Theoretical Computer Science 108 (1993) 311–329
Elsevier

Mathematical Games

Rotating-table games and derivatives of words

Reuven Bar Yehuda*, Tuvi Etzion** and Shlomo Moran**
Department of Computer Science, Technion IIT, Haifa 32000, Israel

Communicated by A.S. Fraenkel
Received June 1991
Revised May 1992

Abstract

Bar Yehuda, R., T. Etzion and S. Moran, Rotating-table games and derivatives of words, Theoretical Computer Science 108 (1993) 311–329.

We consider two versions of a game for two players, A and B. The game consists of manipulations of words of length n over an alphabet of size σ, for arbitrary n and σ. For $\sigma = 2$ the game is described as follows: Initially, player A puts n drinking glasses on a round table, some of which are upside down. Player B attempts to force player A to set all the glasses in the upright position. For this, he instructs player A to invert some of the glasses. Before following the instruction, player A has the freedom to rotate the table, and then to invert the glasses that are in the locations originally pointed by player B. In one version of the game, player B is blindfolded and in the other he is not. We show that player B has winning strategies for both games iff n and σ are powers of the same prime. In both games we provide optimal winning strategies for B.

The analysis of the games is closely related to the concept of the *derivative* of a σ-ary word of length n. In particular, it is related to the *depth* of such word, which is the smallest k such that the kth derivative of the word is the all-zero word. We give tight upper bounds on the depth of σ-ary words of length n, where σ and n are powers of the same prime.

Correspondence to: S. Moran, Department of Computer Science, Technion-Israel Institute of Technology, Technion city, Haifa 32000, Israel.

*Work supported in part by the Technion V.P.R. Fund and the Albert Einstein Research Fund.
**The work of this author was supported in part by the Technion V.P.R. Fund.

1. Introduction

1.1. The open glass-inverting game

Consider the following game for two players, A and B, seated by a rotating round table: The game starts when player A (the *adversary*) puts four drinking glasses on the north, west, south and east sides of the table, such that some of the glasses are in the upright position, and others are upside down. The goal of player B (who sees the table) is to set all the glasses in the upright position, while player A tries to prevent him from doing so. The first round of the game starts when player B points to some of the glasses, and asks player A to invert them. Next, player A rotates the table counter-clockwise in an angle which is an arbitrary multiple of 90°, and then he inverts the glasses at the locations pointed out by player B (i.e., if player B pointed out the south and east glasses and player A rotates the table by 90°, then he inverts the glasses that originally were at the west and south sides, see Fig. 1). This completes the first round.

Fig. 1. Illustration of the open game.

The second round starts similarly by having player B select a subset of the glasses, and so on and so forth.

We now generalize the game for an arbitrary number of drinking glasses. For this, we view n glasses as a sequence of n zeros (for upright glasses) and ones (for upside down glasses). Players B's instructions are also viewed as binary words, where ones indicate "invert" and zeroes indicate "leave as it is". The game is, thus, described as follows: Initially, player A chooses a binary word W_0 of length n. The game continues in rounds as before, where at the ith round ($i \geqslant 1$), the new position of the glasses is generated as a binary word W_i as follows:

(1) Player B gives player A a binary word, called key_i. This word denotes which glasses should be inverted, after the table is rotated.

(2) Player A selects an integer s_i in the range $[0, \ldots, n-1]$. s_i corresponds to rotating the table by an angle of $s_i \cdot 360°/n$. Thus, $W_i = W_{i-1} + \mathbf{E}^{s_i} key_i$, where the vector addition is done modulo 2, and $\mathbf{E}^s key$ denotes a (left) cyclical shift of the word key by s entries.

Player B wins the game if he can force player A to generate the all-zero word $[0]^n$. The question we wish to study is for what values of n player B has a winning strategy, and in those cases when there is such a strategy, how many rounds are required, in the worst case, to win.

1.2. A generalization for larger alphabet sizes

The open game described above can be generalized to words over alphabets of arbitrary size $\sigma > 2$, as follows. Instead of n drinking glasses, we now have on the rotating table n roulettes of σ sides each. Denote the sides of the roulettes by $0, \ldots, \sigma - 1$. Each round starts when player B selects some of the roulettes, and for each selected roulette, player B also selects an angle by which it should be rotated. After receiving these instructions, player A first rotates the table, and then he follows player B's instructions on the roulettes which after the rotation are at the locations originally selected by player B. Player B wins the game if he can force player A to set all the roulettes so that the side which is closest to the center of the table is the one marked by zero. Describing this in the notation of words over alphabet $\{0, \ldots, \sigma - 1\}$, we get a description similar to the one for binary words (where the addition now is modulo σ).

1.3. The blind game

This game is essentially the same as the open game, with one important exception: player B is blindfolded from the very beginning of the game. This means that he sees neither the initial configuration of the glasses, nor any of the subsequent configurations generated by player A.

The blind game can be also described in a different way, which is more convenient to handle: Since player B gets no information during the game, the sequence

$(key_1, \ldots, key_m)$ which he generates during the game depends only on n (and σ). Therefore, we can describe the blind game as a *one* player game, in which the adversary plays against the sequence $KEY = (key_1, \ldots, key_m)$ as follows:

Initially, the sequence KEY is given to A.

Using this sequence, A generates the sequence $S = W_0, \ldots, W_m$ as follows:

(r1) Choose arbitrary vector as W_0.

Given W_{i-1}, W_i is created as follows:

(r2) Select an integer s_i in the range $[0, \ldots, n-1]$, and set $W_i = W_{i-1} + \mathbf{E}^{s_i} key_i$.

Player A loses the game if one of the W_i's is the word $[0]^n$.

The sequence KEY is a (σ, n) *universal* (or simply *universal*) if A must lose the game (i.e., if he must generate the word $[0]^n$) when playing against this sequence. Thus, Player B (in the original formulation of the game) has a winning strategy for the blind game iff there exists a universal sequence.

We note that the blind game for $\sigma = 2$ resembles the rotating table game of [7, 5]. Lasser and Ramshaw [5] described the history of rotating-table games. These games are different from our games and the techniques used in analyzing these games are quite different.

1.4. Summary of results

We show that Player B can win either the open or the blind game iff σ and n are powers of the same prime. We also provide optimal bounds on the number of rounds needed to win the game in both cases.

The rest of the paper is organized as follows. In Section 2 we prove that player B cannot have a winning strategy for the open game, unless σ and n satisfies the condition above. In section 3 we define derivative, linear complexity and depth of a word, which appear to be closely related to the games above. In section 4 we give a very simple strategy for winning the open game, and proves its optimality. In section 5 we provide optimal strategy for winning the blind game, and an exact bound on the number of rounds needed by this strategy. Finally, in Section 6 we provide a detailed analysis on the depth of σ-ary words, which provides exact bounds on the number of rounds needed to win the open game.

2. A necessary condition for winning

In this section we prove that player B cannot win the open game unless n and σ are powers of the same prime. Clearly, this result applies also to blind game.

Theorem 2.1. *If player B can win the open game, then there is a prime p such that* $\sigma = p^\alpha$ *and* $n = p^\beta$ *for some integers* $\alpha \geq 0$ *and* $\beta > 0$.

Proof. We prove this theorem by showing that if n and σ do not satisfy the above property, then player A has a winning strategy. We do this in two stages, each time weakening the assumptions on the relation between n and σ.

Assume first that $\gcd(\sigma, n)=1$. We show that A can generate words $W_0, W_1, \ldots$ such that for all i, $w_i(0) \neq w_i(1)$ ($w_i(j)$ denotes the jth entry of W_i).

W_0 is taken to be the word $(1, 0, \ldots, 0)$. We now assume that $w_{i-1}(0) \neq w_{i-1}(1)$, and show that for every word $key = key_i$ supplied by player B, there is an $s = s_i$ such that in $W = W_i = W_{i-1} + \mathbf{E}^s key$, it holds that $w(0) \neq w(1)$. Let $d \equiv w_{i-1}(0) - w_{i-1}(1) \pmod{\sigma}$. By induction, $0 < d < \sigma$. Let $key = (key(0), \ldots, key(n-1))$. Then it is easily verified that an integer s in $[0, \ldots, n-1]$ satisfies the above iff it satisfies the following:

$$key(s+1) - key(s) \not\equiv d \pmod{\sigma}, \quad \text{where } key(n) = key(0).$$

Thus, it is sufficient to prove that for some s, the inequality above holds. Assume for contradiction that for all s, $key(s+1) = key(s) + d \pmod{\sigma}$. Then we have

$$key(0) = key(0) + \sum_{i=0}^{n-1} (key(i+1) - key(i)) \equiv key(0) + nd \pmod{\sigma}.$$

In particular, we get that $nd \equiv 0 \pmod{\sigma}$. However, since $\gcd(\sigma, n)=1$, this last equality implies that σ divides d; but this is impossible, since $0 < d < \sigma$. This contradiction completes the proof for the case that $\gcd(\sigma, n)=1$.

Next, we consider the general case, where σ and n are not powers of the same prime. This implies that there are integers g and f, where g divides σ and f divides n, and $\bar{\sigma} = \sigma/g$ and $\bar{n} = n/f$ are distinct primes. In particular, $\gcd(\bar{\sigma}, \bar{n})=1$ and $1 < \min\{\bar{\sigma}, \bar{n}\}$. We handle this case by essentially reducing it to the former one. For this, we use the following notation:

With each word $U = (u(0), \ldots, u(n-1))$ of length n whose entries are in $\{0, \ldots, \sigma-1\}$ associate a word $\bar{U} = (\bar{u}(0), \ldots, \bar{u}(\bar{n}-1))$ of length $\bar{n}$ whose entries are in $\{0, \ldots, \bar{\sigma}-1\}$ in the following way: For $i = 0, \ldots, \bar{n}-1$,

$$\bar{u}(i) \equiv u(fi) \pmod{\bar{\sigma}}$$

(i.e., the ith entry in $\bar{U}$ is the fith entry in U modulo $\bar{\sigma}$).

Using the above notation, the proof proceeds along lines similar to the previous case, as follows. Given any sequence $KEY = (key_1, \ldots, key_m)$, we prove that KEY is not universal by showing that A can generate words $W_0, W_1, \ldots, W_m$ such that for all i, $\bar{w}_i(0) \neq \bar{w}_i(1)$. We start by taking $W_0 = (1, 0, \ldots, 0)$ (which means that also $\bar{W}_0 = (1, 0, \ldots, 0)$).

We now assume that the claim holds for W_{i-1}, i.e., $\bar{w}_{i-1}(0) \neq \bar{w}_{i-1}(1)$, and show that for every word $key = key_i$ there is an $s = s_i$ such that for $W = W_i = W_{i-1} + \mathbf{E}^s key$, it holds that $\bar{w}(0) \neq \bar{w}(1)$.

This is done by first considering the words $\overline{W_{i-1}}$ and $\overline{key}$. Since $\gcd(\bar{\sigma}, \bar{n})=1$, the proof of the previous case implies that for some s it holds that in $U = \overline{W_{i-1}} + \overline{\mathbf{E}^s key}$, we have that $u(0) \neq u(1)$ and, hence, $\bar{w}(0) \neq \bar{w}(1)$. □

3. Derivatives and linear complexity

In both the open and blind games we are making use of derivatives and linear complexity of words. The derivative was first used by [3, 8] for binary words. [4] is an excellent reference for the linear complexity.

For a word $W=[w(0), w(1),\ldots,w(k-1)]$, the derivative of W is defined by $(\mathbf{E}-\mathbf{1})W=\mathbf{E}W-W$. The depth of W, denoted by $depth(W)$, is the least x such that $(\mathbf{E}-\mathbf{1})^x W=0$ if such x exists, and ∞ otherwise. For the binary case $\mathbf{E}-\mathbf{1}$ is often called the D-morphism [6]. The proof of the following lemma is easy and left to the reader.

Lemma 3.1. *Let $W=[w(0), w(1),\ldots,w(n-1)]$ be a given word. Let $W'=[w(n-1), w(n-2),\ldots,w(0)]$ be the word W written in reverse order, and let $W''=\mathbf{E}^k W$ for some integer k. Then $depth(W)=depth(W')=depth(W'')$.*

3.1. Linear complexity

In this section we assume that the entries of the words are from $GF(q)$, $q=p^\alpha$, p prime, and the addition is the one of $GF(q)$. Any word $W=[w(0), w(1),\ldots,w(n-1)]$, satisfies a linear recursion

$$w(i+m)+\sum_{j=1}^{m} a_j w(i+m-j)=0, \quad i\geqslant 0,\ a_j\in GF(p),$$

where m, the degree of the recursion, is less than or equal to the length of W. In terms of the shift operator $\mathbf{E}$, the linear recursion takes the form

$$f(\mathbf{E})W=\left(\mathbf{E}^m+\sum_{j=1}^{m} a_j \mathbf{E}^{m-j}\right)W=[0]^n.$$

The (linear) *complexity* $C(W)$ of W is defined as the least integer m for which there exists a polynomial $f(\mathbf{E})$ of degree m such that $f(\mathbf{E})W=[0]^n$. As we see in Lemma 3.3, in this case the linear complexity and the depth coincide. Games and Chan [2] gave an efficient algorithm for computing the linear complexity of words of length 2^β. A generalization of this algorithm for words of length q^β, q prime power, with entries from $GF(q)$, was given by Ding [1].

In Lemmas 3.2 and 3.3, let W be a word of length $n=p^r$, for a prime p, with entries from $GF(q)$, $q=p^\alpha$.

Lemma 3.2. *If $f(\mathbf{E})$ is a polynomial with the least degree, with coefficients from $GF(p)$, such that $f(\mathbf{E})W=[0]^n$ and there exists a polynomial $g(\mathbf{E})$ such that $g(\mathbf{E})W=[0]^n$ then $f(\mathbf{E})$ divides $g(\mathbf{E})$.*

Proof. Assume that $f(\mathbf{E})$ does not divide $g(\mathbf{E})$; then we can find two polynomials $h_1(\mathbf{E})$ and $h_2(\mathbf{E})$ such that $g(\mathbf{E})=h_1(\mathbf{E})f(\mathbf{E})+h_2(\mathbf{E})$ and the degree of $h_2(\mathbf{E})$ is less than the

degree of $f(\mathbf{E})$. Now $[0]^n = g(\mathbf{E})W = (h_1(\mathbf{E})f(\mathbf{E}) + h_2(\mathbf{E}))W = (h_1(\mathbf{E})f(\mathbf{E}))W + h_2(\mathbf{E})W = h_2(\mathbf{E})W$, a contradiction to the fact that $f(\mathbf{E})$ is a polynomial with the least degree such that $f(\mathbf{E})W = [0]^n$. □

Lemma 3.3. *$C(W) = c$ if and only if $(\mathbf{E}-\mathbf{1})^{c-1}W = [d]^n$, for some constant $d \neq 0$.*

Proof. Let $f(\mathbf{E})$ be the polynomial with the least degree such that $f(\mathbf{E})W = [0]^n$. Since $\mathbf{E}^n W - W = (\mathbf{E}^n - 1)W = [0]^n$, then by Lemma 3.2 $f(\mathbf{E})$ divides $\mathbf{E}^n - 1$. It is also easy to verify that p divides $\binom{n}{i}$ for $1 \leqslant i \leqslant p^r - 1$ and, therefore, $\mathbf{E}^n - 1 = (\mathbf{E}-\mathbf{1})^n$ (note that in $GF(2^k)$ minus and plus are the same). Hence, $f(\mathbf{E}) = (\mathbf{E}-\mathbf{1})^c$ and by the definition of linear complexity $C(W) = c$ if and only if $(\mathbf{E}-\mathbf{1})^{c-1}W = [d]^n$, for some constant $d \neq 0$. □

3.2. Derivatives

For words of length p^β with entries taken from Z_{p^α} we have to prove first that the depth is finite.

Lemma 3.4. *Given a word W of length $n = p^\beta$, p prime, whose entries are from Z_{p^α}, then $(\mathbf{E}-\mathbf{1})^{\alpha n}W = [0]^n$.*

Proof. From the proof of Lemma 3.3, we have that in the word $(\mathbf{E}-\mathbf{1})^{p^\beta}W$ all the entries are congruent to 0 modulo p. By induction, in the word $(\mathbf{E}-\mathbf{1})^{ip^\beta}W$ all the entries are congruent to 0 modulo p^i. Therefore, $(\mathbf{E}-\mathbf{1})^{\alpha p^\beta}W = [0]^n$. □

From Lemma 3.4 we infer the following theorem.

Theorem 3.5. *Given a word W of length $n = p^\beta$, p prime, whose entries are from Z_{p^α}, then the depth of W is finite.*

Another simple observation is the following lemma.

Lemma 3.6. *Given a word W of length $n = p^\beta$, p prime, whose entries are from Z_{p^α}, then $depth(W) = x$ if and only if $(\mathbf{E}-\mathbf{1})^{x-1}W = [d]^n$, for some constant $d \neq 0$.*

4. A winning strategy for the open game

The winning strategy for the open game is very simple. Player B just have to ignore the fact that player A can rotate the table:

Winning strategy for the open game

(O.1) Assume that in step i the adversary holds the word W_i.

(O.2) We choose $key_i = -W_{i-1}$.

We claim that if the depth of W_0 is r, then in at most r steps the adversary will hold the all zero word. This claim is based on the following lemma which can be verified by simple algebraic manipulations.

Lemma 4.1. *If $f(\mathbf{E})$ is a polynomial with coefficients in Z_{p^s}, W a word with entries from Z_{p^s}, and $d \in Z_{p^s}$ then $f(\mathbf{E})(dW) = df(\mathbf{E})W$.*

Lemma 4.2. *If depth $(W_0) = r$ then in at most r steps the adversary will hold the all-zero word.*

Proof. It is sufficient to prove that for every j, $depth(W_{i+1}) = depth(W_i + \mathbf{E}^j key_{i+1}) < depth(W_i)$. If $depth(W_i) = x+1$ then $(\mathbf{E}-\mathbf{1})^x W_i = [d]^n$ by Lemma 3.6. Then $(\mathbf{E}-\mathbf{1})^x key_{i+1} = (\mathbf{E}-\mathbf{1})^x(-W_i) = [-d]^n$; so, for every j, $(\mathbf{E}-\mathbf{1})^x(W_i + \mathbf{E}^j key_{i+1}) = [0]^n$ and, therefore, $depth(W_i + \mathbf{E}^j key_{i+1}) < depth(W_i)$. □

Now we prove the following theorem.

Theorem 4.3. *If W_0 is the initial word of the adversary, then there is no strategy that forces a win in less than r steps.*

The proof is an immediate observation from the following two lemmas.

Lemma 4.4. *Assume that W and U are two words of length n, where the depth of W is c_1, and the depth of U is c_2, $c_1 < c_2$, then the depth of $\mathbf{E}^i W + \mathbf{E}^j U$, for any i, j, is c_2.*

Proof. By the definition of the depth, $(\mathbf{E}-\mathbf{1})^{c_2-1} W = [0]^n$ and $(\mathbf{E}-\mathbf{1})^{c_2-1} U = [d]^n$, for some $d \neq 0$. Hence, $(\mathbf{E}-\mathbf{1})^{c_2-1}(\mathbf{E}^i W + \mathbf{E}^j U) = [d]^n$ and the depth of $\mathbf{E}^i W + \mathbf{E}^j U$ is c_2. □

Lemma 4.5. *Let W and U be two words of length n, with the same depth c. Then there exists some i such that the depth of $\mathbf{E}^i W + U$ is at least $c-1$.*

Proof. Assume that the depth of $W+U$ is at most $c-2$. By the definition of the depth, $(\mathbf{E}-\mathbf{1})^{c-2}(W+U) = [0]^n$ and, therefore, $(\mathbf{E}-\mathbf{1})^{c-2} W = [v(0), v(1), \ldots, v(n-1)]$ and $(\mathbf{E}-\mathbf{1})^{c-2} U = [-v(0), -v(1), \ldots, -v(n-1)]$. Since the depth of W is c, not all the $v(j)$ are equal. Thus, $v(0) \neq v(i)$ for some i and, hence, $(\mathbf{E}-\mathbf{1})^{c-2}\mathbf{E}^i W + (\mathbf{E}-\mathbf{1})^{c-2} U = (\mathbf{E}-\mathbf{1})^{c-2}(\mathbf{E}^i W + U) \neq [0]^n$ and, therefore, the depth of $\mathbf{E}^i W + U$ is at least $c-1$. □

A winning strategy for words of length q^β with entries taken from $GF(q)$ and the addition is in $GF(q)$ is the same.

5. A winning strategy for the blind game

5.1. Lower bound on the length of universal sequences

Recall that player B can win the blind game iff there exists a (σ, n) universal sequence, as defined in the introduction.

Lemma 5.1. *If $KEY=(key_1,\ldots,key_m)$ is universal, then in every play of the game all the σ-ary words of length n must be generated. In particular, $m\geqslant\sigma^n-1$.*

Proof. We assume the contrary, and show that A can win the game. Assume that in some play of the game at least one σ-ary word of length n, say U, is never generated. Let $W=W_0$ be the first word generated by A in this game.

Consider now another play of the game, in which A makes exactly the same moves as in the original game, with one exception: The first word it generates is not W but $W-U$. It is easy to see that a σ-ary word V is generated in the former game iff the word $V-U$ is generated in the latter game. In particular, $U-U=[0]^n$ is not generated in the latter game. This means that KEY is not universal, which is the desired contradiction. □

We now show that if σ and n are powers of the same prime p, then a universal sequence of optimal length indeed exists. First we consider the case where $\sigma=p$.

5.2. Optimal universal sequences for a prime σ

In this section we assume that $|\Sigma|=\sigma=p$ and $n=p^\beta$ for some prime p and nonnegative integer β. The construction is based on the following lemma, which asserts that if the depth r of a word is known, then this depth can be reduced by a blind application of a sequence of length $p-1$, all of its entries are an arbitrary fixed word of the same depth r.

Lemma 5.2. *Let U and V be words of length n over Σ, such that $depth(U)=depth(V)=r>0$. Let $j_1,\ldots,j_{p-1}$ be arbitrary integers in $[0,\ldots,n-1]$. Let further $V_i=\mathbf{E}^{j_i}V$, and $W_i=U+\sum_{j=1}^{i}V_j$. Then for some i, $depth(W_i)<r$.*

Proof. Since $depth(U)=depth(V)=r$, there are constants c and d such that

(a) $(\mathbf{E}-1)^{r-1}U=[c]^n$, and

(b) for all i, $(\mathbf{E}-1)^{r-1}V_i=[d]^n$.

Since p is a prime, there is i_0 such that $i_0 d\equiv -c(\mathrm{mod}\ p)$. This implies that

$$(\mathbf{E}-1)^{r-1}\left(U+\sum_{i=1}^{i_0}V_i\right)=(\mathbf{E}-1)^{r-1}W_{i_0}=[0]^n,$$

which means that $depth(W_{i_0})<r$. □

We now describe the construction of a (σ, n) universal sequence of optimal length, KEY. The construction is done in $n+1$ stages, where at stage i, $0 \leqslant i \leqslant n$, we construct a sequence KEY_i of length $\sigma^i - 1$, having the following properties:

$(i{:}1)$ All the words in KEY_i are of depth at most i.

$(i{:}2)$ Let W_0 be the first word generated by the adversary A. If $depth(W_0) \leqslant i$, then A must lose the game when playing against KEY_i.

Note that $(i{:}2)$ implies that $KEY = KEY_n$ is a universal sequence.

KEY_0 is the empty sequence of length $0 = p^0 - 1$. It is easily verified that it indeed satisfies $(0{:}1)$ and $(0{:}2)$. Assume now that we are given a sequence KEY_i of length $l_i = \sigma^i - 1$ which satisfies $(i{:}1)$ and $(i{:}2)$, where $0 \leqslant i < n$. A sequence KEY_{i+1} of length $\sigma^{i+1} - 1$ which satisfies $(i+1{:}1)$ and $(i+1{:}2)$ is constructed as follows:

Let V be an arbitrary word such that $depth(V) = i+1$, and for $i = 1, \ldots, \sigma - 1$, let $V_i = V$. Then $KEY_{i+1} = KEY_i \circ (V_1) \circ KEY_i \circ (V_2) \circ \cdots \circ (V_{\sigma-1}) \circ KEY_i$.

It is easily observed that l_{i+1}, the length of KEY_{i+1}, is $\sigma l_i + \sigma - 1 = \sigma^{i+1} - 1$. It remains to show that $(i+1{:}1)$ and $(i+1{:}2)$ are indeed satisfied by it:

$(i+1{:}1)$ holds by the induction hypothesis and the construction of KEY_{i+1}. To see that $(i+1{:}2)$ holds, assume first that $depth(W_0) \leqslant i$. Then by the induction hypothesis, A loses the game during the first application of KEY_i on W_0. Thus, we are left with the case where $depth(W_0) = i+1$. Assume for the moment that the sequence given to A is only the subsequence $(V_1, V_2, \ldots, V_{\sigma-1})$. By Lemma 5.2, when A plays against this subsequence only, there exists an i_0 such that after applying (a cyclic shift of) V_{i_0}, A must generate a word W such that $depth(W) \leqslant i$. Now, by induction, the remaining words in KEY_{i+1} (excluding the V_i's) are of depth at most i. Hence, by an argument similar to the one in Lemma 4.4, the application of any subset of them on W cannot increase its depth above i. In particular, when A is using the complete sequence KEY_{i+1}, the word W' that it generates after applying V_{i_0} is also of depth at most i. Since immediately after applying V_{i_0} the complete sequence KEY_i is applied by A on W', A must lose the game by using the induction hypothesis on W'. This proves $(i+1{:}2)$.

5.3. Optimal universal sequences for the general case

In this section we extend the construction of Section 5.2 to the case where $\sigma = p^\alpha$ for arbitrary positive integer α. Thus, we prove the following theorem.

Theorem 5.3. *Let $\sigma = p^\alpha$ and $n = p^\beta$ for positive integers α and β. Then there is a (σ, n) universal sequence of optimal length $\sigma^n - 1$.*

Proof. We prove, by induction on α, that there is a (p^α, n) universal sequence KEY_α of length $l_\alpha = p^{\alpha n} - 1$. For $\alpha = 1$, the theorem holds by the construction in Section 5.2. The (p, n) universal sequence $KEY_1 = (U_1, \ldots, U_{l_1})$ (where $l_1 = p^n - 1$) is used in the recursive construction, as described below. Assume now that the theorem holds for α, and prove it for $\alpha + 1$.

Let KEY_α be the (p^α, n) universal sequence of length $l_\alpha = p^{\alpha n} - 1$ whose existence is guaranteed by the induction. We use KEY_α to construct a sequence KEY' of words whose entries are in $\{0, p, 2p, \ldots, p^{\alpha+1} - p\}$, as follows: Replace each word $key = [key(1), \ldots, key(n)]$ in KEY_α by the word $p \cdot key = [p \cdot key(1), \ldots, p \cdot key(n)]$. The following observation follows easily by the induction hypothesis and the definition of KEY'.

Observation 5.4. Let W_0 be a word of length n over alphabet $0, p, \ldots, p^{\alpha+1} - p$. Then A must lose the game when playing against KEY'.

The construction of $KEY_{\alpha+1}$ is done by interleaving the sequence KEY' between the words of the sequence KEY_1 as follows: $KEY_{\alpha+1} = KEY' \circ (U_1) \circ KEY' \circ (U_2) \circ \cdots \circ (U_{l_1}) \circ KEY'$.

$l_{\alpha+1}$, the length of $KEY_{\alpha+1}$, is given by $l_{\alpha+1} = p^n - 1 + p^n l_\alpha = p^{(\alpha+1)n} - 1$, as claimed. To see that $KEY_{\alpha+1}$ is a $(p^{\alpha+1}, n)$ universal sequence, observe that if all entries of W_0 are divisible by p then Observation 5.4 implies that A must lose the game. Otherwise, an argument similar to the one in Section 5.2 shows that if A is playing against the sequence KEY_1, then for some j in $[0, \ldots, p^n - 1]$, all the entries of the word W generated by A after using (a cyclic shift of) the word U_j are divisible by p. Since all the entries of the remaining words in $KEY_{\alpha+1}$ are also divisible by p, this holds also for the word W' generated by A after using U_j when playing against the full sequence $KEY_{\alpha+1}$. Immediately after using U_j, A must use the complete sequence KEY_α; the proof is now completed by using the induction hypothesis on W' and KEY_α. □

5.4. Generalization for $GF(q)$

We generalize the blind game algorithm for the case where the entries of the words are taken from $GF(q)$, $q = p^\alpha$, p prime, and the word length is $n = q^\beta$. We will make use of the following lemma.

Lemma 5.5. *Let $W = [w(0), w(1), \ldots, w(n-1)]$ and $U = [u(0), u(1), \ldots, u(n-1)]$ be two words with linear complexity c. Let γ be a primitive element in $GF(q)$. There exist an integer i, $0 \leqslant i \leqslant q-2$, such that $W + [\gamma^i u(0), \gamma^i u(1), \ldots, \gamma^i u(n-1)]$ is a word with linear complexity less than c.*

Proof. Since the linear complexity of W and U is c, there exist two nonzero entries d_1 and d_2 in $GF(q)$ such that $(\mathbf{E}-\mathbf{1})^{c-1} W = [d_1]^n$ and $(\mathbf{E}-\mathbf{1})^{c-1} U = [d_2]^n$. Now, let i be the integer such that $\gamma^i = -d_1 (d_2)^{-1}$ and $V = [\gamma^i u(0), \gamma^i u(1), \ldots, \gamma^i u(n-1)]$. It follows that $(\mathbf{E}-\mathbf{1})^{c-1} V = \gamma^i (\mathbf{E}-\mathbf{1})^{c-1} U = [\gamma^i d_2]^n = [-d_1]^n$ and, hence, $(\mathbf{E}-\mathbf{1})^{c-1}(W+V) = [0]^n$; therefore, the linear complexity of $W+V$ is less than c. □

Let KEY_0 be the empty sequence. Given a universal sequence KEY_i which beats a word with linear complexity at most i, we construct a universal sequence KEY_{i+1}

which beats a word with linear complexity at most $i+1$. Let V be an arbitrary word with linear complexity $i+1$ and let γ be a primitive element in $GF(q)$. Let $V_0 = V$ and for $1 \leqslant j \leqslant q-2$, $V_j = \gamma^j V - V_{j-1}$. Then $KEY_{i+1} = KEY_i \circ (V_0) \circ KEY_i \circ (V_1) \circ \cdots \circ (V_{q-2}) \circ KEY_i$. It is easy to observe that KEY_{i+1} is a universal sequence which beats any word with linear complexity at most $i+1$, as claimed.

6. Bounds on the depth of words for $\sigma = p^\alpha$

A very interesting question in this context is to find what is the maximal depth of a word. If the length of the word is $n = p^\beta$ and the entries are taken from Z_{p^α}, Lemma 3.4 implies that an upper bound on this depth is αn. We will improve this bound to $n + (\alpha - 1)(n - p^{\beta-1})$ and show that this is tight. In both upper and lower bound proofs we first consider the simple case where $\alpha = 1$, and then generalize the proof to arbitrary α.

Lemma 6.1. *If $\alpha = 1$ the maximal depth of a word of length n is n and any word W for which the sum of entries is d, $d \not\equiv 0 (\mathrm{mod}\ p)$ has depth n.*

Proof. By Lemma 3.4, the depth of each word is at most n. Since when $\alpha = 1$ the computations are modulus a prime p, we have

$$(\mathbf{E}-\mathbf{1})^{n-1} = \frac{(\mathbf{E}-\mathbf{1})^n}{\mathbf{E}-\mathbf{1}} = \frac{\mathbf{E}^n - \mathbf{1}}{\mathbf{E}-\mathbf{1}} = \sum_{i=0}^{n-1} \mathbf{E}^i,$$

and thus $(\mathbf{E}-\mathbf{1})^{n-1} W = [d]^n$ for some $d \neq 0$ and, therefore, W has depth n. □

For the case where $\alpha > 1$ we distribute all the nonzero words of length $n = p^\beta$ with entries taken from Z_{p^α} into α layers. Each layer is divided into n levels. The layers are labelled by $0, 1, \ldots, \alpha - 1$. We denote layer i of the words over $\sigma = p^\alpha$ by $L_{\alpha,i}$. When there is no ambiguity, we will denote $L_{\alpha,i}$ by L_i. Layer L_i consists of all the words in which p^i divides all the entries, and there is some entry which is not divisible by p^{i+1}. We now describe how the words in each layer are partitioned into n levels, labelled by $1, 2, \ldots, n$.

Assume first that $\alpha = 1$, in which case there is only one layer, $L_{1,0}$. Level 1 of that layer consists of all words $W = [w(0), \ldots, w(n-1)]$ for which $\sum_{i=0}^{n-1} w(i) \not\equiv 0 (\mathrm{mod}\ p)$. Levels of higher indices are defined by induction, as follows: A word V is in level $i+1$ iff there is a word U in level i such that $V = (\mathbf{E}-\mathbf{1})U$. Note that, by the proof of Lemma 6.1, there are exactly n levels, and a word V is in level i iff its depth is $n-i+1$.

For $\alpha > 1$, the levels of layer $L_{\alpha,i}$ $(0 \leqslant i \leqslant \alpha - 1)$ are defined as follows: Let $V = [v(0), \ldots, v(n-1)]$ be a word in layer $L_{\alpha,i}$. Then $v(k)$ is divisible by p^i for $k = 0, \ldots, n-1$ and, hence, the word $(1/p^i)V (\mathrm{mod}\ p) = [(v(0)/p^i) (\mathrm{mod}\ p), \ldots, (v(n-1)/p^i) (\mathrm{mod}\ p)]$ is well-defined. Then V is in level j of layer $L_{\alpha,i}$ if $(1/p^i)V (\mathrm{mod}\ p)$ is in level j of $L_{1,0}$. A more illustrative way to describe this definition is as follows: each

entry $v(k)$ of V can be written by α *p-ary* digits, out of which the i least significant digits, i.e., the digits in positions 0 through $i-1$, are zeroes. Then V is in level j iff the word obtained from V by replacing each entry $v(k)$ by the $(i+1)$th least significant digit, i.e., the digit in position i, of $v(k)$ is in level j of $L_{1,0}$.

We start with two useful lemmas that follows directly from the definitions and from Lemma 6.1 and its proof.

Lemma 6.2. (1) *If V is in level n of some layer L_i, then $(\mathbf{E}-\mathbf{1})V$ is either the all-zero word, or is a word in layer $L_{i'}$ for $i'>i$.*

(2) *If V is in level j of some layer L_i, where $j<n$, then $(\mathbf{E}-\mathbf{1})V$ is in level $j+1$ of L_i.*

Lemma 6.3. *Let V be a word in level j of layer $L_{\alpha,i}$ and let $V'=(1/p^{i'})V(\mathrm{mod}\, p^{\alpha'})$ for some $i'\leqslant i$ and some $\alpha'>i-i'$. Then V' is in level j of layer $L_{\alpha',i-i'}$. Moreover, let U and U' be nonzero words defined by $U=(\mathbf{E}-\mathbf{1})^k V$ and $U'=(\mathbf{E}-\mathbf{1})^k V'$. Then U is in level j_1 of layer L_{α,i_1} iff U' is in level j_1 of layer $L_{\alpha',i_1-i'}$.*

Before proceeding, we need two more definitions. The *height* of a word V, denoted by *height*(V), is the maximum integer i such that $(\mathbf{E}-\mathbf{1})^i W=V$ for some word W (note that $(\mathbf{E}-\mathbf{1})^0 V=V$ by definition; hence, this definition is valid for all words). The *trace* of a word V, to be denoted by *trace*(V), is the set of all nonzero words U such that $(\mathbf{E}-\mathbf{1})^i V=U$ for some $i\geqslant 0$. Note that $|trace(W)|=depth(W)$ and that, by Lemma 6.2, *trace*(W) contains at most one word in each level of each layer.

An easy and useful consequence of the above definitions is the following lemma.

Lemma 6.4. *If U is in trace(V), then $depth(V)\leqslant height(U)+depth(U)$.*

The upper bound proof is based on the following lemma.

Lemma 6.5. *Let W be a word over $\sigma=p^\alpha$, and let $0\leqslant i\leqslant\alpha-2$. Let $S=trace(W)\cap(L_i\cup L_{i+1})$. If for some $1\leqslant j\leqslant n/p$, S contains a word U in level j of layer L_{i+1}, then $|S|\leqslant n$.*

The proof of Lemma 6.5 proceeds in few steps. First we consider the case $\alpha=2$ (which implies that $i=0$), and then we use Lemma 6.3 to reduce the general case to this one. The proof for the case $\alpha=2$ involves some manipulations of binomial coefficients and polynomials with coefficients from Z_{p^2}.

Lemma 6.6. *Let $f(\mathbf{E})=\sum_{i=0}^{k} a_i\mathbf{E}^i$ be a polynomial with coefficients from Z_{p^2}, $k\leqslant p^\beta-1$, $a_k=1$, and $a_0=(-1)^k$. $\mathbf{E}-\mathbf{1}$ divides $f(\mathbf{E})$ and the result is $g(\mathbf{E})=f(\mathbf{E})/(\mathbf{E}-\mathbf{1})=\sum_{i=0}^{k-1} b_i\mathbf{E}^i$ if and only if $b_{i-1}-b_i=a_i(\mathrm{mod}\, p^2)$, $1\leqslant i\leqslant k-1$, $b_{k-1}=1$ and $b_0=-a_0(\mathrm{mod}\, p^2)$.*

Proof. Follows immediately by computing $f(\mathbf{E})=g(\mathbf{E})(\mathbf{E}-1)$. □

A simple calculation of the binomial coefficients shows that Lemma 6.7 holds.

Lemma 6.7. *For $0\leqslant j\leqslant p^r$, p^2 divides $\binom{p^r}{j}$ if and only if $j\not\equiv 0 \pmod{p^{r-1}}$.*

Now, we remind the reader that in the Pascal triangle in row k, $k\geqslant 0$, and diagonal i, $0\leqslant i\leqslant k$, we have the binomial coefficients $\binom{k}{i}$. We use the Pascal triangle with computations modulo p^2. The following two properties of the Pascal triangle are needed for our proof:

(P1) $\binom{k}{i}+\binom{k}{i+1}=\binom{k+1}{i+1}$;

(P2) the first number in each diagonal is 1.

Lemma 6.8. *The largest x such that $(\mathbf{E}-\mathbf{1})^x$ divides $\mathbf{E}^{p^\beta}-1$, where the coefficient are computed in Z_{p^2},* is $x=p^{\beta-1}$.

Proof. A simple division shows that

$$\frac{\mathbf{E}^{p^\beta}-\mathbf{1}}{\mathbf{E}-\mathbf{1}}=\sum_{i=0}^{p^\beta-1}\mathbf{E}^i.$$

Now, note that, by (P2), these coefficients are the 0 diagonal in the Pascal triangle from row 0 to row $p^\beta-1$. By (P1) and (P2), and Lemma 6.6, if the numbers of diagonal k from row k to row $p^\beta-1$, are the coefficients of $(\mathbf{E}^{p^\beta}-1)/(\mathbf{E}-\mathbf{1})^{k+1}$ then the numbers of diagonal $k+1$ from row $k+1$ to row $p^\beta-1$, are the coefficients of $(\mathbf{E}^{p^\beta}-1)/(\mathbf{E}-\mathbf{1})^{k+2}$ if and only if $\binom{p^\beta-1}{k+1}\equiv(-1)^{k+1}\pmod{p^2}$.

By Lemma 6.7, all the first $p^{\beta-1}$ entries, except for the first one, in the p^βth row of the Pascal triangle are zeros and the next element is not zero. By using the facts that the first element in each row is 1 and (P1) it follows that $\binom{p^\beta-1}{i+1}\equiv(-1)^{i+1}\pmod{p^2}$ for $i\leqslant p^{\beta-1}-2$. For $i=p^{\beta-1}-1$, $\binom{p^\beta-1}{i+1}\not\equiv(-1)^{i+1}\pmod{p^2}$ since $\binom{p^\beta-1}{i+2}\equiv(-1)^{i+2}\pmod{p^2}$ and $\binom{p^\beta}{p^{\beta-1}}\not\equiv 0\pmod{p^2}$. □

We now proceed with the proof of Lemma 6.5 for the case $\alpha=2$. By Lemma 6.8, for each j, $1\leqslant j\leqslant p^{\beta-1}$, we can write $\mathbf{E}^{p^\beta}-\mathbf{1}=f_j(\mathbf{E})(\mathbf{E}-\mathbf{1})^j$, where $f_j(\mathbf{E})=\sum_{i=0}^{p^\beta-j}a_i\mathbf{E}^i$. We use this to prove the following lemma.

Lemma 6.9. *Let $1\leqslant j\leqslant p^{\beta-1}$ and let W be a word over $\sigma=p^2$. Then height(W) is $j-1$ iff $f_j(\mathbf{E})\,W=[d]^n$ for some $d\neq 0$.*

Proof. A word is in level 1 of layers 0 or 1 iff the sum of its entries is not congruent to $0\pmod{p^2}$. Hence, a word W is in level 1 iff $[(\mathbf{E}^{p^\beta}-1)/(\mathbf{E}-\mathbf{1})]\,W=\sum_{i=0}^{p^n-1}\mathbf{E}^i\,W=f_1(\mathbf{E})\,W=[d]^n$ for some $d\neq 0$. Hence, by the definition of the levels, for a word W and $1\leqslant j\leqslant p^{\beta-1}$, *height*$(W)=j-1$ iff $f_j(\mathbf{E})\,W=[d]^n$. □

Lemma 6.10. *Let j and W be as in Lemma 6.9. If W is in level j of L_1 $(=L_{2,1})$, then $height(W)=j-1$.*

Proof. By Lemma 6.9, it is sufficient to prove that for each word W in level j of L_1 it holds that $f_j(\mathbf{E})W=[d]^n$ for some $d\neq 0$, where $1\leqslant j\leqslant p^{\beta-1}$. For $j=1$ this holds since the sum of the entries of a word W in level 1 is not congruent to $0(\mathrm{mod}\, p^2)$. The proof for $1<j\leqslant p^{\beta-1}$ is by induction, using the equality of $f_j(\mathbf{E})=(\mathbf{E}-\mathbf{1})\, f_{j+1}(\mathbf{E})$ and Lemma 6.2. □

Proof of Lemma 6.5. Assume first that $\alpha=2$ and $i=0$. In this case, $|S|=depth(W)$. Assume that $trace(W)$ contains a word U at level j of L_1 for some $1\leqslant j\leqslant n/p$. Then, by Lemma 6.10, $height(U)=j-1$, and by Lemmas 6.1 and 6.2 and the definitions, $depth(U)=n-j+1$. Using Lemma 6.4, we get

$$depth(W)\leqslant height(U)+depth(U)=n,$$

which proves the lemma for $\alpha=2$.

Assume now that $\alpha>2$, and let W and i be given $(0\leqslant i\leqslant\alpha-2)$. The lemma holds trivially if S does not contain a word in L_i, so assume that V is a word of $S\cap L_i$ of minimum possible level. Let $V'=(1/p^i)\,V(\mathrm{mod}\, p^2)$. Then, using Lemma 6.3, we get that for $0\leqslant k$ and $\varepsilon=0, 1$, $(\mathbf{E}-\mathbf{1})^k V$ is in level j of $L_{\alpha,i+\varepsilon}$ iff $(\mathbf{E}-\mathbf{1})^k V'$ is in level j of $L_{2,\varepsilon}$. In particular, $|S\cap(L_i\cup L_{i+1})|=depth(V')\leqslant n$. □

Theorem 6.11. *The depth of a word of length $n=p^\beta$ over $\sigma=p^\alpha$ is at most $n+(\alpha-1)(n-p^{\beta-1})=n+(\alpha-1)(n-n/p)$.*

Proof. Since $depth(W)=|trace(W)|$, it is sufficient to prove that $|trace(W)|\leqslant n+(\alpha-1)(n-n/p)$. We define $T_i=trace(W)\cap L_i$ and prove that $\sum_{i=0}^{\alpha-1}|T_i|\leqslant n+(\alpha-1)(n-n/p)$.

Denote T_i as *critical* if $0<i\leqslant\alpha-1$ and T_i contains a word V in level j of L_i, where $1\leqslant j\leqslant n/p$. If no T_i is critical, then $|T_i|\leqslant n-n/p$ for all i except possibly $i=0$, and the theorem follows. So, assume that some T_i is critical. Let i_1 be the maximal index such that T_{i_1} is critical. Then by Lemma 6.5, $|T_{i_1}\cup T_{i_1-1}|\leqslant n$. Now, let i_2 be the maximal $i<i_1-1$ for which T_{i_2} is critical (if there is such an i). Then $|T_{i_2}\cup T_{i_2-1}|\leqslant n$. Continuing this way, we eventually get a sequence $i_1,\ldots,i_k$ such that $i_{l+1}<i_l-1$, each T_{i_l} is critical, and for every i which is not in $\{i_1, i_1-1, i_2, i_2-1,\ldots,i_k, i_k-1\}$, T_i is not critical. The $2k$ indices $i_1, i_1-1,\ldots,i_k, i_k-1$ correspond to $2k$ layers which contains at most kn entries of $trace(W)$. Out of the remaining $\alpha-2k$ layers, no one is critical. This means that except possibly L_0, each of these remaining layers contains at most $n-n/p$ entries of $trace(W)$. Thus, we get

$$\sum_{i=0}^{\alpha-1}|T_i|\leqslant n+kn+(\alpha-2k-1)(n-n/p).$$

Since $n-n/p \geqslant n/2$, the above inequality attains its maximum when $k=0$. This completes the proof of the theorem. □

We now prove that the lower bound of Theorem 6.11 is tight. Specifically, we prove a slightly stronger result.

Theorem 6.12. *For $l=1,\ldots,\alpha$, all the words in level 1 of layer $L_{\alpha,\alpha-l}$ are of depth $n+(l-1)(n-n/p)$.*

The proof of Theorem 6.12 is by induction on l. The base $l=1$ follows from Lemmas 6.1 and 6.3. Before proving the induction step, we next prove that, for each i, all the words in level 1 of $L_{\alpha,i}$ have the same depth.

Lemma 6.13. *For all α and i $(i<\alpha)$, all the words in level 1 of $L_{\alpha,i}$ have the same depth.*

Proof. Let $W^*=[p^i,0,\ldots,0]$. Then all the words in layer L_i are spanned by W^* and its cyclic shifts, which means, by the linearity of the operator $\mathbf{E}$, that for every word V in L_i, $depth(V) \leqslant depth(W^*)$. We will show that for every V in level 1 of layer L_i, $depth(V)=depth(W^*)$.

Let $depth(W^*)=k$ for some k. Then $(\mathbf{E}-\mathbf{1})^{k-1}W^*=[b]^n$ for some $b \not\equiv 0 \pmod{p^\alpha}$. It is sufficient to prove that for every V in level 1 of layer L_i, $(\mathbf{E}-\mathbf{1})^{k-1}V=[d]^n$ for some $d \not\equiv 0 \pmod{p^\alpha}$. Since V is in level 1, $V=p^iU$ for some $U=[u(0),\ldots,u(n-1)]$, where $\sum_{i=0}^{n-1} u(i)=c$ for some $c \not\equiv 0 \pmod{p}$. In particular, by Lemma 3.1, V has the same depth as $V'=(\sum_{i=0}^{n-1} u(i)\mathbf{E}^i)(W^*)$ and, hence, again by the linearity of the operator $\mathbf{E}$, $(\mathbf{E}-\mathbf{1})^{k-1}V'=c(\mathbf{E}-\mathbf{1})^{k-1}W^*=c[b]^n=[bc]^n=[d]^n$, where $d=bc$. Since $b \not\equiv 0 \pmod{p^\alpha}$ and $c \not\equiv 0 \pmod{p}$, we have that $d \not\equiv 0 \pmod{p^\alpha}$, which proves the lemma. □

By Lemma 6.13, in proving Theorem 6.12 it is sufficient to consider words of the form $[p^i,0,\ldots,0]$ or cyclic shifts of such words. Lemma 6.3 can now be used to reduce this further.

Lemma 6.14. *Let $W=[p^i,0,\ldots,0]$ be a word in level 1 of layer $L_{\alpha,i}$. Then $depth(W)=depth(W')$, where $W'=[1,0,\ldots,0]$ is in level 1 of layer $L_{\alpha-i,0}$.*

Substituting $i=\alpha-l$ in Lemma 6.14, the induction step in the proof of Theorem 6.12 will follow from Lemma 6.15.

Lemma 6.15. *Assume that Theorem 6.12 holds for $l-1$ $(l>1)$, and let $W=[1,0,\ldots,0]$ be in level 1 of layer $L_{l,0}$. Then there exists a word U in layer $L_{l,1}$ such that*

(1) $U=(\mathbf{E}-\mathbf{1})^n W$.

(2) $U=(\mathbf{E}-\mathbf{1})^{n/p}V$ *for some V in level 1 of layer $L_{l,1}$. Hence, by induction, $depth(U)=(l-1)(n-n/p)$.*

In particular, $depth(W)=depth(U)+n=n+(l-1)(n-n/p)$.

Thus, it only remains to prove Lemma 6.15. As in the case of the lower bound proof, we use Lemmas 6.2 and 6.3 to reduce Lemma 6.15 to the case $\alpha=2$. In particular, Lemma 6.15 will follow from the induction hypothesis for $l-1$ and from Lemma 6.15′.

Lemma 6.15′. *Let* $W=[1,0,\ldots,0]$ *be in level* 1 *of layer* $L_{2,0}$. *Then there exists a word* U *in layer* $L_{2,1}$ *such that*

(1) $U=(\mathbf{E}-\mathbf{1})^n W$.

(2) $U=(\mathbf{E}-\mathbf{1})^{n/p}V$ *for some* V *in level* 1 *of layer* $L_{2,1}$. *Hence,* $depth(U)=n-n/p$.

In particular, $depth(W)=depth(U)+n=n+(n-n/p)$.

The proof of Lemma 6.15′ will follow from some results concerning the binomial coefficients (mod p^2), which are presented next.

Lemma 6.16. *Let* p *be an odd prime, then* $\binom{p^r}{ip^{r-1}}\equiv\binom{p}{i}\equiv(-1)^{i-1}\,p/i \pmod{p^2}$, *for* $i<p$, *where* $1/i$ *is the inverse of* i *modulo* p^2.

Proof. We compute the two binomial coefficients

$$\binom{p}{i}\equiv\frac{p!}{(p-i)!\,i!}\equiv\frac{(p-i+1)(p-i+2)\cdots(p-2)(p-1)p}{1\cdot2\cdots(i-2)(i-1)i}$$

$$\equiv\frac{(i-1)(i-2)\cdots2\cdot1\cdot(-1)^{i-1}p}{1\cdot2\cdots(i-2)(i-1)i}\equiv(-1)^{i-1}\,p/i \pmod{p^2}.$$

$$\binom{p^r}{ip^{r-1}}\equiv\frac{(p^r)!}{(p^r-ip^{r-1})!(ip^{r-1})!}$$

$$\equiv\frac{(p^r-ip^{r-1}+1)(p^r-ip^{r-1}+2)\cdots(p^r-2)(p^r-1)p^r}{1\cdot2\cdots(ip^{r-1}-2)(ip^{r-1}-1)ip^{r-1}}$$

$$\equiv\frac{(ip^{r-1}-1)(ip^{r-1}-2)\cdots2\cdot1\cdot(-1)^{ip^{r-1}-1}p}{1\cdot2\cdots(ip^{r-1}-2)(ip^{r-1}-1)i}$$

$$\equiv(-1)^{i-1}\,p/i \pmod{p^2}. \qquad \square$$

Lemma 6.17. *Let* p *be an odd prime, then* $(\mathbf{E}-\mathbf{1})^{p^r}=\sum_{i=0}^{p}(-1)^{(p^r-ip^{r-1})}\binom{p^r}{ip^{r-1}}\mathbf{E}^{ip^{r-1}}$, *where the coefficients are computed modulo* p^2.

Proof. Follows immediately from expanding $(\mathbf{E}-\mathbf{1})^{p^r}$ and Lemma 6.7. $\square$

Lemma 6.18. *Let* p *be an odd prime,* $n=p^\beta$, W *a word with entries from* Z_{p^2} *which are divisible by* p. *Then* $(\mathbf{E}-\mathbf{1})^{p^{\beta-1}}W=(\mathbf{E}^{p^{\beta-1}}-\mathbf{1})W$.

Proof. Follows from Lemma 6.17 and the fact that p divides $\binom{p^{\beta-1}}{j}$, $1 \leqslant j \leqslant p^{\beta-1}-1$, and $\binom{p^{\beta-1}}{ip^{\beta-2}}$ $yp \equiv 0 (\mathrm{mod}\, p^2)$ for any y (any entry in W is yp for some y). □

Lemma 6.19. *Let* $X=[x(0), x(1), \ldots, x(p-1)]$ *be a word defined by* $x(0)=0$, $x(i)=(-1)^{i-1}\binom{p}{i}$, $1 \leqslant i \leqslant p-1$. *Then, there exists a word* Y *such that* $(\mathbf{E}-\mathbf{1})Y=X$, *where computation performed modulo* p^2, *and the sum of entries in* Y *is not congruent to* 0 *modulo* p^2.

Proof. Let $Y=[y(0), y(1), \ldots, y(p-1)]$, where $y(0)=0$, $y(i)=\sum_{j=1}^{i} x(j)=\sum_{j=1}^{i}(-1)^{j-1}\binom{p}{j}$, $1 \leqslant i \leqslant p-1$. It is clear that $(\mathbf{E}-\mathbf{1})Y=X$. Also, $y(p-1)=0$ since $p-1$ is even and $\binom{p}{i}=\binom{p}{p-i}$. Therefore, by using Lemma 6.16 and the following equality,

$$(-1)^{i-1}(p-i-1)\binom{p}{i}+(-1)^{p-i-1}(i-1)\binom{p}{p-i}=(-1)^{i-1}(p-2i)\binom{p}{i}$$

$$\equiv(-1)^{i-1}(-2i)\binom{p}{i}(\mathrm{mod}\, p^2),$$

we have

$$\sum_{i=0}^{p-1} y(i) \equiv \sum_{i=1}^{p-2}\sum_{j=1}^{i}(-1)^{j-1}\binom{p}{j} \equiv \sum_{i=1}^{p-2}(-1)^{i-1}(p-i-1)\binom{p}{i}$$

$$\equiv \sum_{i=1}^{\frac{p-1}{2}}(-2i)(-1)^{i-1}\binom{p}{i} \equiv \sum_{i=1}^{\frac{p-1}{2}}(-2)(-1)^{i-1}(-1)^{i-1} ip/i$$

$$\equiv \sum_{i=1}^{\frac{p-1}{2}}(-2p) \equiv p(\mathrm{mod}\, p^2). \qquad \square$$

Proof of Lemma 6.15′. Assume first that p is an odd prime, and let $n=p^{\beta}$, as before. Let $\alpha=2$, $m=p^{\beta-1}-1$ and X the word defined in Lemma 6.19. Let $U'=(\mathbf{E}-\mathbf{1})^{p^{\beta}}W$. By Lemmas 3.1 and 6.17, U' has the same depth as $U=[x(0), 0^m, x(1), \ldots, 0^m, x(p-1), 0^m]$. Then, by Lemmas 6.18 and 6.19, the word $V=[y(0), 0^m, y(1), \ldots, 0^m, y(p-1), 0^m]$ is in layer 1 level 1 and $(\mathbf{E}-\mathbf{1})^{p^{\beta-1}}V=(\mathbf{E}^{p^{\beta-1}}-1)V=U$. By the correctness of the theorem for $l=1$, $depth(V)=n$ and, hence, $depth(U)=n-n/p$, meaning that $depth(W)=n+(n-n/p)$, as claimed.

For $p=2$, $\alpha=2$, we have by Lemma 6.7 that $(\mathbf{E}-\mathbf{1})^{2^{\beta}}=\mathbf{E}^{2^{\beta}}+2\mathbf{E}^{2^{\beta-1}}+1$ and, hence, for $W^*=[1,0,\ldots,0]$, we have $(\mathbf{E}-\mathbf{1})^{2^{\beta}}W^*=[2, 0^{2^{\beta-1}-1}, 2, 0^{2^{\beta-1}-1}]$. The word $V=[2, 0^{2^{\beta-1}-1}]$ is the one in layer 1 level 1, for which $(\mathbf{E}-\mathbf{1})^{2^{\beta-1}}V=(\mathbf{E}-\mathbf{1})^{2^{\beta}}W^*$. □

As mentioned before, the proof of Theorem 6.12 follows immediately from Lemmas 6.15 and 6.15′.

References

[1] C. Ding, A fast algorithm for determining the linear complexity of sequences over $GF(p^m)$ with period p^n, preprint.
[2] R.A. Games and A.H. Chan, A fast algorithm for determining the complexity of a binary sequence with a period 2^n, *IEEE Trans. Inform. Theory* **IT-29** (1983) 144–146.
[3] T. Goka, An operator on binary sequences, *SIAM Rev.* **12** (1970) 264–266.
[4] E.L. Key, An analysis of the structure and complexity of nonlinear binary sequence generators, *IEEE Trans. Inform. Theory* **IT-22** (1976) 732–736.
[5] W.T. Lasser and L. Ramshaw, Probing the rotating table, *The Mathematical Gardner*, ed. David Klarner (1981), 285–307.
[6] A. Lempel, On a homomorphism of the de Bruijn graph and its applications to the design of feedback shift registers, *IEEE Trans. Comput.* **C-19** (1970) 1204–1209.
[7] T. Lewis and S. Willard, The rotating table, *Math. Mag.* **53** (1980) 174–179.
[8] M.B. Nathanson, Derivatives of binary sequences, *SIAM J. Appl. Math.* **21** (1971) 407–412.