EXPONENT OF PERIODICITY OF WORD EQUATIONS IN FIXED DIMENSION IS POLYNOMIAL

CLAUDIO GUTIÉRREZ

ABSTRACT. The exponent of periodicity is a key parameter used in all currently known algorithms for solving word equations. A lower bound for it is $2^{c|E|}$, where $|E|$ is the length of the equation E. We prove that in fixed dimension, i.e., when the variables belong to a fixed set V, the exponent of periodicity can be bound by a polynomial $p(|E|)$ of degree no more than thrice the size of the set V.

1. Introduction

Traditional analysis of the complexity of solvability of word equations has been done by considering the length of (number of symbols occurring in) the word equation as parameter. Studies using finer parameters, like the number of variables, number of occurrence of variables, have been done for particular cases (one variable [6], two variables [5], each variable occurring no more than twice [2], total number of occurrences of variables fixed [3]). It has been conjectured that satisfiability of word equations in fixed dimension is tractable, very much like the case of integer programming, word matching, disjoint paths, etc.

The *exponent of periodicity* of a word equation E is a key parameter used in all currently known algorithms for solving word equations (see e.g. [3], [7]) and as Koscielski and Pacholski showed in [4], a lower bound for it is $2^{0.29|E|}$, where $|E|$ is the number of symbols occurring in E.

We prove in this paper that the exponent of periodicity of word equations E in fixed dimension (i.e., with variables in a fixed set V) is bounded by a polynomial $p(|E|)$ of degree no more $3|V|$, where $|V|$ is the size of the set V.

The proof goes as follows: first, a system of linear diophantine equations $\Sigma(E;S)$ is associated to each solvable word equation E and minimal solution S, with the property that minimal solutions of $\Sigma(E;S)$ correspond to minimal exponent of periodicity of the solution S (an idea going back to Bulitko [1]). Then we transform the system to get another one with better parameters and similar bounds on their solutions. Finally, we use some standard bounds on minimal solutions of linear diophantine equations.

2. Preliminaries and Definitions

Given two alphabets, $\mathcal{C}$ of constants and $\mathcal{V}$ of variables, a *word equation* E is a pair of words U, V (usually written $U = V$) in the alphabet $\mathcal{C} \cup \mathcal{V}$.

A *solution* of E is a map $\mathcal{V} \longrightarrow \mathcal{C}^*$ such that the word $S(U)$ obtained by replacing each variable x occurring in U by $S(x)$ is equal to $S(V)$.

The *exponent of periodicity* of a word W is the maximum number n such that it can be written $W = UV^nZ$, for words U, V, Z with V not empty. The *exponent of periodicity* of a solution S of a word equation $E : U = V$ is the exponent of periodicity of $S(U)$.

Definition 1. *Let W be any word, and P a primitive word (i.e. P cannot we written as $P = V^n$ for every word V and integer $n \geq 2$). A P-*stable sequence *for W is a sequence of words $W_0, \dots, W_n$ such that*

$$W = W_0 P^{k_1} \cdots P^{k_n} W_n, \tag{1}$$

and:

1. *P^2 is not a subword of W_i for $i = 0, \dots, n$.*
2. *$W_i \neq P$ for $0 < i < n$.*
3. *P is a suffix of W_i for $i < n$.*
4. *P is a prefix of W_i for $0 < i \leq n$.*

The right hand side of (1) is called a P-stable presentation of W.

It is not difficult to prove that a word W has a unique P-presentation (cf. Lemma 2.8 in [4]). The n of such a P-stable presentation of W is called the *P-order* of W.

To the P-stable presentation of the word W in (1) is associated the parameterized word

$$W[\lambda_1, \dots, \lambda_n] = W_0 P^{\lambda_1} W_1 P^{\lambda_2} \cdots P^{\lambda_n} W_n,$$

where $\lambda_1, \dots, \lambda_n$ represent non-negative integer variables. We will call λ_1 and λ_n *boundary* parameters, and $\lambda_2, \dots, \lambda_{n-1}$ *internal.*

3. A system of linear diophantine equations (LDE) associated to the word equation E

Consider the word equation $E : U = V$, with $U = U_0 \cdots U_u$ and $V = V_0 \cdots V_v$, a solution $S(U) = S(V)$, and a fixed primitive word P. We have on one hand the parameterized word associated with the P-stable decomposition of $S(U)$,

$$S(U)[L_1, \dots, L_n] = U_0 P^{L_1} U_1 P^{L_2} \cdots P^{L_u} U_u, \tag{2}$$

which, by the way, is the same as that of $S(V)$.

On the other hand, we get another parameterization of $S(U)$ by using $S(U) = S(U_0) \cdots S(U_u)$ and the parameterized words associated to each $S(U_j)$, namely $S(U_j) = U_{j0} P^{\alpha_{j1}} \cdots P^{\alpha_{ju_j}} U_{ju_j}$,

$$\begin{aligned} S(U_0)[\alpha_{01}, \dots, \alpha_{0u_0}] S(U_1)[\alpha_{11}, \dots, \alpha_{1u_1}] \cdots S(U_u)[\alpha_{u1}, \dots, \alpha_{uu_u}] \\ = S(U)[\alpha_{01}, \dots, \alpha_{0u_0}, \alpha_{11}, \dots, \alpha_{1u_1}, \dots, \alpha_{u1}, \dots, \alpha_{uu_u}]. \end{aligned} \tag{3}$$

When $S(U_j)$ has P-order 0 we assume that the corresponding set of parameters $\alpha_{j1}, \dots, \alpha_{ju_j}$ does not appear.

How do the parameters of the expressions (2) and (3) relate?

Lemma 1. *Each L_j correspond exactly to one of the following cases:*

$$L_l = \alpha_{ij}, \tag{4}$$

or

$$L_l = \alpha_{pu_p} + c(p, j_1) + \alpha_{j_1 1} + c(j_1, j_2) + \cdots + \alpha_{j_m 1} + c(j_m, q) + \alpha_{q1}, \tag{5}$$

where $p < j_1 < \cdots < j_m < q$ and:

1. *α_{pu_p} is the last parameter of $S(U_p)$.*
2. *α_{q1} is the first parameter of $S(U_q)$.*
3. *For $i = 1, \ldots, m$, the words $S(U_{j_i})$ have P-order 1.*
4. *$c(i, j)$ is given by the equation*

   $$P^{c(i,j)} = U_{iu_i} U_{(i+1)0} \cdots U_{(j-1)0} U_{j0}$$

   where $S(U_{i+1}), \ldots, S(U_{j-1})$ are of P-order 0.
5. *The parameters α_{pu_p} or α_{q1} (or both) could not appear. If α_{pu_p} does not appear, then $S(U_p)$ is of P-order 0 and $c(p, j_1)$ is given by the equation*

   $$P^{c(p,j_1)} = W_s U_{(p+1)0} \cdots U_{(j_1-1)0} U_{j_1 0},$$

   where W_s is a proper suffix of $S(U_p)$ and $S(U_{p+1}), \ldots, S(U_{j_1-1})$ are of P-order 0. A symmetric analysis holds if α_{q1} does not appear.

Proof. For each L_j there are only two possible cases:

(i) The occurrence of P^{L_j} fits completely inside one $S(U_i)$. In this case, from the definition of P-stability, obviously we will have an equation like (4).

(ii) The occurrence of P^{L_j} covers several adjacent words $S(U_j)$. Suppose that $S(U_p)S(U_{p+1}) \cdots S(U_q)$ is the smallest set of consecutive words $S(U_j)$ which cover P^{L_j} Also recall that the P-stable presentation of $S(U_j)$ is given by:

$$S(U_j) = U_{j0} P^{\alpha_{j1}} \cdots P^{\alpha_{ju_j}} U_{ju_j}.$$

From here the conditions 1 and 2 follow immediately.

For 3, 4 and 5 observe that because for each $p < j < q$, $S(U_j)$ is a subword of P^{L_j} (our choice of minimality of the sequence) all such $S(U_j)$ are of P-order either 0 or 1. By grouping adjacent $S(U_j)$ of P-order 0 and using the definition of P-stability we get the decomposition of (5). □

Observe that a similar analysis (which we will skip) holds for the P-stable presentation of $S(V)$,

$$V_0 P^{L'_1} V_1 P^{L'_2} \cdots P^{L'_v} V_v. \tag{6}$$

Lemma 2. *The coefficients of L in (5) are bounded as follows:*

1. *$m \leq q - p \leq |E|$.*
2. *$\sum c(i, j) \leq 2|E|$.*

Proof. Item 1 follows directly from the definitions of m and of p, q in the proof of Lemma 1.

Item 2 is a consequence of conditions 4 and 5 of Lemma 1 and the fact that each $S(U_k)$ of P-order 0 cannot have PP as subword. So $\sum c(i,j)$ is no bigger than twice the number of symbols in E. □

3.1. **The associated system of LDE.** From the above data we will build the system $\Sigma(E;S)$ of LDE associated to the solvable word equation E, a *minimal* solution S, and a primitive word P as follows:

1. Observe that for every symbol U_i and V_j denoting the same variable x, $S(U_i)$ (resp. $S(V_j)$) is the same word (so, same P-stable representation). Hence we can use the same set of variables, say $\lambda_1^x, \ldots, \lambda_{n_x}^x$ for each of these occurrences.
2. Because S is a solution, $S(U) = S(V)$. So it follows that $u = v$ and we get the following set of LDE:

$$L_1 = L'_1, \cdots, L_u = L'_v. \tag{7}$$

3. The final system $\Sigma(E;S)$ of LDE is got by replacing the L_j by the corresponding right hand side of (4) or (5), and similarly for the L'_j.

For a system Σ of LDE and solutions $u = (u_1, \ldots, u_n)$ and $v = (v_1, \ldots, v_n)$ of it, define $u \le v$ if $u_i \le v_i$ for each $i = 1, \ldots, n$. A solution u of Σ is *minimal* if there are no other solutions v with $v < u$.

Lemma 3. *Every solution in non-negative integers to $\Sigma(E;S)$ gives a solution to the word equation E. Moreover, the exponents associated to the P-stable presentation of $S(U) = S(V)$ give a minimal solution to $\Sigma(E;S)$.*

Proof. The first statement is clear. For the second, suppose it is not minimal. Then there is a smaller solution to $\Sigma(E;S)$. The replacement of this smaller solution into the parameterized words where they came from gives a smaller solution to the word equation E, in contradiction with the choice of S. □

We are looking for good bounds on the size of exponent of periodicity of a minimal solution of a word equation. From the above lemma, this translates into looking for good bounds for the size of a minimal solution to $L(E;S)$.

4. Getting better parameters for $\Sigma(E;S)$

We will modify the system $\Sigma(E;S)$ to get a system of LDE with good parameters. From here on, by solution of a system of LDE we will always mean *non-negative* integer solution. We need some definitions first.

For a system Σ of LDE, define the *size* of a solution $u = (u_1, \ldots, u_n)$ as $||u|| = \sum_i |u_i|$, and

$$||\Sigma|| = \max\{||u|| : u \text{ is a minimal solution of } \Sigma \}.$$

The number $||\Sigma||$ is a uniform bound on the size of all minimal solutions. That it is well defined follows from the fact that the set of minimal (non-negative) solutions of a system of LDE is a finite set (a finitely generated sub-monoid of $\mathbb{N}^n$ in the case of homogeneous systems of LDE).

There are three types of equations $L = L'$ in $\Sigma(E; S)$, depending on if L and L' are of the form (4) or (5):

1. Both of type (4). The equation is $\lambda = \lambda'$.
2. One of each type (w.l.o.g. suppose $L = \lambda$). The equation is then of the form $\lambda = L'$, with L' of type (5).
3. Both of type (5).

First, observe that the equations in 1 define certain equivalence classes E_i of variables, two variables λ, λ' being in the same class if $\lambda = \lambda'$ is an equation in 1. Pick one representative of each class, and define Σ_1 as those equations in $\Sigma(E; S)$ of the form 2 and 3 after replacing all the variables of each class E_i by its corresponding representative. Observe that

$$||\Sigma(E; S)|| = ||\Sigma_1||, \tag{8}$$

and Σ_1 does not have equations of type 1.

Second, define Σ_2 as follows: For each λ, list all equations of type 2 of Σ_1, namely $\lambda = L_{i_1}, \ldots, \lambda = L_{i_q}$, and replace them by $L_{i_1} = L_{i_2}, L_{i_1} = L_{i_3}, \ldots, L_{i_1} = L_{i_q}$. So Σ_2 has only equations of type 3, i.e., of the form $L = L'$, where L and L' are of the form (5). As for the parameters of Σ_2 we have:

Lemma 4. *Let the system Σ_2 be $AX = B$. Then it holds:*

1. *Σ_2 has no more than $2|V|$ variables.*
2. $|b_j| \leq 2|E| + 4$.
3. $|a_{ij}| \leq 4|E|$.
4. $||\Sigma_1|| \leq (|E| + 2)||\Sigma_2|| + 2|E|$.

Proof. 1. First note that if U_i is a symbol of constant in the word equation E, then $S(U_i)$ is of P-order 0, hence generates no variables for $\Sigma(E; S)$ (hence for Σ_2). Similar analysis hold for symbols V_j. We can conclude that the only variables that count are those arising from symbols of variables in E. Because Σ_2 has only equations of the form $L = L'$ with L, L' as in (5), it is enough to analyze (5). For each such L, there occur only boundary variables (one final, α_{pu_p}, and one initial, α_{q1}) and variables arising from $S(U_j)$ of P-order 1. Hence the total number of variables is no bigger than twice the number of $S(U_j)$ (or $S(V_j)$) of P-order ≥ 2 (for the initial and final boundary variables) plus the number of $S(U_j)$ (or $S(V_j)$) of P-order 1. It is easy to see than $2|V|$ is a good bound.

2 and 3. For each L as in (5), group all constant coefficients and identical variables in it. Then the constant coefficients are no bigger than $\sum c(i, j)$, and a variable cannot occur more than $m + 2$ times, hence the factors of the variables cannot be bigger than $m + 2$. In the equation $L = L'$, these bounds will at most be doubled. Then use Lemma 2.

4. As for the size of the minimal solutions, observe that each solution s of Σ_2 can be extended to one of Σ_1 by using the equations $\lambda = L_{i_j}$ for the variables of Σ_1 not in Σ_2. Hence it holds $||\Sigma_1|| \leq (m+2)||\Sigma_2|| + \sum c(i,j)$. From here, the bounds follow using Lemma 2. □

The next lemma shows that there is a system of LDE equivalent to Σ_2 whose rank is no more than its number of variables.

Lemma 5. *Let Σ be a system of linear diophantine equations with M equations and N variables, and suppose that Σ has a non-negative solution. Then there is a subsystem $\Sigma' \subseteq \Sigma$ with no more than N equations such that s is a solution of Σ iff s is a solution of Σ'.*

Proof. Let Σ be $AX = B$ with $A = (a_{ij})$ and $M \times N$ matrix, and $B = (b_1, \dots, b_M)$, and consider the tuples $A_i = (a_{i1}, \dots, a_{iN})$ as vectors in $\mathbb{Q}^N$. There are at most N linearly independent, w.l.o.g. suppose $A_1, \dots, A_N$. Let A' the matrix with these rows, $B' = (b_1, \dots, b_N)$ and let Σ' be $A'X = B'$.

Because Σ is solvable there is S_0 with $AS_0 = B$. Hence, for every A_k with $k > N$, it holds $A_k = \sum \beta_{ki} A_i$ for certain β_{ki}, so

$$b_k = A_k S_0 = (\sum \beta_{ki} A_i) S_0 = \sum \beta_{ki}(A_i S_0) = \sum \beta_{ki} b_i.$$

Now, obviously every solution of Σ is a solution of Σ'. Conversely, let $S = (s_1, \dots, s_N)$ be a solution of Σ' and $k > N$. Then

$$A_k S = (\sum \beta_{ki} A_i) S = \sum \beta_{ki}(A_i S) = \sum \beta_{ki} b_i = b_k.$$

Hence $AS = B$, so S is a solution of Σ. □

5. Bounds for minimal solutions of $\Sigma(E;S)$

We will use the following theorem which bounds uniformly the minimal solutions of homogeneous LDE.

Theorem 1 (Pottier, [8]). *Let $\Sigma : AX = 0$ be a system of homogeneous linear diophantine equations. Then*

$$||\Sigma|| \leq (1 + ||A||_{1,\infty})^{\operatorname{rank} A},$$

where $||A||_{1,\infty} = \sup_i \{\sum_j |a_{ij}|\}$.

A similar result holds for non-homogeneous system of linear diophantine equations. In fact, from the above theorem we get:

Corollary 1. *Let $AX = B$ be a system of non-homogeneous linear diophantine equations. Then*

$$1 + ||\Sigma|| \leq (1 + ||C||_{1,\infty})^{\operatorname{rank} C},$$

where C is the matrix whose rows are $(a_{i1}, a_{i2}, \dots, a_{in}, -b_i)$.

Proof. We can assume that $B \neq (0, \ldots, 0)^t$. Consider the homogeneous system $CX' = 0$, where $X' = (x_1, \ldots, x_n, z)$. We only need to prove that if $(s_1, \ldots, s_n)$ is a minimal solution of $AX = B$, then $s = (s_1, \ldots, s_n, 1)$ is a minimal solution of $CX' = 0$.

Suppose that this is not the case. Then there must be a solution $s' < s$ of $CX' = 0$ of the form $s' = (s'_1, \ldots, s'_n, 1)$ with $s'_i \leq s_i$ for all i and $s'_j < s_j$ for some j (a key point is that the last component cannot be zero). But then $(s'_1, \ldots, s'_n)$ is a solution of $AX = B$, in contradiction with the minimality of s. □

Finally we can present the main result of the paper:

Theorem 2. *The minimal solutions of $\Sigma(E; S)$ are uniformly bounded as follows:*

$$||\Sigma(E; S)|| \leq (8|V||E|)^{2|V|+1} + \textit{smaller terms}$$

Proof. The texts in parenthesis refer to what result was used.

$$\begin{aligned}
||\Sigma(E; S)|| &= ||\Sigma_1|| \quad \text{(Eq. 8)} \\
&\leq (|E| + 2)||\Sigma_2|| + 2|E| \quad \text{(Lem 4)} \\
&\leq (|E| + 2)((1 + ||C||_{1,\infty})^{\operatorname{rank} C} - 1) + 2|E| \quad \text{(Cor 1)} \\
&\leq (|E| + 2)((1 + 8|V||E|)^{2|V|} - 1) + 2|E| \quad \text{(Lem 4, 5)}
\end{aligned}$$

□

Corollary 2. *The exponent of periodicity of a minimal solution of a word equation E is bounded by a polynomial $p(|E|)$ of degree no bigger than $2|V| + 1$, where $|V|$ is the number of different variables in E.*

References

[1] V. Bulitko, *Equations and inequalities in a free group an a free semigroup*, Tul. Gos. Ped. Inst. Ucen. Zap. Mat. Kafedr, Geometr. i Algebra 2, 242-252 (in Russian).

[2] V. Diekert and J. M. Robson, *Quadratic word equations*, In "Jewels are forever – Contributions on Theoretical Computer Science in Honor of Arto Salomaa", J. Karhumäki et al. Ed., Springer-Verlag, 314–326, 1999.

[3] C. Gutiérrez, *Satisfiability of Word Equations with Constants is in Exponential Space*, in Proceedings FOCS'98, pp. 112-119, IEEE Comp. Soc. Press, 1998.

[4] A. Koscielski, L. Pacholski, *Complexity of Makanin's Algorithm*, Journal of the ACM, Vol. 43, No. 4, July 1996, pp. 670-684.

[5] W. Charatonik, L. Pacholski, *Word Equations With Two Variables*, in H. Abdulrab, J-P. Pécuchet Eds., Word Equations and Related Topics, LNCS 677, Springer-Verlag, 1991.

[6] S. Eyono Obono, P. Goralcik, M. Maksimenko, *Efficient Solving of the Word Equations in One Variable*, in I. Privara et al. Eds., Proceedings of the 19th MFCS, LNCS 841, pp. 336-341, Springer-Verlag, 1994.

[7] W. Plandowski, *Satisfiability of Word equations with constants is in PSPACE*, In Proceedings of the FOCS'99, pp. 495-500, IEEE Comp. Soc. Press, 1999.

[8] L. Pottier, *Minimal solutions of linear diophantine systems: bounds and algorithms*, in R.V. Book, Ed., "Rewriting Techniques and Applications", LNCS vol. 488, pp. 162-173, Springer 1991.

Depto. de Ciencias de la Computación, Universidad de Chile, Blanco Encalada 2120, Santiago de Chile, Chile
E-mail address: cgutierr@dcc.uchile.cl