Rotating-Table Games and Derivatives of Words

by

R. Bar-Yehudah, T. Etzion, S. Moran

Technical Report #675
June 1991
Rotating-Table Games and Derivatives of Words

Reuven Bar Yehuda* Tuvi Etzion† Shlomo Moran‡
Dept. of Computer Science
Technion IIT, Haifa 32000 — Israel

June 10, 1991

Abstract

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 \( \sigma \), for arbitrary \( n \) and \( \sigma \). 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 inverts 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 \( \sigma \) are powers of the same prime. In boths games we provide optimal winning strategies for B.

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

---

*The work of this author was supported in part by the Technion V.P.R. Fund - Albert Einstein Research Fund.
†The work of this author was supported in part by the Technion V.P.R. 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 on some of the glasses, and asks player A to invert them. Next, player A rotates the table counterclockwise 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 Figure 1). This completes the first round. 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 zeroes (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 indicates "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 i-th round ($i \geq 1$), 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. This word denotes which glasses should be inverted, after the table is rotated.

2: Player A select an integer $s_i$ in the range $[0 \cdots n - 1]$. $s_i$ corresponds to rotating the table by an angle of $\frac{360\cdot s_i}{n}$. Thus, $W_i = W_{i-1} + B^s \text{key}$, where the vector addition is done modulo 2, and $B^s \text{key}$ denotes a (left) cyclical shift of the word $\text{key}$ 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 where 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 $\sigma > 1$, as follows. Instead of n drinking glasses, we now have on the rotating table n roulettes of $\sigma$ sides each. denote the sides of the roulettes by $0, \cdots, \sigma - 1$. 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
Figure 1: Illustration of the open game
zero. Describing this in the notation of words over alphabet \(\{0, \cdots, \sigma - 1\}\), we get a description similar to the one for binary words (where the addition now is modulo \(\sigma\)).

### 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 does not see the initial configuration of the glasses, neither 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 \((key_0, \cdots, key_m)\) which he generates during the game depends only on \(n\) (and \(\sigma\)). Therefore, we can describe the blind game as a one player game, in which the adversary plays against the sequence \(KEY = (key_0, \cdots, key_n)\) as follows:

Initially, the sequence \(KEY\) is given to \(A\).

Using this sequence, \(A\) generates the sequence \(S = W_0, \cdots, W_m\) as follows:

1. Choose an arbitrary vector as \(W_0\).
2. Given \(W_{i-1}\), \(W_i\) is created as follows: \(W_i = W_{i-1} + E^\alpha(key_i)\).

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

The sequence \(KEY\) is a \((\sigma, n)\) 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 [LW80]. However, the results, as well as the techniques used in analyzing these games, appear to be quite different.

### 1.4 Summary of results

We show that Player \(B\) can win either the open or the blind game iff \(\sigma\) 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 the next section we prove that player \(B\) cannot have a winning strategy for the open game, unless \(\sigma\) 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 provides a detailed analysis on the depth of \(\sigma\)-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 \( \sigma \) are powers of the same prime. Clearly, this result applies also to blind game.

**Theorem 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 \( \sigma \) does 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 \( \sigma \).

1. **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 \( j \)-th 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 \( W = W_i = W_{i-1} + E \cdot key \), it holds that \( w(0) \neq w(1) \). Let \( d \equiv w_{i-1}(0) - w_{i-1}(1)(\mod \sigma) \). 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 if it satisfies the following:

   \[
   key(s + 1) - key(s) \neq d(\mod \sigma), \text{ where } key(n) = key(0).
   \]

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

   \[
   key(0) = key(0) + \sum_{i=0}^{n-1} (key(i + 1) - key(i)) \equiv key(0) + nd(\mod \sigma).
   \]

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

2. **Next, we consider the general case, where \( \sigma \) and \( n \) are not powers of the same prime.** This implies that there are integers \( g \) and \( f \), where \( g \) divides \( \sigma \) and \( f \) divides \( n \), and \( \overline{\sigma} = \sigma/g \) and \( \overline{n} = n/f \) are distinct primes. In particular, \( \gcd(\overline{\sigma}, \overline{n}) = 1 \) and \( 1 < \min\{\overline{\sigma}, \overline{n}\} \). 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 \( \overline{U} = (\overline{u}(0), \ldots, \overline{u}(\overline{n} - 1)) \) of length \( \overline{n} \) whose entries are in \( \{0, \ldots, \overline{\sigma} - 1\} \) in the following way: For \( i = 0, \ldots, \overline{n} - 1 \),

   \[
   \overline{u}(i) \equiv u(fi) \pmod{\overline{\sigma}}
   \]

   (i.e., the \( i \)-th entry in \( \overline{U} \) is the \( fi \)-th entry in \( U \) modulo \( \overline{\sigma} \)).

   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 $W_0, W_1, \cdots, W_m$ such that for all $i$, $\overline{w_i}(0) \neq \overline{w_i}(1)$. We start by taking $W_0 = (1, 0, \cdots, 0)$ (which means that also $W_0 = (i, 0, \cdots, 0)$).

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

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

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 [G70] and [N71] for binary words. [K76] is an excellent reference for the linear complexity.

For a word $W = [w(0), w(1), \cdots, w(k-1)]$, the derivative of $W$ is defined by $(E - 1)W = EW - W$. The depth of $W$, denoted by $\text{depth}(W)$, is the least $z$ such that $(E - 1)^z W = 0$ if such $z$ exists, and $\infty$ otherwise. For the binary case $E - 1$ is often called the $D$-morphism[70]. The proof of the following lemma is easy and left to the reader.

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

3.1 Linear complexity

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

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

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

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

The (linear) complexity $C(W)$ of $W$ is defined as the least integer $m$ for which there exists a polynomial $f(E)$ of degree $m$ such that $f(E)W = [0]^k$. As we see in Lemma 3.3, in this case the linear complexity and the depth coincide. Games and Chan[GC83] gave an efficient algorithm for computing the linear complexity of words of length $2^n$. A generalization of this algorithm for words of length $q^n$, $q$ prime power, with entries from $GF(q)$, was given by Ding[D].
In Lemmas 3.2 and 3.3, let \( W \) be a word of length \( n = p^r \), for a prime \( p \), with entries from \( GF(q) \), \( q = p^r \).

**Lemma 3.2:** If \( f(E) \) is a polynomial with the least degree, with coefficients from \( GF(p) \), such that \( f(E)W = 0 \) and there exists a polynomial \( g(E) \) such that \( g(E)W = 0 \) then \( f(E) \) divides \( g(E) \).

**Proof:** Assume \( f(E) \) does not divide \( g(E) \) then we can find two polynomial \( h_1(E) \) and \( h_2(E) \) such that \( g(E) = h_1(E)f(E) + h_2(E) \) and the degree of \( h_2(E) \) is less than the degree of \( f(E) \). Now \( 0 = g(E)W = (h_1(E)f(E) + h_2(E))W = (h_1(E)f(E))W + h_2(E)W = h_2(E)W \), a contradiction to the fact that \( f(E) \) is a polynomial with the least degree such that \( f(E)W = 0 \).

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

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

### 3.2 Derivatives

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

**Lemma 3.4:** Given a word \( W \) of length \( n = p^d \), \( p \) prime, whose entries are from \( Z_{p^d} \), then \( (E - 1)^{pn}W = 0^n \).

**Proof:** From the proof of Lemma 3.3 we have that in the word \( (E - 1)^{p^n}W \) all the entries are congruent to 0 modulo \( p \). By induction, in the word \( (E - 1)^{p^n}W \) all the entries are congruent to 0 modulo \( p^i \). Therefore, \( (E - 1)^{p^n}W = 0 \).

From Lemma 3.4 we infer the following theorem.

**Theorem 2:** Given a word \( W \) of length \( n = p^d \), \( p \) prime, whose entries are from \( Z_{p^d} \), then the depth of \( W \) is finite.

Another simple observation is the following lemma.

**Lemma 3.5:** Given a word \( W \) of length \( n = p^d \), \( p \) prime, whose entries are from \( Z_{p^d} \), then \( \text{depth}(W) = z \) if and only if \( (E - 1)^{z-1}W = [d]^n \), 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**

(0.1) Assume in step $i$ the adversary holds the word $W_i$.

(0.2) We choose $key_i = -W_i$.

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 $f(E)$ is a polynomial with coefficients in $Z_p^n$, $W$ a word with entries from $Z_p^n$, and $d \in Z_p^n$ then $f(E)(dW) = df(E)W$.

**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($W_i + E^jkey_i$) < depth($W_i$). If $(E - 1)^sW_i = [d]^n$ then $(E - 1)^skey_i = (E - 1)^s(-W_i) = [-d]^n$ and hence for every $s$, $(E - 1)^s(W_i + E^jkey_i) = [0]^n$ and therefore $(E - 1)^{r-1}(W_i + key_i) = [e]^n$ for some $t \geq 1$, and some constant $e \neq 0$. Therefore, the result follows immediately from Lemma 3.5 and the fact that a word $[d]^n$ is the same in any cyclic shift.

Now we prove the following theorem.

**Theorem 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 4.3:** Assume $W$ and $U$ be 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 $E^iW + E^jU$, for any $i,j$, is $c_2$.

**Proof:** By the definition of the depth $(E - 1)^cW = [0]^n$ and $(E - 1)^{c-1}U = [d]^n$, for some $d \neq 0$. Hence, $(E - 1)^{c-1}(E^iW + E^jU) = [d]^n$, and the depth of $E^iW + E^jU$, is $c_2$.

**Lemma 4.4:** 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 $E^iW + U$ is at least $c - 1$.

**Proof:** Assume that the depth of $W + U$ is at most $c - 2$. By the definition of the depth $(E - 1)^c(W + U) = [0]^n$ and therefore $(E - 1)^{c-2}W = [v(0), v(1), \ldots, v(n-1)]$ and $(E - 1)^{c-2}U = [-v(0), -v(1), \ldots, -v(n-1)]$. 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 $(E - 1)^{c-2}E^iW + (E - 1)^{c-2}U = (E - 1)^{c-2}(E^iW + U)$ $\neq [0]^n$, and therefore the depth of $E^iW + U$ is at least $c - 1$.

A winning strategy for words of length $q^d$ 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 if and only if there exists a $(\sigma, n)$ universal sequence, as defined in the introduction.

**Lemma 5.1:** If $\text{KEY} = (\text{key}_1, \cdots, \text{key}_m)$ is universal, then in every play of the game all the $\sigma$-ary words of length $n$ must be generated. In particular, $m \geq \sigma^n - 1$.

**Proof:** We assume the contrary, and show that $A$ can win the game. Assume that in some play of the game at least one $\sigma$-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 $\sigma$-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 $\text{KEY}$ is not universal, which is the desired contradiction. \hfill $\Box$

We now show that if $\sigma$ 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 $\sigma$

In this subsection we assume that $|\Sigma| = \sigma = p$ and $n = p^d$ for some prime $p$ and non-negative integer $d$. 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 $\Sigma$, such that $\text{depth}(U) = \text{depth}(V) = r > 0$. Let $j_1, \cdots, j_{p-1}$ be arbitrary integers in $[0, \cdots, n-1]$. Let further $V_i = E \cdot j_i V$, and $W_i = U + \sum_{j=1}^{p-1} V_j$. Then for some $i$, $\text{depth}(W_i) < r$.

**Proof:** Since $\text{depth}(U) = \text{depth}(V) = r$, there are constants $c$ and $d$ such that

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

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

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

$$(E - 1)^{r-1}(U + \sum_{i=i_0}^{i_0} V_i) = (E - 1)^{r-1}W_0 = [0]^n,$$
which means that $\text{depth}(W_i) < r$. □

We now describe the construction of a $(\sigma, n)$ universal sequence of optimal length, $KEY$. The construction is done in $n + 1$ stages, where at stage $i$, $0 \leq i \leq n$, 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 $\text{depth}(W_0) \leq i$, 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 it indeed satisfies (0:1) - (0:2). Assume now that we are given a sequence $KEY_i$ of length $l_i = \sigma^i - 1$ which satisfies (i:1) - (i:2), where $0 \leq i \leq n$. A sequence $KEY_{i+1}$ of length $\sigma^{i+1} - 1$ which satisfies (i+1:1) - (i+1:2) is constructed as follows:

Let $V$ be an arbitrary word such that $\text{depth}(V) = i + 1$, 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 $\sigma i + \sigma - 1 = \sigma^{i+1} - 1$. It remains to show that (i+1:1) - (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 $\text{depth}(W_0) \leq i$. 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 that $\text{depth}(W_0) = i + 1$. Assume for the moment that the sequence given to $A$ is only the subsequence $(V_1, V_2, \cdots, V_{\sigma - 1})$. By Lemma 5.2, when $A$ plays against this subsequence only, there exists an $i_0$ such that after applying (a cyclic shift of) $V_0$, $A$ must generate a word $W$ such that $\text{depth}(W) \leq i$. 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 4.3, 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 $V_0$ is also of depth at most $i$. Since immediately after applying $V_0$ 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 subsection we extend the construction of the previous section to the case where $\sigma = p^\alpha$ for arbitrary positive integer $\alpha$. Thus, we prove the following

**Theorem 4:** Let $\sigma = p^\alpha$ and $n = p^\beta$ for positive integers $\alpha$ and $\beta$. Then there is a $(\sigma, n)$ universal sequence of optimal length $\sigma^n - 1$.

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

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

**Observation 5.1:** Let \(W_0\) be a word of length \(n\) over alphabet \(0, p, \ldots, p^{n+1} - p\). Then \(A\) must lose the game when playing against \(KEY'\).

The construction of \(KEY_{n+1}\) is done by interleaving the sequence \(KEY'\) between the words of the sequence \(KEY_n\) as follows: \(KEY_{n+1} = KEY' \circ (U_0 \circ KEY' \circ (U_2 \circ \cdots \circ (U_h \circ KEY')))\). Let \(l_{n+1}\), the length of \(KEY_{n+1}\), is given by \(l_{n+1} = p^n - 1 + p^n l_n = p^{n+1} - 1\), as claimed. To see that \(KEY_{n+1}\) is a \((p^{n+1}, n)\) universal sequence, observe that if all entries of \(W_0\) are divisible by \(p\) then Observation 5.1 implies that \(A\) must lose the game. Otherwise, an argument similar to the one in the previous subsection shows that if \(A\) is playing against the sequence \(KEY_n\), 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 \(KEY_{n+1}\) 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 \(KEY_{n+1}\). Immediately after using \(U_j\), \(A\) must use the complete sequence \(KEY_n\), the proof is now completed by using the induction hypothesis on \(W'\) and \(KEY_n\). \(\square\)

### 5.4 Generalization for \(GF(q)\)

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

**Lemma 5.3:** 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 \(\gamma\) be a primitive element in \(GF(q)\). There exist an integer \(i\), \(0 \leq i < q - 2\), 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 non-zero entries \(d_1\) and \(d_2\) in \(GF(q)\) such that \((E - 1)^{d_1 - 1} W = [d_1]^\gamma\) and \((E - 1)^{d_2 - 1} U = [d_2]^\gamma\). Let \(i\) be the integer such that \(\gamma^i = -d_1 \cdot (d_2)^{-1}\) and \(V = \gamma^i u(0), \gamma^i u(1), \ldots, \gamma^i u(n - 1)\). It follows that \((E - 1)^{d_1 - i} V = \gamma^i (E - 1)^{d_1 - 1} U = [d_1]^\gamma\) and hence \((E - 1)^{i - 1} (W + V) = [0]^\gamma\) and therefore the linear complexity of \(W + V\) is less than \(c\). \(\square\)

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 $\gamma$ be a primitive element in $GF(q)$. Let $V_0 = V$ and for $1 \leq j \leq q - 2$, $V_j = \gamma^j V - V_{j-1}$. Then $KEY_{i+1} = KEY_1 \cdot (V_0) \cdot KEY_2 \cdot (V_1) \cdots (V_{q-2}) \cdot KEY_i$. 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 words. If the length of the word is $n = p^\alpha$ and the entries are taken from $Z_{p^\alpha}$. Lemma 3.4 implies that an upper bound on this depth is $an$. We will improve this bound to $a + (\alpha - 1)(n - p^\alpha - 1)$, and show that this is tight. In both upper and lower bound proofs we first consider the simple case where $\alpha = 1$, and the generalize the proof to arbitrary $\alpha$.

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 $d$, $d \neq 0 (mod p)$ has depth $n$.

Proof: By Lemma 3.3 the depth of each word is at most $n$. Since when $\alpha = 1$ the computations are modulus a prime $p$, we have

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

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

For the case where $\alpha > 1$ we distribute all the non-zero words of length $n = p^\alpha$ with entries taken from $Z_{p^\alpha}$ into $\alpha$ layers. Each layer is divided into $n$ levels. The layers are labeled 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, labeled by $1, 2, \ldots, n$.

Assume first that $\alpha = 1$, in which case there is only one layer, $L_{1,0}$. Level $i$ of that layer consists of all words $W = [w(0), \ldots, w(n-1)]$ for which $\sum_{i=0}^{n-1} w(i) \neq 0 (mod p)$. 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 $V = (E - 1)U$. 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 $L_{\alpha,i}$ ($0 \leq i \leq \alpha - 1$) are defined as follows: Let $V = [v(0), \ldots, v(n-1)]$ be a word in level $L_{\alpha,i}$. Then $v(k)$ is divisible by $p^i$ for $k = 0, \ldots, n - i$, and hence the word $\frac{1}{p^i} V (mod p) = [\frac{v(0) (mod p), \ldots, v(n-1) (mod p)}{p^i}]$ is well defined. Then $V$ is in level $j$ of layer $L_{\alpha,i}$ iff $\frac{1}{p^j} V (mod p)$ 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 $\alpha - ary$ digits, out of which the $i - 1$ least significant digits are zeroes. Then $V$ is in level $j$ iff the word obtained from $V$ by replacing each entry $v(k)$ by the $i$th least significant digit 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 $(E - 1)V$ 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 $(E - 1)V$ is in level $j + 1$ of $L_i$.

Lemma 6.3: Let $V$ be a word in level $j$ of layer $L_{a,j}$, and let $V' = \frac{1}{p^i}V \pmod{p^{a'}}$ for some $i' \leq i$ and some $a' > i - i'$. Then $V'$ is in level $j$ of layer $L_{a',i'}$. Moreover, Let $U$ and $U'$ be non-zero words defined by $U = (E - 1)^kV$ and $U' = (E - 1)^kV'$. Then $U$ is in level $j_k$ of layer $L_{a,i}$ if $U'$ is in level $j_k$ of layer $L_{a',i'}$.

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

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

Lemma 6.4: If $U$ is in $\text{trace}(V)$, then $\text{depth}(V) \leq \text{height}(U) + \text{depth}(U)$.

The upper bound proof is based on the following lemma

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

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 $Z_p$.

Lemma 6.6: Let $f(E) = \sum_{i=0}^{k} a_i E^i$, be a polynomial with coefficients from $Z_{p^2}$, $k \leq p^2 - 1$, $a_0 = 1$, and $a_0 = (-1)^k \cdot \sigma - 1$ divides $f(E)$ and the result is $g(E) = \frac{f(E)}{E - 1} = \sum_{i=0}^{k-1} b_i E^i$ if and only if $b_{i+1} - b_i = a_i (\pmod{p^2})$, $1 \leq i < k - 1$, $b_{k-1} = 1$ and $b_0 = -a_0 (\pmod{p^2})$.

Proof: Follows immediately by computing $f(E) = g(E)/E - 1$. □

A simple calculation of the binomial coefficients shows that

Lemma 6.7: For $0 \leq j \leq p^r$, $p^j$ divides $\binom{p^r}{j}$ if and only if $j \not\equiv 0 (\pmod{p^{r-i}})$.
Now, we remind the reader that in the Pascal triangle in row $k$, $k \geq 0$, and diagonal $i$, $0 \leq i \leq k$, 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.

(P.1) \( \binom{k}{i} + \binom{k}{i+1} = \binom{k+1}{i+1} \)

(P.2) the first number in each diagonal is 1.

Lemma 6.8: The largest $z$ such that $(E - 1)^z$ divides $Ep^p - 1$, where the coefficients are computed in $\mathbb{Z}_{p^2}$, is $z = p^{a-1}$.

**Proof:** A simple division shows that

\[
\frac{Ep^p - 1}{E - 1} = \sum_{i=0}^{p^a-1} E^i
\]

Now, note that, by (P.2), these coefficients are the 0 diagonal in the Pascal triangle from row 0 to row $p^a - 1$. By (P.1), (P.2), and Lemma 6.6, if the numbers of diagonal $k$ from row $k$ to row $p^a - 1$, are the coefficients of $\left(\frac{E^p - 1}{E - 1}\right)^{k+1}$ then the numbers of diagonal $k + i$ from row $k + 1$ to row $p^a - 1$, are the coefficients of $\left(\frac{E^p - 1}{E - 1}\right)^{k+i+1}$ if and only if $\left(\frac{p^a - 1}{k + i}\right) \equiv (-1)^{k+i+1} (mod p^2)$.

By Lemma 6.7 all the first $p^{a-1}$ entries, except for the first one, in the $p^a$-th row of the Pascal triangle are zeroes and the next element is not zero. By using the facts that the first element in each row is 1 and (P.1) it follows that $\left(\frac{p^a - 1}{i + 1}\right) \neq (-1)^{i+1} (mod p^2)$ for $i \leq p^{a-1} - 2$.

For $i = p^{a-1} - 1$, $\left(\frac{p^a - 1}{i + 1}\right) \neq (-1)^{i+1} (mod p^2)$ since $\left(\frac{p^a - 1}{i + 2}\right) \equiv (-1)^{i+2} (mod p^2)$ and $\left(\frac{p^a}{p^{a-i}}\right) \neq 0 (mod p^2)$.

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

Lemma 6.9: Let $1 \leq j \leq p^{a-1}$, and let $W$ be a word over $\sigma = p^2$. Then the height $(W)$ is $j - 1$ iff $f_j(E)W = [d]^n$ 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 (mod $p^2$). Hence, a word $W$ is in level 1 iff $\frac{Ep^p - 1}{E - 1}W = \sum_{i=0}^{p^a-1} E^i W = f_j(E)W = [d]^n$ for some $d \neq 0$. Hence, by the definition of the levels, for a word $W$ and $1 \leq j \leq p^{a-1}$, height $(W) = j - 1$ iff $f_j(E)W = [d]^n$.

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 $(W) = j - 1$. 13
Proof: By Lemma 6.9, it is sufficient to prove that for each word \( W \) in level \( j \) of \( L_1 \) it holds that \( f_j(E)W = [d]^n \) for some \( d \neq 0 \), where \( 1 \leq j \leq p^{\beta-1} \). For \( j = 1 \) this holds since the sum of the entries of a word \( W \) in level 1 is not congruent to 0 (mod \( p^\beta \)). The proof for \( 1 < j \leq p^{\beta-1} \) is by induction, using the equality of \( f_j(E) = (E - 1) f_{j+1}(E) \) and Lemma 6.2.

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

\[
\text{depth}(W) \leq \text{height} \ (U) + \text{depth}(U) = n
\]

which proves the lemma for \( \alpha = 2 \).

Assume now that \( \alpha > 2 \), and let \( W \) and \( i \) be given \( (0 \leq i \leq \alpha - 2) \). 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 \( V' = \frac{1}{p} V \) (mod \( p^\beta \)). Then using Lemma 6.3 we get that for \( 0 \leq k \) and \( e = 0, 1 \), \( (E - 1)^k V \) is in level \( j \) of \( L_{a,i+e} \) iff \( (E - 1)^k V' \) is in level \( j \) of \( L_{a,i} \). In particular, \( |S \cap (L_i \cup L_{i+1})| = \text{depth}(V') \leq n \). Box

Theorem 5: The depth of a word of length \( n = p^\alpha \) over \( \sigma = p^\alpha \) is at most \( n + (\alpha - 1)(n - \lceil n/p \rceil) \).

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

Denote \( T_i \) as critical if \( 0 < i < \alpha - 1 \) and \( T_i \) contains a word \( V \) in level \( j \) of \( L_i \), where \( 1 \leq j \leq \lceil n/p \rceil \). If no \( T_i \) is critical, then \( |T_i| \leq n - \lceil n/p \rceil \) 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, \( |T_{i_1} \cup T_{i_1-1}| \leq n \). 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 \( |T_{i_2} \cup T_{i_2-1}| \leq n \). Continuing this way, we eventually get a sequence \( i_1, i_2, \ldots, i_k \) such that \( i_{k+1} < i_k - 1 \), each \( T_{i_k} \) 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 \( \text{trace} \ (W) \). 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 \( n - \lceil n/p \rceil \) entries of \( \text{trace} \ (W) \). Thus we get:

\[
\sum_{i=0}^{\alpha-1} |T_i| \leq n + kn + (\alpha - 2k - 1)(n - \lceil n/p \rceil)
\]

Since \( n - \lceil n/p \rceil \geq n/2 \), 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 5 is tight. Specifically, we prove a slightly stronger result:

Theorem 6: For \( I = 1, \ldots, \alpha \), all the words in level 1 of layer \( L_{\alpha, \alpha-1} \) are of depth \( n + (I - 1)(n - \lceil n/p \rceil) \).
The proof of Theorem 6 is by induction on \( I \). The base \( I = 1 \) follows from Lemma 6.1 and Lemma 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 6.11:** For all \( \alpha \) 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 \( E \), that for every word \( V \) in \( L_i \), depth(\( V \)) \( \leq \) 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 \( (E - 1)^{k-1}W^* = [b]^n \) for some \( b \not\equiv 0 \pmod{p^\alpha} \). It is sufficient to prove that for every \( V \) in level 1 of layer \( L_i \), \( (E - 1)^{k-1}V = [d]^n \) 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 \( c \not\equiv 0 \pmod{d} \). In particular, by Lemma 3.1, \( V \) has the same depth as \( V' = (E - 1)^{k-1}U' = [c]^n \) 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. \( \Box \)

By Lemma 6.11 above, in proving Theorem 6 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 6.12:** 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 \( i = \alpha - 1 \) in Lemma 6.12 above, the induction step in the proof of Theorem 6 will follow from:

**Lemma 6.13:** Assume that Theorem 6 holds for \( I = 1 \) \((I > 1) \), and let \( W = [1, 0, \ldots, 0] \) be in level 1 of layer \( L_{I,0} \). Then there exist a word \( U \) in layer \( L_{4,1} \) such that:

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

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

Thus, it only remains to prove Lemma 6.13 above. As in the case of the lower bound proof, we use lemmas 6.2 and 6.3 to reduce Lemma 6.13 to the case \( \alpha = 2 \). In particular, Lemma 6.13 will follow from the induction hypothesis for \( I = 1 \) and from:

**Lemma 6.13** Let \( W = [1, 0, \ldots, 0] \) be in level 1 of layer \( L_{2,0} \). Then there exist a word \( U \) in layer \( L_{2,1} \) such that:

1. \( U = (E - 1)^nW \).
2. $U = (E - 1)^{n/p}V$ 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 5.13 will follow from some results concerning the binomial coefficients (mod $p^2$), which are presented next.

Lemma 6.14: Let $p$ be an odd prime, then $\left( \begin{array}{c} p' \\ ip_{p' - 1} \end{array} \right) \equiv \left( \begin{array}{c} p \\ i \end{array} \right) \equiv (-1)^{i-1}p (\text{mod } p^2)$

Proof: We compute the two binomial coefficients

$\left( \begin{array}{c} p \\ i \end{array} \right) \equiv \frac{p!}{(p-i)!i!} \equiv \frac{(p-i+1)(p-i+2)\cdots(p-2)(p-1)p}{1\cdot2\cdots(i-2)(i-1)i}$

$\left( \begin{array}{c} p' \\ ip_{p' - 1} \end{array} \right) \equiv \frac{(p')!}{(p'-ip_{p' - 1})!(ip_{p' - 1})!} \equiv \frac{(p'-ip_{p' - 1}+1)(p'-ip_{p' - 1}+2)\cdots(p'-2)(p'-1)p'}{1\cdot2\cdots(ip_{p' - 1}-2)(ip_{p' - 1}-1)ip_{p' - 1}}$

$\equiv (-1)^{i-1}p (\text{mod } p^2)$.

Lemma 6.15: Let $p$ be an odd prime, then $(E - 1)^p = \sum_{i=0}^{p} (-1)^{(p'-ip_{p' - 1})} \left( \begin{array}{c} p' \\ ip_{p' - 1} \end{array} \right) E^{ip_{p' - 1}}$ where the coefficients are computed modulo $p^2$.

Proof: Follows immediately from expanding $(E - 1)^p$ and Lemma 6.7.

Lemma 6.16: Let $p$ be an odd prime, $n = p^2$, $W$ a word with entries from $Z_{p^2}$ which are divisible by $p$. Then $(E - 1)^{p^2-1}W = (E^{p^2-1} - 1)W$.

Proof: Follows from Lemma 6.15 and the fact that $p$ divides $\left( \begin{array}{c} p^2-1 \\ j \end{array} \right)$, $1 \leq j \leq p^2-1$, and $\left( \begin{array}{c} p^2-1 \\ ip_{p^2-2} \end{array} \right)y \equiv 0 (\text{mod } p^2)$ for any $y$ (any entry in $W$ is $yp$ for some $y$).

Lemma 6.17: Let $X = [x(0), x(1), \ldots, x(p - 1)]$ be a word defined by $x(0) = 0$, $x(i) = (-1)^{i-1} \left( \begin{array}{c} p \\ i \end{array} \right)$, $1 \leq i \leq p - 1$. Then, there exists a word $Y$ such that $(E - 1)Y = X$, where computation performed modulo $p^2$, and the sum of entries in $Y$ is not congruent to 0 modulo $p^2$. 

16
Proof: Let \( Y = [y(0), y(1), \ldots, y(p-1)] \), where \( y(0) = 0 \), \( y(i) = \sum_{j=1}^{i} z(j) \), \( p = -1 \). It is clear that \((E - 1)Y = X\). Also, \( y(p - 1) = 0\) since \( p - 1 \) is even and \( \binom{p}{i} = \binom{p}{p-i} \). Therefore, by using Lemma 6.14 and the following equality,

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

we have

\[
\sum_{i=0}^{p-1} \sum_{j=1}^{i} (-1)^{j-1} \binom{p}{j} \equiv \sum_{i=1}^{\frac{p-1}{2}} (-2i)\binom{p}{i} \equiv \sum_{i=1}^{\frac{p-1}{2}} (-2i)(-1)^{i-1}(-1)^{i-1}i^{-1}p \equiv \sum_{i=1}^{\frac{p-1}{2}} (-2p) \equiv p \mod p^2
\]

\( \square \)

Proof of Lemma 6.13: Assume first that \( p \) is an odd prime, and let \( n = p^a \) as before. Let \( \alpha = 2 \), \( m = p^{a-1} - 1 \) and \( X \) the word defined in Lemma 6.17. Let \( U' = (E - 1)^a W \). By Lemmas 3.1 and Lemma 6.15, \( U' \) has the same depth of \( U = [z(0), 0^m, z(1), \ldots, 0^m, z(p-1), 0^m] \). Then by Lemmas 6.16 and 6.17 the word \( V = [y(0), 0^m, y(1), \ldots, 0^m, y(p-1), 0^m] \) is in layer 1 level 1 and \((E - 1)^{p-1} V = (E^{p-1} - 1) V = U \). By the correctness of the theorem for \( l = 1 \), \( \text{depth}(V) = n \), and hence \( \text{depth}(U) = n - n/p \), meaning that \( \text{depth}(W) = n + (n-n/p) \), as claimed.

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

As mentioned before, the proof of Theorem 6 follows immediately from Lemmas 6.13 and 6.13.

References

[D] C. Ding, A fast algorithm for determining the linear complexity of sequences over \( GF(p^n) \) with period \( p^n \), preprint.


