Properties of the Error Linear Complexity Spectrum

Tuvi Etzion, *Fellow, IEEE*, Nicholas Kalouptsidis, *Senior Member, IEEE*, Nicholas Kolokotronis, *Member, IEEE*, Konstantinos Limniotis, and Kenneth G. Paterson, *Member, IEEE*

***Abstract*—This paper studies the error linear complexity spectrum of binary sequences with period 2^n. A precise categorization of those sequences having two distinct critical points in their spectra, as well as an enumeration of these sequences, is given. An upper bound on the maximum number of distinct critical points that the spectrum of a sequence can have is proved, and a construction which yields a lower bound on this number is given. In the process simpler proofs of some known results on the linear complexity and k-error linear complexity of sequences with period 2^n are provided.**

***Index Terms*—Binary sequences, linear complexity.**

I. Introduction

BINARY sequences with good pseudorandomness and complexity properties are widely used as keystreams in cryptographic applications [11], [16]. Among the measures commonly used to measure the complexity of a sequence s is its *linear complexity* $\mathrm{c}(s)$, defined to be the length of the shortest *linear feedback shift register* that generates s. Sequences of low linear complexity are fully determined via a solution of $\mathrm{c}(s)$ linear equations if $2\mathrm{c}(s) - 1$ consecutive terms of the sequence are known. Hence, high linear complexity is a prerequisite for cryptographic applications. If a sequence has period N, the Berlekamp–Massey algorithm requires $\mathcal{O}(N^2)$ operations [10] to determine its linear complexity. If $N = 2^n$, for $n \geq 1$, then the linear complexity is more efficiently computed via the Games–Chan algorithm, which has complexity $\mathcal{O}(N)$ [5]. Although the latter requires knowledge of the entire period, and thus is not practical from a cryptographic point of view, it reveals important properties that can be used in constructions of sequences and arrays with certain window properties [3], [15]. Rueppel [16] introduced the notion of the *linear complexity profile* that describes how the linear complexity grows in terms of the sequence length.

If a sequence has large linear complexity, and a small number of changes to its terms greatly reduce its linear complexity, then the resulting keystream is also cryptographically weak: knowledge of the first few bits allows the efficient generation of a sequence that closely approximates the original one. So the linear complexity of a sequence s should also remain high even if some of its terms are altered. This observation led to the definition of the *k-error linear complexity* $\mathrm{c}_k(s)$ of a periodic sequence s [18] that was first introduced in [1] and [2] as *sphere complexity* for finite length sequences. The *error linear complexity spectrum* of a periodic sequence indicates how linear complexity decreases as the number k of bits allowed to be modified per period increases [9]; the same notion was defined as *k-error linear complexity profile* in [18]. We note that Niederreiter in [14] has given an alternative definition of k-error linear complexity profile: it is defined there as a measure of how the linear complexity of a finite length sequence s changes when considering an increasing number of initial bits of s but a fixed number of errors. An efficient algorithm to compute, for fixed k, the value of $\mathrm{c}_k(s)$ for binary sequences with period $N = 2^n$ was presented by Stamp and Martin [18]. Lauder and Paterson [9] generalized this algorithm to compute the entire error linear complexity spectrum of such sequences. A formula relating the minimum number of bits that need to be altered in order to reduce the linear complexity of a sequence s to the value of $\mathrm{c}(s)$ was given in [8]. In [17], an algorithmic method was presented, based on the Lauder–Paterson algorithm, which computes the minimum number of bits, as well as their positions, that should be modified in order to reduce the linear complexity below any given constant c. Furthermore, exact formulas for the counting function and the expected value for the 1-error linear complexity of 2^n-periodic binary sequences, as well as corresponding bounds for the expected value for the k-error linear complexity for $k \geq 2$, were given in [12]. Generalization of these results to p^n-periodic sequences over the finite field $\mathbb{F}_p$, where p is prime, was presented in [13]. The case of p^m-periodic binary sequences was studied in [6], whereas the 1-error linear complexity of binary sequences with period $2^n - 1$ was treated in [7].

In this paper, we study the error linear complexity spectrum of sequences with period 2^n. This notion has not been extensively treated in the literature, apart from the algorithm given in [9]. This is despite its natural interpretation as a complexity measure and its intrinsic mathematical interest. In particular, we prove some lower and upper bounds on the maximum number of *critical points* in such a spectrum, these being the points where the linear complexity actually decreases as k increases. The lower bounds arise from specific constructions for sequences with large numbers of critical points. Additionally, we derive

Manuscript received September 29, 2008; revised February 10, 2009. Current version published September 23, 2009. This work was supported in part by the EPSRC under Grant EP/F056486/1 and the Greece-Britain Joint Research & Technology Programme, co-funded by GSRT and the British Council, under Contract GSRT 132-C. The material in this paper was presented in part at the IEEE International Symposium on Information Theory, Toronto, ON, Canada, July 2008.

T. Etzion is with the Department of Computer Science, Technion—Israel Institute of Technology, Haifa 32000, Israel (e-mail: etzion@cs.technion.ac.il).

N. Kalouptsidis and K. Limniotis are with the Department of Informatics and Telecommunications, National and Kapodistrian University of Athens, 15784 Athens, Greece (e-mail: kalou@di.uoa.gr; klimn@di.uoa.gr).

N. Kolokotronis is with the Department of Computer Science and Technology, University of Peloponnese, 22100 Tripolis, Greece (e-mail: nkolok@uop.gr).

K. G. Paterson is with the Information Security Group, Royal Holloway, University of London, Egham, Surrey TW20 0EX, U.K. (e-mail: kenny.paterson@rhul.ac.uk).

Communicated by G. Gong, Associate Editor for Sequences.

Digital Object Identifier 10.1109/TIT.2009.2027495

a new algorithm, based on the Games–Chan algorithm, which computes sequences of a given linear complexity having the minimum possible weight. We also prove that this is exactly the set of sequences having two critical points, this being the minimum possible number of critical points in a nonzero sequence.

The paper is organized as follows. Section II introduces the basic definitions. Section III focuses on sequences with two critical points, whereas Section IV provides constructions of sequences achieving controllable high number of critical points. Concluding remarks are given in Section V.

II. Preliminaries

Let $\mathbb{F}_2$ be the finite field of two elements and let $s = \{s_i\}_{i\geq 0}$ be a sequence of period N over $\mathbb{F}_2$, also given as the vector $s = (s_0, \ldots, s_{N-1})$ of length N. Any such sequence satisfies a linear recurrence relation

$$s_{i+m} = a_1 s_{i+m-1} \oplus \cdots \oplus a_{m-1} s_{i+1} \oplus a_m s_i, \qquad i \geq 0 \quad (1)$$

of order $m \leq N$, where $a_j \in \mathbb{F}_2$ and $\oplus$ represents the addition modulo 2. The linear complexity $\mathrm{c}(s)$ of s is defined as the least m for which (1) holds. In terms of a shift operator $\boldsymbol{E}$, defined as $\boldsymbol{E}s_i = s_{i+1}$, the linear recursion (1) takes the form

$$\left(\boldsymbol{E}^m \oplus \sum_{j=1}^{m} a_j \boldsymbol{E}^{m-j}\right) s_i = 0$$

where the addition is taken modulo 2. When applied on the whole sequence s the shift operator is defined by $\boldsymbol{E}s = (s_1, \ldots, s_{N-1}, s_0)$.

In this paper, we focus on binary sequences of period 2^n for some integer $n > 0$. In the sequel, we write such sequences as $s = [L\, R]$, where L, R correspond to the left and right halves of s, respectively. The all-zero sequence of length N is denoted by $\mathbf{0}_N$, or $\mathbf{0}$ whenever its length is clear from the context. A similar notation is used for the all-one sequence. The complemented sequence $s \oplus \mathbf{1}$ of s is denoted by $\bar{s}$.

The linear complexity $\mathrm{c}(s)$ of a binary sequence $s = [L\ R]$ of period 2^n can be recursively computed by the Games–Chan algorithm as follows [5]: when $L \oplus R = \mathbf{0}$, then $\mathrm{c}(s) = \mathrm{c}(L)$; otherwise, we set $\mathrm{c}(s) = 2^{n-1} + \mathrm{c}(L \oplus R)$. We can describe that algorithm in more details as follows. The input to the Games–Chan algorithm is a sequence s of length $\ell(s) = 2^n$. If $s \neq \mathbf{0}$, the linear complexity c of s is computed recursively as follows. Initially, set $c_n = 0$ and $\mathcal{A}_n = s$. At a typical step of the algorithm the left half of $\mathcal{A}_m$, $L(\mathcal{A}_m) = [b_0, \ldots, b_{2^{m-1}-1}]$, is added to the right half, $R(\mathcal{A}_m) = [b_{2^{m-1}}, \ldots, b_{2^m-1}]$, the result being a sequence $\mathcal{B}_m$, of length 2^{m-1}. If $\mathcal{B}_m = \mathbf{0}_{2^{m-1}}$, $\mathcal{A}_m$ is replaced by $\mathcal{A}_{m-1} = L(\mathcal{A}_m)$, and the linear complexity is left unchanged, i.e., $c_{m-1} = c_m$. If $\mathcal{B}_m \neq \mathbf{0}_{2^{m-1}}$, $\mathcal{A}_m$ is replaced by $\mathcal{A}_{m-1} = \mathcal{B}_m$, and c_m is replaced by $c_{m-1} = c_m + 2^{m-1}$. The linear complexity of s is given by $c(s) = c_0 + 1$. Note that we made a slight change in the algorithm since we have started with a nonzero sequence.

The proof that the algorithm indeed finds the linear complexity of a sequence s is relatively long and complicated [5]. Hence, for the sake of completeness and methodology, we provide a short proof of its correctness.

Theorem 1: Given a sequence s of period 2^n, the Games–Chan algorithm finds the linear complexity of s, $c(s)$.

Proof: Let $c = c(s)$ and assume $c - 1 = \sum_{i=0}^{n-1} a_i 2^i$, $a_i \in \{0, 1\}$. Clearly, $(\boldsymbol{E} \oplus 1)^{c-1} s = (\prod_{a_i=1} (\boldsymbol{E} \oplus 1)^{2^i}) s = (\prod_{a_i=1} (\boldsymbol{E}^{2^i} \oplus 1)) s$. The Games–Chan algorithm terminates when the final sequence consists only of *ones*. This relates to the equation $(\boldsymbol{E} \oplus 1)^{c-1} s = \mathbf{1}$, i.e., $c - 1$ consecutive applications of $\boldsymbol{E}s \oplus s$, but since $(\boldsymbol{E} \oplus 1)^{2^m} = \boldsymbol{E}^{2^m} \oplus 1$, we can speed the process as done in the algorithm. Moreover, the algorithm only performs $(\prod_{a_i=1} (\boldsymbol{E}^{2^i} \oplus 1)) s$, since whenever the two halves of the sequence are equal we have $a_i = 0$. □

For 2^n-periodic binary sequences, the following well-known result holds [8].

Lemma 1: Let s, t be two binary sequences of period 2^n. Then:

- if $\mathrm{c}(s) = \mathrm{c}(t)$, then $\mathrm{c}(s \oplus t) < \mathrm{c}(t)$;
- if $\mathrm{c}(s) < \mathrm{c}(t)$, then $\mathrm{c}(s \oplus t) = \mathrm{c}(t)$.

The *k-error linear complexity* $\mathrm{c}_k(s)$ equals the minimum linear complexity of the sequences in $\{s \oplus e : \mathrm{wt}(e) \leq k\}$, where the error vector e is interpreted as a binary vector of length equal to the length of s. Kurosawa *et al.* proved the following interesting result.

Theorem 2 [8]: Let s be a binary sequence with period $N = 2^n$. Then, the smallest k, $k_{\min}$, for which $\mathrm{c}_k(s) < \mathrm{c}(s)$ equals

$$k_{\min} = 2^{\mathrm{wt}(2^n - \mathrm{c}(s))}$$

where $\mathrm{wt}(t)$ denotes the Hamming weight of the integer t.

The critical error linear complexity spectrum (CELCS) of the sequence s comprises the ordered set of points $(k, \mathrm{c}_k(s))$ satisfying $\mathrm{c}_k(s) > \mathrm{c}_{k'}(s)$, for $k' > k$ [9]; these are the points where a decrease occurs in the k-error linear complexity, and are called critical points (CPs). The CELCS of s is denoted by $\mathrm{celcp}(s)$. If (k, c) is a CP and k is odd (resp., even), we say that it has odd (resp., even) parity, while we denote by $\mathrm{cp}(s)$ the number of CPs of sequence s. An efficient algorithm for computing the CELCS of s is given in [9] and uses the notion of *costed sequences*. In this setting, a nonnegative integer $\sigma(s_i)$, referred to as a *cost*, is associated with each term s_i of the sequence s. Costs are used in [9] to track to the number of bits affected in an original sequence when changing a bit of an intermediate sequence in the Games–Chan algorithm. We define the total cost of adding some error vector e to s as

$$\mathrm{cost}(s \to s \oplus e) = \sum_{e_i = 1} \sigma(s_i) \qquad (2)$$

and the k-error linear complexity of the costed sequence s as $\min_{\mathrm{cost}(s \to s \oplus e) \leq k} \{\mathrm{c}(s \oplus e)\}$. Clearly, if $\sigma(s_i) = 1$ for all $i = 0, 1, \ldots, N-1$, then the above definition coincides with the typical notion of k-error linear complexity.

We say that e is a *critical error sequence* of s if $(k, c_k(s)) = (\mathrm{cost}(s \to s \oplus e), \mathrm{c}(s \oplus e))$ belongs to the CELCS of s. Note

that if e is a critical error sequence of s, then $\mathrm{c}(e) = \mathrm{c}(s)$ due to Lemma 1.

Definition 1 [9]: Let s be a costed sequence with period $N = 2^n$. For $0 \le i < N/2$, set $\Delta\sigma(s_i) = \sigma(L_i) - \sigma(R_i)$ and define the mappings $\mathcal{B}, \mathcal{L} : \mathbb{F}_2^N \to \mathbb{F}_2^{N/2}$ as follows:

1) $\mathcal{B}(s)_i = L_i \oplus R_i$ and $\sigma(\mathcal{B}(s)_i) = \min\{\sigma(L_i), \sigma(R_i)\}$;
2) if $L_i = R_i$, then $\mathcal{L}(s)_i = R_i$ and $\sigma(\mathcal{L}(s)_i) = \sigma(L_i) + \sigma(R_i)$;
3) if $L_i \neq R_i$, then $\mathcal{L}(s)_i = R_i$ when $\Delta\sigma(s_i) \le 0$, and $\mathcal{L}(s)_i = L_i$ otherwise, while $\sigma(\mathcal{L}(s)_i) = |\Delta\sigma(s_i)|$.

The following lemma is an immediate consequence of a result proved in [9].

Lemma 2: Let s be a sequence of period 2^n. Then:

- s has a critical point $(k, c_k(s))$, $c_k(s) > 2^{n-1}$, if and only if $\mathcal{B}(s)$ has a critical point $(k, c_k(\mathcal{B}(s)))$, $c_k(\mathcal{B}(s)) > 0$, where $c_k(s) = 2^{n-1} + c_k(\mathcal{B}(s))$;
- s has a critical point $(k, c_k(s))$, $c_k(s) \le 2^{n-1}$, if and only if $\mathcal{L}(s)$ has a critical point $(k', c_{k'}(\mathcal{L}(s)))$, where $c_{k'}(\mathcal{L}(s)) = c_k(s)$.

Hence, the critical points of s can be calculated from the critical points of $\mathcal{B}(s)$ and the critical points of $\mathcal{L}(s)$. As a consequence we have the following result [9, Lemma 5].

Corollary 1:

$$\mathrm{cp}(s) = \mathrm{cp}(\mathcal{B}(s)) + \mathrm{cp}(\mathcal{L}(s)) - 1$$

Corollary 1 allows to compute recursively the number of CPs of the sequence s, by also taking into account its associated costs.

For any sequence of mappings $\mathcal{F}_1, \ldots, \mathcal{F}_r$, each being either $\mathcal{B}$ or $\mathcal{L}$, we will denote $(\mathcal{F}_r \circ \cdots \circ \mathcal{F}_1)(s)$ by $\mathcal{F}_r \cdots \mathcal{F}_1(s)$. Finally, the following lemma which is very useful, throughout our discussion, can be easily verified. It asserts that the cost of the bits of $\mathcal{L}(s)$ depends on the bits of $\mathcal{B}(s)$.

Lemma 3: If $\sigma(s_i) = 1$ for all $0 \le i < N$, then $\sigma(\mathcal{B}(s)_i) = 1$, $\mathcal{L}(s)$ equals the *right* half of $s = [L\ R]$, and $\sigma(\mathcal{L}(s)_i) \in \{0, 2\}$ where $\sigma(\mathcal{L}(s)_i) = 2$ if and only if $\mathcal{B}(s)_i = 0$.

Hence, if the cost vector of s is the all-ones vector, then the cost vector of $\mathcal{L}(s)$ is equal to $2\overline{\mathcal{B}(s)}$.

III. Sequences With Two Critical Points

It is obvious that any nonzero binary sequence s of period 2^n has at least two CPs, namely, $(0, \mathrm{c}(s))$ and $(\mathrm{wt}(s), 0)$. In this section, we study sequences whose CELCP has exactly two CPs.

Lemma 4: A period 2^n binary sequence s has two CPs if and only if s is of minimum weight among all period 2^n sequences with linear complexity $\mathrm{c}(s)$.

Proof: By Lemma 1 if s and e are sequences for which $\mathrm{c}(s) = \mathrm{c}(e)$, then $\mathrm{c}(s \oplus e) < \mathrm{c}(s)$. By definition, a sequence s has exactly two critical points if and only if the only critical error sequence of s is s itself. Thus, s has two CPs if and only if s is of minimum weight among all sequences with linear complexity $\mathrm{c}(s)$. □

Algorithm 1

input: an integer $n > 0$ and linear complexity c, with $0 < c \le 2^n$, where $c - 1 = \sum_{i=0}^{n-1} a_i 2^i$
output: the number $m = \mathcal{M}(c)$ of sequences with period 2^n and linear complexity c having minimum weight k, and a sequence s with these properties

```
k ← 1                                   \\ initialize weight
s ← 1                                   \\ a sequence of length 1 and weight 1
m ← 1
for i = 0, ..., n − 1 do
    if a_i = 1 then
        s ← [0 s]                       \\ pad with 2^i zeros
        m ← 2^k m                       \\ each "1" can be in either half
    else
        s ← [s s]                       \\ replicate sequence
        k ← 2 k                         \\ only weight is doubled
    end if
end for
```

Lemma 5: Let $s = [L\ R]$ be a binary sequence with period 2^n. Then, $\mathrm{cp}(s) = 2$ if and only if s has one of the following forms:

1) $L = R = t$, for some t of period 2^{n-1} and two CPs;
2) $L \oplus R = t$, for some t of period 2^{n-1} and two CPs, and there is no i such that $L_i = R_i = 1$.

Proof:

1) If $s = [t\ t]$, where $\mathrm{cp}(t) = 2$, then $\mathcal{B}(s) = \mathbf{0}$ and $\mathcal{L}(s) = t$, whereas $\sigma(\mathcal{L}(s))_i = 2$ for all $i = 0, \ldots, 2^{n-1} - 1$; hence, $\mathrm{cp}(\mathcal{B}(s)) = 1$, $\mathrm{cp}(\mathcal{L}(s)) = 2$, and $\mathrm{cp}(s) = 2$ by Corollary 1.
2) If s has the second form, we have $\mathrm{cp}(\mathcal{B}(s)) = \mathrm{cp}(t) = 2$. For each i, $\sigma(\mathcal{L}(s)_i) \in \{0, 2\}$. If $\sigma(\mathcal{L}(s)_i) = 2$, then $\mathcal{L}(s_i) = 0$, and hence, $\mathrm{cp}(\mathcal{L}(s)) = 1$. Thus, by Corollary 1, we have $\mathrm{cp}(s) = 2$.

The converse statement is proved by noting that there is no other way of choosing s such that $\mathrm{cp}(\mathcal{B}(s)) = 1$ and $\mathrm{cp}(\mathcal{L}(s)) = 2$ or $\mathrm{cp}(\mathcal{B}(s)) = 2$ and $\mathrm{cp}(\mathcal{L}(s)) = 1$. □

We next present an algorithm, which, for any $0 < c \le 2^n$, computes a minimum weight sequence of period 2^n with linear complexity c, as well as the total number $\mathcal{M}(c)$ of sequences with these properties. The correctness of the algorithm is subsequently proved in Propositions 1, 2.

Proposition 1: The sequence s found by Algorithm 1 is a sequence of minimum weight with $\mathrm{c}(s) = c > 0$.

Proof: Let us first recall the basic characteristics of the Games–Chan algorithm. At the ith step, $1 \le i \le n$, of the Games–Chan algorithm, the sequence considered has length 2^{n+1-i}, while its linear complexity is incremented by 2^{n-i} $(i \le n)$ if its two halves are different. At the end of the algorithm, the linear complexity is incremented by 1 only if the sequence is nonzero, in which case $c > 0$. Let $c - 1 = \sum_{i=0}^{n-1} a_i 2^i$.

Let s^i be the sequence of length 2^{i+1}, linear complexity c_i, and weight k_i that is obtained at the ith step, $i = 0, \ldots, n-1$, of Algorithm 1. We next prove by induction on i that $c_i = 1 + \sum_{j=0}^{i} a_j 2^j$ and k_i is the minimum possible weight. The initial conditions of the algorithm are $s^{-1} = 1$, $k_{-1} = 1$, and $c_{-1} = 1$. Assume that the claim is true for all integers less than i; to prove that it also holds for i, we distinguish the following two cases.

Case $a_i = 1$: the linear complexity is increased by 2^i in the Games–Chan algorithm, and therefore, the two halves of s^i do not coincide. Hence, we add 2^i zeros before s^{i-1} to keep the

TABLE I
EXECUTION OF ALGORITHM 1 FOR $c = 152$ AND $n = 8$

i	a_i	s^i	k_i	m_i
-1	$-$	1	1	1
0	1	01	1	2
1	1	$\mathbf{0}_3 1$	1	2^2
2	1	$\mathbf{0}_7 1$	1	2^3
3	0	$\mathbf{0}_7 1 \mathbf{0}_7 1$	2	2^3
4	1	$\mathbf{0}_{23} 1 \mathbf{0}_7 1$	2	$2^5 = 2^2 \cdot 2^3$
5	0	$\mathbf{0}_{23} 1 \mathbf{0}_7 1 \mathbf{0}_{23} 1 \mathbf{0}_7 1$	4	2^5
6	0	$\mathbf{0}_{23} 1 \mathbf{0}_7 1 \mathbf{0}_{23} 1 \mathbf{0}_7 1 \mathbf{0}_{23} 1 \mathbf{0}_7 1 \mathbf{0}_{23} 1 \mathbf{0}_7 1$	8	2^5
7	1	$\mathbf{0}_{151} 1 \mathbf{0}_7 1 \mathbf{0}_{23} 1 \mathbf{0}_7 1 \mathbf{0}_{23} 1 \mathbf{0}_7 1 \mathbf{0}_{23} 1 \mathbf{0}_7 1$	8	$2^{13} = 2^8 \cdot 2^5$

weight k_i minimal (see Lemma 5; note that s^{i-1} is of minimum weight by the induction hypothesis).

Case $a_i = 0$: the linear complexity is not increased by 2^i in the Games–Chan algorithm, and therefore, the two halves of s^i are identical. Hence, the sequence s^{i-1} is doubled and so is the weight $k_i = 2k_{i-1}$. Suppose that there exists another sequence $t^i = [L\ R]$ of period 2^{i+1} such that $\mathrm{c}(t^i) = \mathrm{c}(s^i)$ and $\mathrm{wt}(t^i) < k_i$. Since $L \oplus R = \mathbf{0}$ by hypothesis, we get $\mathrm{wt}(L) < k_{i-1}$, contradicting the minimality of $\mathrm{wt}(s^{i-1})$. □

Proposition 2: The value m output by Algorithm 1 is equal to $\mathcal{M}(c)$, which is the number of sequences with period 2^n and linear complexity c having minimum weight.

Proof: The claim follows from the proof of Proposition 1 and the following observations:

1) there exist one sequence s^{-1} of length 1 and weight 1;
2) if $a_i = 1$, i.e., the weight of s^i is not increased compared to s^{i-1}, then each of the k_{i-1} ones in s^{i-1} can be in either of the two halves of s^i, leading to an increase by a factor of $2^{k_{i-1}}$ in m;
3) if $a_i = 0$, then there exists a one-to-one correspondence between the set of sequences formed at the ith step of the algorithm and those formed at the previous step, i.e., m is unchanged. □

An example of the execution of Algorithm 1 for $c = 152$ and $n = 8$ is given in Table I.

We are now in a position to give a simple and short proof of Theorem 2.

Corollary 2: The weight of the sequence s determined by Algorithm 1 is $2^{\mathrm{wt}(2^n - \mathrm{c}(s))}$.

Proof: The initial sequence s^{-1} of length 1 used in the algorithm has weight 1. For every $i \geq 0$, the weight of s^i remains unchanged if $a_i = 1$, and is doubled if $a_i = 0$. Hence, $\mathrm{wt}(s) = 2^\ell$, where $\ell = |\{i : a_i = 0 \text{ and } 0 \leq i < n\}|$. By noting that

$$2^n = 1 + \sum_{i=0}^{n-1} 2^i \Rightarrow 2^n - \mathrm{c}(s) = \sum_{i=0}^{n-1} (1 - a_i) 2^i$$

we immediately derive that $\ell = \mathrm{wt}(2^n - \mathrm{c}(s))$. □

Clearly, Corollary 2 yields another proof of Theorem 2 as an immediate consequence from Lemma 1.

Theorem 3: Define $\lambda : \mathbb{Z} \to \mathbb{Z}$ by

$$\lambda(u) = 2^{u_0} + 2^{u_1 - 1} + \cdots + 2^{u_{\tau-1} - (\tau - 1)}, \qquad u \in \mathbb{Z}$$

where $u = 2^{u_0} + 2^{u_1} + \cdots + 2^{u_{\tau-1}}$ and $0 \leq u_0 < \cdots < u_{\tau-1}$. Then, the number of sequences with linear complexity c with two CPs is given by $\mathcal{M}(c) = 2^{\lambda(c-1)}$.

Proof: Recall that by Lemma 4 a sequence s has two CPs if and only if s is of minimum weight among all sequences with linear complexity $\mathrm{c}(s)$. Let n be any integer such that $c \leq 2^n$. From the proof of Proposition 2, we deduce that at the end of the ith step of Algorithm 1, we have $(m_i, k_i) = (2^{a_i k_{i-1}} m_{i-1}, 2^{1-a_i} k_{i-1})$, $i = 0, \ldots, n-1$, where m_i and k_i are the values of m and k, respectively, at the end of the ith step. From the initial conditions of Algorithm 1 and the fact that $\mathcal{M}(c) = m_{n-1}$, we subsequently derive

$$\mathcal{M}(c) = 2^{a_0 k_{-1} + a_1 k_0 + \cdots + a_{n-1} k_{n-2}}$$

where $k_i = 2^{i+1-(a_0 + \cdots + a_i)}$ for all $i = -1, \ldots, n-2$. Now, assume that $c - 1 = \sum_{i=0}^{n-1} a_i 2^i = 2^{t_1} + \cdots + 2^{t_\upsilon}$, where $0 \leq t_1 < \cdots < t_\upsilon < n$, so that $\mathrm{wt}(c-1) = \upsilon$. Hence, we have

$$\begin{aligned}
\log_2 \mathcal{M}(c) &= a_0 k_{-1} + a_1 k_0 + \cdots + a_{n-1} k_{n-2} \\
&= a_{t_1} k_{t_1 - 1} + a_{t_2} k_{t_2 - 1} + \cdots + a_{t_\upsilon} k_{t_\upsilon - 1} \\
&= k_{t_1 - 1} + k_{t_2 - 1} + \cdots + k_{t_\upsilon - 1} \\
&= 2^{t_1 - (a_0 + \cdots + a_{t_1 - 1})} + 2^{t_2 - (a_0 + \cdots + a_{t_2 - 1})} \\
&\quad + \cdots + 2^{t_\upsilon - (a_0 + \cdots + a_{t_\upsilon - 1})} \\
&= 2^{t_1} + 2^{t_2 - 1} + \cdots + 2^{t_\upsilon - (\upsilon - 1)} \\
&= \lambda(c - 1)
\end{aligned}$$

and the claim of the corollary follows. □

IV. SEQUENCES WITH MANY CPS

In this section, we study the number of critical points that may occur in the CELCP of a sequence. Let $\rho(n)$ denote the maximum number of CPs that a sequence of period 2^n can have. We first derive an upper bound on $\rho(n)$ and determine the weight of a sequence that might attain this bound.

Theorem 4: Let s be a sequence with period 2^n. Then, $\rho(n) \leq 2^{n-2} + 2$ for all $n > 1$; moreover, if $\mathrm{cp}(s) = 2^{n-2} + 2$, then $\mathrm{wt}(s) = 2^{n-1} + 1$.

Proof: Note that all CPs of a sequence s with odd (resp., even) weight, have odd (resp., even) parity, the only exception being the point $(0, \mathrm{c}(s))$. Therefore, sequences of weight $2^{n-1} + 1$, 2^{n-1}, or less than 2^{n-1}, have at most $2^{n-2} + 2$, $2^{n-2} + 1$, and 2^{n-2} CPs, respectively. Moreover, for all $i > 0$, any sequence of weight $2^{n-1} + 2i$ or $2^{n-1} + 2i + 1$ admits the CP $(2^{n-1} - 2i, 1)$ or $(2^{n-1} - 2i - 1, 1)$, respectively; hence, there could be at most $2^{n-2} - i$ CPs with complexities greater than 1, and one CP with linear complexity less than 1 (for a total number of at most $2^{n-2} - i + 2$ CPs). Thus, any sequence s of period 2^n satisfies $\mathrm{cp}(s) \leq 2^{n-2} + 2$, and if $\mathrm{cp}(s) = 2^{n-2} + 2$, then $\mathrm{wt}(s) = 2^{n-1} + 1$. □

Computer search shows that the upper bound $\rho(n) = 2^{n-2} + 2$ is attained for $n \leq 6$. However, it remains an open problem whether this bound can be attained for $n \geq 7$; we have found sequences of period 2^7 with 31 CPs, but not more (see Table II). We would like to remark that there are sequences of period 2^n with the maximum number of $2^{n-2} + 2$ CPs, but values of $\mathrm{cp}(\mathcal{B}(s))$ different from $2^{n-3} + 2$.

TABLE II
SEQUENCES WITH MAXIMUM CPS IN HEXADECIMAL REPRESENTATION

n	s	$\mathrm{cp}(\mathcal{B}(s))$	$\mathrm{cp}(\mathcal{L}(s))$	$\mathrm{cp}(s)$	Thm. 4
2	E	2	2	3	3
3	5B	3	2	4	4
4	8CD7	4	3	6	6
5	4ABCC66B	6	5	10	10
6	EBFCE6FF4030804B	10	9	18	18
7	F1F8F0FFEFFEE77F 0140A0904AA0844A	18	14	31	34

Next, we provide a construction for sequences with a relatively large number of CPs, resulting in lower bounds for $\rho(n)$. For this purpose, we first prove the following lemma.

Lemma 6: Let s be a binary sequence (costed or not) with period 2^n. Then, $|\mathrm{cp}(s) - \mathrm{cp}(\bar{s})| \leq 1$.

Proof: By definition $\mathcal{B}(\bar{s}) = \mathcal{B}(s)$ with the same costs for $\mathcal{B}(\bar{s})$ and $\mathcal{B}(s)$; $\mathcal{L}(\bar{s}) = \mathcal{L}(s) \oplus \mathbf{1}$ with the same costs for $\mathcal{L}(\bar{s})$ and $\mathcal{L}(s)$. The claim follows now by induction on n and Corollary 1. □

In the sequel, we denote by $s_{[t]}$ the sequence s which is costed according to the rule $\sigma(s_i) = t_i$. If a sequence s is not explicitly costed, then we assume that $\sigma(s_i) = 1$ for all $0 \leq i < N$.

Theorem 5: Let $s = [LR]$, $L \neq R$, be a sequence of period 2^n, such that $R_i = 1$ implies that $L_i = 1$. Suppose $\mathrm{cp}(\mathcal{B}(s)) = k$ and $\mathrm{cp}(\mathcal{L}(s)) = k'$. Let

$$t = [\mathbf{1}\, L \oplus\ R\, \mathbf{1}\, R\, \mathbf{0}\, \mathbf{0}\, \mathbf{1}\, R]$$

be a sequence with period 2^{n+2}, where $\mathbf{0}$ and $\mathbf{1}$ have length 2^{n-1}. Then, we have $\mathrm{cp}(\mathcal{B}(t)) \geq k$ and $\mathrm{cp}(\mathcal{L}(t)) \geq 2k'$, and t satisfies the same requirement on the left and right halves as s does.

Proof: By definition, we have that $b = \mathcal{B}(s) = L \oplus R \neq \mathbf{0}$ and $\mathcal{L}(s) = R_{[2\bar{b}]}$. Therefore, $\mathcal{B}(t) = [\mathbf{1}\ b\ \mathbf{0}\ \mathbf{0}]$, $\mathcal{B}^2(t) = [\mathbf{1}\ b]$, and $\mathcal{LB}(t) = [\mathbf{0}_{[\mathbf{0}]}\ \mathbf{0}_{[2\bar{b}]}]$ satisfying $\mathrm{cp}(\mathcal{LB}(t)) = 1$. If we proceed one step further, we have that $\mathcal{B}^3(t) = \bar{b}$ and $\mathcal{LB}^2(t) = b_{[2b]}$. By Lemma 6, $\mathrm{cp}(\mathcal{B}^3(t)) \geq k - 1$; $\mathrm{cp}(\mathcal{LB}^2(t)) = 2$ (since $\mathrm{cost}(b_{[2b]} \to \mathbf{1}_{[2b]}) = 0$ and $\mathrm{cost}(b_{[2b]} \to \mathbf{0}) > 0$). Hence, by using Corollary 1, we have $\mathrm{cp}(\mathcal{B}^2(t)) \geq k$ and $\mathrm{cp}(\mathcal{B}(t)) \geq k$. Let us consider now the costed sequence

$$\mathcal{L}(t) = \left[\mathbf{0}_{[\mathbf{0}]}\ \mathbf{0}_{[2\bar{b}]}\ \mathbf{1}_{[\mathbf{2}]}\ R_{[\mathbf{2}]}\right]$$

where costs are calculated by Definition 1 and Lemma 3. To determine the number of CPs of $\mathcal{L}(t)$ using Corollary 1, we need to study the sequences $\mathcal{BL}(t)$ and $\mathcal{L}^2(t)$. First, note that $\mathcal{BL}(t) = [\mathbf{1}_{[\mathbf{0}]}\ R_{[2\bar{b}]}]$, while $\mathcal{LBL}(t) = R_{[2\bar{b}]} = \mathcal{L}(s)$ and hence $\mathrm{cp}(\mathcal{LBL}(t)) = k'$. $\mathcal{B}^2\mathcal{L}(t) = \bar{R}_{[\mathbf{0}]}$ and hence $\mathrm{cp}(\mathcal{B}^2\mathcal{L}(t)) = 1$, which implies $\mathrm{cp}(\mathcal{BL}(t)) = k'$ by Corollary 1. Now, $\mathcal{L}^2(t) = [\mathbf{1}_{[\mathbf{2}]}\ R_{[\delta]}]$, where $\delta_i = 2 + 2\bar{b}_i$ if $R_i = 0$ and $\delta_i = 2 - 2\bar{b}_i$ if $R_i = 1$. To compute the exact value of δ_i, we need to consider the following three cases.

1) If $R_i = 1$, then $L_i = 1$, and hence, $b_i = 0$, $\bar{b}_i = 1$, and $\delta_i = 0$.
2) If $R_i = L_i = 0$, then $b_i = 0$, $\bar{b}_i = 1$, and $\delta_i = 4$.
3) If $R_i = 0$ and $L_i = 1$, then $b_i = 1$, $\bar{b}_i = 0$, and $\delta_i = 2$.

Now, consider the sequence $\mathcal{L}^3(t)$.

TABLE III
NUMBER OF SEQUENCES OF PERIOD DIVIDING 2^n WITH A GIVEN NUMBER OF CRITICAL POINTS

# CPs $/n$	0	1	2	3	4	5
1	1	1	1	1	1	1
2	1	3	11	59	795	144091
3			4	140	10044	9896156
4				56	22936	86527224
5					23440	359369968
6					8320	895797344
7						1222095360
8						1130881024
9						502761472
10						87494656

1) If $R_i = 1$, then $\mathcal{L}^3(t)_i = 1$, $b_i = 0$, and $\delta_i = 0$, and hence, $\sigma(\mathcal{L}^3(t)_i) = 2 + \delta_i = 2\bar{b}_i$.
2) If $R_i = 0$, then $\Delta\sigma(\mathcal{L}^2(t))_i = 2 - \delta_i = 2 - (2 + 2\bar{b}_i) = -2\bar{b}_i \leq 0$. Hence, $\mathcal{L}^3(t)_i = R_i$ and $\sigma(\mathcal{L}^3(t)_i) = |2 - \delta_i| = |2 - (2 + 2\bar{b}_i)| = 2\bar{b}_i$.

Therefore, $\mathcal{L}^3(t) = R_{[2\bar{b}]} = \mathcal{L}(s)$ and $\mathrm{cp}(\mathcal{L}^3(t)) = k'$. $\mathcal{BL}^2(t) = \bar{R}_{[\gamma]}$, where $\gamma_i > 0$ whenever $\bar{R}_i = 1$, and hence $\mathrm{cp}(\mathcal{BL}^2(t)) \geq 2$, which implies $\mathrm{cp}(\mathcal{L}^2(t)) \geq k' + 1$ by Corollary 1. Since $\mathrm{cp}(\mathcal{BL}(t)) = k'$, it follows that $\mathrm{cp}(\mathcal{L}(t)) \geq 2k'$.

Finally, writing $t = [\mathbf{1}\ L \oplus\ R\ \mathbf{1}\ R\ \mathbf{0}\ \mathbf{0}\ \mathbf{1}\ R] = [L'\ R']$, we clearly have that $R'_i = 1$ implies that $L'_i = 1$, and hence, t satisfies the same requirement concerning the left and right halves as s. □

The sequences s, s' of period 2^6 and 2^7 from Table II satisfy $\mathrm{cp}(\mathcal{B}(s)) = 10$, $\mathrm{cp}(\mathcal{L}(s)) = 9$, and $\mathrm{cp}(\mathcal{B}(s')) = 18$, $\mathrm{cp}(\mathcal{L}(s')) = 14$. They also satisfy the requirement of Theorem 5 concerning the left and the right halves. Hence, by applying Theorem 5 iteratively, we obtain the following lower bounds on $\rho(n)$.

Corollary 3: For odd $n \geq 7$, we have $\rho(n) \geq 17 + 7 \cdot 2^{(n-5)/2}$, and for even $n \geq 6$, we have $\rho(n) \geq 9 \cdot (2^{(n-6)/2} + 1)$.

In [4], we present further bounds by using similar methods, but these bounds given in the next theorem do not yield an asymptotic improvement.

Theorem 6: For even $n \geq 10$, we have $\rho(n) \geq 17 + 7 \cdot (2^{(n-6)/2} + 2^{(n-8)/2})$. For $n \geq 7$, $n \equiv 1 \pmod 3$, we have $\rho(n) \geq 2^{(n+8)/3} - 1$ and for $n \geq 11$, $n \equiv 2 \pmod 3$, we have $\rho(n) \geq 3 \cdot (2^{(n+4)/3} - 1)$.

V. CONCLUSION

In this paper, we studied the numbers of CPs in the error linear complexity spectra of sequences with period 2^n. We fully characterized sequences having the minimum number of two CPs in terms of weight and linear complexity. We also gave an efficient algorithm which leads to a closed formula enumerating this class. We derived an upper bound on the maximum number of CPs that a sequence of period 2^n may possess and a construction showing how to build sequences with many CPs.

In the process, we have simplified considerably some proofs of known results concerning linear complexity.

The research in this paper opens many directions for further research. In Table III, we present the distribution of sequences

of period dividing 2^n, $n \leq 5$ according to their number of CPs. It is not difficult to show why each class is large, since many operations like certain types of bit exchanges, reversing, etc., preserve the number of CPs. However, the exact numbers appearing in this table largely remain to be explained. The main open problem is whether there exists a sequence of period 2^n with $2^{n-2}+2$ critical points for each $n \geq 2$.

REFERENCES

[1] C. Ding, "Lower bounds on the weight complexity of cascaded binary sequences," in *Lecture Notes in Computer Science*. Berlin, Germany: Springer-Verlag, 1990, vol. 453, pp. 39–43.

[2] C. Ding, G. Xiao, and W. Shan, "The stability theory of stream ciphers," in *Lecture Notes in Computer Science*. Berlin, Germany: Springer-Verlag, 1991.

[3] T. Etzion, "Constructions for perfect maps and pseudo-random arrays," *IEEE Trans. Inf. Theory*, vol. IT-34, no. 5, pp. 1308–1316, Sep. 1988.

[4] T. Etzion, N. Kalouptsidis, N. Kolokotronis, K. Limniotis, and K. G. Paterson, "On the error linear complexity profiles of binary sequences of period 2^n," in *Proc. Int. Symp. Inf. Theory*, Jul. 2008, pp. 2400–2404.

[5] R. A. Games and A. H. Chan, "A fast algorithm for determining the complexity of a binary sequence with period 2^n," *IEEE Trans. Inf. Theory*, vol. IT-29, no. 1, pp. 144–146, Jan. 1983.

[6] Y. K. Han, J.-H. Chung, and K. Yang, "On the k-error linear complexity of p^m-periodic binary sequences," *IEEE Trans. Inf. Theory*, vol. 53, no. 6, pp. 2297–2304, Jun. 2007.

[7] N. Kolokotronis, P. Rizomiliotis, and N. Kalouptsidis, "Minimum linear span approximation of binary sequences," *IEEE Trans. Inf. Theory*, vol. 48, no. 10, pp. 2758–2764, Oct. 2002.

[8] K. Kurosawa, F. Sato, T. Sakata, and W. Kishimoto, "A relationship between linear complexity and k-error linear complexity," *IEEE Trans. Inf. Theory*, vol. 46, no. 2, pp. 694–698, Mar. 2000.

[9] A. G. B. Lauder and K. G. Paterson, "Computing the error linear complexity spectrum of a binary sequence with period 2^n," *IEEE Trans. Inf. Theory*, vol. 49, no. 1, pp. 273–281, Jan. 2003.

[10] J. L. Massey, "Shift register synthesis and BCH decoding," *IEEE Trans. Inf. Theory*, vol. IT-15, no. 1, pp. 122–127, Jan. 1969.

[11] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*. Boca Raton, FL: CRC Press, 1996.

[12] W. Meidl, "On the stability of 2^n-periodic binary sequences," *IEEE Trans. Inf. Theory*, vol. 51, no. 3, pp. 1151–1155, Mar. 2005.

[13] W. Meidl and A. Venkateswarlu, "Remarks on the k-error linear complexity of p^n-periodic sequences," *Des. Codes Cryptogr.*, vol. 42, no. 2, pp. 181–193, 2007.

[14] H. Niederreiter, "Some computable complexity measures for binary sequences," in *Sequences and Their Applications—Proc. SETA98*, C. Ding, T. Helleseth, and H. Niederreiter, Eds., Berlin, Germany, 1999, pp. 67–78, Springer-Verlag.

[15] K. G. Paterson, "Perfect maps," *IEEE Trans. Inf. Theory*, vol. 40, no. 3, pp. 743–753, May 1994.

[16] R. A. Rueppel, *Analysis and Design of Stream Ciphers*. Berlin, Germany: Springer-Verlang, 1986.

[17] A. Sălăgean, "On the computation of the linear complexity and the k-error linear complexity of binary sequences with period a power of two," *IEEE Trans. Inf. Theory*, vol. 51, no. 3, pp. 1145–1150, Mar. 2005.

[18] M. Stamp and F. Y. Martin, "An algorithm for the k-error linear complexity of binary sequences with period 2^n," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1398–1401, Jul. 1993.

Tuvi Etzion (M'89–SM'99–F'04) was born in Tel Aviv, Israel, in 1956. He received the B.A., M.Sc., and D.Sc. degrees from the Technion—Israel Institute of Technology, Haifa, Israel, in 1980, 1982, and 1984, respectively.

Since 1984 he has held a position in the Department of Computer Science, Technion, where he is currently a Professor. During 1986–1987, he was a Visiting Research Professor at the Department of Electrical Engineering-Systems, University of Southern California, Los Angeles. During summer 1990 and 1991, he was visiting Bellcore, Morristown, NJ. During 1994–1996, he was a Visiting Research Fellow at the Computer Science Department, Royal Holloway College, Egham, U.K. He also had several visits to the Coordinated Science Laboratory, University of Illinois at Urbana-Champaign, Urbana, during 1995–1998, two visits to HP Bristol in summer 1996 and 2000, a few visits to the Department of Electrical Engineering, University of California at San Diego, during 2000–2009, and several visits to the Mathematics Department at Royal Holloway College, Egham, U.K., during 2007–2009. His research interests include applications of discrete mathematics to problems in computer science and information theory, coding theory, and combinatorial designs.

Dr. Etzion was an Associate Editor for Coding Theory for the IEEE TRANSACTIONS ON INFORMATION THEORY from 2006 to 2009.

Nicholas Kalouptsidis (M'82–SM'85) was born in Athens, Greece, in 1951. He received the B.Sc. degree in mathematics (with highest honors) from the National and Kapodistrian University of Athens, Athens, Greece, in 1973 and the M.Sc. and Ph.D. degrees in systems science and mathematics from Washington University, St. Louis, MO, in 1975 and 1976, respectively.

He has held visiting positions at Washington University, St. Louis, MO; Politecnico di Torino, Turin, Italy; Northeastern University, Boston, MA; and CNET Lannion, France. He has been an Associate Professor and Professor with the Department of Physics, University of Athens, Athens, Greece. In fall 1998, he was a Clyde Chair Professor with the School of Engineering, University of Utah, Salt Lake City. In Spring 2008, he was a Visiting Scholar at Harvard University. He is currently a Professor at the Department of Informatics and Telecommunications, University of Athens. He is the author of the textbook *Signal Processing Systems: Theory and Design* (New York: Wiley, 1997) and coeditor, with S. Theodoridis, of the book *Adaptive System Identification and Signal Processing Algorithms* (Englewood Cliffs, NJ: Prentice-Hall, 1993). His research interests are in system theory, signal processing, and cryptography.

Nicholas Kolokotronis (S'98–M'04) was born in Athens, Greece, in 1972. He received the B.Sc. degree in mathematics from the Aristotle University of Thessaloniki, Thessaloniki, Greece, in 1995 and the M.Sc. and Ph.D. degrees in computer science (with highest honors) from the National and Kapodistrian University of Athens, Athens, Greece, in 1998 and 2003, respectively.

He was awarded by the Greek State Scholarship's Foundation, in 1995, for his undergraduate performance. He has held visiting positions at the Department of Technology Education and Digital Systems, University of Piraeus, Piraeus, Greece. He has been a Research Associate with the Digital Signal Processing Lab, Department of Informatics and Telecommunications, National and Kapodistrian University of Athens, since 1998, and is currently a Faculty Member at the Department of Computer Science and Technology, University of Peloponnese, Tripolis, Greece. His research interests include cryptography, analysis and design of pseudorandom sequences and Boolean functions, error-correcting codes, finite field theory, as well as, network security; he has over 25 publications in those areas.

Konstantinos Limniotis was born in Karditsa, Greece, in 1977. He received the B.Sc. degree in computer science (with highest honors), the M.Sc. degree in communications systems and networks, and the Ph.D. degree in cryptography from the Department of Informatics and Telecommunications, University of Athens, Athens, Greece, in 1999, 2002, and 2007, respectively.

Currently, he is a Research Associate with the Digital Signal Processing Lab, Department of Informatics and Telecommunications, National and Kapodistrian University of Athens. His research interests include cryptography and sequence analysis.

Kenneth G. Paterson (M'97) was born in Moffat, Scotland, in 1969. He received the B.Sc. degree in mathematics from the University of Glasgow, Glasgow, Scotland, in 1990 and the Ph.D. degree in mathematics from the University of London, London, U.K., in 1993.

He was a Royal Society Research Fellow at the Swiss Federal Institute of Technology, Zürich, Switzerland, from 1993 to 1994, and then a Lloyds of London Tercentenary Research Fellow at Royal Holloway, University of London, from 1994 to 1996. He then joined Hewlett-Packard Laboratories, becoming a project manager in 1999. In 2001, he returned to Royal Holloway, University of London, as a Lecturer, becoming Reader in Mathematics in 2002 and Professor of Information Security in 2004. His research interests include sequences, cryptography, and network security.

Dr. Paterson was an Associate Editor for Sequences for the IEEE TRANSACTIONS ON INFORMATION THEORY from 2003 to 2006.