A Construction of Long-Period Sequences Based on Lightweight Generation and High Probability

Min Zeng, Yuan Luo, and A. J. Han Vinck, *Fellow, IEEE*

***Abstract*—In practice, sequences with long period but lightweight generation are always welcome in the applications of communication systems; however, the generation is not easy. From a certain angle of very high probability, this paper presents a solution, which is performed using cyclic difference sequences. As an application, the generated sequences can be interleaved to obtain good correlation properties. Furthermore, synchronization with blind detection is often required but difficult to be achieved. Even harder, periodic sequences may be affected to be ultimately periodic sequences with overhead because of device switching or noise. The determinations of the ultimate periods of above sequences and corresponding distributions are also investigated in this paper.**

***Index Terms*—Cyclic difference operator, high probability, lightweight generation, period distribution, ultimately periodic sequence.**

I. Introduction and Preliminary

COMPLEXITY measurements on sequences with finite or infinite lengths over a finite field, play an important role in cryptology and communication. Extensive research has been done in this field by using linear recurrence relations among the terms of sequences (e.g., linear feedback shift register or LFSR) [3]–[5], [8]–[10], [12], [17]. For a sequence with finite length, Etzion [1], [6] introduced a complexity called *depth* by using derivative (i.e., differences of adjacent terms [2]), which is one of the three kinds of depths used to depict the complexity. The three kinds are classified as the first, the second and the third respectively according to their operators such as derivative, polynomial factorization, and cyclic difference [19].

Let F_q be the Galois field with q elements and characteristic p. F_q^n is the n-dimensional vector space over F_q. For a sequence $\boldsymbol{s} = (s_0, s_1, \ldots, s_{n-1}) \in F_q^n$, its derivative is defined as $D(\boldsymbol{s}) = (s_1 - s_0, s_2 - s_1, \ldots, s_{n-1} - s_{n-2}) \in F_q^{n-1}$. In the following paragraphs, $[\lambda^i]$ denotes a sequence with i consecutive appearances of λ, and period means the least period.

Definition 1: The first depth of $\boldsymbol{s}$ is the smallest nonnegative integer i such that $D^i(\boldsymbol{s}) = D(D^{i-1}(\boldsymbol{s})) = [0^{n-i}]$. If no such i exists, the first depth of $\boldsymbol{s}$ is defined to be n.

For an $[n, k]$ linear code, Etzion [6] showed that the first depth distribution of the nonzero codewords consists of exactly k nonzero values. Luo, Fu and Wei [13] studied more counting properties about the first depth distributions of linear codes. According to [6], Roth introduced another complexity, here called the second depth, of a sequence according to the factors of its generating function.

Definition 2: The second depth of $\boldsymbol{s}$ is defined to be the smallest nonnegative integer i such that $(x-1)^i s(x) \equiv 0 (mod (x-1)^n)$. If no such i exists, the second depth of $\boldsymbol{s}$ is defined to be n.

Let L be the cyclic-left-shift operator, i.e., $L(\boldsymbol{s}) = (s_1, s_2, \ldots, s_{n-1}, s_0)$. Then the cyclic-left-shift-difference operator is defined as $(L-1)(\boldsymbol{s}) = (s_1 - s_0, s_2 - s_1, \ldots, s_{n-1} - s_{n-2}, s_0 - s_{n-1}) \in F_q^n$, which is also called cyclic difference operator for short. By using this cyclic difference operator, Mitchell [14] extended the first depth for sequences with infinite length, which is called the third depth in this research.

Definition 3: The third depth of $\boldsymbol{s}$ is defined to be the smallest nonnegative integer i such that $(L-1)^i(\boldsymbol{s}) = [0^n]$. If there exist two nonnegative integers $i < j$ such that $(L-1)^i(\boldsymbol{s}) = (L-1)^j(\boldsymbol{s}) \neq [0^n]$, the third depth of $\boldsymbol{s}$ is defined to be ∞.

Remark 1: For all of the i, the number of the states of $(L-1)^i(\boldsymbol{s})$ is finite. So, there exist two nonnegative integers $i < j$ such that the value $(L-1)^i(\boldsymbol{s}) = (L-1)^j(\boldsymbol{s})$. If the value is zero, the third depth of $\boldsymbol{s}$ is finite. If the value is nonzero, the third depth of $\boldsymbol{s}$ is ∞.

Mitchell showed that the set of infinite sequences with finite third depth is equal to a set of equivalence classes of rational polynomials, and then characterized infinite sequences with finite third depth in terms of their periodicity.

In fact, for a sequence of period n over F_q, the above three kinds of depth are the same as its linear complexity if $n = p^r$ $(r \geq 0)$, see [1], [6]. In other words, a sequence over F_q has finite third depth if and only if its period is a power of the prime p [14].

This paper focuses on the sequences $\boldsymbol{s} \in F_q^n$ where $n \neq p^r (r > 0)$, especially on the case $n = p^r - 1$, and investigates a sequence $\{(L-1)^i(\boldsymbol{s})\}_{i \geq 0}$ defined as follows.

Definition 4: The sequence $\{(L-1)^i(\boldsymbol{s})\}_{i \geq 0}$, defined as:

$$\left(\boldsymbol{s}, (L-1)(\boldsymbol{s}), (L-1)^2(\boldsymbol{s}), \ldots, (L-1)^i(\boldsymbol{s}), \ldots\right), \quad (1)$$

Manuscript received April 11, 2014; revised September 20, 2014 and September 27, 2014; accepted September 30, 2014. Date of publication August 10, 2014; date of current version November 18, 2014. This work was supported in part by the National Basic Research Program of China under Grants 2012CB316100 and 2013CB338004 and in part by the National Natural Science Foundation of China under Grant 61271222. A summary of the preliminary of this paper was presented in the IEEE 2012 International Symposium on Information Theory. The associate editor coordinating the review of this paper and approving it for publication was K. Abdel-Ghaffar.

M. Zeng and Y. Luo are with the Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai 200240, China (e-mail: informcode@sjtu.edu.cn; yuanluo@sjtu.edu.cn).

A. J. Han Vinck is with the Institute for Experimental Mathematics, University of Duisburg-Essen, 45326 Essen, Germany (e-mail: Vinck@iem.unidue.de).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TCOMM.2014.2361763

is called the cyclic-left-shift-difference sequence of $\boldsymbol{s}$ (or cyclic difference sequence $\mathcal{S}$ for short) [19]. Its least ultimate period, denoted by per($\mathcal{S}$), is the least positive integer P such that there exists M, for all $i \geq M$,

$$(L-1)^i(\boldsymbol{s}) = (L-1)^{i+P}(\boldsymbol{s}), \tag{2}$$

where the smallest M with respect to the least P is called the preperiod [4]. If $M = 0$, the sequence is said to be a periodic sequence.

Observing that the number of the sequences with *infinite third depth* is quite large if n is not a power of p, we present a distribution of them in terms of the least ultimate periods of their corresponding cyclic difference sequence $\{(L-1)^i(\boldsymbol{s})\}_{i\geq 0}$. Furthermore, based on this distribution, a construction of long period sequences is proposed by using lightweight generation and very high probability (almost 99% in most cases), which is the main contribution of this paper. As an application, the generated sequences can be interleaved to obtain good correlation properties.

As we know, sequences with long period but lightweight generation are always welcome in communication systems. Before the description of the main results, one example is illustrated as follows.

Example 1: Let $\boldsymbol{s} = (1, 2, 0, 2, 1) \in F_3^5$. Then $\boldsymbol{s}$ has infinite third depth. And it follows that $\boldsymbol{s} = (L-1)^{80}(\boldsymbol{s})$ and $(L-1)^i(\boldsymbol{s}) \neq (L-1)^j(\boldsymbol{s})$ for $i \neq j$ $(0 \leq i, j < 80)$. If we interpret each $(L-1)^i(\boldsymbol{s})$ $(0 \leq i < 80)$ as an element in F_{3^5}, a new sequence with period 80 over F_{3^5} is obtained and denoted by $\mathcal{V} = (v_0, v_1, \ldots)$. Let $f(x)$ be the primitive polynomial $x^5 + x^4 + x^2 + 1$ over F_3 and β be a root of $f(x)$ over F_{3^5}. Under the basis $\{1, \beta, \beta^2, \beta^3, \beta^4\}$, the terms in the first period of $\mathcal{V}$ are given below:

$$\begin{array}{ccccccccc}
\beta^{154} & \beta^{28} & \beta^{94} & \beta^{193} & \beta^{24} & \beta^{152} & \beta^{37} & \beta^{65} & \beta^{52} \\
\beta^{148} & \beta^{5} & \beta^{189} & \beta^{83} & \beta^{102} & \beta^{48} & \beta^{185} & \beta^{42} & \beta^{39} \\
\beta^{120} & \beta^{67} & \beta^{166} & \beta^{222} & \beta^{79} & \beta^{63} & \beta^{162} & \beta^{19} & \beta^{240} \\
\beta^{97} & \beta^{58} & \beta^{100} & \beta^{199} & \beta^{56} & \beta^{231} & \beta^{107} & \beta^{95} & \beta^{112} \\
\beta^{128} & \beta^{220} & \beta^{77} & \beta^{176} & \beta^{33} & \beta^{149} & \beta^{215} & \beta^{72} & \beta^{145} \\
\beta^{31} & \beta^{158} & \beta^{186} & \beta^{173} & \beta^{27} & \beta^{126} & \beta^{68} & \beta^{204} & \beta^{223} \\
\beta^{169} & \beta^{64} & \beta^{163} & \beta^{160} & \beta^{241} & \beta^{188} & \beta^{45} & \beta^{101} & \beta^{200} \\
\beta^{184} & \beta^{41} & \beta^{140} & \beta^{119} & \beta^{218} & \beta^{179} & \beta^{221} & \beta^{78} & \beta^{177} \\
\beta^{110} & \beta^{228} & \beta^{216} & \beta^{233} & \beta^{7} & \beta^{99} & \beta^{198} & \beta^{55}. &
\end{array}$$

For example, $(L-1)^{10}(\boldsymbol{s}) = (2, 0, 2, 0, 2) \rightarrow v_{10} = 2 + 2\beta^2 + 2\beta^4 = \beta^5$, and $(L-1)^{90}(\boldsymbol{s}) = (L-1)^{10}((L-1)^{80}(\boldsymbol{s})) = (L-1)^{10}(\boldsymbol{s}) \rightarrow v_{90} = \beta^5$. In this way, we can select a suitable $\boldsymbol{s}$ among F_3^5 with probability greater than 98.77% to construct such a type of sequence $\mathcal{V}$ with period 80 only using the cyclic difference operator, where $98.77\% = \frac{3^5-3}{3^5}$ follows from the fact that, except for three vectors $\boldsymbol{s}$: (0, 0, 0, 0, 0), (1, 1, 1, 1, 1) and (2, 2, 2, 2, 2), the least ultimate periods of sequences $\mathcal{V}$ are always 80, see Fig. 2.

Another application of the above sequences is about synchronization with blind detection, which is also required but difficult to be achieved. Even harder, periodic sequences may be affected to be ultimately periodic sequences with overhead because of device switching or noise, see Fig. 1. The overhead means all items encountered before the sequence synchronization. In this paper, the synchronization happens in periodic part. The determination of the ultimate periods of above sequences is also investigated in this paper which is organized as follows.

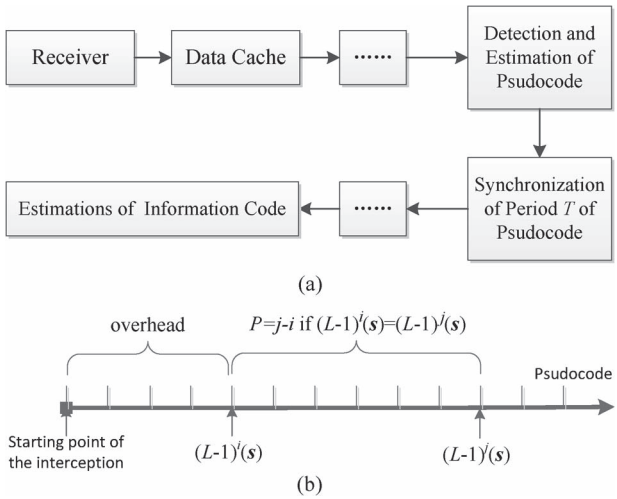

Fig. 1. Synchronization with blind period detection. (a) Simplified scheme of analysis and interception of signal. (b) Detection and estimation of the period of psudocode.

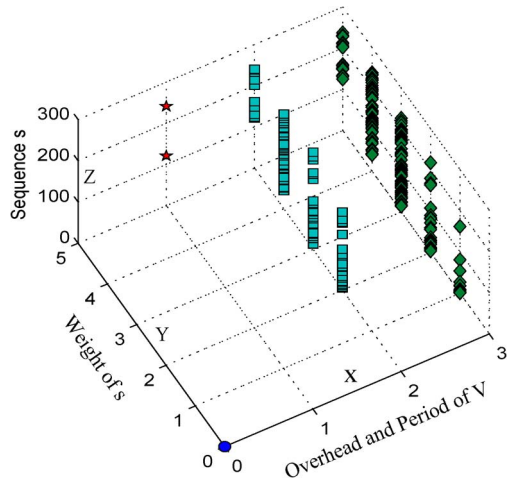

Fig. 2. The distribution of $\boldsymbol{s} \in F_3^5$ in terms of the least ultimate periods of $\mathcal{V}$. (a) Axis X denotes the overhead and period of $\mathcal{V}$, where "0" means that the overhead is 0 and the period is 1; "1": the overhead is 1 and the period is 1; "2": the overhead is 0 and the period is 80; "3": the overhead is 1 and the period is 80. b) Axis Y denotes the weight of $\boldsymbol{s}$. (c) Axis Z denotes the sequences $\boldsymbol{s} \in F_3^5$ converted to decimals from 0 to 242.

In Section II, we introduce some notations related to the sequence $\{(L-1)^i(\boldsymbol{s})\}_{i\geq 0}$ and main results such as:

- an upper bound on the ultimate periods of the sequence $\{(L-1)^i(\boldsymbol{s})\}_{i\geq 0}$ regrading $\boldsymbol{s} \in F_q^n$ where $n \neq p^r$;
- a formula of the least ultimate period of the sequence $\{(L-1)^i(\boldsymbol{s})\}_{i\geq 0}$;
- a distribution of $\boldsymbol{s} \in F_q^n$ in terms of the least ultimate periods of their corresponding sequences $\{(L-1)^i(\boldsymbol{s})\}_{i\geq 0}$.

In Section III, for $n \neq p^r$, an algorithm is provided to determine the distributions, and show that a kind of long period sequences

over F_{q^n} can be constructed from sequences in F_q^n with very high probability by only using cyclic difference operator. Section IV is an application in generating the sequences with good correlation properties from $\{(L-1)^i(\boldsymbol{s})\}_{i\geq 0}$, which is based on interleaving techniques. Final conclusion is in Section V. In addition, the proofs of three theorems in Section II are presented in Appendices A–C, respectively.

Note that the sequence $\{(L-1)^i(\boldsymbol{s})\}_{i\geq 0}$ for $q=2$ resembles the sequence of [15]. Nathanson proved that the binary sequence is eventually periodic if and only if its derivative sequence is eventually periodic. The sequence and the techniques of [15] are quite different from our techniques.

II. Main Results

In this section, some notations and main results are listed. For $n \neq p^r$, Proposition 3 gives an upper bound on the ultimate periods of $\{(L-1)^i(\boldsymbol{s})\}_{i\geq 0}$ regarding $\boldsymbol{s} \in F_q^n$, and Theorem 1 provides a formula for determining the least ultimate period of $\{(L-1)^i(\boldsymbol{s})\}_{i\geq 0}$. For special $n = p^r - 1$, Theorems 2 and 3 present a kind of distribution of $\boldsymbol{s} \in F_q^n$ in the cases $p=2$ and $p>2$, respectively.

- per($\boldsymbol{a}$): If $\boldsymbol{a}$ is a periodic sequence, its period only refers to its least period denoted by per($\boldsymbol{a}$). If $\boldsymbol{a}$ is an ultimately periodic sequence, its least ultimate period is also denoted by per($\boldsymbol{a}$), while its ultimate period means a multiple of the least ultimate period.
- $\mathrm{ord}_p(n)$ denotes the largest integer v such that $p^v | n$.
- $(\cdot)^\top$ denotes the transpose of an vector or matrix.
- Let $L(\boldsymbol{s}) = \boldsymbol{s}T$ where

$$T = \begin{pmatrix} 0 & 0 & \dots & 0 & 1 \\ 1 & 0 & \ddots & 0 & 0 \\ 0 & 1 & \ddots & \vdots & 0 \\ \vdots & \vdots & \ddots & 0 & 0 \\ 0 & 0 & \dots & 1 & 0 \end{pmatrix}_{n\times n}. \tag{3}$$

Then $L^i(\boldsymbol{s}) = L(L^{i-1}(\boldsymbol{s})) = \boldsymbol{s}T^i$ $(i \geq 1)$ and $L^0(\boldsymbol{s}) = \boldsymbol{s}$. It is easy to see that

$$T^n = I \text{ (the identity matrix of order } n). \tag{4}$$

- Let $(L-1)(\boldsymbol{s}) = \boldsymbol{s}A$ where

$$A = \begin{pmatrix} -1 & 0 & \dots & 0 & 1 \\ 1 & -1 & \ddots & 0 & 0 \\ 0 & 1 & \ddots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & -1 \end{pmatrix}_{n\times n} = T - I. \tag{5}$$

Then $(L-1)^i(\boldsymbol{s}) = (L-1)((L-1)^{i-1}(\boldsymbol{s})) = \boldsymbol{s}A^i$ $(i \geq 1)$ and $(L-1)^0(\boldsymbol{s}) = \boldsymbol{s}$. Consequently, (2) can be rewritten as follows:

$$(L-1)^i(\boldsymbol{s}) = (L-1)^{i+P}(\boldsymbol{s}) \Leftrightarrow \boldsymbol{s}(A^{i+P} - A^i) = [0^n]. \tag{6}$$

For $1 \leq i \leq n-1$ we have the following lemma which will be used in proving Theorem 2 and Theorem 3 in appendices.

Lemma 1 ([19]): $(L-1)^i(\boldsymbol{s}) = \boldsymbol{s}A^i = (s_0^{(i)}, s_1^{(i)}, \dots, s_{n-1}^{(i)}) \times (1 \leq i \leq n-1)$ where

$$A^i = \begin{pmatrix} \alpha_{i,0} & 0 & \dots & 0 & \dots & \vdots & \alpha_{i,1} \\ \alpha_{i,1} & \alpha_{i,0} & \ddots & \vdots & \ddots & \alpha_{i,i} & \vdots \\ \vdots & \alpha_{i,1} & \ddots & 0 & \vdots & 0 & \alpha_{i,i} \\ \alpha_{i,i} & \vdots & \ddots & \alpha_{i,0} & \ddots & \vdots & 0 \\ 0 & \alpha_{i,i} & \vdots & \alpha_{i,1} & \ddots & 0 & \vdots \\ \vdots & 0 & \ddots & \vdots & \ddots & \alpha_{i,0} & 0 \\ 0 & \vdots & \dots & \alpha_{i,i} & \dots & \alpha_{i,1} & \alpha_{i,0} \end{pmatrix}_{n\times n},$$

$$\alpha_{i,j} = (-1)^{i+j}\binom{i}{j} mod\ p,\ j = 0, 1, \dots, i,$$

$$\begin{aligned} s_k^{(i)} &= \alpha_{i,0}s_k + \alpha_{i,1}s_{k+1} + \dots + \alpha_{i,i}s_{k+i} \\ &= \sum_{j=0}^{i} \alpha_{i,j} \cdot s_{(k+j)\ mod\ n},\ k = 0, 1, \dots, n-1. \end{aligned} \tag{7}$$

For $i \geq 1$, the rank of A^i can be determined by the following proposition.

Proposition 1 ([20]): With the notation above, let p be the characteristic of F_q and $m = \mathrm{ord}_p(n)$ where n is the order of A. Then

$$rank(A^i) = \begin{cases} n-i & if\ 1 \leq i \leq p^m, \\ n-p^m & if\ i > p^m. \end{cases}$$

Using Proposition 1, we prove in Proposition 2 that the number of sequences $\boldsymbol{s} \in F_q^n$ with infinite third depth is quite large in the cases that n is not a power of p.

Proposition 2: Let p be the characteristic of F_q and $m = \mathrm{ord}_p(n)$. Then the number of sequences $\boldsymbol{s} \in F_q^n$ with infinite third depth is $q^n - q^{p^m}$.

Proof: Let d denote the third depth of a sequence $\boldsymbol{s} \in F_q^n$. According to [14, Theorem 17], it follows that $d \in \{0, 1, \dots, p^m\}$, where $d=0$ if $\boldsymbol{s} = [0^n]$, and $d=1$ if $\boldsymbol{s} = [\lambda^n], \lambda \in F_q$. For $1 \leq d \leq p^m$, $\boldsymbol{s}A^d = [0^n]$, which means that the null space of $\boldsymbol{s}A^d = [0^n]$ is an $[n, d]$ cyclic code because $\mathrm{rank}(A^d) = n - d$ in Proposition 1. Thus the number of sequences with third depth d is

$$\left|\{\boldsymbol{s} : \boldsymbol{s}A^d = [0^n]\} - \{\boldsymbol{s} : \boldsymbol{s}A^{d-1} = [0^n]\}\right| = q^d - q^{d-1} \tag{8}$$

since $\boldsymbol{s}A^{d-1} = [0^n]$ implies $\boldsymbol{s}A^d = [0^n]$. Therefore, the number of sequences with infinite third depth is $q^n - (1 + \sum_{d=1}^{p^m}(q^d - q^{d-1})) = q^n - q^{p^m}$. This result holds. ■

The following two propositions give the upper bounds on ultimate periods of $\{(L-1)^i(\boldsymbol{s})\}_{i\geq 0}$ for general or special n, respectively, which will be also used in proving Theorems 2 and 3.

TABLE I
THE DISTRIBUTION OF SEQUENCES $\boldsymbol{s} \in F_2^n$ IN TERMS OF THE LEAST ULTIMATE PERIODS OF SEQUENCES $\{(L-1)^i(\boldsymbol{s})\}_{i\geq 0}$ FOR $n = 2^r - 1 (2 \leq r \leq 6)$

n	P=1		P=3	P=5	P=7	P=9	P=15	P=21	P=31	P=63	$\frac{D_{P_{max}}}{2^n}$
	finite third depth	infinite third depth	infinite third depth								
3	2	-	6	-	-	-	-	-	-	-	75%
7	2	-	-	-	126	-	-	-	-	-	98.44%
15	2	-	6	30	-	-	$2^{15}-2^3$ -2^5+2	-	-	-	98.88%
31	2	-	-	-	-	-	-	-	$2^{31}-2$	-	99.99%
63	2	-	6	-	126	2^9-2^3	-	$2^{21}-2^3$ -2^7+2	-	$2^{63}-2^{21}$ -2^9+2^3	99.99%

1. P denotes the least ultimate period of $\{(L-1)^i(\boldsymbol{s})\}_{i\geq 0}$, and $P_{max} = \max\{P : D_P > 0\}$.
2. The columns, labeled as "finite third depth" and "infinite third depth", list the numbers of sequences $\boldsymbol{s} \in F_2^n$ with finite third depth and infinite third depth, respectively.

Proposition 3 ([20]): Let $\boldsymbol{s} \in F_q^n$ where $n \neq p^r$ and p is the characteristic of F_q. Then $p^{m'} - p^m$ is an upper bound on ultimate periods of $\{(L-1)^i(\boldsymbol{s})\}_{i\geq 0}$, where $m = \text{ord}_p(n)$, $m' = m + \phi\left(\frac{n}{p^m}\right)$, and $\phi(x)$ is the Euler phi-function.

Proposition 4 ([20]): Let $r > r' \geq 0$, $\boldsymbol{s} \in F_q^n$ and p be the characteristic of F_q.

i) If $n = p^r - p^{r'}$, then n is an upper bound on ultimate periods of $\{(L-1)^i(\boldsymbol{s})\}_{i\geq 0}$.
ii) If $n = p^r + p^{r'}$, then $p^{2r} - p^{2r'}$ is an upper bound on ultimate periods of $\{(L-1)^i(\boldsymbol{s})\}_{i\geq 0}$.

According to Definition 4, the least ultimate period of $\{(L-1)^i(\boldsymbol{s})\}_{i\geq 0}$ can be determined in the following theorem, whose idea was proposed in [19], but was not proved in the original paper.

Theorem 1: For $\boldsymbol{s} \in F_q^n$ with infinite third depth, let

$$J(\boldsymbol{s}) = \left\{j : (L-1)^i(\boldsymbol{s}) = (L-1)^j(\boldsymbol{s}) \text{ for some } i, 0 \leq i < j\right\} \tag{9}$$

and $I(\boldsymbol{s})$ be the unique $i < J(\boldsymbol{s})$ such that $(L-1)^i(\boldsymbol{s}) = (L-1)^{J(\boldsymbol{s})}(\boldsymbol{s})$. Then the least ultimate period $\text{per}(\mathcal{S})$ is $J(\boldsymbol{s}) - I(\boldsymbol{s})$.

The proof of Theorem 1 is presented in Appendix A.

Remark 2: In Theorem 1, the calculation of (9) needs to find the first j (increasing from 0) such that there exists $i < j$ satisfying $(L-1)^i(\boldsymbol{s}) = (L-1)^j(\boldsymbol{s})$. Then $\text{per}(\mathcal{S}) = j - i$ and the preperiod is i. For example, if $\boldsymbol{s} = (\beta, 0, 1, 1, \beta^2, 1, \beta) \in F_4^7$, where β is a root of $f(x) = x^2 + x + 1$ over F_{2^2}, then $\text{per}(\mathcal{S}) = 7$ and the preperiod is 1.

Furthermore, a distribution of $\boldsymbol{s} \in F_q^n$ in terms of the least ultimate periods of sequences $\{(L-1)^i(\boldsymbol{s})\}_{i\geq 0}$ is defined in Definition 5, and two results about the distributions are given in Theorem 2 and Theorem 3 for $n = p^r - 1$.

Definition 5: Let D_P be the number of sequences $\boldsymbol{s} \in F_q^n$, whose cyclic-left-shift-difference sequences $\{(L-1)^i(\boldsymbol{s})\}_{i\geq 0}$, i.e., $\mathcal{S}$, have the same least ultimate period P, i.e., $\text{per}(\mathcal{S}) = P$. Then the set

$$\{D_P : P \geq 1\} \tag{10}$$

is called the distribution of sequences $\boldsymbol{s} \in F_q^n$ in terms of the least ultimate periods of their corresponding sequences $\{(L-1)^i(\boldsymbol{s})\}_{i\geq 0}$ (or the least ultimate period distribution of $\boldsymbol{s} \in F_q^n$ for short), and the set

$$\{P : D_P > 0\} \tag{11}$$

is called the least ultimate period spectrum of the sequence $\{(L-1)^i(\boldsymbol{s})\}_{i\geq 0}$ regarding $\boldsymbol{s} \in F_q^n$ (or the least ultimate period spectrum of $\{(L-1)^i(\boldsymbol{s})\}_{i\geq 0}$ for short).

Theorem 2: Let $p = 2$ be the characteristic of F_q and $\boldsymbol{s} \in F_q^n$. Suppose that $n = p^r - 1 = \prod_{i=1}^N w_i^{n_i}$ where w_i's are distinct prime factors of n and n_i's are all positive integers. Then the least ultimate period spectrum of $\{(L-1)^i(\boldsymbol{s})\}_{i\geq 0}$ is the set

$$\left\{P : P = \prod_{i=1}^N w_i^{t_i},\ 0 \leq t_i \leq n_i\right\}, \tag{12}$$

and the least ultimate period distribution of $\boldsymbol{s} \in F_q^n$ is the set in recursive form

$$\left\{D_P : D_P = q^P - \sum_{k\in K} D_k\right\} \text{ where } K = \{k :\ k | P \text{ and } k < P\}. \tag{13}$$

In particular, $D_1 = q$, $D_{w_i} = q^{w_i} - q$, $D_{w_i^{t_i}} = q^{w_i^{t_i}} - q^{w_i^{t_i-1}}$, and $D_{w_i w_j} = q^{w_i w_j} - q^{w_i} - q^{w_j} + q$.

The proofs of Theorem 2 and the following Theorem 3 are presented in Appendices B and C, respectively.

Example 2: Table I illustrates Theorem 2. For example, if $n = 15$, the least ultimate period spectrum of $\mathcal{S}$ for $\boldsymbol{s} \in F_2^{15}$ is {1, 3, 5, 15} which consists of exactly 4 factors of 15, and the corresponding distribution is {2, 6, 30, 32 730}, where the set of sequences $\boldsymbol{s}$ whose cyclic difference sequences $\mathcal{S}$ have the same least ultimate period 3 has 6 elements: (001001001001001), (010010010010010), (011011011011011), (100100100100100), (101101101101101), and (110110110110110).

TABLE II
THE DISTRIBUTION OF SEQUENCES $\boldsymbol{s} \in F_3^n$ IN TERMS OF THE LEAST ULTIMATE PERIODS OF SEQUENCES $\{(L-1)^i(\boldsymbol{s})\}_{i\geq 0}$

n	P=1		P=3	P=4	P=8	P=40	P=80	P=364	P=223040	$\frac{D_{P_{max}}}{3^n}$
	finite third depth	infinite third depth	infinite third depth							
2	3	6	-	-	-	-	-	-	-	-
4	3	6	-	-	72	-	-	-	-	88.89%
5	3	-	-	-	-	-	240	-	-	98.77%
6	27	54	648	-	-	-	-	-	-	88.89%
7	3	-	-	-	-	-	-	2184	-	99.86%
8	3	6	-	72	6480	-	-	-	-	98.77%
10	3	6	-	-	-	720	58320	-	-	98.77%
17	3	-	-	-	-	-	-	-	129140160	99.99%

Theorem 3: Let $p > 2$ be the characteristic of F_q and $\boldsymbol{s} \in F_q^n$. Suppose that $n = p^r - 1 = \prod_{i=1}^N w_i^{n_i}$ where w_i's are distinct prime factors of n and n_i's are all positive integers. Then the least ultimate period spectrum of $\{(L-1)^i(\boldsymbol{s})\}_{i\geq 0}$ is the set

$$\left\{P : P = \prod_{i=1}^{N} w_i^{t_i}, 0 \leq t_i \leq n_i, \text{ and } P \neq 2\right\}, \tag{14}$$

and the least ultimate period distribution of $\boldsymbol{s} \in F_q^n$ is the set

$$\left\{D_P : D_P = q^P - \sum_{k\in K} D_k \text{ if } P \text{ is even, and } D_P = q^{P+1} - \sum_{k\in K} D_k \text{ if } P \text{ is odd}\right\}, \tag{15}$$

where $K = \{k : k|P \text{ and } k < P\}$.

Example 3: The 8th row of Table II illustrates Theorem 3. If $n = 8$, the least ultimate period spectrum is {1, 4, 8} which does not include the factor 2 of 8, and the corresponding distribution is {9, 72, 6480}, where the nine sequences $\boldsymbol{s}$ with $\text{per}(\mathcal{S}) = 1$ are classified into two types. One type is the set {(01010101), (02020202), (10101010), (12121212), (20202020), (21212121)} whose elements have infinite third depth, and the other is the set {(00000000), (11111111), (22222222)} whose elements have finite third depths.

III. HIGH PROBABILITY OF IMPLEMENTATION OF LONG PERIOD SEQUENCES OVER F_{q^n}

In this section, first, for general number $n \neq p^r$, we introduce Algorithm 1 to determine the distribution of sequences $\boldsymbol{s} \in F_q^n$ in terms of the least ultimate periods of corresponding sequences $\{(L-1)^i(\boldsymbol{s})\}_{i\geq 0}$, which is described again by using a recursive formula in Proposition 5. Second, from experiments and proofs, it is surprising that the least ultimate periods of $\{(L-1)^i(\boldsymbol{s})\}_{i\geq 0}$ regarding $\boldsymbol{s} \in F_q^n$ are almost the same as the biggest one of the least ultimate period spectrum. In other words, the sequences $\boldsymbol{s} \in F_q^n$ that can generate long period sequences $\{(L-1)^i(\boldsymbol{s})\}_{i\geq 0}$ almost occupy the whole space (even 99.99% sometimes), see Corollary 1, Example 4, Corollary 2, and Example 5. Finally, we illustrate an implementation of these long period sequences.

A. An Algorithm of Computing the Least Ultimate Period Distribution

From Proposition 3, with i traversing from p^m to $p^{m'}$, the two sets $\{D_P : P \geq 1\}$ and $\{P : D_P > 0\}$ (see Definition 5) can be determined by Algorithm 1 whose proof is omitted for space reasons.

Algorithm 1 Computing the distribution of sequences in F_q^n

1: **Input**: n, the length of sequences over F_q; p, the characteristic of F_q.
2: **Output**: $\{D_P : P \geq 1\}$, the distribution of sequences in F_q^n; $\{P : D_P > 0\}$, the least ultimate period spectrum.
3: Step 1: Generate an $n \times n$ matrix A satisfying (5).
4: Step 2: Determine $m = \text{ord}_p(n)$ and $m' = m + \phi\left(\frac{n}{p^m}\right)$ where $\phi(x)$ is the Euler phi-function of a positive integer x.
5: Step 3: $G \longleftarrow \emptyset$; $j \longleftarrow p^m + 1$;
6: Step 4: Obtain all different generator matrices G_P,
7: **while** $j \leq p^{m'}$ **do**
8: **if** $(j - p^m)|(p^{m'} - p^m)$ **then**
9: $P \longleftarrow j - p^m$; $H_P \longleftarrow (A^j - A^{p^m})^\top$;
10: **if** $(H_P == 0)$ **then**
11: $G_P \longleftarrow I$; $G \longleftarrow G \bigcup \{G_P\}$; goto Step 5;
12: **end if**
13: Transform H_P into $[I_{R_P}, \Gamma]$;
14: $G_P \longleftarrow [-\Gamma^\top, I_{n-R_P}]$;
15: **if** $(G_P \notin G)$ **then**
16: $G \longleftarrow G \bigcup \{G_P\}$;
17: **end if**
18: **end if**
19: $j \longleftarrow j + 1$;
20: **end while**
21: Step 5: For each P, generate cyclic code C_P from G_P.
22: Step 6: For each P, compute the number of sequences $\boldsymbol{s} \in F_q^n$ with $\text{per}(\mathcal{S}) = P$, that is, $D_P = |C_P - \cup_{k\in K} C_k| = |C_P| - |\cup_{k\in K} C_k|$ where $K = \{k : k|P \text{ and } k < P\}$.
23: Step 7: Return $\{D_P : P \geq 1\}$ and $\{P : D_P > 0\}$.

Remark 3: Fortunately, Algorithm 1 will end before $j = p^{m'}$, which is guaranteed when $(A^j - A^{p^m})^\top = 0$ for the first time, see Line 10. At this point, let $P_{max} = j - p^m$, then P_{max}

TABLE III
THE DISTRIBUTION OF SEQUENCES $\boldsymbol{s} \in F_2^n$ IN TERMS OF THE LEAST ULTIMATE PERIODS OF SEQUENCES $\{(L-1)^i(\boldsymbol{s})\}_{i\geq 0}$ WHERE n IS PRIME AND $5 \leq n \leq 19$

n	P=1		P=15	P=85	P=255	P=341	P=819	P=9709	$\frac{D_{P_{max}}}{2^n}$
	finite third depth	infinite third depth	infinite third depth						
5	2	-	30	-	-	-	-	-	93.75%
11	2	-	-	-	-	2046	-	-	99.91%
13	2	-	-	-	-	-	8190	-	99.98%
17	2	-	-	510	130560	-	-	-	99.61%
19	2	-	-	-	-	-	-	524286	99.99%

is the least P such that $A^{P+p^m} - A^{p^m} = 0$, i.e. $C_{P_{max}} = F_q^n$, which implies that P_{max} is the least upper-bound of the ultimate periods of $\{(L-1)^i(\boldsymbol{s})\}_{i\geq 0}$. In particular if $n \neq p^r - 1$ and $p \nmid n$, then $p^{m'} - p^m = p^{\phi(n)} - 1$ will be very large, which leads to $P_{max} \gg n$. This statement can be checked by the 5th, 7th, 9th, and 10th rows in Tables II and III.

B. The Probability of per($\mathcal{S}$) Taking P_{max}

Recalling Definition 5 again, from the inclusion-exclusion principle, a formula for computing D_P can be derived in Proposition 5. Then the probability of per($\mathcal{S}$) taking P_{max} can be determined by using $\frac{D_{P_{max}}}{q^n}$ in Corollary 1.

Definition 6: x is called an extremal factor of y if $x(<y)|y$ and $x \nmid z$ for $\forall\, z(\neq x, y)|y$.

For example, both 9 and 21 are two extremal factors of 63. Consequently, the following result is clear.

Lemma 2: If $y = \prod_{i=1}^N w_i^{n_i}$ where w_i's are distinct prime factors of y and n_i's are all positive integers, then

$$x_i = \prod_{j=1}^{i-1} w_j^{n_j} w_i^{n_i - 1} \prod_{j=i+1}^{N} w_j^{n_j} \ (i = 1, 2, \ldots, N)$$

are the extremal factors of y.

Proposition 5: With the above notations, let $P \in \{P : D_P > 0\}$ and $R_P = \text{rank}(H_P)$ where $H_P = (A^{P+p^m} - A^{p^m})^\top$ and $m = \text{ord}_p(n)$. If k is an extremal factor of P, the k is denoted by k^*. Let $l = |\{k_i^* : i = 1, 2, \cdots\}|$. Then the number of sequences $\boldsymbol{s} \in F_q^n$ with per($\mathcal{S}$) $= P$ is

$$D_P = q^{n-R_P} - \sum_{1\leq i\leq l} q^{n-R_{k_i^*}} + \sum_{\substack{1\leq i<j\leq l \\ k_{ij}=gcd(k_i^*,k_j^*)}} q^{n-R_{k_{ij}}} + \ldots + (-1)^l q^{n-R_{k_w}}, \quad (16)$$

where k_w is the greatest common divisor of all $k_i^* (i = 1, \ldots, l)$.

Proof: From Algorithm 1, it follows that

$$D_P = |C_P - \cup_{k\in K} C_k| = |C_P| - |\cup_{k\in K} C_k|,$$

where $|C_P| = q^{n-R_P}$, $K = \{k : \ k|P \text{ and } k < P\}$, and C_k is the cyclic code with parity check matrix H_k. Since $k_i^* (i = 1, \ldots, l)$ are the extremal factors of P,

$$\cup_{k\in K} C_k = \cup_{1\leq i\leq l} C_{k_i^*}.$$

Let $C_{k_{ij}} = C_{k_i^*} \bigcap C_{k_j^*}$ where $k_{ij} = \gcd(k_i^*, k_j^*)$. Using the inclusion-exclusion principle, we have

$$\begin{aligned} |\cup_{1\leq i\leq l} C_{k_i^*}| &= \sum_{1\leq i\leq l} |C_{k_i^*}| - \sum_{\substack{1\leq i<j\leq l \\ k_{ij}=\gcd(k_i^*,k_j^*)}} |C_{k_{ij}}| + \ldots \\ &\quad + (-1)^{l+1} |C_{k_w}| \\ &= \sum_{1\leq i\leq l} q^{n-R_{k_i^*}} - \sum_{\substack{1\leq i<j\leq l \\ k_{ij}=\gcd(k_i^*,k_j^*)}} q^{n-R_{k_{ij}}} + \ldots \\ &\quad + (-1)^{l+1} q^{n-R_{k_w}}, \end{aligned}$$

where k_w is the greatest common divisor of all k_i^*. Thus the proposition holds. ■

Since $R_{k_i^*} = \text{rank}(H_{k_i^*}) = \text{rank}(A^{k_i^*+p^m} - A^{p^m}) = \text{rank}(A^{p^m}(A^{k_i^*} - I))$ and $\text{rank}(A^{p^m}) = n - p^m$ (see Proposition 1), it follows from Remark 3 that $R_{P_{max}} = 0$ and $0 < R_{k_i^*} \leq n - p^m$, that is, $p^m \leq n - R_{k_i^*} < n$. Thus we have $|C_{P_{max}}| = q^n$ so that $D_{P_{max}} > 0$, i.e., $P_{max} \in \{P : D_P > 0\}$, which yields Corollary 1 and 2. These results indicate that we can select a suitable $\boldsymbol{s}$ in F_q^n with high probability (even 99.99% sometimes) to construct a long period sequence.

Corollary 1: Let $l = |\{k_i^* : i = 1, 2, \cdots\}|$, where k_i^* is an extremal factor of P_{max}. Then

$$\begin{aligned} \frac{D_{P_{max}}}{q^n} &= 1 - \sum_{1\leq i\leq l} \frac{1}{q^{R_{k_i^*}}} + \sum_{\substack{1\leq i<j\leq l \\ k_{ij}=gcd(k_i^*,k_j^*)}} \frac{1}{q^{R_{k_{ij}}}} + \ldots \\ &\quad + (-1)^l \frac{1}{q^{R_{k_w}}} \quad (17) \\ &\geq 1 - \sum_{1\leq i\leq l} \frac{1}{q^{R_{k_i^*}}} \geq 1 - \frac{l}{q^{R_{min}}} \quad (18) \end{aligned}$$

where k_w is the greatest common divisor of all k_i^* and R_{min} is the minimum of all $R_{k_i^*} (i = 1, \ldots, l)$.

Proof: From (16), it is clear that (17) is true. And since $|\cup_{1\leq i\leq l} C_{k_i^*}| \leq \sum_{i=1}^l |C_{k_i^*}|$,

$$\frac{D_{P_{max}}}{q^n} \geq 1 - \sum_{1\leq i\leq l} \frac{1}{q^{R_{k_i^*}}} \geq 1 - \frac{l}{q^{R_{min}}}.$$

■

Example 4: Tables I–III illustrate Corollary 1. For example,

- Row 5 ($n = 15,\ q = 2$) of Table I implies that $P_{max} = 15 = 3 * 5$ and both of its two extremal factors are in

$\{P : D_P > 0\}$. Since $R_{k_1^*} = R_5 = 12$ and $R_{k_2^*} = R_3 = 10$, $\frac{D_{P_{max}}}{q^n} = \frac{D_{15}}{2^{15}} = 98.88\% > 1 - \left(\frac{1}{2^{12}} + \frac{1}{2^{10}}\right) = 98.87\%$.

- Row 10 $(n = 17,\ q = 3)$ of Table II implies that $P_{max} = 223040 = 2^6 * 5 * 17 * 41$ and all of its four extremal factors are not in $\{P : D_P > 0\}$. Since $R_{k_i^*} = 16 (i = 1, 2, 3, 4)$, $\frac{D_{P_{max}}}{q^n} = \frac{D_{223040}}{3^{17}} = 99.99\% \geq 1 - \frac{4}{3^{16}} = 99.99\%$.
- Row 6 $(n = 17,\ q = 2)$ of Table III implies that $P_{max} = 255 = 3 * 5 * 17$ and only one of its three extremal factors, 85, is in $\{P : D_P > 0\}$. Since $R_{k_1^*} = R_{85} = 8$, $R_{k_2^*} = R_{51} = n - 1 = 16$, and $R_{k_3^*} = R_{15} = 16$, it follows that $\frac{D_{P_{max}}}{q^n} = \frac{D_{255}}{2^{17}} = 99.61\% > 1 - \frac{3}{2^8} = 98.83\%$.

In particular, if $n = p^r - 1$, the following corollary holds, where the bound on $\frac{D_{P_{max}}}{q^n}$ is more specific than Corollary 1, although it is not tight yet.

Corollary 2: Let $n = p^r - 1 = \prod_{i=1}^{N} w_i^{n_i} \geq 6$, where p is the characteristic of F_q, w_i's are distinct prime factors of n, and n_i's are all positive integers. Then

$$\frac{D_{P_{max}}}{q^n} > \begin{cases} 1 - \frac{1}{q^3} & if\ N = 1, \\ 1 - \sum_{i=1}^{N} \frac{1}{q^{\frac{w_i - 1}{w_i} e^{(1+o(1))N log N} - 1}} & otherwise \end{cases}$$

where $o(\cdot)$ is the little-o notation and $e^{(1+o(1))NlogN}$ is to estimate the product of the first N primes [7].

Proof: From the proofs of Theorem 2 and 3, for $P \in \{P : D_P > 0\}$, it follows that

$$R_P = \begin{cases} n - P & \text{if } p \neq 2 \text{ and } P \text{ is even, or } p = 2, \\ n - (P + 1) & \text{if } p \neq 2 \text{ and } P \text{ is odd,} \end{cases} \tag{19}$$

and

$$P_{max} = n = \prod_{i=1}^{N} w_i^{n_i}. \tag{20}$$

According to Lemma 2, the extremal factors of P_{max} can be determined by

$$P_i^* = \prod_{j=1}^{i-1} w_j^{n_j} w_i^{n_i - 1} \prod_{j=i+1}^{N} w_j^{n_j}, \tag{21}$$

where $i = 1, 2, \ldots, N$. Using Theorems 2 and 3 again,

$$P_i^* \in \{P : D_P > 0\}. \tag{22}$$

So it follows from (18) and (19) that,

$$\begin{aligned} \frac{D_{P_{max}}}{q^n} &\geq 1 - \sum_{1 \leq i \leq N} \max\left\{ \frac{1}{q^{n - P_i^*}}, \frac{1}{q^{n - (P_i^* + 1)}} \right\} \\ &= 1 - \sum_{1 \leq i \leq N} \frac{1}{q^{n - P_i^* - 1}}. \end{aligned} \tag{23}$$

Case 1 $(N = 1)$*:* From (20) and (21), $n = w_1^{n_1} \geq 6$ and $P_1^* = w_1^{n_1 - 1}$.

i) If $n_1 = 1$, $w_1 \geq 7$. This leads to $n - P_1^* - 1 = w_1^{n_1 - 1}(w_1 - 1) - 1 = w_1 - 2 \geq 5$.

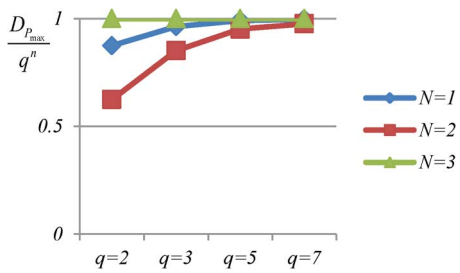

Fig. 3. The probabilities $\frac{D_{P_{max}}}{q^n}$ for $q = 2$, $q = 3$, $q = 5$, and $q = 7$.

ii) If $n_1 = 2$, $w_1 \geq 3$ and $n - P_1^* - 1 = w_1(w_1 - 1) - 1 \geq 5$.

iii) If $n_1 > 2$, $w_1 \geq 2$. This leads to $n - P_1^* - 1 \geq w_1^2(w_1 - 1) - 1 \geq 3$.

So, it is easy to see that $\frac{D_{P_{max}}}{q^n} > 1 - \frac{1}{q^3}$.

Case 2 $(N \neq 1)$*:* Let $p_N\#$ denote the product of the first N primes [7]. Then

$$p_N\# = \prod_{i=1}^{N} p_i = e^{(1+o(1))N \log N} \tag{24}$$

where p_i is the ith prime number and $o(\cdot)$ is the little-o notation. Since

$$\begin{aligned} n - P_i^* - 1 &= \frac{w_i - 1}{w_i} \prod_{j=1}^{N} w_j^{n_j} - 1 \geq \frac{w_i - 1}{w_i} \prod_{j=1}^{N} w_j - 1 \\ &> \frac{w_i - 1}{w_i} p_N\# - 1, \end{aligned} \tag{25}$$

we have that

$$\frac{D_{P_{max}}}{q^n} > 1 - \sum_{i=1}^{N} \frac{1}{q^{\frac{w_i - 1}{w_i} e^{(1+o(1))N \log N} - 1}}.$$

■

Example 5: From Corollary 2, if $n = p^r - 1 \geq 6$, it follows that

$$\frac{D_{P_{max}}}{q^n} > \begin{cases} 1 - \frac{1}{q^3} & if\ N = 1, \\ 1 - \left(\frac{1}{q^2} + \frac{1}{q^3}\right) & if\ N = 2, \\ 1 - \left(\frac{1}{q^{14}} + \frac{1}{q^{19}} + \frac{1}{q^{23}}\right) & if\ N = 3. \end{cases}$$

Fig. 3 shows the trend of $\frac{D_{P_{max}}}{q^n}$ in the above three cases with increasing q. Although these bounds are not tight, it is still easy to see that the probability $\frac{D_{P_{max}}}{q^n}$ are almost close to 1 when q is large. For example,

- Case 1 $(N = 1)$. The 8th row $(n = 8,\ q = 3)$ in Table II implies that, (i) $P_{max} = 8 = 2^3$ has an extremal factor $4 \in \{P : D_P > 0\}$; (ii) $\frac{D_{P_{max}}}{q^n} = 98.77\% > 1 - \frac{1}{3^3} = 96.30\%$.
- Case 2 $(N = 2)$. The 7th row $(n = 63,\ q = 2)$ in Table I shows that, (i) $P_{max} = 63 = 3^2 * 7$ has two extremal factors $9, 21 \in \{P : D_P > 0\}$; (ii) $\frac{D_{P_{max}}}{q^n} = 99.99\% > 1 - \left(\frac{1}{2^2} + \frac{1}{2^3}\right) = 62.50\%$.

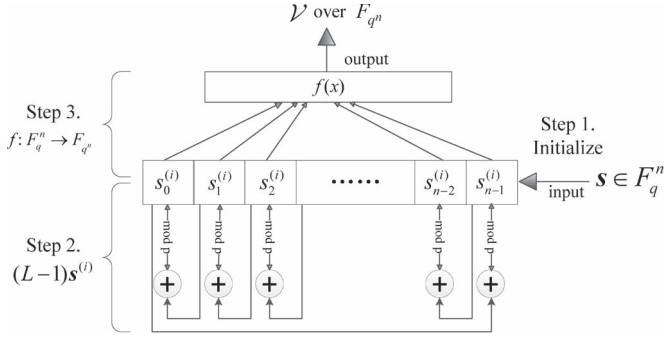

Fig. 4. Constructing a long period sequence $\mathcal{V}$ over F_{q^n} from a vector $\boldsymbol{s} \in F_q^n$ in the following three steps. Step 1: Initialize an n-stage register with $\boldsymbol{s}$, and output $\boldsymbol{s} = \boldsymbol{s}^{(0)} = (s_0^{(0)}, s_1^{(0)}, \ldots, s_{n-1}^{(0)})$ as $v_0 \in F_{q^n}$ under a basis of F_{q^n} determined by a primitive polynomial $f(x)$ over F_q with degree n. Step 2: Update the register state from the ith to the $(i+1)$th by calculating $s_j^{(i+1)} = s_{j+1 \bmod n}^{(i)} - s_j^{(i)} = (s_{j+1 \bmod n}^{(i)} + (-s_j^{(i)} \bmod p)) \bmod p$. Step 3: Under the above basis, output $\boldsymbol{s}^{(i+1)} = (s_0^{(i+1)}, s_1^{(i+1)}, \ldots, s_{n-1}^{(i+1)})$ as $v_{i+1} \in F_{q^n}$ using $f(x)$.

- Case 3 $(N = 3)$. If $n = 255 = 2^8 - 1$, it follows from Theorem 2 that $P_{max} = 255 = 3 * 5 * 17$. (i) P_{max} has three extremal factors $15, 51, 85 \in \{P : D_P > 0\}$; (ii) $\frac{D_{P_{max}}}{q^n} \cong 100\% > 1 - \left(\frac{1}{2^{14}} + \frac{1}{2^{19}} + \frac{1}{2^{23}}\right) = 99.99\%$.

Remark 4: If $n = p^r - 1$, according to Theorems 2 and 3, the extremal factors of P_{max} are all in the least ultimate period spectrum. However, if $n \neq p^r - 1$ and $p \not| n$, the extremal factors are not all in the least ultimate period spectrum. It is interesting that the probabilities $\frac{D_{P_{max}}}{q^n}$ in these two cases are both close to 1, which can be checked by Tables I–III. In other words, it suggests from Remark 3 that a kind of long period sequences over F_{q^n} can be constructed from vectors in F_q^n with very high probability, see Example 1 in Section I.

C. An Implementation of Long Period Sequences Over F_{q^n}

In reality, sequences with long period but lightweight generation are often demanded in the applications of communication. Here we present an efficient implementation of constructing the sequences by means of cyclic difference operator, see Fig. 4.

In Fig. 4, F_{q^n} is defined by $f(x)$ that is a primitive polynomial over F_q of degree n. $\boldsymbol{s}^{(i)} = (L-1)^i \boldsymbol{s} = (s_0^{(i)}, s_1^{(i)}, \ldots, s_{n-1}^{(i)})$ where $i = 0, 1, \ldots$ and $\boldsymbol{s}^{(0)} = \boldsymbol{s}$, is stored in an n-stage register consisting of n consecutive p-state storage units regulated by a single clock. "$x \leftarrow \bmod p \rightarrow \bigoplus \leftarrow y$" means to calculate $y - x = (y + (-x \bmod p)) \bmod p$ and store it in the storage unit of x.

- In the first step of implementation, $\boldsymbol{s}$ is used to initialize the n-register. The corresponding output is an element $v_0 \in F_{q^n}$ under a basis of F_{q^n} over F_q using $f(x)$, see Example 1 in Section I.
- Secondly, at each clock pulse, there is a transition in the register from the ith state $\boldsymbol{s}^{(i)}$ to the next $\boldsymbol{s}^{(i+1)} = (L-1)\boldsymbol{s}^{(i)} = (s_0^{(i+1)}, s_1^{(i+1)}, \ldots, s_{n-1}^{(i+1)})$, where $s_j^{(i+1)} = s_{j+1 \bmod n}^{(i)} - s_j^{(i)}$ and $j = 0, 1, \ldots, n-1$.
- Thirdly, output $\boldsymbol{s}^{(i+1)}$ in the register as an element $v_{i+1} \in F_{q^n}$ using the same method of the first step.
- In the consecutive clock pulses, repeating the second and the third steps accordingly, the n-stage register outputs a sequence $\mathcal{V}$ over F_{q^n}:

$$v_0, v_1, \ldots, v_{i+1}, \ldots. \tag{26}$$

Since the implementation only involves the addition operator of finite field, the algorithm is lightweight. In addition, the LFSR is a simple hardware. In fact, for $q = 2$ and $n = 2^r - 1$, the computational complexity of the algorithm is $\Theta(n^2)$ where Θ is the standard Big Theta notation, and the number of GEs (Gate Equipments) is n.

IV. Application

In code division multiple access systems, families of sequences with good correlation property are needed [11]. In this section, as an application, the above generated sequences can be interleaved to obtain good correlation properties, see [20]. Those results in [20] are briefly mentioned here. First, the interleaved sequence based on $\{(L-1)^i(\boldsymbol{s})\}_{i \geq 0}$ is introduced in Definition 7. Then, good correlation properties are analyzed and illustrated in several figures, where the condition on good correlation in this paper is a little larger than the Welch bound [10, p. 126].

Let $n = 2^r - 1$. $\mathcal{C}$ denotes the set consisting of binary sequences of period n with 2-level autocorrelation, and let $\mathcal{C}^* = \{\boldsymbol{s} : \boldsymbol{s} \in \mathcal{C}$ and $\boldsymbol{s}$ is not an m-sequence$\}$.

Definition 7 ([20]): Rearrange $\mathcal{S}$ as the array form

$$U = \Big(\boldsymbol{s}^\top, ((L-1)(\boldsymbol{s}))^\top, \left((L-1)^2(\boldsymbol{s})\right)^\top, \ldots, \left((L-1)^{per(\mathcal{S})+M-1}(\boldsymbol{s})\right)^\top\Big) \tag{27}$$

and read it out row by row, from left to right within a row, beginning with the top row, then an interleaved sequence is obtained. We call it an *interleaved cyclic difference sequence constructed from the base sequence* $\boldsymbol{s}$, which is denoted by $\boldsymbol{u}$ and called interleaved difference sequence for short.

Let $\mathcal{U} = \{\boldsymbol{u}$: the base sequence $\boldsymbol{s} \in \mathcal{C}^*\}$. Recall that the periodic correlation of two binary sequences $\boldsymbol{a} = \{a_i\}_{i=0}^{\infty}$ and $\boldsymbol{b} = \{b_i\}_{i=0}^{\infty}$ over F_2 with the same period N is defined as

$$C_{\boldsymbol{a},\boldsymbol{b}}(\tau) = \sum_{k=0}^{N-1} (-1)^{(a_k - b_{k+\tau})}, 0 \leq \tau \leq N-1. \tag{28}$$

If the sequences $\boldsymbol{a}$ and $\boldsymbol{b}$ are the same, we call it the autocorrelation and denote it by $C_{\boldsymbol{a}}(\tau)$.

The sequences $\boldsymbol{a}$ and $\boldsymbol{b}$ are said to have "good" correlation properties if, for all $\tau \neq 0$, the absolute values of $C_{\boldsymbol{a}}(\tau)$, $C_{\boldsymbol{b}}(\tau)$, and $C_{\boldsymbol{a},\boldsymbol{b}}(\tau)$ are all very small comparing with N. That is,

$$\max\left(|C_{\boldsymbol{a}}(\tau)|, |C_{\boldsymbol{b}}(\tau)|, |C_{\boldsymbol{a},\boldsymbol{b}}(\tau)|\right) \ll N. \tag{29}$$

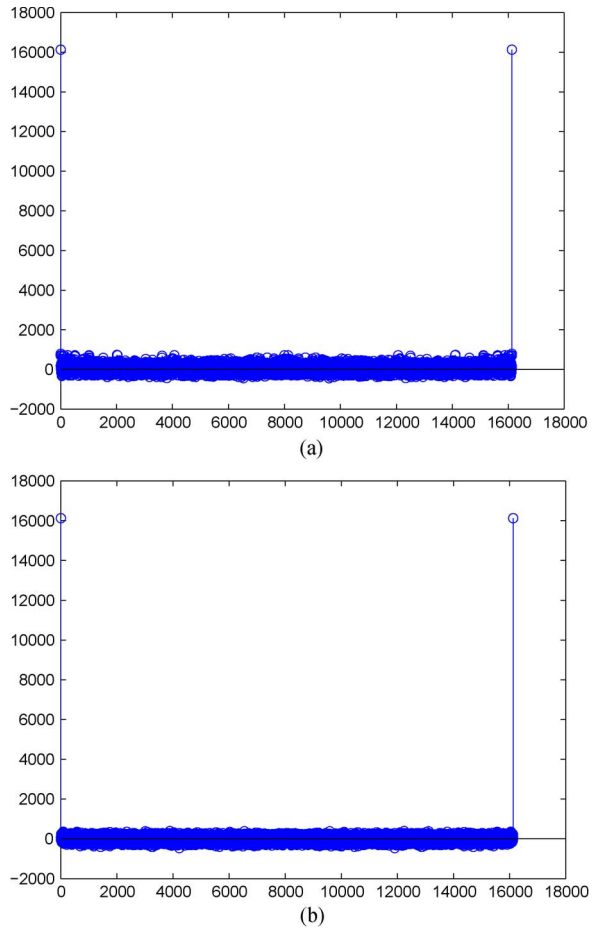

Fig. 5. The autocorrelation functions of $\boldsymbol{u}$ for $n = 127$ [20], where the horizontal and vertical axes represent the correlation time and correlation value, respectively. (a) based on QR sequence. (b) based on Hall sequence.

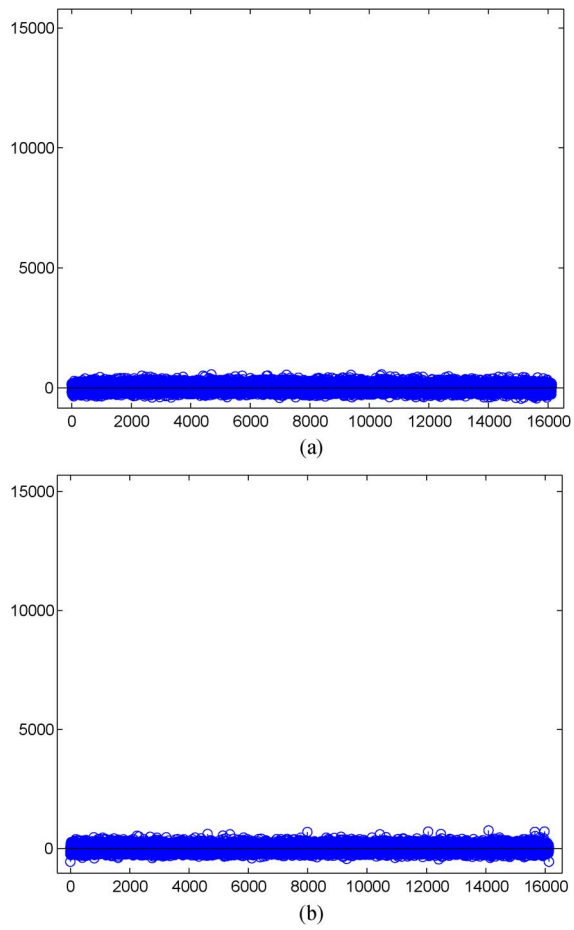

Fig. 6. The crosscorrelation functions of $\mathcal{U}$ for $n = 127$ [20], where the horizontal and vertical axes represent the correlation time and correlation value, respectively. (a) based on QR and Hall sequences. (b) based on 5-term and WG sequences.

Example 6: Fig. 5 illustrates the autocorrelation functions of $\boldsymbol{u}$ whose base sequences are quadratic residue (i.e., QR for short) and Hall sextic residue (i.e., Hall) sequences of period $n = 127$. Fig. 6 illustrates partly the crosscorrelation functions of $\mathcal{U}$ where the periods of the base sequences are 127. As shown, all of the auto- and cross- correlations in these two figures are good. (For details, please refer to Tables 1 and 4 in [20].) This experimental evidence enables us to propose the following conjecture.

Conjecture [20]: For $n = 2^r - 1$, the maximum correlation magnitude R_{max} [16] of $\mathcal{U}$ with period $N = n^2$ is bounded by $r\sqrt{N}$, i.e.,

$$R_{max} < r\sqrt{N}$$

which is a little larger than the Welch bound.

V. Conclusion

In this paper, we introduce a novel class of ultimately periodic sequences $\{(L-1)^i(\boldsymbol{s})\}_{i\geq 0}$, and investigate their least ultimate period spectrum with respect to $\boldsymbol{s} \in F_q^n$. In terms of the least ultimate periods of $\{(L-1)^i(\boldsymbol{s})\}_{i\geq 0}$, a distribution of $\boldsymbol{s} \in F_q^n$ is analyzed, where $\frac{D_{P_{max}}}{q^n}$ is almost close to 1. Based on this point, a method of constructing long period sequences over F_{q^n} from vectors in F_q^n with very high probability is proposed. Furthermore, the implementation of the long period sequences only involves the addition operator of finite field, which can be carried out by a simple LFSR. Thus it is lightweight.

Appendix A
Proof of Theorem 1

By Definition 4, the least ultimate period of $\{(L-1)^i(\boldsymbol{s})\}_{i\geq 0}$ (i.e., $\mathcal{S}$) is defined as follows:

$$\mathrm{per}(\mathcal{S}) = \min\left\{j - i : i < j \text{ and } (L-1)^i(\boldsymbol{s}) = (L-1)^j(\boldsymbol{s})\right\}. \tag{30}$$

From the definition of $I(\boldsymbol{s})$ and (9), it is clear that

$$J(\boldsymbol{s}) - I(\boldsymbol{s}) \in \left\{j - i : i < j \text{ and } (L-1)^i(\boldsymbol{s}) = (L-1)^j(\boldsymbol{s})\right\}.$$

So it is sufficient to show that, for any pair of integers i, j such that $(L-1)^i(\boldsymbol{s}) = (L-1)^j(\boldsymbol{s})$, there is $J(s) - I(s) \leq j - i$. Below we will use the reduction to absurdity to prove this statement.

Suppose that there exists a pair of integers i, j such that $j - i < J(s) - I(s)$ satisfying $(L-1)^i(\boldsymbol{s}) = (L-1)^j(\boldsymbol{s})$. From (9) we have $J(\boldsymbol{s}) < j$ and then $I(\boldsymbol{s}) < i$. Let

$$u = i - I(\boldsymbol{s}) \text{ and } v = j - I(\boldsymbol{s}) \bmod J(\boldsymbol{s}) - I(\boldsymbol{s}). \quad (31)$$

i) If $u = v$, (31) leads to $J(\boldsymbol{s}) - I(\boldsymbol{s}) | j - i$, which contradicts the supposition.
ii) If $u \neq v$, without loss of generality, assume $v > u$, then

$$(L-1)^i(\boldsymbol{s}) = (L-1)^j(\boldsymbol{s}) \Leftrightarrow (L-1)^{I(\boldsymbol{s})+u}(\boldsymbol{s}) = (L-1)^{I(\boldsymbol{s})+v}(\boldsymbol{s}).$$

Since $u < v < J(\boldsymbol{s}) - I(\boldsymbol{s})$, we have $I(\boldsymbol{s}) + u < I(\boldsymbol{s}) + v < J(\boldsymbol{s})$, which is in contradiction with (9). This theorem holds.

APPENDIX B
PROOF OF THEOREM 2

Recall that

$$\begin{aligned} C_P &= \left\{ \boldsymbol{s} \in F_q^n : P \text{ is an ultimate period of } \left\{ (L-1)^i(\boldsymbol{s}) \right\}_{i \le 0} \right\} \\ &= \left\{ \boldsymbol{s} \in F_q^n : (L-1)^{P+1}(\boldsymbol{s}) = (L-1)(\boldsymbol{s}) \right\} \\ &= \left\{ \boldsymbol{s} \in F_q^n : \boldsymbol{s}(A^{P+1} - A) = [0^n] \right\}. \end{aligned} \quad (32)$$

Since $n = 2^r - 1 = \prod_{i=1}^N w_i^{n_i}$, it is clear from Proposition 4 i) that $\text{per}(\mathcal{S}) | n$ for any $\boldsymbol{s} \in F_q^n$ where $\text{per}(\mathcal{S})$ is the least ultimate period of difference sequence $\mathcal{S}$, i.e., $\{(L-1)^i(\boldsymbol{s})\}_{i \ge 0}$. This implies

$$\{P : D_P > 0\} \subseteq \left\{ P : P = \prod_{i=1}^N w_i^{t_i},\ 0 \le t_i \le n_i \right\}. \quad (33)$$

Below we only need to prove $\{P : P = \prod_{i=1}^N w_i^{t_i},\ 0 \le t_i \le n_i\} \subseteq \{P : D_P > 0\}$ in two steps. First, we shall show that C_P is an $[n, P]$ cyclic code. Second, for $\boldsymbol{s} \in C_P - \bigcup_{k \in K} C_k$, where

$$K = \{k :\ k | P \text{ and } k < P\}, \quad (34)$$

prove that $\text{per}(\mathcal{S}) = P$, i.e.,

$$D_P = \left| C_P - \bigcup_{k \in K} C_k \right| > 0. \quad (35)$$

Proof of the 1st part: Consider a parity check matrix $H = (A^{P+1} - A)^\top$ in (32) to obtain an $[n, P]$ cyclic code C_P in the following way.

- *If $P = n$, then $C_P = F_q^n$.* In fact, from Proposition 4 i), it follows that $A^{P+1} - A = 0$ if $P = n$, which implies $C_P = F_q^n$.
- *If $P < n$, try to prove that C_P is an $[n, P]$ cyclic code.* From Corollary 1, the first row of H is denoted by

$$\begin{aligned} \boldsymbol{h} &= (\alpha_{P+1,0} + 1, \alpha_{P+1,1} - 1, \ldots, \alpha_{P+1,P+1}, 0, \ldots, 0) \\ &= (0, 1, \ldots, 1, 0, \ldots, 0) \text{ since } \alpha_{i,j} = \binom{i}{j} \bmod 2. \end{aligned}$$

Evidently, H is a circulant matrix whose row polynomial is

$$h(x) = (x-1)^{P+1} - (x-1).$$

We just prove that the row space with generator matrix H is a cyclic code, denoted by C, which will be used as the dual code of C_P in the following paragraphs. For convenience, we circulate the rows of H to the bottom once and obtain an equivalently circulant matrix $\overline{H}$ with the first row

$$\overline{\boldsymbol{h}} = (1, \alpha_{P+1,2}, \ldots, \alpha_{P+1,P}, 1, 0, \ldots, 0).$$

and then the cyclic code C can be denoted by

$$C = \left\{ \gamma(x)\overline{h}(x) \bmod x^n - 1 : \gamma(x) \in F_q[x] \right\}. \quad (36)$$

We now show $\overline{h}(x) | x^n - 1$, then $\overline{h}(x)$ is proved to be a generator polynomial of C since the generated code is the same as (36). It is sufficient to prove $x\overline{h}(x) | x(x^n - 1)$. Let $x' = x - 1$. Then

$$x\overline{h}(x) = (x-1)^{P+1} - (x-1) = x'^{P+1} - x' = x'(x'^P - 1),$$

and

$$x(x^n - 1) = (x'+1)^{n+1} - (x'+1) = x'^{n+1} - x' = x'(x'^n - 1)$$

since $n + 1 = 2^r$. It is easy to see that $(x'^P - 1) | (x'^n - 1)$ since $P | n$. Thus $\overline{h}(x) | x^n - 1$. This confirms that $\overline{h}(x)$ is a generator polynomial of C with generator matrix $\overline{H}$, which implies $\text{rank}(\overline{H}) = n - P$. Hence the null space of

$$\overline{H}\boldsymbol{s}^\top = [0^n]^\top, \quad (37)$$

i.e., C_P, is an $[n, P]$ cyclic code, which is the dual code of C.

Therefore, for any $P = \prod_{i=1}^N w_i^{t_i}$ where $0 \le t_i \le n_i$, there exists an $[n, P]$ cyclic code C_P such that P is an ultimate period of $\{(L-1)^i(\boldsymbol{s})\}_{i \ge 0}$ for $\boldsymbol{s} \in C_P$. In addition, for every $k \in K$ we have $C_k \subset C_P$ since

$$\begin{aligned} & \boldsymbol{s}A^{k+1} = \boldsymbol{s}A \\ \overset{P=uk}{\Longrightarrow} \quad & \boldsymbol{s}A^{P+1} = \boldsymbol{s}A^{k+1}(A^k)^{u-1} = \ldots = \boldsymbol{s}A. \end{aligned} \quad (38)$$

Proof of the 2nd part: Try to determine D_P for $1 \le P \le n$.

- *If $P = 1$, then $D_1 = q$.* In fact, since

$$\boldsymbol{s}A^{i+1} = \boldsymbol{s}A^i \Leftrightarrow \boldsymbol{s}A^i(A - I) = 0 \Leftrightarrow \boldsymbol{s}A^i = 0, \quad (39)$$

and $\text{rank}(A^i) = n - 1$ in Proposition 1, the null space of $\boldsymbol{s}A^{i+1} = \boldsymbol{s}A^i$ is the set $\{[\lambda^n] :\ \lambda \in F_q\}$. That is, $D_1 = q$.
- *If $1 < P \le n$, try to prove that $D_P = q^P - \sum_{k \in K} D_k$.* Let $\boldsymbol{s} \in C_P$. Then P is an ultimate period of $\{(L-1)^i(\boldsymbol{s})\}_{i \ge 0}$ corresponding to $\boldsymbol{s}$. In addition, if the least ultimate period of $\{(L-1)^i(\boldsymbol{s})\}_{i \ge 0}$ corresponding to $\boldsymbol{s}$ is $k (< P)$, i.e., $\text{per}(\mathcal{S}) = k \in K$, then $\boldsymbol{s} \in C_k \subset C_P$ since (38). Let $X = C_P - \bigcup_{k \in K} C_k$. Then for $\boldsymbol{s} \in X \neq \emptyset$

(an empty set) we have $\mathrm{per}(\mathcal{S}) = P$, which implies $P \in \{P : D_P > 0\}$ since $D_P = |X| > 0$. That is to say,

$$\left\{ P : P = \prod_{i=1}^{N} w_i^{t_i},\ 0 \le t_i \le n_i \right\} \subseteq \{P : D_P > 0\}. \quad (40)$$

Thus (12) holds. Furthermore, according to Definition 5 and (38), the following recurrence formula is obtained:

$$D_P = q^P - \sum_{k \in K} D_k. \quad (41)$$

Thus (13) also holds.

Specifically, from (38) and (41), we have

$$D_{w_i} = q^{w_i} - q,\ D_{w_i^{t_i}} = q^{w_i^{t_i}} - q^{w_i^{t_i - 1}},\ \text{and}$$
$$D_{w_i w_j} = q^{w_i w_j} - q^{w_i} - q^{w_j} + q$$

since $C_{w_i} \bigcap C_{w_j} = C_1 = \{[\lambda^n] : \lambda \in F_q\}$. Therefore the theorem follows.

Appendix C
Proof of Theorem 3

The proof is similar to that of Theorem 2, and we just need to prove the following two statements. i) $\mathrm{per}(\mathcal{S}) \neq 2$ for any $\boldsymbol{s} \in F_q^n$. ii) The code C_P is an $[n, P]$ cyclic code if P is even, and an $[n, P+1]$ cyclic code if P is odd.

i) For $i \ge 1$, since

$$\boldsymbol{s}A^{i+2} = \boldsymbol{s}A^i$$
$$\iff \boldsymbol{s}A^i(A^2 - I) = [0^n] \overset{(5)}{\iff} \boldsymbol{s}A^i(A - I)T = [0^n]$$
$$\overset{(3)}{\iff} \boldsymbol{s}A^i(A - I) = [0^n] \iff \boldsymbol{s}A^{i+1} = \boldsymbol{s}A^i,$$

C_2 is the same as C_1. It is easy to see from (35) that $D_2 = 0$, i.e., $2 \notin \{P : D_P > 0\}$. Thus (14) holds.

ii) Since $p \neq 2$ is a prime, $n = p^r - 1$ is even. Let $P = \prod_{i=1}^{N} w_i^{t_i}$ where $0 \le t_i \le n_i$.
- If P is even, then $\alpha_{P+1,0} + 1 = 0$ and $\alpha_{P+1,1} - 1 \equiv P \pmod p$ which is nonzero since $\gcd(P, p) = 1$. Let $\overline{h}(x) = ((x-1)^{P+1} - (x-1))/x$. Analogous to Theorem 2, $\overline{h}(x)$ is a generator polynomial of an $[n, n-P]$ cyclic code C, which implies that there exists an $[n, P]$ cyclic code C_P such that P is an ultimate period of $\{(L-1)^i(\boldsymbol{s})\}_{i \ge 0}$, for $\boldsymbol{s} \in C_P$.
- If P is odd, then $\alpha_{P+1,0} + 1 \equiv 2 \pmod p \neq 0$. Let

$$h(x) = (x-1)^{P+1} - (x-1).$$

Next, we show $h(x) | x^n - 1$. Let $x' = x - 1$. Then $h(x) = x'^{P+1} - x'$ and $x^n - 1 = (x'+1)^n - 1$. Since P is odd and n is even, it follows that $\gcd(x'^P - 1, x' + 1) = 1$ and $x' + 1 | x'^n - 1$. In addition, $x'^P - 1 | x'^n - 1$ since $P | n$. Thus $(x'+1)(x'^P - 1) | x'^n - 1$. And since

$$(x'+1)(x'^P - 1) | x'^n - 1$$
$$\overset{n+1=p^r}{\iff} x'(x'+1)(x'^P - 1) | (x'+1)^{n+1} - (x'+1)$$
$$\iff h(x) | x^n - 1,$$

$h(x)$ is a generator polynomial of an $[n, n - (P+1)]$ cyclic code, which implies that there exists an $[n, P+1]$ cyclic code C_P such that P is an ultimate period of $\{(L-1)^i(\boldsymbol{s})\}_{i \ge 0}$ for $\boldsymbol{s} \in C_P$. Thus (15) holds.

Therefore the theorem follows.

References

[1] R. Bar-Yehuda, T. Etzion, and S. Moran, "Rotating-table games and derivatives of words," *Theor. Comput. Sci.*, vol. 108, no. 2, pp. 311–329, Feb. 1993.

[2] R. A. Brualdi, *Introductory Combinatorics*, 4th ed. Beijing, China: China Machine Press, 2006, p. 276.

[3] C. Ding, "A fast algorithm for determining the linear complexity of sequences over GF (p^m) with period p^n," *IEEE Trans. Inf. Theory*, vol. 46, no. 6, pp. 2203–2206, Sep. 2000.

[4] C. Ding and G. Xiao, *Stream Cryptography and Its Applications*. Beijing, China: National Defence Industry Press, 1994, pp. 39–71.

[5] T. Etzion, "Linear complexity of de Bruijn sequences—Old and new results," *IEEE Trans. Inf. Theory*, vol. 45, no. 2, pp. 693–698, Mar. 1999.

[6] T. Etzion, "The depth distribution—A new characterization for linear codes," *IEEE Trans. Inf. Theory*, vol. 43, no. 4, pp. 1361–1363, Jul. 1997.

[7] H. Dubner, "Factorial and primorial primes," *J. Recr. Math.*, vol. 19, no. 3, pp. 197–203, 1987.

[8] 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.

[9] S. W. Golomb, *Shift Register Sequence*. Laguna Hills, CA, USA: Aegen Park Press, 1982.

[10] S. W. Golomb and G. Gong, *Signal Design for Good Correlation for Wireless Communication, Cryptography, Radar*. Cambridge, U.K.: Cambridge Univ. Press, 2005.

[11] G. Gong and T. Helleseth, "A three-valued Walsh transform from decimations of Helleseth–Gong sequences," *IEEE Trans. Inf. Theory*, vol. 58, no. 2, pp. 1158–1162, Feb. 2012.

[12] R. Lidl and H. Niederreiter, *Finite Fields*. Cambridge, U.K.: Cambridge Univ. Press, 1983, p. 410.

[13] Y. Luo, F. Fu, and V. K. Wei, "On the depth distribution of linear codes," *IEEE Trans. Inf. Theory*, vol. 46, no. 6, pp. 2197–2203, Sep. 2000.

[14] C. J. Mitchell, "On integer-valued rational polynomials and depth distributions of binary codes," *IEEE Trans. Inf. Theory*, vol. 44, no. 7, pp. 3146–3150, Nov. 1998.

[15] M. B. Nathanson, "Derivatives of binary sequences," *SIAM J. Appl. Math.*, vol. 21, no. 3, pp. 407–412, Nov. 1971.

[16] J. S. No, K. Yang, H. Chung, and H. Y. Song, "New construction for families of binary sequences with optimal correlation properties," *IEEE Trans. Inf. Theory*, vol. 43, no. 5, pp. 1596–1602, Sep. 1997.

[17] M. J. B. Robshaw, "On evaluating the linear complexity of a sequence of least period 2^n," *Des. Codes Cryptogr.*, vol. 4, no. 4, pp. 263–269, Oct. 1994.

[18] K. H. Rosen, *Elementary Number Theory and its Applications*, 4th ed. Beijing, USA: China Machine Press, 2004, pp. 222–229, pp. 53–61.

[19] M. Zeng, Y. Luo, and G. Gong, "Rotating-table game and construction of periodic sequences with lightweight calculation," in *Proc. IEEE Int. Symp. Inf. Theory*, 2012, pp. 1221–1225.

[20] M. Zeng, Y. Luo, and G. Gong, "Sequence with good correlation property based on depth and interleaving techniques," *Des. Codes Cryptogr.*, to be published online in 2014 with DOI: 10.1007/s10623-014-0004-z.

Min Zeng received the B.E. degree in mathematics from Central China Normal University, Wuhan, China, in 1988 and the M.S. degree in software engineering from Shanghai Jiao Tong University, Shanghai, China, in 2007. He is currently working toward the Ph.D. degree in computer science and technology at Shanghai Jiao Tong University. His research interests are in sequences and coding theory, with a focus on algebraic coding, combinatorics, and finite fields.

Yuan Luo received the B.S., M.S., and Ph.D. degrees from Nankai University, Tianjin, China, in 1993, 1996, and 1999, respectively, all in applied mathematics. From July 1999 to April 2001, he held a postdoctoral position with the Institute of Systems Science, Chinese Academy of Sciences, Beijing, China. From May 2001 to April 2003, he held a postdoctoral position with the Institute for Experimental Mathematics, University of Duisburg-Essen, Essen, Germany. Since June 2003, he has been with the Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai, China, where he has been a Full Professor since 2006. His current research interests include coding theory and information theory.

A. J. Han Vinck (M'77–SM'91–F'06) received the Ph.D. degree in electrical engineering from the University of Eindhoven, Eindhoven, The Netherlands, in 1980. Since 1990, he has been a Full Professor of digital communications at the University of Duisburg-Essen, Essen, Germany. In 1991–1993, 1998–2000, and 2006–2008, he was the Director of the Institute for Experimental Mathematics in Essen. He was also the Director (1997–1999) of the Postgraduate School on Networking, "CINEMA." From 2000 to 2004, he was the Chairman of the Communication Division at the Institute for Critical Infrastructures (CRIS). In 2003, he was an Adjoint Professor at the National Sun Yat-sen University, Kaohsiung, Taiwan. His interests include information and communication theory, coding, and network aspects in digital communications. Dr. Vinck was elected a Fellow of the IEEE in 2006 for his "contributions to coding techniques." In 1990, he organized the IEEE Information Theory Workshop held in Veldhoven, The Netherlands. He was the Founding Chairman (1995–1998) of the IEEE German Information Theory Chapter. He acted as a Cochairman for the 1997 IEEE Information Theory Symposium held in Ulm, Germany. He served on the Board of Governors of the IEEE Information Theory Society from 1997 to 2006. In 1999, he was the Program Chairman for the IEEE Information Theory Workshop held in Kruger Park, South Africa. In 2003, he was elected President of the IEEE Information Theory Society. He served as a Member-at-Large (2001–2002) in the Meetings and Services Committee of the IEEE. He is the initiator of the Japanese-Benelux Workshops on Information Theory (now Asia-Europe) and the International Winter Meeting on Coding, Cryptography, and Information Theory. He started and still supports the organization of the series of conferences on Power Line Communications and its Applications. He was a recipient of the IEEE ISPLC2006 Achievement Award in Orlando, FL, USA, for his contributions to Powerline Communications and for facilitating the transition of ISPLC to a fully financially and technically sponsored IEEE Communications Society conference. The SA-IEE annual award was presented to him for the best paper published in the SA-IEE Africa Research Journal in 2008. He is a Cofounder and the President of the Shannon and Gauss Foundations, which stimulate research and help young scientists in the field of information theory and digital communications.