ be a word equation of the length d that has at least two appearances of constants. If $p > 2$ is the exponent of periodicity of a minimal solution of $\mathscr{E}$, then $p - 2$ is a coordinate of a minimal solution of a set*

$$\mathscr{M} = \{M_1(\vec{u}, \vec{w}) = v'_1, \ldots, M_m(\vec{u}, \vec{w}) = v'_m\}$$

of linear Diophantine equations with nonnegative coefficients $m_{i,j}$, $m'_{i,j}$, m_i, such that

$$M_i = \sum_j m_{i,j}u_j + \sum_j m'_{i,j}w_j + m_i,$$

and moreover

(*i*) $2 \sum_{i,j} m_{i,j} + \sum_{i,j} m'_{i,j} \leq 2d - 4$,
(*ii*) $m'_{i,j} \leq 1$,
(*iii*) $\sum_i m_i \leq 3d - 5$,
(*iv*) $m \leq 2d - 2$,
(*v*) *there are at most* $4d - 6$ *variables in* $\mathscr{M}$.

PROOF. The proof of Theorem 3.2 will be divided into several lemmas. We first need some additional definitions.

Recall that Σ is a set of constant letters and $\Xi = \{x_1, \ldots, x_\mu\}$ is a set of variables. For the rest of this chapter, we assume that a fixed function $S: \Xi \to \Sigma^+$ and a primitive word P are given.

Definition 3.3. If $x \in \Xi$, and $ord(S(x)) = m$, then x is called a (word) variable of order m.

To simplify notation, we assume that variables in Ξ are ordered in a nondecreasing *ord*-order.

In the remaining part of this chapter and in the formulation of the Reduction Lemma above we distinguish several types of integer variables. To help the reader to understand the distinction, we first give an intuitive and informal description of the notation introduced in the definition below. The integer variables u_j correspond to word variables of order 1, and the integer variables w_j, v_j to word variables of order > 1. If $U = U_0P^{k_1}U_1P^{k_2} \cdots P^{k_u}U_u$, with P-stable $(U_0, \ldots, U_u)$, then we say that P^{k_1} and P^{k_u} are in boundary nesting and $P^{k_2}, \ldots, P^{k_{u-1}}$ are in internal nesting. The variables w_j correspond to boundary nesting of P, and the variables v_j correspond to internal nesting of P. In the definition below, j_k denotes the number of integer variables corresponding to internal nesting of P in word variables $x_1, \ldots, x_k$. By t, we denote the number of integer variables, u_i is the integer variable corresponding to $x_{i+\mu_0}$ (the ith word variable of order 1), and $w_{i'+1}$, $w_{i'+2}$ are integer variables corresponding to boundary nesting of P in $S(x_i)$, for a word variable x_i of order > 1.

Definition 3.4. Let μ_0 (μ_1) be the number of word variables in Ξ of order 0 (order 1) respectively. Let $j_0 = 0$, and for $k = 1, \ldots, \mu$, let $j_k = \sum_{l=1}^{k} max(0,$

$ord(S(x_l)) - 2)$, finally let $t = j_\mu + \mu_1 + 2(\mu - \mu_0 - \mu_1)$. For every word $W \in (\Sigma \cup \Xi)^*$, we define a function $\{W\}\colon \mathbb{N}^t \to \Sigma^*$ as follows:

(i) for $x_i \in \Xi$, $\quad \{x_i\}(\vec{u}, \vec{w}, \vec{v}) =$

$$\begin{cases} S(x_i), & \text{if } ord(S(x_i)) = 0, \\ [[S(x_i)]^{-1}](u_{i-\mu_0}), & \text{if } ord(S(x_i)) = 1, \\ [[S(x_i)]^{-1}](w_{i'+1}, v_{j_{i-1}+1}, v_{j_{i-1}+2}, \ldots, v_{j_i}, w_{i'+2}), & \text{if } ord(S(x_i)) > 1, \end{cases}$$

where $i' = 2(i - \mu_0 - \mu_1 - 1)$.

(ii) for $a \in \Sigma \cup \{\mathscr{E}\}$, $\quad \{a\}(\vec{u}, \vec{w}, \vec{v}) = a$,

(iii) for $W \in (\Sigma \cup \Xi)^*$ and $b \in (\Sigma \cup \Xi)$, $\quad \{Wb\}(\vec{u}, \vec{w}, \vec{v}) = \{W\}(\vec{u}, \vec{w}, \vec{v})\{b\}(\vec{u}, \vec{w}, \vec{v})$.

LEMMA 3.5. *If $W = W_1W_2$, then $\{W\}(\vec{u}, \vec{w}, \vec{v}) = \{W_1\}(\vec{u}, \vec{w}, \vec{v})\{W_2\}(\vec{u}, \vec{w}, \vec{v})$.*

PROOF. The lemma follows by a straightforward induction. □

Definition 3.6. Assume we are given an equation $\mathscr{E} = (W, W')$ in (Σ, Ξ). (Recall that each letter in $(\Sigma \cup \Xi)$ appears in $\mathscr{E}$).

(i) If $i = 0$ or $i = 1$, then d_i (d'_i) is the number of appearances of variable letters of order i in W (in W'),

d_2 (d'_2) is the number of appearances of variable letters of order > 1 in W (in W'), and

d_c (d'_c) is the number of appearances of constant letters in W (in W').

(ii) We put $d_0^+ = d_0 + d'_0$, $d_1^+ = d_1 + d'_1$, $d_2^+ = d_2 + d'_2$, $d_c^+ = d_c + d'_c$.

Clearly $|W| = d_0 + d_1 + d_2 + d_c$ and $|W'| = d'_0 + d'_1 + d'_2 + d'_c$.

LEMMA 3.7. *For every $W \in (\Sigma \cup \Xi)^+$, every primitive $P \in \Sigma^+$, and every function $S\colon \Xi \to \Sigma^*$, there exists a sequence $(L_1, \ldots, L_l)$ of linear functions $L_i(\vec{u}, \vec{w}, \vec{v}) = \sum_j c_{i,j}u_j + \sum_j c'_{i,j}w_j + \sum_j c''_{i,j}v_j + c_i$ with nonnegative integer coefficients such that*

(i) $\{W\}(\vec{u}, \vec{w}, \vec{v}) = [[S(W)]^{-1}](L_1(\vec{u}, \vec{w}, \vec{v}), \ldots, L_l(\vec{u}, \vec{w}, \vec{v}))$,

(ii) $\sum_{i,j} c_{i,j} = d_1$, $\quad \sum_{i,j} c'_{i,j} = 2d_2$, $c'_{i,j} \leq 1$,

(iii) for each i we have $card\{j\colon c'_{i,j} > 0\} \leq 2$,

(iv) if for some i, j, $c''_{i,j} > 0$, then $L_i = v_j$,

(v) $\sum_i c_i < 2d_0 + 3(d_1 + d_2) + d_c$.

PROOF. The sequence $(L_1, \ldots, L_l)$ such that l is the order of $S(W)$ and (i) holds is constructed by induction on the length of W using Lemma 2.12 and Lemma 3.5. Properties (ii)–(v) easily follow from the construction. For example, (iii) and (iv) describe the fact that either $L_i = v_j$, for some j, or $L_i = c'_{i,j}w_j + c'_{i,j'}w_{j'} + c_i + \sum_j c_{i,j}u_j$, where j, j' correspond respectively to the left and right boundary nesting in variables of order > 1. To prove (v) notice, that adding a variable of order ≥ 1 at the end of a word will contribute at most 3 to $\sum_i c_i$ (if case (1) of Lemma 2.12 (ii) for $c = 1$ holds). A word variable of order 0 can contribute at most 2, when case (2) holds, and a constant letter can contribute at most 1 (the second case of (i)). □

CONTINUATION OF THE PROOF OF THEOREM 3.2. Let S be a solution of $\mathscr{E}$, and let $V = S(W)$ and $V' = S(W')$. Let $p > 2$ be the exponent of periodicity of S, and let P be a primitive word such that for some $i \leq \mu$, and some U, U' we have $S(x_i) = UP^pU'$. Let $(\vec{\mathbf{u}}, \vec{\mathbf{w}}, \vec{\mathbf{v}})$ be a sequence of integers such that for each $i \leq n$, we have

$$S(x_i) = \{x_i\}(\vec{\mathbf{u}}, \vec{\mathbf{w}}, \vec{\mathbf{v}}). \tag{3}$$

By Lemma 3.5, $V = \{W\}(\vec{\mathbf{u}}, \vec{\mathbf{w}}, \vec{\mathbf{v}})$ and $V' = \{W'\}(\vec{\mathbf{u}}, \vec{\mathbf{w}}, \vec{\mathbf{v}})$. Consequently, by Lemma 3.7, there exist two sequences $(L_1, \ldots, L_l)$ and $(L'_1, \ldots, L'_{l'})$ of linear functions, such that

$$\{W\}(\vec{\mathbf{u}}, \vec{\mathbf{w}}, \vec{\mathbf{v}}) = [[V]_P^{-1}]_P(L_1(\vec{\mathbf{u}}, \vec{\mathbf{w}}, \vec{\mathbf{v}}), \ldots, L_l(\vec{\mathbf{u}}, \vec{\mathbf{w}}, \vec{\mathbf{v}})),$$

and

$$\{W'\}(\vec{\mathbf{u}}, \vec{\mathbf{w}}, \vec{\mathbf{v}}) = [[V']_P^{-1}]_P(L'_1(\vec{\mathbf{u}}, \vec{\mathbf{w}}, \vec{\mathbf{v}}), \ldots, L'_{l'}(\vec{\mathbf{u}}, \vec{\mathbf{w}}, \vec{\mathbf{v}})).$$

Since $V = V'$, by Lemma 2.8, we get $l = l'$ and $L_i(\vec{\mathbf{u}}, \vec{\mathbf{w}}, \vec{\mathbf{v}}) = L'_i(\vec{\mathbf{u}}, \vec{\mathbf{w}}, \vec{\mathbf{v}})$, for $0 < i \leq l$. Let

$$\mathscr{L} = \{L_1 = L'_1, \ldots, L_l = L'_l\}. \tag{4}$$

It is obvious that $\mathscr{L}$ is a consistent system of linear Diophantine equations, and that $p - 2$ is a coordinate of a solution $(\vec{\mathbf{u}}, \vec{\mathbf{w}}, \vec{\mathbf{v}})$ of $\mathscr{L}$. We shall analyze $\mathscr{L}$, but first we need one more definition and a lemma.

Definition 3.8. A linear form L is called proper unless $L = c$, for a constant $c \leq 1$, or $L = v_i$, where v_i corresponds to an internal nesting of P.

LEMMA 3.9. *There is at most* $d_0 + d_1 + 2d_2 + \frac{1}{2}d_c$ *proper forms in the set* $\{L_1, \ldots, L_l\}$ *and at most* $d'_0 + d'_1 + 2d'_2 + \frac{1}{2}d'_c$ *in the set* $\{L'_1, \ldots, L'_l\}$.

PROOF. Clearly, in $\{L_1, \ldots, L_l\}$, there is at most d_1 forms containing variables of order 1, and there is at most $2d_2$ forms containing variables corresponding to boundary nesting of P. Moreover, there is at most $d_0 + 1/2d_c$ forms of the form c, for $c > 1$. In fact, by Lemma 2.12 it follows that, if two variables (both of order > 0) are concatenated, then the constant form c can be created only for $c \leq 1$. Moreover, the forms so obtained will not be changed by any further concatenation. Therefore, the constant forms c with $c \geq 2$ can be divided into two categories. The ones in the first category are obtained using variables of order 0, and the ones in the second are obtained without variables of order 0. Note that there is at most d_0 forms of the first category. To get a constant form of the second category, a word containing P^4 as a subword must be obtained from, at most, two words not containing P^2, and from any number of letters. It is easy to check that for this at least two letters are necessary. □

END OF THE PROOF OF THEOREM 3.2. Assume, in addition to the assumptions made earlier, that S is a minimal solution of $\mathscr{E}$. Let $\mathscr{L}$ be the system of equations defined by (4), and let $(\vec{\mathbf{u}}, \vec{\mathbf{w}}, \vec{\mathbf{v}})$ be a solution of $\mathscr{L}$ that satisfies (3). It is easy to check that $(\vec{\mathbf{u}}, \vec{\mathbf{w}}, \vec{\mathbf{v}})$ is a minimal solution of $\mathscr{L}$.

Now, we are going to transform $\mathscr{L}$ into a system $\mathscr{M}$ of linear Diophantine equations that satisfies the conclusion of Theorem 3.2. By Lemma 3.9, the

number of equations $L = L'$ in $\mathcal{L}$, such that either L or L' is proper, is bounded by $d_0^+ + d_1^+ + 2d_2^+ + \frac{1}{2}d_c^+$. We, however, do not have any bounds on the number of other equations in $\mathcal{L}$. First, we are going to define a system $\mathcal{L}'$ by elimination from $\mathcal{L}$ of all equations whose both sides are nonproper. We denote by $\equiv_{\mathcal{L}}$ the smallest equivalence relation in the set of variables of order > 1 in internal nesting such that if either $(v_i = v_j) \in \mathcal{L}$, or $(L = v_i) \in \mathcal{L}$ and $(L = v_j) \in \mathcal{L}$, with proper L, then $v_i \equiv_{\mathcal{L}} v_j$.

Let v' be a new variable. Let $[v]$ be a $\equiv_{\mathcal{L}}$-equivalence class. To define $\mathcal{L}'$, we consider three cases.

Case 1. For some $v_i \in [v]$, $(v_i = 1) \in \mathcal{L}$. Then all occurrences in $\mathcal{L}$ of variables in $[v]$ are replaced by v'.

Case 2. For some $v_i \in [v]$, $(v_i = 0) \in \mathcal{L}$. Then all occurrences in $\mathcal{L}$ of variables in $[v]$ are replaced by 0. Since we have assumed that $p > 2$, the variable corresponding to $p - 2$ will not be eliminated in this way.

Case 3. For any $v_i \in [v]$, and for each constant $c \leq 1$, $(v_i = c) \notin \mathcal{L}$. Then we choose an element $v_i \in [v]$, and for each $v_j \in [v]$ we replace all occurrences of v_j in $\mathcal{L}$ by v_i.

Let $\mathcal{L}'$ denote the system of equations obtained in this way. To obtain $\mathcal{M}$, we first eliminate from $\mathcal{L}'$ all equations of the forms $v_i = v_i$ and $c = c$. Moreover, if L is proper and $L = 1 \in \mathcal{L}'$, then $L = 1$ is replaced by two equations $L = v'$ and $v' = 1$, where v' is the distinguished variable, that have been previously chosen. Finally, if L_i and L_i' are proper and $L_i = L_i' \in \mathcal{L}'$, then we introduce a new variable v_i', and replace $L_i = L_i'$ by two equations $L_i = v_i'$ and $L_i' = v_i'$.

We say that a sequence $\vec{\mathbf{u}}, \vec{\mathbf{w}}$ is the main part of a solution of $\mathcal{L}$ (respectively $\mathcal{M}$) if there exists a sequence $\vec{\mathbf{v}}$ ($\vec{\mathbf{v}}'$, respectively) such that $(\vec{\mathbf{u}}, \vec{\mathbf{w}}, \vec{\mathbf{v}})$ is a solution of $\mathcal{L}$ ($(\vec{\mathbf{u}}, \vec{\mathbf{w}}, \vec{\mathbf{v}}')$ is a solution of $\mathcal{M}$). Clearly the systems $\mathcal{L}$ and $\mathcal{M}$ are equivalent in the sense that $(\vec{\mathbf{u}}, \vec{\mathbf{w}})$ is the main part of a solution of $\mathcal{L}$ if and only if $(\vec{\mathbf{u}}, \vec{\mathbf{w}})$ is the main part of a solution of $\mathcal{M}$. Moreover, if $p - 2$ is a coordinate of a minimal solution of $\mathcal{M}$, then it is a coordinate of a minimal solution of $\mathcal{L}$. Thus, to finish the proof, it suffices to check that conditions (i)–(v) hold.

By Lemma 3.9 and the assumption that $d_c^+ \geq 2$, the number of equations in $\mathcal{M}$ is not greater than $d_0^+ + d_1^+ + 2d_2^+ + \frac{1}{2}d_c^+ + 1 \leq 2d - 2$, so (iv) holds. To prove (v) notice, that the number of variables in $\mathcal{M}$ can be bounded by the sum of: d_1^+ – the number of word variables of order 1, $2d_2^+$ – the doubled number of variables of order at least two, and the number of variables that appear at the right hand side of equations in $\mathcal{M}$, that is, the number of equations. So, the number of variables in $\mathcal{M}$ is at most $(d_1^+ + 2d_2^+) + (d_0^+ + d_1^+ + 2d_2^+ + \frac{1}{2}d_c^+ + 1) \leq 4d - 6$. Moreover, it is easy to notice that Lemma 3.7 (ii) and (v) implies (i), (ii), and (iii) of Theorem 3.2, so, the proof is completed. □

4. *Upper Bounds*

In this part using the result of Section 3, we shall prove an upper bound on the exponent of periodicity of minimal solutions of word equations. To obtain this bound, we use an upper bound on coordinates of minimal solutions of linear Diophantine equations, which is a variant of a bound given in Von Zur Gathan and Sieveking [1978] and Lambert [1987].

THEOREM 4.1. *Let* $\mathcal{N} = \{\vec{n}_i \cdot \vec{q} + n_i = 0 : i = 1, \ldots, n\}$ *be a system of linear Diophantine equations with* $\vec{n}_i = (n_{i,1}, \ldots, n_{i,r}) \in \mathbb{Z}^r$, *let* $\sum_{i=1}^{n} |n_i| = w$, *and let* D *be the upper bound on the absolute values of the determinants of square submatrices of the matrix* $(n_{i,j})$. *Then for each minimal solution* $(q_{0,1}, \ldots, q_{0,r})$ *of* $\mathcal{N}$, *and each* i, $1 \le i \le r$, *we have* $q_{0,i} \le (w + r)D$.

A Note on a Proof. Let A denote the upper bound of the absolute values of the determinants of square submatrices of the matrix obtained from $(n_{i,j})$ by adjoining the vector (n_i) to it, (sometimes denoted by $((n_{i,j})(n_i))$ and called a full matrix of the system $\mathcal{N}$). Von Zur Gathan and Sieveking [1978] and Lambert [1987] agreed[3] that $q_{0,i} \le rA$, so a direct application of the bounds given in these two papers gives $q_{0,i} \le (wr)D$. However, by a modification of their proofs, this slight improvement can be obtained.

LEMMA 4.2. *For any* $n \times k$*-matrix* $(c_{i,j})$, *if* $c = \sum_{i=1}^{n} \sum_{j=1}^{k} |c_{i,j}|$, *then we have*

$$\prod_{j=1}^{k} \sum_{i=1}^{n} |c_{i,j}| \le \left(\frac{\sum_{i=1}^{n} \sum_{j=1}^{k} |c_{i,j}|}{k} \right)^k = \left(\frac{c}{k} \right)^k < (e^{1/e})^c.$$

PROOF. Routine. □

Below, we recall the well-known Hadamard inequality.

LEMMA 4.3. *For any* $n \times n$*-matrix* $C = (c_{i,j})$, *we have*

$$det^2(C) \le \prod_{j=1}^{n} \sum_{i=1}^{n} c_{i,j}^2.$$

COROLLARY 4.4. *Let* $\mathcal{N} = \{\vec{n}_i \cdot \vec{q} + n_i = 0 : i = 1, \ldots, n\}$ *be a system of linear Diophantine equations. Let* $\vec{n}_i = (n_{i,1}, \ldots, n_{i,r}) \in \mathbb{Z}^r$, $w = \sum_{i=1}^{n} |n_i|$, *and* $c = \sum_{i=1}^{n} \sum_{j=1}^{r} |n_{i,j}|$. *If* $(q_{0,1}, \ldots, q_{0,r})$ *is a minimal solution of* $\mathcal{N}$, *then* $q_{0,i} \le (w + r)(e^{1/e})^c$.

PROOF. Routine application of Theorem 4.1, Lemmas 4.2, and 4.3, and the obvious inequality $\sum_{i=1}^{n} a_i^2 \le (\sum_{i=1}^{n} |a_i|)^2$. □

Now, we are ready to prove the main result of this paper.

THEOREM 4.5. *If* $\mathcal{E}$ *is a word equation of the length* d, $d_c^+ \ge 2$ *and* p *is the exponent of periodicity of a minimal solution of* $\mathcal{E}$, *then* $p \le (7d - 11)(e^{1/e})^{2d-3} + 2 \le (3d - 4)2^{1.0615d} = O(2^{1.07d})$.

PROOF. Assume that $\mathcal{E}$ is a word equation of the length d and $d_c^+ \ge 2$. Let $\mathcal{M}$ be the set of linear Diophantine equations given in Theorem 3.2. The main matrix M of $\mathcal{M}$ has the form:

$$M = \begin{pmatrix} m_{1,1} & \cdots & m_{1,k} & m''_{1,1} & \cdots & m''_{1,l} \\ m_{2,1} & \cdots & m_{2,k} & m''_{2,1} & \cdots & m''_{2,l} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ m_{m,1} & \cdots & m_{m,k} & m''_{m,1} & \cdots & m''_{m,l} \end{pmatrix},$$

[3] The result in Von Zur Gathan and Sieveking [1978] is stated for one of solutions, but the proof works without much change for all minimal solutions.

The nonprimed entries of M correspond to non-primed coefficients $m_{i,j}$ of equations in $\mathcal{M}$, and double primed entries of M correspond to primed coefficients $m'_{i,j}$ of equations in $\mathcal{M}$, and the right-sides of these equations. Clearly, we have

(i) for $1 \leq i \leq m$ and $1 \leq j \leq l$, $\quad |m''_{i,j}| \leq 1$, and
(ii) $2 \sum_{i=1}^{m} \sum_{j=1}^{k} m_{i,j} + \sum_{i=1}^{m} \sum_{j=1}^{l} |m''_{i,j}| \leq 2d - 4 + 2d - 2 = 4d - 6.$

Let $C = (c_{i,j})$ be a square submatrix of M, and let k', l' denote the numbers of columns of C consisting, respectively of nonprimed and double primed elements. Let c be the sum of nonprimed elements of C, and let c'' be the sum of absolute values of double primed elements of C. By Lemma 4.3 and (i), we have

$$det^2(C) \leq \left(\prod_{j=1}^{k'} \sum_{i=1}^{n} c_{i,j}^2 \right) \left(\prod_{j=k'+1}^{k'+l'} \sum_{i=1}^{n} c_{i,j}^2 \right) \leq \left(\prod_{j=1}^{k'} \sum_{i=1}^{n} \left| c_{i,j} \right| \right)^2 \left(\prod_{j=k'+1}^{k'+l'} \sum_{i=1}^{n} \left| c_{i,j} \right| \right).$$

Consequently, by Lemma 4.2 and (ii), we obtain that

$$det^2(C) \leq \left(\frac{c}{k'} \right)^{2k'} \left(\frac{c''}{l'} \right)^{l'} \leq (e^{1/e})^{2c+c''} \leq (e^{1/e})^{4d-6}.$$

So, Theorem 4.1, and the estimates given in Theorem 3.2 imply, that for $p > 2$,

$$p \leq (7d - 11)(e^{1/e})^{2d-3} + 2 \leq (3d - 4)2^{1.0615d} = O(2^{1.07d}).$$

It is very easy to check that the inequality above is true also if $p \leq 2$. □

COROLLARY 4.6. *The problem of satisfiability of word equations is in* $NTIME(2^{2^{2^{cd}}})$, *where* c *is a constant, and* d *is the length of equation.*

PROOF. The problem of satisfiability of word equations is in $\mathrm{NTIME}(2^{2^{c'p(d)}})$, where c' is a constant and $p(d)$ is a bound on the exponent of periodicity of minimal solutions of word equations of the length d (see Jaffar [1990] and Schultz [1993]). Therefore, the claim follows by Theorem 4.5. □

For the completeness sake we should comment on the assumption that $d_c^+ \geq 2$. It is known (see, e.g., Abdulrab and Pecuchet [1989]), that the problem of satisfiability of word equations in the alphabet having only one constant letter reduces to the problem of solving one linear Diophantine equation, and the estimates for the periodicity exponent are, in this case, not needed for the problem of satisfiability of word equations. However, using the above mentioned fact and the estimates that can be found in Lambert [1987b], one can easily prove that the periodicity exponents of minimal solution are in this case very small.

Fact 4.7. If $\mathscr{E}$ is a word equation in $(\{a\}, \Xi)$ and each letter appears in $\mathscr{E}$ at most m times, then the exponent of periodicity of any minimal solution of $\mathscr{E}$ does not exceed m.

Moreover, if Siegel's Lemma [Siegel 1979] is used instead of the bound given in Lambert [1987b], then for equations having a large number of distinct variables the bound m above, can be replaced by a much smaller bound $1 + 2(\sqrt[n]{m})$, where n is the number of distinct variables in $\mathscr{E}$.

To conclude we give a simple result, which shows, that Theorem 4.1 can not be substantially improved.

THEOREM 4.8. *For each positive integer n, the equation*

$$x_n a x_n b x_{n-1} b \cdots b x_2 b x_1 = a x_n x_{n-1}^5 b x_{n-2}^5 b \cdots b x_1^5 b a^5 \tag{5}$$

has the unique solution S whose periodicity exponent is $5^{(d-2)/8} = 2^{((d-2)/8)log_2 5}$, *where d is the length of Eq.* (5). *Moreover, if n is large, then the periodicity exponent is at least* $2^{0.29d}$.

PROOF. Let S be a solution of (5). By Lemma 2.1, $S(x_n) \in \{a\}^*$. An easy calculation shows that $|S(x_n)| = 5 + 4 \sum_{i=1}^{n-1} |S(x_i)|$ and $0 = |S(x_n)|_b = 4 \sum_{i=1}^{n-1} |S(x_i)|_b$, where for a word W, $|W|_b$ is the number of appearances of b in W, so $|S(x_i)|_b = 0$. This implies that $|S(x_n)| = 5|S(x_{n-1})|$ and an easy induction shows that for each $i \leq n$, $|S(x_i)| = 5|S(x_{i-1})|$. Since $S(x_1) \in \{a\}^*$, it follows that $S(x_1) = a^5$, and consequently $S(x_n) = a^{5^n}$, thus the exponent of periodicity of (5) is equal $5^{(d-2)/8} = 2^{((d-2)/8)\log_2 5}$, which for large d is greater than $2^{0.29d}$. □

ACKNOWLEDGMENTS. We are very grateful to the anonymous referees for very careful reading of consecutive versions of this paper and for the comments that have lead to improvement of the presentation.

REFERENCES

ABDULRAB, H. 1987. Résolution d'équations sur les mots: étude et implémentation LISP de l'algorithme de Makanin. Ph.D. dissertation. Univ. Rouen, Rouen, France.

ABDULRAB, H., AND PECUCHET, J. P. 1989. Solving word equations. *J. Symb. Comput. 8*, 499–521.

ADYAN, S. I., AND MAKANIN, G. S. 1984/1986. Investigation on algorithmic questions of algebra. *Trudy Matem. Inst. Steklova 168*, 197–217, 1984 (in Russian). (English translation in *Proc. of Steklov Institute of Mathematics 3*, 207–226, 1986).

BENANAV, D., KAPUR, D., AND NARENDRAN, P. 1985. Complexity of matching problems. In *Proceedings of the 1st International Conference on Rewriting Techniques and Applications*, J.-P. Jouannaud, ed., Lecture Notes in Computer Science, vol. 202. Springer-Verlag, New York, pp. 417–429.

BOMBIERI, E., AND VAALER, J. 1983. On Siegel's lemma. *Invent. Math. 73*, 11–32.

BULITKO, V. K. 1970. Equations and inequalities in a free group and a free semigroup. *Tul. Gos. Ped. Inst. Ucen. Zap. Mat. Kafedr, Geometr. i Algebra 2*, 242–252 (in Russian).

JAFFAR, J. 1990. Minimal and complete word unification. *J. ACM 37*, 47–85.

KHMELEVSKIĬ, YU. I. 1967. Solution of word equations in three unknowns. *Dokl. Akad. Nauk SSSR 177*, 1023–1025 (in Russian).

KOSCIELSKI, A., AND PACHOLSKI, L. 1989. On the index of periodicity of a minimal solution of a word equation. Unpublished.

LAMBERT, J. L. 1987a. Le Problème de l'accessibilité dans les réseaux de Petri. Ph.D. dissertation. Orsay, France.

LAMBERT, J. L. 1987b. Une borne pour les générateurs des solutions entières positives d'une équation diophantienne linéaire. *Compte-rendu de L'Académie des Sciences de Paris 305*, 1, 39–40.

LENTIN, A. 1972. Equations in free monoids. In *ICALP: Annual International Colloquium on Automata, Languages and Programing*, M. Nivat, ed., North-Holland, Amsterdam, the Netherlands, pp. 67–85.

MAKANIN, G. S. 1977. The problem of solvability of equations in a free semigroup. *Mat. Sbornik 103*, 147–236 (in Russian). (English translation in *Math. USSR Sbornik 32*, 129–198).

MAKANIN, G. S. 1982/1983. Equations in a free group. *Izvestiya AN SSSR 46*, 1199–1273, 1982 (in Russian). (English translation in *Math. USSR Izvestiya 21*, 483–546, 1983).

MAKANIN, G. S. 1984/1985. Decidability of the universal and positive theories of a free group. *Izvestiya AN SSSR 48*, 735–749, 1984 (in Russian). (English translation in *Math. USSR Izvestiya 25*, 75–88, 1985).

PECUCHET, J. P. 1984. Solutions principales et rang d'un système d'équations avec constantes dans le monoïde libre. *Disc. Math. 48*, 253–274.

PLOTKIN, G. 1972. Building in equational theories. *Mach. Int. 7*, 73–90.

SCHULZ, K. U. 1993. Word unification and transformation of generalized equations. *J. Auto. Reas. 11*, 2, 149–184.

SIEGEL, C. L. 1929. Über einige Anwendungen diophantischer Approximationen. *Abh. der Preuß. Akad. der Wissenschaften. Phys.-math. Kl. 1*, 209–266 (= *Ges. Abh. I*, 209–266).

VON ZUR GATHEN, J., AND SIEVEKING, M. 1978. A bound on solutions of linear integer equations and inequalities. *Proc. AMS 72*, 155–158.

RECEIVED MARCH 1992; REVISED FEBRUARY 1996; ACCEPTED APRIL 1996