Trace Representation and Linear Complexity of Binary eth Power Residue Sequences of Period p

Zongduo Dai, Guang Gong, Hong-Yeop Song, *Senior Member, IEEE*, and Dingfeng Ye

***Abstract*—Let $p = ef + 1$ be an odd prime for some e and f, and let F_p be the finite field with p elements. In this paper, we explicitly describe the trace representations of the binary characteristic sequences (of period p) of all the cyclic difference sets D which are some union of cosets of eth powers H_e in $F_p^* (\triangleq F_p \backslash \{0\})$ for $e \leq 12$. For this, we define eth power residue sequences of period p, which include all the binary characteristic sequences mentioned above as special cases, and reduce the problem of determining their trace representations to that of determining the values of the generating polynomials of cosets of H_e in F_p^* at some primitive pth root of unity, and some properties of these values are investigated. Based on these properties, the trace representation and linear complexity not only of the characteristic sequences of all the known eth residue difference sets, but of all the sixth power residue sequences are determined. Furthermore, we have determined the linear complexity of a nonconstant eth power residue sequence for any e to be either $p - 1$ or p whenever $(e, (p-1)/n) = 1$, where n is the order of 2 mod p.**

***Index Terms*—Binary sequences with two-level autocorrelation, cyclic difference sets, *e*th residue cyclic difference sets, linear complexity, minimal polynomials, trace representations.**

I. Introduction

A (v, k, λ)-CYCLIC difference set D is a k-subset of the integers mod v, denoted by Z/vZ, such that any nonzero $a \in Z/vZ$ can be represented as a difference $x - y$ (where $x, y \in D$) in exactly λ ways [1]. It is well known [8], [10] that its characteristic sequence $\mathbf{s} = \{s(t) | t \geq 0\}$ of period v defined by

$$s(t) = \begin{cases} 0 & \text{for } t \in D \\ 1 & \text{for } t \notin D \end{cases} \tag{1}$$

has the two-level autocorrelation function

$$R_s(\tau) = \begin{cases} v & \text{for } \tau \equiv 0 \pmod v \\ v - 4(k - \lambda) & \text{otherwise,} \end{cases} \tag{2}$$

where the periodic unnormalized autocorrelation function $R_s(\tau)$ of the sequence $\mathbf{s}$ is defined as

$$R_s(\tau) \triangleq \sum_{t=0}^{v-1} (-1)^{s(t+\tau) - s(t)}.$$

For this reason and many other randomness properties, the binary sequences from cyclic difference sets as given in (1) have been used in many communications engineering and cryptography [10], [31], [8]. In these applications, in particular, one requires the out-of-phase value $v - 4(k - \lambda)$ in (2) be as small as possible [8], and this is achieved by cyclic Hadamard difference sets which have parameters $v = 4t - 1$, $k = 2t - 1$, and $\lambda = t - 1$ for some integer t[1], [17]. The characteristic sequences of cyclic Hadamard difference sets are called *Hadamard sequences* [9], [33], [18], and these include the well-known m-sequences [7], [32], [10] and GMW sequences [30], [31], quadratic residue difference set sequences [34], [36], [1], [8], [20], Hall's sextic residue difference set sequences [13], [34], [1], [8], [19], twin-prime difference set sequences [34], [35], [1]. For the period of the form $2^m - 1$, some recent investigation reveals many more new families and their properties, including 3-term or 5-term sequences with or without Welch-Gong Transformations [11], [27], [12], sequences from 2-to-1 map [3], [26], [4], and hyperoval difference set sequences [6], [24], etc.

Let p be an odd prime and $F_p^* = F_p \backslash \{0\}$ be the cyclic multiplicative group mod p. In this paper, we will investigate mainly the characteristic sequences of cyclic difference sets which are some unions of cosets of the eth powers in F_p^*. These are called eth power residue cyclic difference sets [1], [2]. Existence and constructions for eth power residue cyclic difference sets are well summarized in [1], [2]. Following gives a complete solution toward this direction for $e \leq 12$. We will concentrate only on these cases because not much have been known for those $e > 12$.

Fact 1 (eth Power Residue Cyclic Difference Sets, [1, Th. 5.26]): Let $p = ef + 1$ be an odd prime, and let $e = 4, 6, 8, 10$, or 12. Let H_e be the set of all the eth powers in F_p^*. A union of cosets of H_e forms a nontrivial (v, k, λ) cyclic difference set D modulo p if and only if D consists of the following: **(Q)** the quadratic residues; **(H)** the Hall's set for $p = 4x^2 + 27$; **(B)** the biquadratic residues with or without $\{0\}$; **(O)** the octic residues with or without $\{0\}$; or **(D)** the union of the tenth powers and its coset uH_{10} for the special case $p = 31 = 10f + 1$ with

Manuscript received February 20, 2008; revised August 01, 2010; accepted August 21, 2010. Date of current version February 18, 2011. The work of G. Gong was supported by a NSERC Discovery Grant, Canada. The work of H.-Y. Song was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (2009-0083888). Part of the material in this paper was presented at the 2003 Workshop on Coding and Cryptography, INRIA, France, 2003.

Z. Dai and D. Ye are with the State Key Laboratory of Information Security, Graduate School of Chinese Academy of Sciences, 100039, Beijing, China (e-mail: daizongduo@is.ac.cn; ydf@is.ac.cn).

G. Gong is with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON N2L 3G1 Canada (e-mail: ggong@uwaterloo.ca).

H.-Y. Song is with the School of Electrical and Electronic Engineering, Yonsei University, Seoul, Korea (e-mail: hysong@yonsei.ac.kr).

Communicated by T. Fujiwara, Associate Editor for Complexity and Cryptography.

Digital Object Identifier 10.1109/TIT.2010.2103757

the generator $u = 11$ of F_{32}^*. Of these, **(Q)** and **(H)** are cyclic Hadamard difference sets with parameters $v = p, k = (p-1)/2$, and $\lambda = (p-3)/4$. ■

For their applications to streamcipher systems as pseudorandom sequence generators, the linear complexity of sequences play an important role [10], [29]. It is defined as the number of stages in the shortest linear feedback shift register that generates the sequence with a suitable initial loading. This is equivalent to the degree of the minimal polynomial of the sequence.

One could determine the linear complexity of a sequence without determining its trace representation. And the linear complexity of a sequence does not easily induce its trace representation whenever it does not admit 2 as a multiplier [7], [10]. On the other hand, when a trace representation of a sequence is explicitly determined, then the linear complexity can easily be computed. This leads us to not only try to determine the linear complexity of the various important sequences but further analyze them to the point where we could determine their trace representations. Furthermore, trace representation of a sequence gives very specific insight on its "easy" generation using one or more linear feedback shift registers for engineering applications [10]. This paper focuses on those cyclic difference sets described in **Fact** 1 which covers some important classes of sequences including cyclic Hadamard sequences [9], [33].

Some historical remark follows. Linear complexity of quadratic residue difference set sequences (also called as Legendre sequences) has been determined earlier in [36] and [28], later independently in [5]. Trace representation of these sequences of period p which are Mersenne prime was determined in [25], and for any odd prime p in [20] which reconfirmed the calculation of its linear complexity. Trace representation and linear complexity of Hall's sextic residue difference set sequences of period p which are Mersenne prime have been determined in [22]. It is well known that there are only three such primes, namely, 31, 127, and 131071. Linear complexity of these sequences in general has been determined in [19]. Trace representation of these sequences of period $p \equiv 7 \pmod 8$ is determined [21] and the case where $p \equiv 3 \pmod 8$ has been open quite for some time.

In this paper, we explicitly determine the trace representations of the characteristic sequences of all the cyclic difference sets mentioned in **Fact** 1, all of which are new, except for the cases of quadratic residue difference sets and of Hall's sextic residue difference sets for $p \equiv 7 \pmod 8$.

For this, we define eth power residue sequences of period p, which include all the binary characteristic sequences mentioned above, and reduce the problem of determining their trace representations to that of determining the values of the generating polynomials of cosets of H_e in F_p^* at some primitive pth root of unity, and some properties of these values are investigated. Based on these properties, trace representation and linear complexity of not only the characteristic sequences mentioned above, but of all the sixth power residue sequences are determined. Furthermore, we have determined the linear complexity of a nonconstant eth power residue sequences for any e to be either $p-1$ or p whenever $(e, (p-1)/n) = 1$, where n is the order of 2 mod p.

This paper is organized as follows. Section II develops general formula for trace representation of eth power residue sequences of period p. It has five subsections: (A) the notation and properties of parameters in this paper, (B) definitions of a defining pair of a sequence and more, (C) the linear space of binary eth power residue sequences over F_2, (D) introduction of e-tuples $\underline{c} = (c_0, c_1, \ldots, c_{e-1})$ where $c_i = c_{u^i}(\beta)$ for $0 \leq i < e$ which will be defined and investigated in full, and finally, (E) final formula in Theorem 5. All six Theorems in Section II are new. Section III discusses some applications of earlier development in Section II to some specific eth power residue sequences of period $p = 1 + ef$. These include (A) the case $e = 2$ (quadratic residues, known and rediscovered), (B) the case $e = 6$ (sextic residues, the case $p \equiv 7 \pmod 8$ is known but the case $p \equiv 3 \pmod 8$ is new), (C) the cases $e = 4, 8, 10$ in which eth residue cyclic difference set exists, which are all new. Finally, Section IV summarizes this paper and presents some remaining open problems.

II. General Formula for Trace Representation of eth Power Residue Sequences

A. Preliminary and Notations

We will begin by describing some notations for this paper. We let F_q be the finite field of size q for any prime or prime power q. We let p be an odd prime, and let $F_p^* = F_p \backslash \{0\}$, which is the cyclic multiplicative group mod p. We fix a pair (p, e) such that $p = 1 + ef$ with $f > 1$, and let $H_e = \{x^e \mid x \in F_p^*\}$, which is a subgroup of F_p^*. For any $k \in F_p^*$, the coset $kH_e = \{kx | x \in H_e\}$ of H_e will be called simply H_e-coset, and we write $kH_e = -H_e$ when $k = -1$. We let n be the order of 2 mod p, and let $c = (p-1)/n$. We let $d \triangleq \gcd(c, e)$, and let $e_1 = e/d$. We let $\delta(x)$ be 1 or 0 according to whether the integer x is odd or even, respectively, and let $\nu = (e/2)\delta(f)$. It is known that there exists a primitive pth root of unity in F_{2^n}, we let α be such a root, and let $< \alpha >^* = < \alpha > \backslash\{1\}$, where $< \alpha > = \{\alpha^i \mid 0 \leq i < p\}$. For any field F (say, $F = F_2$ or F_{2^n}) and any positive integer m we denote by $F^{(m)}$ the set of all possible m-tuples over F, i.e., $F^{(m)} = \{\underline{r} = (r_0, r_1, \ldots, r_{m-1}) | r_i \in F\}$, and denote by $w_H(\underline{r})$ the Hamming weight of any tuple $\underline{r}$, i.e., the total number of nonzero elements among $r_i, 0 \leq i < m$. Denote $\mathrm{Tr}_1^n(x) = \sum_{0 \leq i < n} x^{2^i}$, which is the trace function from F_{2^n} to F_2. We denote the algebraic closure of F_2 by $\overline{F}_2$.

We list some properties of the parameters mentioned above for later use without proof. Some items are well known, and others can be proved easily (refer to [14]).

Lemma 1 (Properties of the Parameters): Let u be a generator of the cyclic group F_p^*.

1. β is a primitive pth root of unity in $\overline{F}_2$ if and only if $\beta \in < \alpha >^*$.
2. $H_e = < u^e >$ and $F_p^* = \cup_{0 \leq i < e} u^i H_e$.
3. $< 2 > = < u^c > \subseteq F_p^*$ and $F_p^* = \cup_{0 \leq i < c} u^i < 2 >$.
4. $e_1 | n$, and hence, $F_{2^{e_1}} \subseteq F_{2^n}$.
5. $-H_e = u^\nu H_e$, where $\nu = \frac{e\delta(f)}{2}$, that is $\nu = 0$ if $f = 0 \pmod 2$, and $\nu = \frac{e}{2}$ if $f = 1 \pmod 2$.

6. Denote by $\overline{k}$ the element kH_e in the quotient group F_p^*/H_e. Then
$$\mathrm{ord}(\overline{2}) = \mathrm{ord}(\overline{u^d}) = e_1,$$
in other words, $2^{e_1} \in H_e$ but $2^i \notin H_e$ if $0 < i < e_1$. In particular, $< \overline{2} > = < \overline{u^d} > \subseteq F_p^*/H_e$, where $\mathrm{ord}(\overline{2})$ denotes the order of $\overline{2}$ in F_p^*/H_e, and $< \overline{2} >$ denotes the group generated by $\overline{2}$ in F_p^*/H_e. Similarly for $\mathrm{ord}(\overline{u^d})$ and $< \overline{u^d} >$. As a consequence, there exists an integer λ such that $u^d H_e = 2^\lambda H_e$ and $\gcd(\lambda, e_1) = 1$, and λ is uniquely determined up to modulo e_1 by u when $e_1 > 1$. Denote this λ by λ_u, and denote by μ_u the inverse of λ_u modulo e_1, then $u^{d\mu_u} H_e = 2H_e$. Moreover, let m be the integer with the property $\gcd(m, p-1) = 1$ and $m = \mu_u \pmod{e_1}$ (it is known that such m does exists), then $v = u^m$ is a generator of F_p^* and $\lambda_v = \mu_v = 1$. When $e_1 = 1$ or $e = d$, we have $2H_e = H_e = u^d H_e$, and hence we may put $\lambda = \mu = 1$.
7. d is the maximal integer dividing e such that 2 is a dth power in the group F_p^*.

B. Defining Pair, Trace Representation, Minimal Polynomial, and Linear Complexity

In the remaining of this paper, we keep all the notations in Section II, unless specified otherwise. In this paper we consider only binary sequences of period p. Let $\mathbf{s}$ be such a sequence, we denote its tth element by $\mathbf{s}(t) (\in F_2)$, and denote its minimal polynomial (MP) by $m_{\mathbf{s}}(x)$, denote its linear complexity (LC) by $\mathrm{LC}(\mathbf{s})$. In this section, we will define "*defining pair*" for $\mathbf{s}$, and show that the trace representation (TR) of $\mathbf{s}$ and both $m_{\mathbf{s}}(x)$ and $\mathrm{LC}(\mathbf{s})$ can easily be obtained from the defining pair of $\mathbf{s}$.

Given a binary sequence $\mathbf{s} = \{\mathbf{s}(t) | t \geq 0\}$ of period p and a primitive pth root β of unity (*i.e.*, $\beta \in < \alpha >^*$), we have a function $g(x)$ from $< \alpha >$ to F_2 as follows:
$$g(\beta^t) = \mathbf{s}(t) \quad \forall\, t \geq 0. \tag{3}$$
Recall that n is the order of 2 mod p. It is clear that $g(x)$ can be represented as a polynomial with coefficients from F_{2^n}, which is a function from F_{2^n} to F_2[23].

Definition 1 (Defining Pair of Sequences): The polynomial $g(x)$ together with β satisfying (3) form a pair $(g(x), \beta)$, which will be called a **defining pair** of the sequence s; and β will be called the **defining element**, and $g(x)$ the **defining polynomial** of s corresponding to β.

Note that if $g(x)$ is a defining polynomial of s corresponding to β, then $(g(x) + (x^p - 1)f(x), \beta)$ is also a defining polynomial of s corresponding to β for any $f(x)$ with coefficients in F_{2^n}. Therefore, the defining polynomial $g(x)$ can be considered as a residue class of polynomials modulo $x^p - 1$. Moreover, observe that the defining polynomial of s corresponding to a given defining element β is uniquely determined up to modulo $x^p - 1$ by the following lemma.

Lemma 2: Let $f(x) = \sum_i f_i x^i$ and $g(x) = \sum_i g_i x^i$ be two polynomials over F_{2^n}, and let β be a primitive pth root of unity, i.e., $\beta \in < \alpha >^*$. If $f(\beta^t) = g(\beta^t) \ \ \forall\, t \geq 0$, then $f(x) = g(x) \pmod{x^p - 1}$.

The index t in $\mathbf{s}(t)$ or in β^t or in $x^t \pmod{x^p - 1}$ can be considered as an element in F_p, since $\mathbf{s}(t) = \mathbf{s}(t + pk)$, $\beta^{t+pk} = \beta^t$ and $x^{t+pk} = x^t \pmod{x^p - 1}$ for any integer k. Therefore, for the sake of convenience, we will agree the following equalities. Here, $a_i \in F_{2^n}$ is arbitrary
$$\sum_{0 \leq i < p} a_i x^i = \sum_{i \in F_p} a_i x^i \pmod{x^p - 1}$$
$$\sum_{0 \leq i < p} a_i \beta^i = \sum_{i \in F_p} a_i \beta^i$$
which make sense and would not cause any confusion.

Definition 2 (Hamming Weight of Polynomials mod $x^p - 1$): For a polynomial residue class $g(x) = \sum_{0 \leq i < p} r_i x^i \pmod{x^p - 1}$, the total number of the nonzero coefficients r_i, $0 \leq i < p$, will be called the Hamming weight of the class $g(x) \pmod{x^p - 1}$, and will be denoted by $w_H(g(x))$ or simply by $w_H(g)$.

Lemma 3 (Defining Pairs Determining MP, LC, and TR): Let u be a generator of F_p^*, and let $\beta \in < \alpha >^*$ be a primitive element, and let $p_i(x)$ be the irreducible polynomial over F_2 with β^{u^i} as a root. Let $(g(x), \beta)$ be a defining pair of a given binary sequence $\mathbf{s} = \{\underline{s}(t) | t \geq 0\}$ of period p, and let $g(x) = \sum_{i \in F_p} r_i x^i \pmod{x^p - 1}$. Then $r_i \in F_{2^n} \ \forall i \in F_p$, and $r_0 \in F_2$, and $\mathbf{s}$ has a trace representation as follows:
$$\mathbf{s}(t) = r_0 + \sum_{0 < i \leq c} \mathrm{Tr}_1^n(r_{u^i} \beta^{tu^i}), \quad t \geq 0, \tag{4}$$
where β^{u^i} is not conjugate to the element β^{u^j} for $0 \leq i < j < c$; and
$$m_{\mathbf{s}}(x) = (x-1)^{\delta(r_0)} \times \prod_{\substack{r_{u^i} \neq 0 \\ 0 \leq i < c}} p_i(x); \tag{5}$$
$$\mathrm{LC}(\mathbf{s}) = w_H(g(x)). \tag{6}$$

Proof: The proof can be done in the same way as in [10, Ch. 6]. ■

C. Space of eth Power Residue Sequences of Period p

Definition 3 (eth Power Residue Sequences): We say a binary sequence $\mathbf{s} = \{\mathbf{s}(t) | \, t \geq 0\}$ of period $p = ef + 1$ is an eth power residue sequence if $\mathbf{s}(t)$ is constant on each of the H_e-cosets in F_p^*.

Three examples follow. Given $k \in F_p^*$, the coset kH_e determines an eth power residue sequence $\mathbf{b}_k = \{\mathbf{b}_k(t) | t \geq 0\}$, where $\mathbf{b}_k(t) = 1 \Leftrightarrow t \in kH_e$. We call $\mathbf{b}_k$ a single coset sequence. The index k can be also understood as the coset kH_e, since $\mathbf{b}_k = \mathbf{b}_j$ whenever $kH_e = jH_e$. There exist totally e single coset sequences, and they can be represented by $\mathbf{b}_{u^i}$, $0 \leq i < e$, where u is any given generator of F_p^*. The sequence $\underline{\delta} = \{\underline{\delta}(t) | t \geq 0\}$, $\underline{\delta}(t) = 1 \Leftrightarrow t = 0 \pmod{p}$, is an eth power residue sequence for any e, which we call δ-sequence. The sequence $\underline{1} = \{\underline{1}(t) | t \geq 0\}$, $\underline{1}(t) = 1 \ \forall\, t \geq 0$, is an eth power residue sequence for any e, which we call all-1 sequence.

Let u be a generator of F_p^*. Then it is clear that

$$\underline{1} = \underline{\delta} + \sum_{0\le i<e} \mathbf{b}_{u^i}. \tag{7}$$

For any given eth power residue sequence $\mathbf{s} = \{\mathbf{s}(t) | t \ge 0\}$, it is also clear that

$$\begin{aligned} &\mathbf{s} = a_*\underline{\delta} + \sum_{0\le i<e} a_i \mathbf{b}_{u^i} \\ \Leftrightarrow \quad &\mathbf{s}(t) = \begin{cases} a_i & \text{if } t \in u^i H_e \\ a_* & \text{if } t = 0 \pmod{p} \end{cases} \end{aligned} \tag{8}$$

Theorem 1 (Space Spanned by eth Power Residue Sequences): The set of all the eth power residue sequences of period $p\ (= 1 + ef)$, denoted by $\mathcal{L}$, is a linear space over F_2 of dimension $e + 1$, and $\{\mathbf{b}_{u^i} | 0 \le i < e\} \cup \{\underline{1}\}$ is a basis of $\mathcal{L}$ over F_2 for any given generator u of F_p^*. In particular, any eth power residue sequence $\mathbf{s}$ can be uniquely expressed as either $\mathbf{s}_{\underline{a}}$ or $\underline{1} + \mathbf{s}_{\underline{a}}$, where $\mathbf{s}_{\underline{a}} = \sum_{0\le i<e} a_i \mathbf{b}_{u^i}$, $\underline{a} = (a_0, a_1, \ldots, a_{e-1}) \in F_2^{(e)}$.

Proof: Obvious. We note that the basis of $\mathcal{L}$ over F_2 could be alternatively taken as $\{\mathbf{b}_{u^i} | 0 \le i < e\} \cup \{\underline{\delta}\}$, and then any eth power residue sequence $\mathbf{s}$ can be uniquely expressed as in (8). ■

D. Generating Polynomials of Cosets and Related e-Tuples

Definition 4 (Generating Polynomials of Cosets): Given $k \in F_p^*$, the **generating polynomial** of the coset kH_e is defined as

$$\sum_{i\in kH_e} x^i \pmod{x^p - 1} \tag{9}$$

which will be denoted by $c_k(x)$.

Definition 5 (e-Tuples and Matrices Related to Cosets): The e generating polynomials will be ordered as an e-**tuple** according to any given generator u of F_p^*, denoted by $Y_u(x)$, and written as a column vector

$$Y_u(x) = (c_{u^0}(x), c_{u^1}(x), \ldots, c_{u^{e-1}}(x))^\tau \tag{10}$$

where τ is a transpose. Correspondingly, the e elements $c_{u^i}(\beta)$, $0 \le i < e$, which are values of $c_{u^i}(x)$ at $x = \beta \in <\alpha>^*$, will also be ordered as an e-**tuple** over F_{2^n} (since $\beta \in F_{2^n}$) as

$$\mathbf{c}_u(\beta) = (c_{u^0}(\beta), c_{u^1}(\beta), \ldots, c_{u^{e-1}}(\beta)). \tag{11}$$

Based on the e-tuple $\mathbf{c}_u(\beta)$, we define an $e \times e$ **symmetric matrix** as follows:

$$C_u(\beta) = (c_{i,j}), \quad c_{i,j} = c_{u^{i+j}}(\beta), \quad 0 \le i, j < e. \tag{12}$$

It is clear that the index i in both $c_{u^i}(x) \pmod{x^p - 1}$ and $c_{u^i}(\beta)$ in the above definition can be understood as a number modulo e, since $u^{i+e}H_e = u^i H_e$, hence $c_{u^{i+e}}(x) = c_{u^i}(x) \pmod{x^p - 1}$ and $c_{u^{i+e}}(\beta) = c_{u^i}(\beta)$. We now state and prove some properties of these in the following.

Lemma 4:

1. Let $k, l \in F_p^*$, then we have the following:
   (a) $c_k(x)^2 = c_k(x^2) \pmod{x^p - 1}$.
   (b) $c_k(x^l) = c_{kl}(x) \pmod{x^p - 1}$. As a consequence, $c_k(x^l) = c_k(x^j) \pmod{x^p - 1}$ whenever $lH_e = jH_e$.
   (c) $c_k(x)^{2^{e_1}} = c_k(x) \pmod{x^p - 1}$.
2. Let uH_e ($u \in F_p^*$) be a generator of F_p^*/H_e, and let $\lambda = \lambda_u$, $\mu = \mu_u$, where λ_u and μ_u are defined in Lemma 1. Then
   (a) $\sum_{0\le i<e} c_{u^i}(x) = \sum_{0<j<p} x^j \pmod{x^p - 1}$;
   (b) $c_{u^{i+dj}}(x) = c_{u^i}(x)^{2^{\lambda j}} \pmod{x^p - 1}$, $\forall i,\ j$ and $c_{u^{i+d\mu j}}(x) = c_{u^i}(x)^{2^j} \pmod{x^p - 1}$, $\forall i,\ j$. (This will be called the **conjugacy property** of the tuple $Y_u(x)$ in Definition 5.)
3. $w_H(\underline{r}Y_u(x)) = fw_H(\underline{r})$ for any $\underline{r} \in F_{2^n}^{(e)}$.

Proof:

1.

$$\text{(a)}\quad c_k(x)^2 = \left(\sum_{z\in H_e} x^{kz}\right)^2 = \sum_{z\in H_e} x^{2kz} = c_k(x^2) \pmod{x^p - 1}.$$

$$\text{(b)}\quad c_k(x^l) = \sum_{z\in H_e} x^{lkz} = c_{kl}(x) \pmod{x^p - 1}.$$

$$\begin{aligned} \text{(c)}\quad c_k(x)^{2^{e_1}} &= c_k(x^{2^{e_1}}) = c_{k2^{e_1}}(x) \\ &= c_k(x) \pmod{x^p - 1} \\ &\quad \text{(since } 2^{e_1} \in H_e\text{)}. \end{aligned}$$

2.

$$\text{(a)}\quad \sum_{0\le i<e} c_{u^i}(x) = \sum_{0\le i<e}\sum_{z\in H_e} x^{u^i z} = \sum_{0<j<p} x^j \pmod{x^p - 1}.$$

From $2^{e_1} \in H_e$ and $u^d H_e = 2\lambda H_e$ (Lemma 1) and the above item 1, we have

$$\begin{aligned} \text{(b)}\quad c_{u^{i+dj}}(x) &= c_{u^i 2^{\lambda j}}(x) = c_{u^i}(x^{2^{\lambda j}}) \\ &= c_{u^i}(x)^{2^{\lambda j}} \pmod{x^p - 1}; \\ c_{u^{i+d\mu j}}(x) &= c_{u^i 2^{\lambda\mu j}}(x) = c_{u^i 2^j}(x) = c_{u^i}(x^{2^j}) \\ &= c_{u^i}(x)^{2^j} \pmod{x^p - 1}. \end{aligned}$$

3. Let $\underline{r} = (r_0, r_1, \ldots, r_{e-1})$. Note that $H_e = \{u^{ej} | 0 \le j < f\}$, we have

$$c_{u^i}(x) = \sum_{0\le j<f} x^{u^{i+ej}}$$

and

$$\underline{r}Y_u(x) = \sum_{0\le i<e} r_i c_{u^i}(x) = \sum_{\substack{0\le i<e \\ 0\le j<f}} r_i x^{u^{i+ej}}$$

then

$$\begin{aligned} w_H(\underline{r}Y_u(x)) &= \sum_{\substack{0\le i<e\\ r_i\neq 0}} w_H(\sum_{0\le j<f} x^{u^{i+ej}}) \\ &= f\sum_{\substack{0\le i<e\\ r_i\neq 0}} 1 = f w_H(\underline{r}). \end{aligned}$$

■

Now, consider the set $\mathcal{C}$ of the e-tuples $\mathbf{c}_u(\beta)$ over all u and β. That is,

$$\mathcal{C} \triangleq \{\mathbf{c}_u(\beta) \mid <u>=F_p^*,\ \beta \in <\alpha>^*\}. \tag{13}$$

Take a generator uH_e ($u \in F_p^*$) of F_p^*/H_e, it is clear that

$$\mathcal{C} \triangleq \{\mathbf{c}_{u^i}(\beta^{u^j}) \mid 0\le i<e,\ \gcd(i,e)=1,\ 0\le j<e\}.$$

Definition 6 (Cyclic Shifts and Decimation on e-Tuples): Let Ω be the set of all possible e-tuples over F_{2^n}. It is clear that $\mathcal{C} \subseteq \Omega$. Let $\mathbf{x}=(x_0,x_1,\ldots,x_{e-1}) \in \Omega$. We define L to be the **cyclically left-shift** operator and D_λ for $1 \le \lambda < e$ and $(\lambda,e)=1$ to be the λ-**decimation operator** over Ω given as

$$L\mathbf{x} = (x_1,x_2,\ldots,x_{e-1},x_0) \tag{14}$$

$$D_\lambda \mathbf{x} = (x_0,x_\lambda,x_{2\lambda},\ldots,x_{(e-1)\lambda}). \tag{15}$$

It is clear that both the operators L and D_λ are invertible. Let G be the group generated by the operators L and all D_λ, $(\lambda,e)=1$. It can be easily checked that $D_\lambda L^k = L^{\lambda^{-1}k}D_\lambda$, where λ^{-1} is taken mod e, and the size of G is $e\phi(e)$, where ϕ is the Euler's-ϕ-function. It is known [14] that the elements in Ω are divided into some equivalent classes under the action of the group G, and that two elements $\mathbf{x}$ and $\mathbf{y}$ in Ω are equivalent under the action of the group G (in short, G-**equivalent**, and denoted by $\mathbf{x} \sim \mathbf{y}$) if and only if there exists $\sigma \in G$ such that $\sigma(\mathbf{x}) = \mathbf{y}$.

Lemma 5 ($\mathcal{C}$ is an Equivalent Class): We have

$$L^i \mathbf{c}_u(\beta) = \mathbf{c}_u(\beta^{u^i}) \in \mathcal{C},\ \forall\, i; \tag{16}$$

$$D_\lambda(\mathbf{c}_u(\beta)) = \mathbf{c}_{u^\lambda}(\beta) \in \mathcal{C},\ \forall \lambda : \gcd(\lambda,e)=1. \tag{17}$$

Furthermore, the set $\mathcal{C}$ is an equivalent class under the action of the group G.

Proof: We have, by Lemma 4

$$\begin{aligned} L^i(\mathbf{c}_u(\beta)) &= (c_{u^0}(\beta^{u^i}), c_{u^1}(\beta^{u^i}),\ldots,c_{u^{e-1}}(\beta^{u^i})) \\ &= \mathbf{c}_u(\beta^{u^i}) \in \mathcal{C} \end{aligned}$$

and

$$\begin{aligned} D_\lambda(\mathbf{c}_u(\beta)) &= (c_{u^0}(\beta), c_{u^\lambda}(\beta), c_{u^{2\lambda}}(\beta),\ldots,c_{u^{(e-1)\lambda}}(\beta)) \\ &= \mathbf{c}_{u^\lambda}(\beta) \in \mathcal{C}. \end{aligned}$$

This shows that the set $\mathcal{C}$ is closed under the action of the group G.

Now, it is enough to show that $\mathbf{c}_u(\beta) \sim \mathbf{c}_v(\beta')$ for any two generators uH_e and vH_e of F_p^*/H_e and any two elements β and β' in $<\alpha>^*$. We may assume $vH_e = u^\lambda H_e$ for some λ with $(\lambda,e)=1$, and assume $\beta' = \beta^{v^k}$ for some k. Then, from (16) and (17) we have

$$\begin{aligned} \mathbf{c}_v(\beta') &= \mathbf{c}_v(\beta^{v^k}) = L^k(\mathbf{c}_v(\beta)) = L^k(\mathbf{c}_{u^\lambda}(\beta)) \\ &= L^k D_\lambda(\mathbf{c}_u(\beta)) \end{aligned}$$

which proves $\mathbf{c}_u(\beta) \sim \mathbf{c}_v(\beta')$. ■

Theorem 2 (Properties of $\mathbf{c}_u(\beta)$): Let uH_e be a given generator of F_p^*/H_e, and let $\beta \in <\alpha>^*$. Denote by I_m the identity matrix of size m for any positive integer m, and denote by $I_e^{(d)}$ the matrix which is made of the first d columns of I_e, and denote by J_e the all-1 matrix of size $e \times e$. Denote simply

$$\begin{aligned} &c_i = c_{u^i}(\beta),\ \ \underline{c} = (c_0,c_1,\ldots,c_{e-1}) = \mathbf{c}_u(\beta) \\ &C = C_u(\beta),\ \ \lambda = \lambda_u,\ \ \mu = \mu_u,\ \ \nu = \frac{e\delta(f)}{2} \end{aligned}$$

where $\mathbf{c}_u(\beta)$, $C_u(\beta)$ are defined in Definition 5, and λ_u, μ_u are defined in Lemma 1. Let Γ be the square matrix of size e given as

$$\Gamma \triangleq \begin{pmatrix} \mathbf{0} & 1 \\ I_{e-1} & \mathbf{0}^\tau \end{pmatrix} \tag{18}$$

where τ is a transpose and $\mathbf{0}$ is the all-0 row vector of length $e-1$. Then

1. $\sum_{0\le i<e} c_i = 1$. In particular, $\underline{c} \neq (0,0,\ldots,0)$.
2. $c_i \in F_{2^{e_1}}, 0 \le i < e$.
3. $c_{i+dj} = c_i^{2^{\lambda j}}$ and $c_{i+d\mu j} = c_i^{2^j}, 0 \le i < d,\ 0 \le j < e_1$.
4. $\Gamma^\nu C^2 = fJ_e + I_e$. In other words, $\sum_{0\le i<e} c_i c_{i+\nu+j} = f + \delta(j)$ for all $0 \le j < e$. In particular, the matrix C is invertible. Furthermore, if we let $\overline{C} = C + J_e$, then $\Gamma^\nu \overline{C}^2 = fJ_e + I_e$.
5. The tuple $\underline{c}$ has no "period" less than e.
6. Let $\epsilon_i = Tr_1^{e_1}(c_i) \in F_2$ for all i, and let $E = (\epsilon_{i,j})$ be a square matrix of size d, where $\epsilon_{i,j} = \epsilon_{i+j}$. Then
   (a) $\epsilon_i = Tr_1^{e_1}(c_i) = \sum_{0\le j<e_1} c_{i+dj}$.
   (b) $\epsilon_{i+d} = \epsilon_i \quad \forall i$.
   (c) $\sum_{0\le i<d} \epsilon_i = 1$.
   (d) E is invertible.
   (e) In the case when $d > 1$, there exists at least one i such that $\epsilon_i = 0$ among $\epsilon_j, 0 \le j < d$.
7. $w_H(\underline{c}) = e_1 W_d$ and $W_d \ge 1$, where $W_d \triangleq w_H(\underline{c}I_e^{(d)})$ is a constant on the set $\mathcal{C}$, where $\mathcal{C}$ is defined in (13). In particular, $W_1 = 1$ and $w_H(\underline{c}) = e$ when $d = 1$.

Proof:

1. From $\sum_{0\le i<e} c_{u^i}(x) = \sum_{0<j<p} x^j \pmod{x^p - 1}$ (Lemma 4) we get
$$\sum_{0\le i<e} c_i = \sum_{0\le i<e} c_{u^i}(\beta) = \sum_{0<j<p} \beta^j = 1.$$
2. From (c) of item 1 in Lemma 4, we have $c_{u^i}(x)^{2^{e_1}} = c_{u^i}(x) \pmod{x^p - 1}$, and then $c_{u^i}(\beta)^{2^{e_1}} = c_{u^i}(\beta)$, hence $c_i = c_{u^i}(\beta) \in F_{2^{e_1}}$.
3. From (b) of item 2 in Lemma 4 we have, for $0 \le i < d,\ \ 0 \le j < e_1$
$$\begin{aligned} c_{u^{i+dj}}(x) &= c_{u^i}(x)^{2^{\lambda j}} \pmod{x^p - 1} \\ c_{u^{i+d\mu j}}(x) &= c_{u^i}(x)^{2^j} \pmod{x^p - 1} \end{aligned}$$

which leads to the desired result by substituting β into x.

4. Let $C^* = \Gamma^\nu C = (c^*_{i,j})$, then $C^*C = \Gamma^\nu C^2$. Let $C = (c_{i,j})$, we have $c_{i,j} = c_{i+j}$ by definition. From the definition we have

$$c^*_{i,j} = c_{\nu+i,j} = c_{\nu+i+j} = c_{u^{\nu+i+j}}(\beta).$$

Then, based on the fact that $-H_e = u^\nu H_e$ (Lemma 1), we see

$$c^*_{i,j} = c_{u^{\nu+i+j}}(\beta) = c_{-u^{i+j}}(\beta), \quad 0 \le i,j < e. \qquad (19)$$

Let $C^*C = (d_{i,k})$, then it is enough to prove $d_{i,k} = f + \delta_{i,k}, \forall i,k$, where $\delta_{i,k}$ is the the Kronecker delta symbol: $\delta_{i,k} = 1$ if $i = k$, and $\delta_{i,k} = 0$ if $i \neq k$. From (19), we see $\Gamma^\nu C = (c^*_{i,j})$, where $c^*_{i+j} = c_{-u^{i+j}}(\beta)$. Then

$$\begin{aligned} d_{i,k} &= \sum_{0\le j<e} c^*_{i,j}c_{j,k} = \sum_{0\le j<e} c_{-u^{i+j}}(\beta)c_{u^{j+k}}(\beta)\\ &= \sum_{0\le j<e}\left[\sum_{x\in H_e}\beta^{-u^{i+j}x}\sum_{y\in H_e}\beta^{u^{j+k}y}\right]\\ &= \sum_{0\le j<e}\;\sum_{x\in H_e, z\in H_e}\beta^{u^{j+k}x(z-u^{i-k})}\\ &\qquad (\text{use}\quad z \triangleq yx^{-1})\\ &= \sum_{0\le j<e}\;\sum_{x\in H_e,z\in H_e}\gamma_z^{u^j x}\\ &\qquad(\text{use}\quad \gamma_z \triangleq \beta^{u^k(z-u^{i-k})})\\ &= \sum_{w\in F_p^*, z\in H_e}\gamma_z^w \qquad (\text{use}\quad w\triangleq u^j x). \end{aligned}$$

It is easy to see that, for $z \in H_e$

$$\begin{aligned} ``\gamma_z = 1" &\Rightarrow ``\beta^{u^k(z-u^{i-k})} = 1"\\ &\Rightarrow ``u^{i-k} = z \in H_e"\\ &\Rightarrow ``i = k \pmod{e},\quad u^{i-k}=z"\\ &\Rightarrow ``i=k,\quad z=u^0=1"\end{aligned}$$

and the inverse is obvious. So we get, for $z \in H_e$

$$``\gamma_z = 1" \Leftrightarrow ``i=k, z=1".$$

Now we evaluate the value of $c^*_{i,k}$ separately for the case $i\neq k$ and the case $i=k$, with the fact that $\gamma_z \in <\alpha>$. In the case when $i\neq k$, we have $\delta_{i,k}=0$ and $\gamma_z \neq 1$ for any $z\in H_e$. Therefore

$$\begin{aligned} d_{i,k} &= \sum_{w\in F_p^*, z\in H_e}\gamma_z^w\\ &= \sum_{z\in H_e}\sum_{w\in F_p^*}\gamma_z^w\\ &= \sum_{z\in H_e} 1 = f = f+\delta_{i,k}. \end{aligned}$$

In the case when $i=k$, we have $\delta_{i,k}=1$ and we distinguish whether γ_z is 1 ($z=1$) or not ($z\neq 1$). Therefore

$$\begin{aligned} d_{i,k} &= \sum_{w\in F_p^*,z\in H_e}\gamma_z^w\\ &= \sum_{\substack{z=1\\w\in F_p^*}} 1 + \sum_{\substack{1\neq z\in H_e\\ w\in F_p^*}}\gamma_z^w\\ &= p-1+\sum_{\substack{z\neq 1\\w\in F_p^*}}\gamma_z^w\\ &= f-1 = f+\delta_{i,k} \end{aligned}$$

hence $\Gamma^\nu C^2 = C^*C = (d_{i,k}) = (f+\delta_{i,k}) = fJ_e + I_e$. The equivalent expression comes easily from the observation that $c^*_{i,j} = c_{i+\nu,j} = c_{i+\nu+j}$. To show that $\Gamma^\nu\overline{C}^2 = fJ_e+I_e$, it is enough to show that $\overline{C}^2 = C^2$. Recall that C is over F_{2^n}, i.e., the field of characteristic 2, and we restrict the value of e be even from 2 to 12. Therefore

$$\overline{C}^2 = (C+J_e)^2 = C^2 + CJ_e + J_eC + J_e^2 = C^2$$

since $CJ_e = (\sum_{0\le i<e} c_i)J_e = J_eC$ and $J_e^2 = 0$.

5. Assume the period of $\underline{c}$ is less than e, say, equal to k. Then the kth row of C will be the same as the zeroth row of C, and, hence, C is not invertible, a fact which contradicts to the above item 4.

6. Keep the notations in the item 3.

   a) From the fact that $c_{i+d\mu j} = c_i^{2^j}$ (item 3), we see

$$\begin{aligned} \epsilon_i &= Tr_1^{e_1}(c_i) = \sum_{0\le j<e_1} c_i^{2^j}\\ &= \sum_{0\le j<e_1} c_{i+d\mu j} = \sum_{0\le j<e_1} c_{i+dj}. \end{aligned}$$

   b) From the definition of ϵ_i and the fact that $c_{i+dj} = c_i^{2^{\lambda j}}$ (item 3) , we see

$$\epsilon_{i+dj} = Tr_1^{e_1}(c_{i+dj}) = Tr_1^{e_1}(c_i^{2^{\lambda j}}) = Tr_1^{e_1}(c_i) = \epsilon_i.$$

   c) From item 1 above,

$$\sum_{0\le j<d}\epsilon_i = \sum_{0\le j<d}\;\sum_{0\le j<e_1} c_{i+dj} = \sum_{0\le j<e} c_i = 1.$$

   d) Note that

$$(\underbrace{E\,|\,E\,|\,\ldots\,|\,E}_{e_1}) = (\underbrace{I_d\,|\,I_d\,|\,\ldots\,|\,I_d}_{e_1})C$$

   and the fact that C is an invertible matrix, we get

$$\begin{aligned} \text{rank}(E) &= \text{rank}(E\,|\,E\,|\,\ldots\,|\,E)\\ &= \text{rank}((I_d\,|\,I_d\,|\,\ldots\,|\,I_d)C)\\ &= \text{rank}((I_d\,|\,I_d\,|\,\ldots\,|\,I_d)) = d. \end{aligned}$$

e) If all $\epsilon_i = 1$, then $E = J_d$, and then $\mathrm{rank}(E) = \mathrm{rank}(J_d) = 1$. But from the above (d), we see $\mathrm{rank}(E) = d$, a contradiction to the assumption $d > 1$.

7. Since $w_H(\mathbf{c}_u(\beta))$ is unchanged under the action of the operators L and D_λ, $\gcd(\lambda, e_1) = 1$, we see $w_H(\mathbf{c}_u(\beta))$ is a constant on the set $\mathcal{C}$ from Lemma 5. Observe that $\underline{c}I_e^{(d)} = (c_0, c_1, \ldots, c_{e-1})I_e^{(d)} = (c_0, c_1, \ldots, c_{d-1})$. From the conjugacy property of the tuple $\mathbf{c}_u(\beta)$ (the item 3 above), we see that $w_H(\mathbf{c}_u(\beta)) = e_1 w_H(\mathbf{c}_u(\beta)I_e^{(d)})$, and hence, $w_H(\mathbf{c}_u(\beta)I_e^{(d)})$ is also a constant on the set $\mathcal{C}$. From the item 1 above we see $\underline{c} \neq (0, 0, \ldots, 0)$, hence, $w_H(\mathbf{c}_u(\beta)I_e^{(d)}) \geq 1$. In particular, when $d = 1$, we have $e_1 = e$, and $1 \geq w_H(\mathbf{c}_u(\beta)I_e^{(1)}) = w_H(c_0) \geq 1$, then $w_H(\mathbf{c}_u(\beta)I_e^{(1)}) = 1$, hence we have $w_H(\mathbf{c}) = e_1 \times 1 = e$. ■

The property stated in the item 3 of Theorem 2 will be called the **conjugacy property** of the e-tuple vector $\mathbf{c}_u(\beta) = (c_{u^0}(\beta), c_{u^0}(\beta), \ldots, c_{u^{e-1}}(\beta))$ in Definition 5, which is denoted by $\mathbf{c}_u(\beta) = \underline{c} = (c_0, c_1, \ldots, c_{e-1})$ in Theorem 2. We will use this notation in the remaining of this paper. We will further analyze the conjugacy properties of this e-tuple vector.

Lemma 6: Let $\underline{a} \in F_2^{(e)}$ and $\underline{a}C = (r_0, r_1, \ldots, r_{e-1})$. Then

1. The tuple $\underline{a}C$ has the conjugacy property in the sense as shown

$$r_{i+dj} = r_i^{2^{\lambda j}}, \quad r_{i+d\mu j} = r_i^{2^j} \quad \forall j.$$

2. $w_H(\underline{a}C) = e_1 w_H((r_0, r_1, \ldots, r_{d-1}))$.
3. $(L\underline{a})C = L^{-1}(\underline{a}C)$.

Proof: We will show only the first item. The remaining ones are easy to check from this. Note

$$r_i = \sum_{0 \leq k < e} a_k c_{k,i} = \sum_{0 \leq k < e} a_k c_{k+i}, \quad 0 \leq i < e.$$

From the conjugacy property of $\underline{c}$ (refer to the item 3 of Theorem 2), we have

$$\begin{aligned} r_{i+dj} &= \sum_{0 \leq k < e} a_k c_{k,i+dj} = \sum_{0 \leq k < e} a_k c_{k+i}^{2^{\lambda j}} \\ &= \left(\sum_{0 \leq k < e} a_k c_{k+i} \right)^{2^{\lambda j}} = r_i^{2^{\lambda j}}, \\ &\text{and} \\ r_{i+d\mu j} &= \sum_{0 \leq k < e} a_k c_{k,i+d\mu j} = \sum_{0 \leq k < e} a_k c_{k+i}^{2^j} \\ &= \left(\sum_{0 \leq k < e} a_k c_{k+i} \right)^{2^j} = r_i^{2^j}. \end{aligned}$$

■

Lemma 7: Let

$$\begin{aligned} \xi(\underline{a}) &= \underline{a}CI_e^{(d)}, \\ \xi_\nu(\underline{a}) &= \underline{a}\Gamma^\nu CI_e^{(d)}, \\ \zeta(\underline{a}) &= \sum_{0 \leq i < e} a_i c_i \end{aligned}$$

for all $\underline{a} = (a_0, a_1, \ldots, a_{e-1}) \in F_2^{(e)}$. Then both ξ and ξ_ν are bijective maps from $F_2^{(e)}$ to $F_{2^{e_1}}^{(d)}$; and ζ is a surjective map from $F_2^{(e)}$ to $F_{2^{e_1}}$.

Proof: Denote $\underline{r}^{2^j} = (r_0^{2^j}, r_1^{2^j}, \ldots, r_{d-1}^{2^j})$ for all $\underline{r} = (r_0, r_1, \ldots, r_{d-1}) \in F_{2^{e_1}}^{(d)}$. For any $\underline{a} \in F_2^{(e)}$ and any $\underline{b} \in F_2^{(e)}$, from the conjugacy property of $\underline{a}C$ (Lemma 6), we have

$$\begin{aligned} \underline{a}C &= (\underline{r}, \underline{r}^{2^\lambda}, \ldots, \underline{r}^{2^{\lambda(e_1-1)}}), \text{ where} \\ \underline{r} &= (r_0, r_1, \ldots, r_{d-1}) = \xi(\underline{a}) = \underline{a}CI_e^{(d)} \qquad (20) \\ \underline{b}C &= (\underline{s}, \underline{s}^{2^\lambda}, \ldots, \underline{s}^{2^{\lambda(e_1-1)}}), \text{ where} \\ \underline{s} &= (s_0, s_1, \ldots, s_{d-1}) = \xi(\underline{b}) = \underline{b}CI_e^{(d)}. \qquad (21) \end{aligned}$$

If $\underline{a} \neq \underline{b}$, then $\underline{a}C \neq \underline{b}C$, since C is invertible from Theorem 2; and then we see $\underline{r} \neq \underline{s}$ from (20) and (21), *i.e.*, $\xi(\underline{a}) \neq \xi(\underline{b})$. Hence ξ is injective. And then, ξ is surjective since the domain space of ξ has the same size as its image space: $|F_2^{(e)}| = 2^e = 2^{e_1 d} = |F_{2^{e_1}}^{(d)}|$, where $|F_2^{(e)}|$ denotes the size of the set $F_2^{(e)}$ (similar for $|F_{2^{e_1}}^{(d)}|$). Therefore, ξ is bijective.

Denote $\xi(\underline{a}) = (\xi_0(\underline{a}), \xi_1(\underline{a}), \ldots, \xi_{d-1}(\underline{a}))$, where each component $\xi_i(\underline{a})$ is a function from $F_2^{(e)}$ to $F_{2^{e_1}}$. It is clear that $\xi_0(\underline{a})$ is surjective since $\xi(\underline{a})$ is surjective . Therefore, $\zeta(\underline{a})$ is surjective since $\zeta(\underline{a}) = \xi_0(\underline{a})$. The bijection of ξ_ν can be proved similarly. ■

The following result should be well known, but no explicitly written publication was found as far as authors are concerned. Therefore, for the sake of completeness, we give a proof, in Appendix. Let S_i, $1 \leq i \leq m$, be subsets of $\overline{F}_2$, and their sum be given as $\sum_{1 \leq i \leq m} S_i = \{\sum_{1 \leq i \leq m} s_i \mid s_i \in S_i\}$.

Lemma 8 (Sum of Subfields): A finite field F is not a sum of its proper subfields.

Theorem 3: Among the d values $c_i = c_{u^i}(\beta)$, $0 \leq i < d$, there exists at least one i such that $F_2(c_i) = F_{2^{e_1}}$. Moreover, when $d = 1$ $(e = e_1)$, the e elements $c_0^{2^j}, 0 \leq j < e$, make a normal basis of F_{2^e} over F_2, and $c_0 \in F_{2^e}$ satisfies $Tr_1^e(c_0^{1+2^k}) = f + 1$ for $k = \nu \pmod{e}$ and $Tr_1^e(c_0^{1+2^k}) = f$ for $k \neq \nu \pmod{e}$. ■

Proof: Let $\Sigma = \{\sum_{0 \leq i < e} a_i c_i | a_i \in F_2\}$. From Lemma 7 we have $\Sigma = F_{2^{e_1}}$. Then, from Theorem 2 we see

$$\begin{aligned} F_{2^{e_1}} &= \Sigma \subseteq \sum_{0 \leq i < e} F_2(c_i) \\ &= \sum_{\substack{0 \leq i < d \\ 0 \leq j < e_1}} F_2(c_i^{2^{\lambda j}}) \\ &= \sum_{0 \leq i < d} F_2(c_i) \quad \subseteq \quad F_{2^{e_1}} \end{aligned}$$

and thus $F_{2^{e_1}} = \sum_{0\le i<d} F_2(c_i)$. Therefore, from Lemma 8 we see there exists at least one i such that $F_2(c_i) = F_{2^{e_1}}$. When $d = 1$, we have $e_1 = e$. From Theorem 2 we have

$$\sum_{0\le i<e} a_i c_i = \sum_{\substack{0\le i<d=1\\ 0\le j<e_1=e}} a_{i+d\mu j} c_{i+d\mu j} = \sum_{0\le j<e} a_{\mu j} c_0^{2^j}$$

and then

$$\begin{aligned} F_{2^e} = F_{2^{e_1}} = \Sigma &= \left\{ \sum_{0\le i<e} a_i c_i \,\middle|\, a_i \in F_2 \right\} \\ &= \left\{ \sum_{0\le j<e} a_{\mu j} c_0^{2^j} \,\middle|\, a_{\mu j} \in F_2 \right\} \end{aligned}$$

which means that e elements $c_0^{2^j}$, $0 \le j < e$, make a normal basis of F_{2^e} over F_2. Finally, using the item 4 of Theorem 2, when $d = 1$, we have

$$\begin{aligned} Tr_1^e(c_0^{1+2^k}) &= \sum_{0\le i<e} c_0^{(1+2^k)2^i} = \sum_{0\le i<e} c_i c_{i+k} \\ &= \begin{cases} f+1 & \text{if } k = \nu = \frac{e}{2}\delta(f) \pmod e \\ f & \text{otherwise.} \end{cases} \end{aligned}$$

■

E. e-Tuples and Defining Pairs

We have seen that any eth power residue sequence is of the form $\mathbf{s}_{\underline{a}} = \sum_{0\le i<e} a_i \mathbf{b}_{u^i}$ or $\underline{1} + \mathbf{s}_{\underline{a}}$ for some $\underline{a} \in F_2^{(e)}$. In studying the defining pair for eth power residue sequences, note that $(1+g(x), \beta)$ is a defining pair of $\underline{1}+\mathbf{s}_{\underline{a}}$ whenever $(g(x), \beta)$ is that of $\mathbf{s}_{\underline{a}}$, so we need pay attention only to the eth residue sequences of the form $\mathbf{s}_{\underline{a}} = \sum_{0\le i<e} a_i \mathbf{b}_{u^i}$.

Theorem 4 (e-Tuples Determining Defining Pairs): Let u be a generator of F_p^*, in particular, uH_e is a generator of F_p^*/H_e. Let

$$\mathbf{s}_{\underline{a}} = \sum_{0\le i<e} a_i \mathbf{b}_{u^i} \in \mathcal{L}, \quad \underline{a} = (a_0, a_1, \ldots, a_{e-1}) \in F_2^{(e)}.$$

Then

$$\begin{aligned} \underline{a}\Gamma^\nu C Y_u(x) &= \sum_{\substack{0\le i<d\\ 0\le j<e_1}} r_i^{2^j} c_{u^i}(x)^{2^j} && (22) \\ &= \sum_{\substack{0\le i<d\\ 0\le k<e_1 f}} r_i^{2^{\lambda k}} x^{u^{i+dk}} && (23) \end{aligned}$$

where $\underline{r} = (r_0, r_1, \ldots, r_{d-1}) = \underline{a}\Gamma^\nu C I_e^{(d)}$. Furthermore, $(g_{\underline{a}}(x), \beta)$ is a defining pair of $\mathbf{s}_{\underline{a}}$, where

$$g_{\underline{a}}(x) = f w_H(\underline{a}) + \underline{a}\Gamma^\nu C Y_u(x).$$

Proof: Denote $\underline{R} = \underline{a}\Gamma^\nu C = (R_0, R_1, \ldots, R_{e-1})$ and $y_i(x) = c_{u^i}(x)$. It is clear that $R_i = r_i$ for $0 \le i < d$. Note that the index i in both R_i and $y_i(x)$ are understood as a number modulo e, we have

$$\begin{aligned} \underline{a}\Gamma^\nu C Y_u(x) &= \sum_{0\le i<e} R_i y_i(x) \\ &= \sum_{\substack{0\le i<d\\ 0\le j<e_1}} R_{i+d\mu j} y_{i+d\mu j} \\ &= \sum_{\substack{0\le i<d\\ 0\le j<e_1}} R_i^{2^j} y_i(x)^{2^j} \\ &= \sum_{\substack{0\le i<d\\ 0\le j<e_1}} r_i^{2^j} c_{u^i}(x)^{2^j} \end{aligned}$$

and

$$\begin{aligned} \underline{a}\Gamma^\nu C Y_u(x) &= \sum_{0\le i<e} R_i y_i(x) \\ &= \sum_{\substack{0\le i<e\\ 0\le l<f}} R_i x^{u^{i+el}} \\ &= \sum_{\substack{0\le i<d\\ 0\le j<e_1\\ 0\le l<f}} R_i^{2^{\lambda j}} x^{u^{i+dj+el}} \quad \text{(Lemma 6)} \\ &= \sum_{\substack{0\le i<d\\ 0\le j<e_1\\ 0\le l<f}} r_i^{2^{\lambda(j+e_1 l)}} x^{u^{i+d(j+e_1 l)}} \\ &\qquad \text{(since } \ r_i \in F_{2^{e_1}}) \\ &= \sum_{\substack{0\le i<d\\ 0\le k<e_1 f}} r_i^{2^{\lambda k}} x^{u^{i+dk}}. \end{aligned}$$

For the second part, we first consider the case when

$$\underline{a} = \underline{v}_i = (\delta_{i,0}, \delta_{i,1}, \ldots, \delta_{i,e-1}) \in F_2^{(e)}, 0 \le i < e \qquad (24)$$

where $\delta_{i,k}$ is the Kronecker delta symbol, that is $\delta_{i,k} = 1$ if $i = k$, $\delta_{i,k} = 0$ if $i \ne k$. It is clear that $\mathbf{s}_{\underline{v}_i} = \mathbf{b}_{u^i}$. Let $C^* = \Gamma^\nu C = (c_{i,j}^*)$, then $C^*C = \Gamma^\nu C^2 = fJ_e + I_e$ from Theorem 2. Recall $C = (c_{i,j})$ with $c_{i,j} = c_{i+j}$, thus

$$\sum_{0\le j<e} c_{i,j}^* c_{j,k} = f + \delta_{i,k} \ \forall i, k. \qquad (25)$$

Note that $f w_H(\underline{v}_i) = f$, and

$$\begin{aligned} \underline{v}_i \Gamma^\nu C &= \underline{v}_i C^* = (c_{i,0}^*, c_{i,1}^*, \ldots, c_{i,e-1}^*), \\ Y_u(x) &= (c_{u^0}(x), c_{u^1}(x), \ldots, c_{u^{e-1}}(x)) \end{aligned}$$

we get

$$g_{\underline{v}_i}(x) = f + \sum_{0\le j<e} c_{i,j}^* c_{u^j}(x) \pmod{x^p - 1}. \qquad (26)$$

Note that

$$\begin{aligned}\sum_{0\le j<e} c^*_{i,j} &= \sum_{0\le j<e} c_{\nu+i+j} = \sum_{0\le j<e} c_j = 1,\\ c_{u^j}(\beta^0) &= \sum_{0\le j<f} 1 = f,\\ c_{u^j}(\beta^t) &= c_{u^j t}(\beta) = c_{u^{j+k}}(\beta)\\ &= c_{j+k} = c_{j,k},\ \ \forall t\in u^k H_e.\end{aligned}$$

Therefore, for $t = 0 \pmod p$

$$\begin{aligned}g_{\underline{v}_i}(\beta^t) &= f + \sum_{0\le j<e} c^*_{i,j} c_{u^j}(\beta^0) = f + f\sum_{0\le j<e} c^*_{i,j}\\ &= f+f = 0 = \mathbf{b}_{u^i}(t),\ \ \forall t = 0 \pmod p.\end{aligned}$$

For $t\in u^k H_e$

$$\begin{aligned}g_{\underline{v}_i}(\beta^t) &= f + \sum_{0\le j<e} c^*_{i,j} c_{u^j}(\beta^t) = f + \sum_{0\le j<e} c^*_{i,j} c_{j,k}\\ &= f + (f+\delta_{i,k}) = \delta_{i,k} = \mathbf{b}_{u^i}(t),\ \ \forall t\in u^k H_e.\end{aligned}$$

Therefore, $g_{\underline{v}_i}(\beta^t) = \mathbf{b}_{u^i}(t)\ \ \forall t\ge 0$, which proves the theorem for the case when $\underline{a} = \underline{v}_i$. Since

$$\mathbf{s}_{\underline{a}} = \sum_{0\le i<e} a_i \mathbf{b}_{u^i} = \sum_{0\le i<e} a_i \mathbf{s}_{\underline{v}_i}$$

we see $(h(x),\beta)$ is a defining pair of $\mathbf{s}_{\underline{a}}$, where $h(x) = \sum_{0\le i<e} a_i g_{\underline{v}_i}(x)$. We have

$$\begin{aligned}h(x) &= \sum_{0\le i<e} a_i g_{\underline{v}_i}(x) = \sum_{0\le i<e} a_i(f + \underline{v}_i\Gamma^\nu C Y_u(x))\\ &= f\sum_{0\le i<e} a_i + \sum_{0\le i<e} a_i \underline{v}_i \Gamma^\nu C Y_u(x)\\ &= f w_H(\underline{a}) + \underline{a}\Gamma^\nu C Y_u(x) = g_{\underline{a}}(x)\end{aligned}$$

which proves the theorem. ■

We now arrive at the final formula for the trace representation of general eth power residue sequences of period p. Given an eth power residue sequence, one can uniquely determine the corresponding e-tuple $\underline{a} = (a_0, a_1, \ldots, a_{e-1}) \in F_2^{(e)}$ (See Theorem 1). This e-tuple uniquely determines its defining pair $(g_{\underline{a}}(x),\beta)$ (see Theorem 4). Then, from this defining pair, one can determine the trace representation, minimal polynomial, and linear complexity of the sequences as in the following.

Theorem 5 (e-Tuples Determining TR, MP, and LC): Let

$$\mathbf{s}_{\underline{a}} = \sum_{0\le i<e} a_i \mathbf{b}_{u^i} = \{\mathbf{s}_{\underline{a}}(t), t\ge 0\} \in \mathcal{L}$$

where $\underline{a} = (a_0, a_1, \ldots, a_{e-1}) \in F_2^{(e)}$. Denote

$$\begin{aligned}\underline{R} &= (R_0, R_1, \ldots, R_{e-1}) = \underline{a}\Gamma^\nu C \in F_{2^{e_1}}^{(e)},\\ \underline{r} &= \underline{R} I_e^{(d)} \in F_{2^{e_1}}^{(d)},\\ \varepsilon_{\underline{a}} &= \delta(f w_H(\underline{a})) \in \{0,1\},\\ \Delta_{\underline{a}} &= (-1)^{\varepsilon_{\underline{a}}} \in \{+1,-1\}.\end{aligned}$$

Then the following are true:

1. For the sequence $\mathbf{s}_{\underline{a}}$
   (a) A trace representation is given as

$$\begin{aligned}\mathbf{s}_{\underline{a}}(t) &= \varepsilon_{\underline{a}} + \sum_{0\le i<c} Tr_1^n(R_i \beta^{tu^i})\\ &= \varepsilon_{\underline{a}} + \sum_{\substack{0\le i<d\\ 0\le j<c/d}} Tr_1^n(r_i^{2^{\lambda j}} \beta^{tu^{i+dj}}),\ \forall t\ge 0.\end{aligned} \tag{27}$$

   (b) The minimal polynomial is given as

$$m_{\mathbf{s}_{\underline{a}}}(x) = (x-1)^{\varepsilon_{\underline{a}}} \times \prod_{\substack{r_i\ne 0\\ 0\le i<d\\ 0\le j<c/d}} p_{i+dj}(x) \tag{28}$$

   where $p_i(x)$ denotes the irreducible polynomial over F_2 with β^{u^i} as a root.
   (c) The linear complexity is given as

$$\mathrm{LC}(\mathbf{s}_{\underline{a}}) = \varepsilon_{\underline{a}} + f w_H(\underline{R}) = \varepsilon_{\underline{a}} + f e_1 w_H(\underline{r}). \tag{29}$$

   In particular,
   i. When $\mathbf{s}_{\underline{a}} = \mathbf{b}_{u^i}$, for each $0\le i<e$ (a single coset sequence):

$$\mathrm{LC}(\mathbf{b}_{u^i}) = \delta(f) + f e_1 W_d, \tag{30}$$

   where W_d is defined in the item 7 of Theorem 2.
   ii. When $d = 1$:

$$\mathrm{LC}(\mathbf{s}_{\mathbf{a}}) = \begin{cases} p-1+\varepsilon_{\underline{a}}, & \underline{a}\ne(0,\ldots,0)\\ 0, & \underline{a} = (0,\ldots,0).\end{cases} \tag{31}$$

2. For the sequence $\mathbf{s}_{L\underline{a}}$, where L is the cyclically-left-shift operator in Definition 6, we have

$$\mathrm{LC}(\mathbf{s}_{L\underline{a}}) = \mathrm{LC}(\mathbf{s}_{\underline{a}}).$$

3. For the sequence $\underline{1} + \mathbf{s}_{\underline{a}}$, we have

$$\begin{aligned}m_{\underline{1}+\mathbf{s}_{\underline{a}}}(x) &= (x-1)^{\Delta_{\underline{a}}} \times m_{\mathbf{s}_{\underline{a}}}(x)\\ \mathrm{LC}(\underline{1}+\mathbf{s}_{\underline{a}}) &= \Delta_{\underline{a}} + \mathrm{LC}(\mathbf{s}_{\underline{a}}).\end{aligned}$$

Proof:

1. From Theorem 4 we see the polynomial

$$g(x) = \varepsilon_{\underline{a}} + \sum_{\substack{0\le i<d\\ 0\le k<e_1 f}} r_i^{2^{\lambda k}} x^{u^{i+dk}}$$

is a defining polynomial of the sequence $\mathbf{s}_{\underline{a}}$ corresponding to the defining element β, and then, both the trace representation (27) and the minimal polynomial (28) can be obtained from the item 1 and item 2 of Lemma 3 respectively, and the linear complexity (29) can be obtained from the item 3 of Lemma 3 and the item 3 of Lemma 4. The linear complexity of two special cases can be determined as follows:

i. We know that

$$\underline{R} = \underline{v}_i \Gamma^\nu C = (c_{\nu+i}, c_{\nu+i+1}, \ldots, c_{\nu+i+e-1}) \in \mathcal{C}.$$

Therefore, $w_H(\underline{R}) = e_1 W_d$ from the item 7 of Theorem 2.

ii. In the case when $d = 1$, we have $e_1 = e$ and $\xi_\nu(\underline{a}) \in F_{2^e}$. From Lemma 7 we see $\xi_\nu(\underline{a}) = \underline{a}\Gamma^\nu C I_e^{(1)} \neq 0$ whenever $\underline{a} \neq 0$, hence $w_H(\underline{a}\Gamma^\nu C I_e^{(1)}) = 1$. Therefore, whenever $\underline{a} \neq 0$, we have (31) as

$$\begin{aligned}\mathrm{LC}(\mathbf{s}_{\underline{a}}) &= \varepsilon_{\underline{a}} + f w_H(\underline{a}\Gamma^\nu C)\\ &= \varepsilon_{\underline{a}} + f e_1 w_H(\underline{a}\Gamma^\nu C I_e^{(1)})\\ &= \varepsilon_{\underline{a}} + f e_1 = \varepsilon_{\underline{a}} + fe\\ &= \varepsilon_{\underline{a}} + p - 1.\end{aligned}$$

2. From Lemma 6 we see $(L\underline{a})\Gamma^\nu C = L^{-1}(\underline{a}\Gamma^\nu C)$, hence

$$w_H((L\underline{a})\Gamma^\nu C) = w_H(L^{-1}(\underline{a}\Gamma^\nu C)) = w_H(\underline{a}\Gamma^\nu C)$$

and then

$$\begin{aligned}\mathrm{LC}(\mathbf{s}_{L\underline{a}}) &= \delta(f w_H(L\underline{a})) + f w_H((L\underline{a})\Gamma^\nu C)\\ &= \delta(f w_H(\underline{a})) + f w_H(\underline{a}\Gamma^\nu C)\\ &= \mathrm{LC}(\mathbf{s}_{\underline{a}}).\end{aligned}$$

3. We assume $g(x) = \varepsilon + \sum_{i \in F_p^*} r_i x^i$ is a defining polynomial of $\mathbf{s}_{\underline{a}}$ corresponding to β, where $\varepsilon = 0$ or 1, then $1 + g(x) = 1 + \varepsilon + \sum_{i \in F_p^*} r_i x^i$ is a defining polynomial of $\underline{1} + \mathbf{s}_{\underline{a}}$ corresponding to β. Now, let $m^*(x) = \prod_{r_i \neq 0, i \in F_p^*}(x - \beta^i)$. Then $m(x) = (x-1)^\varepsilon m^*(x)$ is the minimal polynomial of $\mathbf{s}_{\underline{a}}$, and $m_1(x) = (x-1)^{\delta(1+\varepsilon)} m^*(x)$ is the minimal polynomial of $\underline{1} + \mathbf{s}_{\underline{a}}$. Since it is easy to check that $\delta(1+\varepsilon) - \varepsilon = (-1)^\varepsilon = \Delta$, we have

$$\begin{aligned}m_1(x) &= (x-1)^{\delta(1+\varepsilon)} m^*(x)\\ &= (x-1)^{\delta(1+\varepsilon)-\varepsilon} m(x)\\ &= (x-1)^\Delta m(x)\end{aligned}$$

and

$$\begin{aligned}\mathrm{LC}(\underline{1} + \mathbf{s}_{\underline{a}}) &= \deg(m_1(x))\\ &= \deg((x-1)^\Delta m(x))\\ &= \Delta + \deg(m(x))\\ &= \Delta + \mathrm{LC}(\mathbf{s}_{\underline{a}}).\end{aligned}$$

■

An immediate application of this to the sequences $\underline{\delta}$ and $\underline{1}$ seems to be intuitive and interesting. Let

$$\begin{aligned}g_{\underline{\delta}}(x) &= \frac{x^p - 1}{x - 1} = 1 + \sum_{0 \le i < e} c_{u^i}(x),\\ g_{\underline{1}}(x) &= 1.\end{aligned}$$

Then $(g_{\underline{\delta}}(x), \beta)$ is the defining pair of $\underline{\delta}$, and $(g_{\underline{1}}(x), \beta)$ is that of $\underline{1}$, for any primitive pth root of unity β, and $LC(\underline{\delta}) = p - 1$ and $LC(\underline{1}) = 1$.

Theorem 6 (Distribution of Linear Complexities): The linear complexity of any eth power residue sequence of period p must be of the form $\eta + k e_1 f$ for some $k \in \{0, 1, 2, \ldots, d\}$ and some $\eta \in \{0, 1\}$. Moreover, let $N_{\eta + k e_1 f}$ be the total number of the eth power residue sequences of period p with the linear complexity being equal to $\eta + k e_1 f$, then

$$N_{\eta + k e_1 f} = \binom{d}{k}(2^{e_1} - 1)^k, \quad 0 \le k \le d.$$

In particular, when $d = 1$, we have $N_{p-1} = N_p = 2^e - 1$ for $k = 1$ and $N_1 = N_0 = 1$ for $k = 0$.

Proof: Recall the bijective map $\xi_\nu(\underline{a}) = \underline{a}\Gamma^\nu C I_e^{(d)}$ from $F_2^{(e)}$ to $F_{2^{e_1}}^{(d)}$ in Lemma 7. Let

$$R_k = \{\underline{r} \in F_{2^{e_1}}^{(d)} | w_H(\underline{r}) = k\},$$

and let A_k be the pre-image of R_k under the map ξ_ν, *i.e.*,

$$A_k = \{\underline{a} \in F_2^{(e)} | \xi_\nu(\underline{a}) = \underline{a}\Gamma^\nu C I_e^{(d)} \in R_k\},$$

and let

$$A_{k,\eta} = \{\underline{a} \in A_k | \delta(f w_H(\underline{a})) = \eta\}, \quad \eta \in \{0, 1\}.$$

It is clear that $A_k = A_{k,0} \bigcup A_{k,1}$, and that

$$\begin{aligned}&\mathrm{LC}(\mathbf{s}) = e_1 f k\\ \Leftrightarrow\quad &\text{“}\mathbf{s} = \mathbf{s}_{\underline{a}},\ \underline{a} \in A_{k,0} \text{ or } \mathbf{s} = \underline{1} + \mathbf{s}_{\underline{a}},\ \underline{a} \in A_{k,1},\text{”}\\ &\mathrm{LC}(\mathbf{s}) = 1 + e_1 f k\\ \Leftrightarrow\quad &\text{“}\mathbf{s} = \mathbf{s}_{\underline{a}},\ \underline{a} \in A_{k,1} \text{ or } \mathbf{s} = \underline{1} + \mathbf{s}_{\underline{a}},\ \underline{a} \in A_{k,0}.\text{”}\end{aligned}$$

Therefore

$$\begin{aligned}N_{\eta + e_1 f k} &= |A_{k,0} \cup A_{k,1}| = |A_k| = |R_k|\\ &= \binom{d}{k}(2^{e_1} - 1)^k, \quad \eta \in \{0, 1\}.\end{aligned}$$

■

III. Determining the Parameters for Specific eth Power Residue Sequences

A. Trace Representation of Legendre Sequences, Rediscovered

Let $p = 2f + 1$ be an odd prime. The trace representation [20] and the linear complexity [5], [20], [28], [36] of a Legendre sequence of period p have been studied earlier by many. It would be an interesting exercise to use all the theory and formula in the earlier sections to recalculate these. The minimal polynomials

TABLE I
CLASSIFICATION OF THE PRIMES $p = 6f + 1$ WITH f ODD AND $4p = a^2 + 27b^2$, THE VALUE OF $d = (6, c)$, AND A REPRESENTATIVE $\underline{c} \in \mathcal{C}$

p (mod 8) & a and b	2 belongs to	d	$\underline{c} \in \mathcal{C}$	comments
7 & both even	H_6	6	$(1,1,0,1,0,0)$	
3 & both even	$H_3 \backslash H_6$	3	$(\omega,1,0,\omega^2,1,0)$	$\omega^2+\omega+1=0$
7 & not both even	$H_2 \backslash H_6$	2	$(\gamma,\gamma^3,\gamma^2,\gamma^6,\gamma^4,\gamma^5)$	$\gamma^3+\gamma+1=0$
3 & not both even	neither H_2 nor H_3	1	$(\vartheta,\vartheta^2,\vartheta^4,\vartheta^8,\vartheta^{16},\vartheta^{32})$	$\vartheta^6+\vartheta^5+1=0$
			$(\theta,\theta^2,\theta^4,\theta^8,\theta^{16},\theta^{32})$	$\theta^6+\theta^5+\theta^2+\theta+1=0$

of Legendre sequences have not explicitly given so far, which turned out to be

$$g(x) = 1 + f + \begin{cases} c_{u^0}(x) & \text{for } p \equiv \pm 1 \pmod 8 \\ \omega c_{u^0}(x) + \omega^2 c_{u^1}(x) & \text{for } p \equiv \pm 3 \pmod 8 \end{cases}$$

where $\omega \in F_4$ is a primitive 3-root of unity, u is a generator of F_p^*, and $c_{u^i}(x)$, for $i = 0, 1$, are given as in Definition 4.

We just note that the Legendre sequences for for $p \equiv 7, 3 \pmod 8$ correspond to the balanced binary sequence with the ideal two-level autocorrelation.

B. The Case $e = 6$ and Hall's Sextic Residue Sequences

Let $p = 6f + 1$ be a prime for some f, and u be a generator of F_p^*. Let $H_i =< u^i >= \{u^{ij} | j \geq 0\}$ be the cyclic subgroup generated by u^i for $i = 1, 2, 3$ and 6. Then, we have

$$F_p^* = H_1 = \bigcup_{0 \leq i < 6} u^i H_6,$$
$$H_3 = H_6 \cup u^3 H_6$$

and

$$H_2 = H_6 \cup u^2 H_6 \cup u^4 H_6.$$

We are mostly interested in the cyclic difference sets (and their characteristic sequences) which are some union of some of these cosets of H_6 with or without $\{0\}$. It is evident that the case f even is not much interesting. We will consider only the case f odd in this paper when $e = 6$. Then $f = 1, 3 \pmod 4$ and hence $p = 7, 3 \pmod 8$, respectively.

From Theorem 2 of [13], we see that Hall's sextic residue sequence $\mathbf{s} = \{\mathbf{s}(t) | t \geq 0\}$ of period $p = 6f + 1 = 4x^2 + 27$ (for some integer x) is defined as follows.

$$s(t) = \begin{cases} 0 & t \in H_6 \cup u^3 H_6 \cup u^j H_6 \\ 1 & \text{otherwise} \end{cases} \tag{32}$$

where j is given by the condition that $3 \in u^j H_6$.

In this subsection, we will first describe defining pairs of the six basis sequences $\mathbf{b}_{u^i}$ for $0 \leq i < 6$ (see Theorem 1). This will lead to the defining pairs of all possible sextic residue sequences (for f odd), and their trace representations, minimal polynomials, and linear complexities (see Theorem 5). Then, we give a complete determination on the linear complexity of all the possible sextic residue sequences (Theorem 8) and discuss on the Hall's sextic residue sequences corresponding to cyclic Hadamard difference sets (Theorem 9).

Let β be a primitive pth root of unity in F_{2^n}, and let $(g_{u^i}(x), \beta)$ be a defining pair of the sequence $\mathbf{b}_{u^i}$. Denote by $\underline{v}_i$ the binary 6-tuple of weight 1 and in which only the ith position has value 1. From the item 2 of Theorem 4, we see clearly that, since f is odd and hence $\nu = 3$ and

$$\begin{aligned} g_{u^i}(x) &= 1 + \underline{v}_i \Gamma^3 C Y_u(x) \\ &= 1 + \sum_{0 \leq j < 6} c_{i+j+3} c_{u^j}(x). \end{aligned} \tag{33}$$

Therefore, the trace representation becomes

$$\begin{aligned} b_{u^i}(t) &= 1 + \sum_{0 \leq j < c} \mathrm{Tr}_1^n \left(c_{i+j+3} \beta^{u^j t} \right) \\ &= 1 + \sum_{0 \leq j < 6} \mathrm{Tr}_1^n \left(\sum_{\substack{0 \leq m < c \\ m \equiv j \pmod 6}} c_{i+m+3} \beta^{u^m t} \right) \\ &\quad \text{for} \quad t = 0, 1, 2, \ldots \end{aligned} \tag{34}$$

Now, it remains to determine the set $\mathcal{C}$ as given in (13). For this, we will distinguish four cases as shown in the left-most column of Table I. This classification will be done using the following:

Fact 2 (Quadratic and Cubic Characters of 2 and 3 mod p[15]): Let $p = 6f + 1$ be a prime for some odd f. Then, $3 \notin H_2$, and

$$2 \in H_2 \Leftrightarrow p \equiv 7 \pmod 8.$$

When $p \equiv 3 \pmod 8$, we have $4 \in H_2$. If we write $4p = a^2 + 27b^2$ for some unique integers a and b (which is possible if $p \equiv 1 \pmod 3$), then we have

$$2 \in H_3 \Leftrightarrow a \equiv b \equiv 0 \pmod 2$$

and

$$3 \in H_3 \Leftrightarrow b \equiv 0 \pmod 3).$$

■

Theorem 7 (The Set $\mathcal{C}$ for $e = 6$): Let $p = 6f + 1$ be a prime for some odd f. Then, $d = (6, c)$ is determined as shown in Table I. Furthermore, for each value of d, there exist (u, β) such that $\mathbf{c}_u(\beta) = (c_{u^0}(\beta), \ldots, c_{u^5}(\beta)) = (c_0, \ldots, c_5) \in \mathcal{C}$ is shown in Table I. For $d = 1$, either one is possible, but not both, as p changes.

Proof: Note first that $\nu = 3\delta(f) = 3$ and $d = (6, c) \in \{1, 2, 3, 6\}$. The item 8 of Lemma 1 says that d is the maximum such that $d|6$ and $2 \in H_d$. From **Fact** 2, one can classify these cases, which are shown in the first two columns of Table I. Then the value of d can be determined as shown in the third column of the table. The remaining columns show the 6-tuples $\underline{c}$ for each case, which will be described. Recall the notation

$$\begin{aligned} \underline{c} &= (c_{u^0}(\beta), c_{u^1}(\beta), \ldots, c_{u^5}(\beta)) \\ &= \mathbf{c}_u(\beta) \triangleq (c_0, c_1, \ldots, c_5) \in \mathcal{C}, \\ C &= (c_{i,j}) \quad \text{where} \quad c_{i,j} = c_{i+j}, \quad 0 \le i, j < e = 6. \end{aligned}$$

Case $d = 6$: In this case, $e_1 = 6/d = 1$ and hence, $c_i \in F_2$ for all i and β. In fact, $w_H(\underline{c}) = 1, 3$, or 5, since $\sum_{0 \le i < 6} c_i = 1$ by Theorem 2. If $w_H(\underline{c}) = 1$, then we have $\underline{c} \sim (1, 0, 0, 0, 0, 0)$, where $\sim$ represents that both sides are G-equivalent (Lemma 5). Without loss of generality, from Lemma 5, we assume that $\underline{c} = (1, 0, 0, 0, 0, 0)$. Then the 6×6 matrix C in (12) becomes $C = I_6$, and hence, $C^2 = I_6$. But the item 4 of Theorem 2 says $\begin{pmatrix} \mathbf{0} & I_3 \\ I_3 & \mathbf{0} \end{pmatrix} C^2 = J_6 + I_6$, which is a contradiction. Therefore, $w_H(\underline{c}) \neq 1$. Now, we can clearly see that $w_H(\underline{c}) \neq 5$ also from the item 4 of Theorem 2 by using $\overline{C} = C + J_6$. Therefore, we must have $w_H(\underline{c}) = 3$. Finally, claim that

$$\underline{c} = (1, 1, 0, 1, 0, 0) \in \mathcal{C}.$$

For this, we classify $\binom{6}{3} = 20$ vectors over F_2 of weight 3 into three G-equivalent classes (Lemma 5) whose representatives are $(1, 1, 1, 0, 0, 0)$ of size 6, $(1, 0, 1, 0, 1, 0)$ of size 2, and $(1, 1, 0, 1, 0, 0)$ of size 12. The first two choices are easily ruled out by the following: if $\underline{c} = (1, 1, 1, 0, 0, 0)$ then C becomes singular which is a contradiction to the item 4 of Theorem 2; similarly the case $\underline{c} = (1, 0, 1, 0, 1, 0)$ is impossible.

Case $d = 3$: In this case, $e_1 = 6/d = 2$, and $c_i \in F_4$ for $0 \le i < 6$. The item 6 of Theorem 2 implies that (i) $\epsilon_i = c_i + c_{i+3} = \mathrm{Tr}_1^2(c_i) = \mathrm{Tr}_1^2(c_{i+3})$ for $i = 0, 1, 2$, (ii) $\sum_{0 \le i < 3} \epsilon_i = 1$, and (iii) at least one of ϵ_i for $0 \le i < 3$ is 0. Note that, if $a \in F_4$, then $\mathrm{Tr}_1^2(a) = 1 \Leftrightarrow a \in F_4 \backslash F_2$. (or, $\mathrm{Tr}_1^2(a) = 0 \Leftrightarrow a \in F_2$.) From (i) above, we have $\underline{c} = (c_0, c_1, c_2, c_0^2, c_1^2, c_2^2)$. From (ii) and (iii) above, we may assume that $(\epsilon_0, \epsilon_1, \epsilon_2) = (1, 0, 0)$ without loss of generality. This implies that

$$\underline{c} = (\omega, a, b, \omega^2, a, b) \in \mathcal{C}$$

where ω is a primitive element of F_4 and $a, b \in F_2$. Now, claim that $a \neq b$. To show this, we need the relation given in the item 4 of Theorem 2 again. Since f is odd, it implies that, $\sum_{0 \le i < 6} c_i c_{i+3+j} = 1 + \delta(j)$ for all $0 \le j < 6$. If $a = b$, then, by considering the case $j = 4$ in the above relation, we have

$$1 = \sum_{i=0}^{5} c_i c_{i+1} = \omega a + a^2 + a\omega^2 + \omega^2 a + a^2 + a\omega = 0$$

which is impossible. Therefore, $a \neq b$, and hence, $\underline{c} = (\omega, 1, 0, \omega^2, 1, 0) \in \mathcal{C}$. Note that the case where $a = 0$ and $b = 1$ is equivalent to the above.

Case $d = 2$: In this case, $e_1 = 6/d = 3$, and $c_i \in F_8$ for $0 \le i < 6$. The item 6 of Theorem 2 now implies that (i) $\epsilon_i = c_i + c_{i+2} + c_{i+4} = \mathrm{Tr}_1^3(c_i) = \mathrm{Tr}_1^3(c_{i+2}) = \mathrm{Tr}_1^3(c_{i+4})$ for $i = 0, 1$ and (ii) $\epsilon_0 + \epsilon_1 = 1$. Let $\gamma \in F_8$ be a primitive seventh root of unity satisfying $\gamma^3 + \gamma + 1 = 0$. Then, $F_8 = \{0\} \cup < \gamma >$, and we have $\mathrm{Tr}_1^3(\gamma) = 0$ and $\mathrm{Tr}_1^3(\gamma^3) = 1$. Using the above (ii) and the item 4 of Theorem 2, the only possible 6-tuple would be $\underline{c} = (c_0, c_1, \ldots, c_5) = (\gamma, \gamma^3, \gamma^2, \gamma^6, \gamma^4, \gamma^5)$.

Case $d = 1$: In this case, $e_1 = 6/d = 6$, and $c_i \in F_{64}$ for $0 \le i < 6$. The item 6 of Theorem 2 implies that $\epsilon_0 = \sum_{0 \le j < 6} c_j = \mathrm{Tr}_1^6(c_i) = 1$ for any i, and the item 3 of the theorem implies that $c_i = c_0^{2^i}$. Thus $c_0 \in F_{64}$ which determines $\underline{c}$ must have $\mathrm{Tr}_1^6(c_0) = 1$. There are 32 elements in F_{64} with trace 1. Following checks one by one whether each of 32 elements can be c_0. Let $\vartheta \in F_{64}$ be a primitive element such that $\vartheta^6 + \vartheta^5 + 1 = 0$. Then, it can be easily checked that $\mathrm{Tr}_1^6(a) = 0$ for $a \in F_8$, and $\mathrm{Tr}_1^6(a) = 1$ for $a \in F_4 \backslash F_2$. The remaining elements of F_{64} which are not in any subfield are partitioned into 9 cosets, and 5 of them have the trace value 1. Note that these cosets are roots of irreducible polynomials whose coefficient of x^5 is 1. Therefore, 30 elements of trace value 1 which are not in F_4. These elements are checked with respect to the relation in the item 4 of Theorem 2. There are exactly 12 elements that satisfy the relation, and they form two conjugate classes and two corresponding G-equivalent classes with minimal polynomials shown in Table I. Note that these two possibilities are not equivalent under the action of the group G in Lemma 5, and hence, cannot both be in $\mathcal{C}$. ■

One can write explicitly a defining pair $(g(x), \beta)$, and hence a trace representation, minimal polynomial and linear complexity of any sextic residue sequence of period $p = 6f + 1$ with f odd using any one member $\mathbf{c}_u(\beta)$ shown in Table I, together with trace representations of $\mathbf{b}_{u^i}$ for $0 \le i < 6$ in (34).

Theorem 8: Let $\mathbf{a} = (a_0, a_1, a_2, a_3, a_4, a_5)$ be a nonzero binary 6-tuple. The linear complexity of the sextic residue sequence of the form $\mathbf{s} = \sum_{0 \le i < 6} a_i \mathbf{b}_{u^i}$ as in Theorem 1 is shown in Table II.

Proof: Note that the linear complexity of the sequence with $\mathbf{a}$ is the same as that with $L\mathbf{a} = (a_1, a_2, a_3, a_4, a_5, a_0)$ from the item 2 of Theorem 5. The linear complexity in Table II are computed from (29) in Theorem 5 using d and the value $\mathbf{c}_u(\beta)$ shown in Table I.

Now, we will simply describe one case $\mathbf{a} = (100100)$ and $d = 6$ in the table. All other cases can be checked similarly. Consider $\mathbf{a} = (100100)$. Recall that $\nu = 3$, f odd, and $\varepsilon_{\underline{a}} = \delta(f w_H(\mathbf{a})) = 0$. From Table I, we see that $\underline{c} = (110100)$. Therefore

$$\begin{aligned} LC(\mathbf{s}_{\underline{a}}) &= \varepsilon_{\underline{a}} + f w_H(\underline{a} \Gamma^{\nu} C) \\ &= 0 + f w_H((100100) \begin{pmatrix} \mathbf{0} & I_3 \\ I_3 & \mathbf{0} \end{pmatrix} C) \\ &= f w_H((100100) C) \\ &= f w_H((110100) + (100110)) = 2f. \end{aligned}$$

It is obvious that the case with $\mathbf{a} = (101010)$ gives Legendre sequences since $\mathbf{a}$ picks up those cosets $u^{2i} H_6$ for $i = 0, 1, 2$. To show that the case with $\mathbf{a} = (110010)$ gives Hall's sextic

TABLE II
LINEAR COMPLEXITY OF SEXTIC RESIDUE SEQUENCES OF THE FORM $\mathbf{s} = \sum_{0\le i<6} a_i \mathbf{b}_{u^i}$ OF PERIOD $p = 6f + 1$ WITH f ODD IN THEOREM 8. THE MARK † INDICATES THAT THEY ARE HALL'S SEXTIC RESIDUE SEQUENCES AND ‡ INDICATES THAT THEY ARE QUADRATIC RESIDUE SEQUENCES

	$\mathbf{a} =$	Linear Complexity			
$w_H(\mathbf{a})$	$(a_0 a_1 \ldots a_5)$	$d = 6$	$d = 3$	$d = 2$	$d = 1$
1	(100000)	$3f+1$	$4f+1$	$6f+1$	$6f+1$
2	(110000)	$4f$	$6f$	$6f$	$6f$
	(101000)	$4f$	$6f$	$6f$	$6f$
	(100100)	$2f$	$2f$	$6f$	$6f$
3	(111000)	$3f+1$	$6f+1$	$6f+1$	$6f+1$
	(110100)	$5f+1$	$2f+1$	$6f+1$	$6f+1$
	(110010)	$f+1^{\dagger}$	$6f+1^{\dagger}$	$4f+1$	$6f+1$
	(101010)	$3f+1^{\ddagger}$	$6f+1^{\ddagger}$	$3f+1$	$6f+1$
4	(111100)	$2f$	$4f$	$3f$	$6f$
	(111010)	$2f$	$4f$	$6f$	$6f$
	(110010)	$4f$	$4f$	$6f$	$6f$
5	(111110)	$3f+1$	$4f+1$	$5f+1$	$6f+1$
6	(111111)	$6f$	$6f$	$6f$	$6f$

residue sequences, we do the following: From (32), we see that Hall's sextic residue sequences are given as

$$\mathbf{s} = \underline{1} + \mathbf{b}_{u^0} + \mathbf{b}_{u^3} + \mathbf{b}_{u^j}$$

where $3 \in u^j H_6$, and $j = 1$ or 5 depending on the choice of u. It is known [19] that when $d = 3$, the linear complexity of Hall's sequence $\mathbf{s}$ is $p - 1$ and its minimal polynomial does not have root 1. Thus, the linear complexity of $\mathbf{s} + \underline{1} = \mathbf{b}_{u^0} + \mathbf{b}_{u^3} + \mathbf{b}_{u^j}$ is p. In Table II, among the rows with $w_H(\mathbf{a}) = 3$, three cases correspond to linear complexity p, which are $(111000), (110010), (101010)$. It is easy to check $(110010) \sim (100101)$, and the other two are equivalent to neither (100101) which corresponds $j = 5$, nor (110100) which corresponds to $j = 1$. Thus, Hall's sextic residue sequences correspond to the case $\mathbf{a} = (110010)$. ■

Note that Theorem 8 includes the sequences which are characteristic sequences of sextic and quadratic residue Hadamard difference sets as special cases. Note also that the linear complexity of these are known. Except for these cases, the result is fully general and covers the totality of sextic residue sequences, regardless of being related with cyclic difference sets.

Theorem 9 (Trace Representation of Hall's Sextic Residue Sequences): Let $\mathbf{s} = \{\mathbf{s}(t) | t \ge 0\}$ be the Hall's sextic residue sequence of period $p = 6f + 1 = 4y^2 + 27$ (for some integer y) given in (32), and let $\beta \in F_{2^n}$ be a primitive pth root of unity such that the 6-tuple $\underline{c}$ be determined as shown in Table I.

When $p = 7 \pmod 8$, (which is known by [21]), we let $g(x) = (1, 0, 0, 0, 0, 0)Y_u(x) = c_{u^0}(x)$ and $\alpha = \beta^{u^5}$. Then $(g(x), \alpha)$ is a defining pair of $\mathbf{s}$ and

$$s(t) = \sum_{0 \le m < c/6} \mathrm{Tr}_1^n \left(\alpha^{u^{6m} t} \right). \tag{35}$$

When $p = 3 \pmod 8$, (which is new), we let $g(x) = (\omega, 1, 1, \omega^2, 1, 1)Y_u(x)$ and $\alpha = \beta^u$, where $\omega \in F_4$ is a primitive third root of unity. Then $(g(x), \alpha)$ is a defining pair of $\mathbf{s}$ and the trace representation of $\mathbf{s}$ is given as shown in (36) at the bottom of the page.

Proof: From **Fact** 2, we see that $j = 1$ or $j = 5$ if $3 \in u^j H_6$. Since $p = 4y^2 + 27$ or $4p = (2y)^2 + 27 \cdot 2^2$, Table I shows that $d = 6$ for $p = 7 \pmod 8$ or $d = 3$ for $p = 7 \pmod 8$. From Theorem 8, we observe that Hall's sextic residue sequences are equivalent to the case $\mathbf{a} = (110010)$. This implies that u in Table I was chosen such that $3 \in u^5 H_6$, or $j = 5$, since $\mathbf{a} = (110010) \sim (100101)$. Therefore

$$\begin{aligned} s(t) &= 1 + b_{u^0}(t) + b_{u^3}(t) + b_{u^5}(t) \\ &= \sum_{0 \le m < c} \mathrm{Tr}_1^n \left((c_m + c_{m+2} + c_{m+3}) \beta^{u^m t} \right) \\ &= \sum_{0 \le j < 6} \sum_{\substack{0 \le m < c \\ m \equiv j \pmod 6}} \mathrm{Tr}_1^n \left((c_m + c_{m+2} + c_{m+3}) \beta^{u^m t} \right). \end{aligned}$$

Using the value $\underline{c} = (c_0, c_1, \ldots, c_5)$ in Table I, we have the following two cases.

When $d = 6$ or $p \equiv 7 \pmod 8$: Since $\underline{c} = (110100)$, we have

$$\begin{array}{rcl} \underline{c} & = & 110100 \\ L^2\underline{c} & = & 010011 \\ L^3\underline{c} & = & 100110 \\ \hline \text{sum} & = & 000001 \end{array}$$

Now, if we choose the primitive pth root of unity to be $\alpha = \beta^{u^5}$ instead of β, then Lemma 5 implies that $\underline{c} = L^5(110100) = (011010)$, and hence, $\underline{c} + L^2\underline{c} + L^3\underline{c} = (100000)$, and (note $6|c$ in this case)

$$\begin{aligned} s(t) &= \sum_{\substack{0 \le m < c \\ m \equiv 0 \pmod 6}} \mathrm{Tr}_1^n \left(\alpha^{u^m t} \right) \\ &= \sum_{0 \le m < c/6} \mathrm{Tr}_1^n \left(\alpha^{u^{6m} t} \right). \end{aligned}$$

$$s(t) = \sum_{\substack{0 \le m < c \\ m \equiv 0 \pmod 6}} \mathrm{Tr}_1^n \left(\omega \alpha^{u^m t} \right) + \sum_{\substack{0 \le m < c \\ m \equiv 3 \pmod 6}} \mathrm{Tr}_1^n \left(\omega^2 \alpha^{u^m t} \right) + \sum_{\substack{0 \le m < c \\ m \not\equiv 0 \pmod 3}} \mathrm{Tr}_1^n \left(\alpha^{u^m t} \right). \tag{36}$$

The linear complexity in this case is $f = (p-1)/6$. Compare this result with those in [21] and [19].

When $d = 3$ *or* $p \equiv 3 \pmod 8$*:* Using $\underline{c} = (\omega^2, 1, 0, \omega, 1, 0)$, we have

$$\begin{array}{lcllllll} \underline{c} & = & \omega^2 & 1 & 0 & \omega & 1 & 0 \\ L^2\underline{c} & = & 0 & \omega & 1 & 0 & \omega^2 & 1 \\ L^3\underline{c} & = & \omega & 1 & 0 & \omega^2 & 1 & 0 \\ \hline \text{sum} & = & 1 & \omega & 1 & 1 & \omega^2 & 1 \end{array}$$

Note that, if we choose the primitive pth root of unity to be $\alpha = \beta^u$ instead of β, Lemma 5 implies that $\underline{c} = L(\omega^2, 1, 0, \omega, 1, 0) = (1, 0, \omega, 1, 0, \omega^2)$, and $\underline{c} + L^2\underline{c} + L^3\underline{c} = (\omega, 1, 1, \omega^2, 1, 1)$. This leads easily to (36).

Note that the change from β into α in both of the above cases does not change the value $j = 5$ for which $3 \in u^j H_6$. ■

Note that the trace representation (36) for $p = 3 \pmod 8$ is new, but the case for $p = 7 \pmod 8$ have been known [21]. Linear complexity for both cases have been known also [19].

C. *The Cases* $e = 4$, $e = 8$, *and* $e = 10$ *in Which Cyclic Difference Sets Exist*

In this subsection, we will concentrate only on the cases of primes $p = ef + 1$ where $e = 4$, $e = 8$, or $e = 10$, such that eth power residue cyclic difference sets exist. We will describe the set $\mathcal{C}$ for the characteristic sequences of these cyclic difference sets. This will be enough to determine their defining pair (and hence, their trace representations, minimal polynomials and linear complexity) of these sequences. Those primes $p = ef + 1$ necessarily have f odd, and are characterized by the following.

Fact 3 (Existence of e*th Residue Difference Sets for* $e = 4, 8,$ *and 10 [1], [34]):* For $e = 4, 8$, and 10, only the following eth residue cyclic difference sets exist.

Case $e = 4$**:** Let $p = 4f + 1$ be an odd prime where f is odd. Then we have the following:

(B) H_4 is a $(p, (p-1)/4, (p-5)/16)$-cyclic difference set if and only if $p = 1 + 4x^2$ for some integer x, i.e., f is an odd square;

(B1) $H_4 \cup \{0\}$ is a $(p, (p+3)/4, (p+3)/16)$-cyclic difference set if and only if $p = 9 + 4x^2$ for some integer x.

Case $e = 8$**:** Let $p = 8f + 1$ be an odd prime where f is odd. Then we have the following:

(O) H_8 is a $(p, (p-1)/8, (p-7)/64)$-cyclic difference set if and only if $p = 1 + 8x^2 = 9 + 64y^2$ for some odd integers x and y;

(O1) $H_8 \cup \{0\}$ is a $(p, (p+7)/8, (p+7)/64)$-cyclic difference set if and only if $p = 49 + 8x^2 = 441 + 64y^2$ for some odd integers x and y. It is known that $p = 26,041$ is the only prime up to 34, 352, 398, 777 that can be written as $p = 49 + 8x^2 = 441 + 64y^2$.

Case $e = 10$**:** Let $p = 10f + 1$ be an odd prime where f is odd. Then

(D) $H_{10} \cup uH_{10} = \{1, 5, 11, 24, 25, 27\}$ is a $(31, 6, 1)$-cyclic difference set mod 31, where $u = 11$ is a generator of F_{32}^*. ■

We will take care of the simple case **(D)** first.

Theorem 10: Let $p = 31$, $e = 10$, and let $\mathbf{s}$ be the characteristic sequence of the cyclic difference set $D = H_{10} \cup 11H_{10} = \{i \pmod{31} \mid i = 1, 5, 11, 24, 25, 27\}$, then $\mathbf{s} = \underline{1} + \mathbf{b}_1 + \mathbf{b}_{11}$. Let β be a root of the polynomial $x^5 + x^2 + 1$, then β is a 31st primitive root of unity. Then $(g(x), \beta)$ is a defining pair of $\mathbf{s}$, where $g(x)$ is given as shown in (37) at the bottom of the page.

Proof: Observe that $n = 5$ is the order of 2 modulo 31. Then, $c = \frac{p-1}{n} = 6$, $d = \gcd(e, c) = 2$, and $e_1 = e/d = 5$. Take $u = 11$, which is a generator of F_{31}^*. Then, $H_e = H_{10} = \{1, 5, 25\}$ and $uH_e = 11H_{10} = \{11, 24, 27\}$. $\lambda_u = \lambda_{11} = 4$ satisfies $u^d = 11^2 \in 2^{\lambda_{11}} H_{10}$. We have $c_{u^0}(x) = c_1(x) = x + x^5 + x^{25}$, and then $c_{u^0}(\beta) = \beta^{24}$. We have $c_{u^1}(x) = c_{11}(x) = x^{11} + x^{24} + x^{27}$, and then get $c_{u^1}(\beta) = c_{11}(\beta) = \beta^{30}$. See that $f = \frac{p-1}{e} = 3$ and $\nu = \frac{e\delta(f)}{2} = 5$. We let $\mathbf{c}_u(\beta) = \mathbf{c}_{11}(\beta) = (c_0, c_1, \ldots, c_9)$. Based on Theorem 4 we see $(g_{u^0}(x) = g_1(x) = 1 + \sum_{0 \le i < 10} c_{5+i} c_{11^i}(x), \beta)$ is a defining pair of the sequence $\mathbf{b}_{u^0} = \mathbf{b}_1$; and $g_{u^1} = g_{11}(x) = 1 + \sum_{0 \le i < 10} c_{5+1+i} c_{11^i}(x), \beta)$ is a defining pair of the sequence $\mathbf{b}_u = \mathbf{b}_{11}$. Take $g(x) = 1 + g_1(x) + g_{11}(x)$, then $(g(x), \beta)$ is a defining pair of the sequence $\mathbf{s} = \underline{1} + \mathbf{b}_1 + \mathbf{b}_{11}$. It is clear that $g(x) = 1 + \sum_{0 \le i < 10} (c_{5+i} + c_{6+i}) c_{11^i}(x)$. Again based on Theorem 4, we have

$$g(x) = 1 + \sum_{0 \le j < 5} r_0^{2^j} c_{11^0}(x)^{2^j} + r_1^{2^j} c_{11^1}(x)^{2^j}$$
$$\text{where } r_0 = c_5 + c_6, \; r_1 = c_6 + c_7. \tag{38}$$

From $c_{i+d} = c_i^{2^{\lambda_u}}$, here we have $c_{i+2} = c_i^{2^4}$. Then it must be $c_5 = c_1^{2^{4\times 2}}$, $c_6 = c_0^{2^{4\times 3}}$ and $c_7 = c_1^{2^{4\times 3}}$. By a straightforward computation, we get $r_0 = \beta^{11}$ and $r_1 = \beta^{18}$, which together with (38) leads the desired result. ■

Theorem 11: Let $p = ef + 1$ with $e = 4$ and f odd. Then there exists a generator u of F_p^* such that $2 \in uH_4$, and that there exists a p-th primitive root β of unity, such that $c_{u^i}(\beta) = c_{u^0}(\beta)^{2^i}, 0 < i < 4$, where $c_{u^0}(\beta) = \theta \in F_{2^4}$, and θ is a root of $f(x)$, where either $f(x) = x^4 + x^3 + 1$ or $f(x) = x^4 + x^3 + x^2 + x + 1$ (but not both).

1. In case when $p = 1 + 4x^2$ for some integer x (it is known that H_4 is a $(p, (p-1)/4, (p-5)/16)$- cyclic difference

$$g(x) = 1 + \sum_{0 \le j < 5} \left(\beta^{11 \cdot 2^j} (x + x^5 + x^{25})^{2^j} + \beta^{18 \cdot 2^j} (x^{11} + x^{24} + x^{27})^{2^j} \right). \tag{37}$$

set module p), let $\mathbf{s} = \underline{1} + \mathbf{b}_{u^0}$. Then $\mathbf{s}$ is the characteristic sequence of H_4, and it has a defining pair $< g(x), \beta >$, where

$$g(x) = \sum_{0 \le i < 4} \theta^{2^{i+2}} c_{u^i}(x),$$

and θ is described as above.

2. In case when $p = 9 + 4x^2$ for some integer x (it is known that $H_4 \cup \{0\}$ is a $(p, (p+3)/4, (p+3)/16)$- cyclic difference set module p), and let $\mathbf{s} = \underline{1} + \underline{\delta} + \mathbf{b}_{u^0}$. Then $\mathbf{s}$ is the characteristic sequence of the difference set $H_4 \cup \{0\}$, and it has a defining pair $< g(x), \beta >$, where

$$g(x) = 1 + \sum_{0 \le i < 4} (\theta^{2^{i+2}} + 1) c_{u^i}(x),$$

and θ is described as above.

Proof: From **Fact** 3 for $e = 4$, if we let u be a generator of F_p^* where $p = 4f + 1$ is a prime with f odd, then $p \equiv 5 \pmod 8$ and the quadratic reciprocity theorem implies that 2 is a quadratic nonresidue mod p. Therefore, $2 \in uH_2 = uH_4 \cup u^3 H_4$. (If $2 \in u^3 H_4$ then we may change the generator from u to $v = u^{4k+3}$ with $(4k+3, p-1) = 1$ for some integer k. Therefore, we may always choose a generator u such that $2 \in uH_4$.) From Lemma 1, this gives $d = 1$. Therefore $e_1 = 4$, and $c_i \triangleq c_{u^i}(\beta) = c_0^{2^i} \in F_{16}$ for $0 \le i < 4$. Thus, $(c_0, c_1, c_2, c_3) = (c_0, c_0^2, c_0^{2^2}, c_0^{2^3})$ and their sum is $\mathrm{Tr}_1^4(c_0) = 1$. Therefore, there are only two possibilities: $c_0 \triangleq \theta$ is a root of $x^4 + x^3 + 1$ or $x^4 + x^3 + x^2 + x + 1$. Note that two 4-tuples above are not G-equivalent. The remaining two items can easily be checked using the fact that $\mathbf{s} = \underline{1} + \mathbf{b}_{u^0}$ for case 1 and $\mathbf{s} = \underline{1} + \underline{\delta} + \mathbf{b}_{u^0}$ for case 2, together with $g_{u^0}(x) = 1 + \sum_{0 \le i < 4} \theta^{2^{i+2}} c_{u^i}(x)$ since $\nu = 2$, and $g_{\underline{\delta}}(x) = 1 + \sum_{0 \le i < 4} c_{u^i}(x)$ (Corollary 1). ■

Fact 4 (Biquadratic and Octic Characters of 2 mod $p = 8f + 1$[2]): Let $p = 8f + 1$ be a prime. Then, (i) 2 is a biquadratic residue mod p if and only if either $p = x^2 + 32y^2 \equiv 1 \pmod{16}$ for some x and y or $p = x^2 + 8y^2 \equiv 9 \pmod{16}$ for some x and y which are both odd; (ii) 2 is an octic residue mod p if and only if either $p = x^2 + 256y^2 \equiv 1 \pmod{16}$ or $p = x^2 + 64y^2 \equiv 9 \pmod{16}$. ■

Theorem 12: Let $p = ef + 1$ with $e = 8$ and f odd, and assume the $d = 8$, where d is the d-parameter corresponding to (p, e). Then there exist u and β such that $\mathbf{c}_u(\beta) = (c_0, c_1, \ldots, c_7)$, where $(c_0, c_1, \ldots, c_7) = (1, 1, 0, 1, 0, 0, 0, 0)$ or $(1, 1, 1, 1, 0, 1, 0, 0)$, but not both.

1. In the case when $p = 1 + 8x^2 = 9 + 64y^2$ for some odd integers x and y (it is known that H_8 is a $(p, (p-1)/8, (p-7)/64)$-cyclic difference set module p), let $\mathbf{s} = \underline{1} + \mathbf{b}_{u^0}$. Then $\mathbf{s}$ is the characteristic sequence of H_8, and it has a defining pair $< g(x), \beta >$, where

$$g(x) = \sum_{0 \le i < 8} c_{4+i} c_{u^i}(x),$$

the index $4 + i$ is modulo 8, and c_i is described as above.

2. In the case when $p = 49 + 8x^2 = 441 + 64y^2$ for some odd integers x and y (it is known that $D = H_8 \cup \{0\}$ is a $(p, (p+7)/8, (p+7)/64)$-cyclic difference set modulo p), let $\mathbf{s} = \underline{1} + \underline{\delta} + \mathbf{b}_{u^0}$. Then $\mathbf{s}$ is the characteristic sequence of $D = H_8 \cup \{0\}$, and it has a defining pair $< g(x), \beta >$, where

$$g(x) = 1 + \sum_{0 \le i < 8} (c_{4+i} + 1) c_{u^i}(x),$$

the index $4 + i$ is modulo 8, and c_i is described earlier.

Proof: Consider the cases **(O)** and **(O1)** in **Fact** 3 for $e = 8$. Let u be a generator of F_p^* where $p = 8f + 1$ is a prime with f odd. We note that $\nu = 4$. Therefore, $p \equiv 9 \pmod{16}$. **Fact** 3 says H_8 is a cyclic difference set if and only if $p = 1 + 8x^2 = 9 + 64y^2$. These two conditions are just sufficient for 2 to be an octic residue mod p (**Fact** 4). Also $H_8 \cup \{0\}$ is a cyclic difference set if and only if $p = 49 + 8x^2 = 441 + 64y^2$ for some odd integers x and y. These are also sufficient for 2 to be an octic residue mod p. Therefore, in all interesting cases where 8-th residue cyclic difference sets exist, the time 8 of Lemma 1 gives $d = 8$, and hence, $c_{u^i}(\beta) \triangleq c_i \in F_2$ for all $0 \le i < 8$. Since $\epsilon_i = c_i \in F_2$, we must have $\sum_{0 \le i < 8} c_i = 1$. Letting $w_H(\underline{c})$ be the Hamming weight of the vector $\underline{c}$, this implies that $w_H(\underline{c}) = 1, 3, 5$, or 7.

Claim that $w_H(\underline{c}) \ne 1$. Otherwise, from Lemma 5, we have $\underline{c} = (1, 0, 0, 0, 0, 0, 0, 0)$, without loss of generality. Then the 8×8 matrix C in (12) becomes $C = I_8$, and hence, $C^2 = I_8$. But the item 4 of Theorem 2 says $\Gamma^4 C^2 = \begin{pmatrix} \mathbf{0} & I_4 \\ I_4 & \mathbf{0} \end{pmatrix} = J_8 + I_8$, which is a contradiction. Now, from the same item of Theorem 2, we must also have that $w_H(\underline{c}) \ne 7$. Therefore, we must have $w_H(\underline{c}) = 3$ or 5.

Consider the case $w_H(\underline{c}) = 3$ first. We may fix $c_0 = 1$ and consider all the $\frac{1}{8}\binom{8}{3} = 7$ cyclically distinct 8-tuples as follows: $\mathbf{z}_1 = (11100000)$, $\mathbf{z}_2 = (11010000)$, $\mathbf{z}_3 = (11000010)$, $\mathbf{z}_4 = (11001000)$, $\mathbf{z}_5 = (11000100)$, $\mathbf{z}_6 = (10010010)$, and $\mathbf{z}_7 = (10001010)$. Of these, $\mathbf{z}_3 \sim \mathbf{z}_2$, $\mathbf{z}_5 \sim \mathbf{z}_4$, and $\mathbf{z}_6 \sim \mathbf{z}_1$. Thus, $\mathbf{z}_3$, $\mathbf{z}_5$ and $\mathbf{z}_6$ can be ruled out, and $\mathbf{z}_1$, $\mathbf{z}_2$, $\mathbf{z}_4$ and $\mathbf{z}_7$ remain. All these 8-tuples except for $\mathbf{z}_2$, can be ruled out by the relation given in the item 4 of Theorem 2. Therefore, only $\mathbf{z}_2$ remains. From the same item of Theorem 2 and above, we see that, for the case $w_H(\underline{c}) = 5$, the only possibility is

$$\underline{c} = \mathbf{z}_2 + \underline{1}$$

which is a complement of $\mathbf{z}_2$. Therefore, as p changes, there are u and β such that $\mathbf{c}_u(\beta) = (c_{u^0}(\beta), \ldots, c_{u^7}(\beta))$ is either

$$(1, 1, 0, 1, 0, 0, 0, 0) \quad \text{or} \quad (1, 1, 1, 1, 0, 1, 0, 0).$$

Note that the above two possibilities are not G-equivalent. The remaining two items can easily be checked using the fact that $\mathbf{s} = \underline{1} + \mathbf{b}_{u^0}$ for case 1 and $\mathbf{s} = \underline{1} + \underline{\delta} + \mathbf{b}_{u^0}$ for case 2, with $\nu = 4$. ■

IV. Concluding Remarks

In this paper, we have explicitly described trace representations of the binary characteristic sequences (of period $p = 1 + ef$) of all the cyclic difference sets D which are some union of cosets of eth powers in F_p^* for $e \le 12$, including the Hall's sextic residue sequences for $p \equiv 3 \pmod 8$ (Theorem 9). For this, we have defined a defining pair $(g(x), \beta)$ of eth power residue sequences, where $g(x)$ is a polynomial over F_{2^n} mod x^p-1, $\beta \in F_{2^n}$ is a primitive p-th root of unity, and n is the order of 2 mod p. We have investigated properties (Theorem 2) of the e-tuple vector $(c_{u^0}(\beta), c_{u^1}(\beta), \ldots, c_{u^{e-1}}(\beta))$, where $c_{u^i}(x) = \sum_{k \in u^i H_e} x^k$ is the generator polynomial of the coset $u^i H_e$, where u is a generator of F_p^* and H_e contains all the e-th powers in F_p^*. Main results in this theory are three lemmas (Lemmas 1, 3, 5) and five theorems (Theorems from 1 to 5).

We have, furthermore, determined the linear complexity of all the sixth power residue sequences of period $p = 6f+1$ with f odd (Theorem 8), and in general, that of all the eth power residue sequences whenever $(e, (p-1)/n) = 1$ (Theorem 6).

How to evaluate the e-tuple $(c_{u^0}(\beta), \ldots, c_{u^{e-1}}(\beta))$ for some u and β for a prime $p = ef+1$ seems to be an interesting problem. Theory developed in this paper has given some way to do it, as we have done here for the characteristic sequences of eth residue cyclic difference sets for $e \leq 12$. Now, how to develop the theory for $p = ef+1$ with general e is worth of studying further.

We will conclude this paper with the following. It turned out that determining the exact value of $\mathbf{c}_u(\beta) = (c_{u^0}(\beta), \ldots, c_{u^{e-1}}(\beta)) \in \mathcal{C}$ for some u and β is enough in all of the above cases, and some problems remain open.

1) When $e = 6$ or $e = 4$ with $d = 1$, any $\underline{c} = (c_0, c_1, \ldots, c_{e-1}) \in \mathcal{C}$ must be G-equivalent to only one of two possible e-tuples (not both, since they are not G-equivalent with each other). It is not known so far whether any one can be ruled out completely, or both occur as p changes.
2) Computations of $(c_{u^0}(\beta), \ldots, c_{u^{e-1}}(\beta))$ for the values of d other than those covered in the subsection for $e = 4$ or $e = 8$ also remain as future research.
3) So do those for the case $e = 6$ with f even.
4) So do the cases with $e > 12$.

APPENDIX
PROOF OF LEMMA 8

Let S, T and S_i, $1 \leq i \leq m$, be subsets of $\overline{F}_2$, $ST = \{\sum_{1 \leq i \leq k} s_i t_i \mid s_i \in S, t_i \in T, k \geq 0\}$, $Sx = \{sx \mid s \in S\}$ for any given $x \in \overline{F}_2$, and $\sum_{1 \leq i \leq m} S_i = \{\sum_{1 \leq i \leq m} s_i \mid s_i \in S_i\}$. We write $\sum_{1 \leq i \leq m} S_i = \bigoplus_{1 \leq i \leq m} S_i$ if the sum is a direct sum, that is, the sum has the property that "if $\sum_{1 \leq i \leq m} s_i = 0$ for some $s_i \in S_i$, then $s_i = 0\ \forall i$." The following lemma is well known.

Lemma 9 ([14], [16]): $F_{q^m} F_{q^n} = F_{q^M}$, where M is the least common multiple of m and n. In case $\gcd(m,n) = 1$, any basis of F_{q^n} over F_q must be a basis of $F_{q^{mn}}$ over F_{q^m}.

Assume $F = F_{p^N}$, where p is a prime, $p = 2$ or odd. It is enough to prove that F_{p^N} is not a sum of its maximal subfields, i.e.

$$\sum_{1 \leq i \leq r} F_{p^{\frac{N}{p_i}}} \subsetneqq F_{p^N}$$

where $N = \prod_{1 \leq i \leq r} p_i^{d_i}$, where p_i's are distinct primes, that is, $p_i \neq p_j$ if $1 \leq i < j \leq r$. Denote $a \triangleq \frac{N}{n}$, where $n = \prod_{1 \leq i \leq r} p_i$, and $q \triangleq p^a$. Then, $F_{p^N} = F_{q^n}$. Denote $n_i = \frac{n}{p_i}$ and $K_i = F_{q^{n_i}}$ for each $i = 1, 2, \ldots, r$. Then $K_i = F_{p^{\frac{N}{p_i}}}$, and hence, it is enough to prove

$$\sum_{1 \leq i \leq r} K_i \subsetneqq F_{q^n}. \tag{39}$$

We will prove (39) by induction on the number r of the prime factors of n. When $r = 1$, (39) is obviously true. Assume (39) is true when the number of the prime factors of n is less than r, and consider the case where the number of the prime factors of n is r. Let $dim_{F_q} F_{q^m}$ denote the vector space dimension of F_{q^m} over F_q, and define $m \triangleq dim_{F_q} \sum_{2 \leq j \leq r} F_{q^{n_1/p_j}}$. By the induction assumption, we know

$$\sum_{2 \leq j \leq r} F_{q^{n_1/p_j}} \subsetneqq F_{q^{n_1}},\ m < n_1.$$

Assume $\{x_i | 1 \leq i \leq m\}$ is a basis of $\sum_{2 \leq j \leq r} F_{q^{n_1/p_j}}$ over F_q, then there exist $\{x_j \mid m < j \leq n_1\}$ such that $\{x_i | 1 \leq i \leq n_1\}$ is a basis of $F_{q^{n_1}}$ over F_q. By Lemma 9 we see the set $\{x_i | 1 \leq i \leq n_1\}$ is also a basis of $F_{q^n} = F_{q^{p_1}} F_{q^{n_1}}$ over $K_0 \triangleq F_{q^{p_1}}$, i.e.

$$F_{q^n} = \bigoplus_{1 \leq i \leq n_1} K_0 x_i.$$

For $j \geq 2$, from Lemma 9 we have

$$K_j = F_{q^{n_j}} = F_{q^{p_1 \frac{n_1}{p_j}}} = F_{q^{p_1}} F_{q^{\frac{n_1}{p_j}}} = K_0 F_{q^{\frac{n_1}{p_j}}}$$

and thus

$$\begin{aligned}\sum_{2 \leq j \leq r} K_j &= \sum_{2 \leq j \leq r} K_0 F_{q^{n_1/p_j}} \\ &= K_0 \left(\sum_{2 \leq j \leq r} F_{q^{n_1/p_j}} \right) \\ &= K_0 \left(\sum_{1 \leq i \leq m} F_q x_i \right) \\ &= \sum_{1 \leq i \leq m} K_0 F_q x_i \\ &= \sum_{1 \leq i \leq m} K_0 x_i.\end{aligned}$$

Therefore

$$\begin{aligned}\sum_{1 \leq j \leq r} K_j &= K_1 + \sum_{2 \leq j \leq r} K_j \\ &= \sum_{1 \leq i \leq n_1} F_q x_i + \sum_{1 \leq i \leq m} K_0 x_i \\ &= \sum_{1 \leq i \leq m} K_0 x_i + \sum_{m < i \leq n_1} F_q x_i.\end{aligned}$$

Note that $m < n_1$ and $F_q \subsetneqq K_0$, we see

$$\sum_{1 \leq i \leq m} K_0 x_i + \sum_{m < i \leq n_1} F_q x_i \subsetneqq \bigoplus_{1 \leq i \leq n_1} K_0 x_i$$

hence

$$\begin{aligned}\sum_{1\leq j\leq r} K_j &= \sum_{m<i\leq n_1} F_q x_i + \sum_{1\leq i\leq m} K_0 x_i \\ &\subsetneqq \bigoplus_{1\leq i\leq n_1} K_0 x_i = F_{q^n}\end{aligned}$$

i.e., (39) is true. ■

ACKNOWLEDGMENT

One of the authors, H.-Y. Song, wishes to thank Prof. G. Gong for her support while he was visiting the University of Waterloo, for one year in 2002, and every summer from 2003 to 2006.

REFERENCES

[1] L. D. Baumert, *Cyclic Difference Sets*. New York: Springer-Verlag, 1971, vol. 182, Lecture Notes in Math..

[2] B. C. Berndt, R. J. Evans, and K. S. Williams, *Gauss and Jacobi Sums*. New York: Wiley, 1998, vol. 21, Canadian Math. Soc. Ser. Monographs and Adv. Texts.

[3] J. F. Dillon, "Multiplicative difference sets via additive characters," *Designs, Codes Cryptogr.*, vol. 17, pp. 225–235, 1999.

[4] J. F. Dillon and H. Dobbertin, "New cyclic difference sets with Singer parameters," *Preprint*, 1999.

[5] C. Ding, T. Helleseth, and W. Shan, "On the linear complexity of Legendre sequences," *IEEE Trans. Inf. Theory*, vol. 44, pp. 1276–1278, 1998.

[6] R. Evans, H. Hollmann, C. Krattenthaler, and Q. Xiang, "Gauss sums, Jacobi sums, and p-ranks of cyclic difference sets," *J. Combinator. Theory, Ser. A*, vol. 87, pp. 74–119, 1999.

[7] S. W. Golomb, *Shift Register Sequences*, Revised ed. San Francisco, CA: Holden-Day, 1967.

[8] S. W. Golomb, "Construction of signals with favourable correlation properties," in *Survey in Combinator.*, A. D. Keedwell, Ed. Cambridge, U.K.: Cambridge Univ. Press, 1991, vol. 166, LMS Lecture Note Series, pp. 1–40.

[9] S. W. Golomb and H. -Y. Song, "A conjecture on the existence of cyclic Hadamard difference sets," *J. Statist. Plan. Infer.*, vol. 62, pp. 39–41, 1997.

[10] S. W. Golomb and G. Gong, *Sequence Design for Good Correlation*. Cambridge, U.K.: Cambridge Univ. Press, 2005.

[11] G. Gong and S. W. Golomb, "Hadamard transform of three term sequences," *IEEE Trans. Inf. Theory*, vol. 45, pp. 2059–2059, 1999.

[12] G. Gong and S. W. Golomb, "Second iteration of decimation-Hadamard transform of two-level autocorrelation sequences," *IEEE Trans. Inf. Theory*, Aug. 2000, submitted for publication.

[13] M. Hall Jr., "A survey of difference sets," *Proc. Amer. Math. Soc.*, vol. 7, pp. 975–986, 1956.

[14] T. W. Hungerford, *Algebra*. New York: Springer, 1980, Graduate Texts in Math..

[15] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, second ed. New York: Springer-Verlag, 1990.

[16] N. Jacobson, *Lectures in Abstract Algebra, III, Theory of Fields and Galois Theory*, Third corrected ed. New York: Springer-Verlag, 1980.

[17] D. Jungnickel, "Difference sets," in *Contemporary Design Theory*, J. H. Dinitz and D. R. Stinson, Eds. New York: Wiley , 1992, pp. 241–324.

[18] J. -H. Kim, "On the Hadamard Sequences," Ph.D., Yonsei Univ., Dep. Electron. Eng., , 2002.

[19] J. -H. Kim and H. -Y. Song, "On the linear complexity of Hall's sextic residue sequences," *IEEE Trans. Inf. Theory*, vol. 47, pp. 2094–2096, Jun. 2001.

[20] J. -H. Kim and H. -Y. Song, "Trace representation of Legendre sequences," *Designs, Codes, Cryptogr.*, vol. 24, no. 3, pp. 343–348, Dec. 2001.

[21] J. -H. Kim, H. -Y. Song, and G. Gong, "Trace function representation of Hall's sextic residue sequences of period $p \equiv 7 (\mathrm{mod}\ 8)$," in *Mathematical Properties of Sequences and Other Related Structures*, J. -S. No, H. -Y. Song, T. Helleseth, and V. Kumar, Eds. Boston, MA: Kluwer, 2003, pp. 23–32.

[22] H. -K. Lee, J. -S. No, H. Chung, K. Yang, J. -H. Kim, and H. -Y. Song, "Trace function representation of Hall's sextic residue sequences and some new sequences with ideal autocorrelation," in *Proc. APCC'97. APCC*, Dec. 1997, pp. 536–540.

[23] R. Lidl and H. Niederreiter, *Finite Fields*. Reading, MA: Addison-Wesley, 1983, vol. 20, Encycl. Math. Appl..

[24] A. Maschietti, "Difference sets and hyperovals," *Designs, Codes Cryptogr.*, vol. 14, pp. 157–166, 1998.

[25] J. -S. No, H. -K. Lee, H. Chung, H. -Y. Song, and K. Yang, "Trace representation of Legendre sequences of Mersenne prime period," *IEEE Trans. Inf. Theory*, vol. 42, pp. 2254–2255, Nov. 1996.

[26] J. -S. No, H. Chung, and M. -S. Yun, "Binary pseudorandom sequences of period $2^m - 1$ with ideal autocorrelation generated by the polynomial $z^d + (z+1)^d$," *IEEE Trans. Inf. Theory*, vol. 44, pp. 1278–1282, May 1999.

[27] J. -S. No, S. W. Golomb, G. Gong, H. K. Lee, and P. Gaal, "Binary pseudorandom sequences of period $2^n - 1$ with ideal autocorrelation," *IEEE Trans. Inf. Theory*, vol. 44, pp. 814–817, Mar. 1998.

[28] A. Pott, "On Abelian difference set codes," *Designs, Codes Cyptogr.*, vol. 2, pp. 263–271, 1992.

[29] R. A. Rueppel, "Stream ciphers," in *Contemporary Cryptology, The Science of Information Integrity*, G. J. Simmons, Ed. New York: IEEE, 1992, ch. 2.

[30] R. A. Scholtz and L. R. Welch, "GMW sequences," *IEEE Trans. Inf. Theory*, vol. 30, pp. 548–553, 1984.

[31] M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt, *Spread Spectrum Communications Handbook*, revised ed. Rockville, MD: Comput. Sci. Press, 1985.

[32] J. Singer, "A theorem in finite projective geometry and some applications to number theory," *Trans. Amer. Math. Soc.*, vol. 43, pp. 377–385, 1938.

[33] H. -Y. Song and S. W. Golomb, "On the existence of cyclic Hadamard difference sets," *IEEE Trans. Inf. Theory*, vol. 40, pp. 1266–1268, Jul. 1994.

[34] T. Storer, *Cyclotomy and Difference Sets*. Chicago: Markham, 1967.

[35] R. G. Stanton and D. A. Sprott, "A family of difference sets," *Canad. Jour. Math.*, vol. 10, pp. 73–77, 1958.

[36] R. Turyn, "The linear generation of the Legendre sequences," *J. Soc. Indust. Appl. Math.*, vol. 12, no. 1, pp. 115–117, 1964.

Zongduo Dai was born in SiChuan, China. She graduated in 1964 from the Department of Applied Mathematics, University of Science and Technology of China.

From 1964 to 1985, she was with the Institute of Mathematics, Academia Sinica; as an Associate Professor from 1981 to 1986. From 1978 to 1981, she was with the Department of Mathematics, University of California, Berkeley, as a Visiting Scholar. From 1988 to 1989, she was a Visiting Professor with Fakultat Informatik, University of Karlsruhe, Germany, from 1989 to 1990, with the Department of Electrical Engineering, University of Linkoping, Sweden , and from 1990 to 1991, with the Department of Mathematics, University of London, RHBNC, U.K. Since 1987, she has been with the Graduate School (Beijing, China), University of Science and Technology of China as a Professor, and with the State Key Laboratory of Information Security since 1991. Her research interests include finite geometry of classical groups, coding theory, cryptography, and discrete mathematics. She has published may papers in journals and proceedings of international conferences. She is a coauthor of the book *Research on Finite Geometry and Incomplete Block Designs* (in Chinese) and the book *Nonlinear Shift Register Sequences* (in Chinese).

Guang Gong received the B.S. degree in mathematics in 1981, the M.S. degree in applied mathematics in 1985, and the Ph.D. degree in electrical engineering in 1990, from Universities in China. She received a Postdoctoral Fellowship from the Fondazione Ugo Bordoni, Rome, Italy, and spent the following year there.

After returning from Italy, she was promoted to an Associate Professor at the University of Electrical Science and Technology of China. During 1995–1998, she worked with several internationally recognized, outstanding coding experts and cryptographers, including Dr. S. W. Golomb, at the University of Southern California, Los Angeles. She first joined in 1998 the University of Waterloo, Canada, and again as an Associate Professor with the Department of Electrical and Computer Engineering in September 2000. She has been a full Professor since 2004. Her research interests are in the areas of sequence design, cryptography, and communications security. She has authored or coauthored more than 200 technical papers and one book, coauthored with Dr. Golomb, entitled as *Signal Design for Good Correlation for Wireless Communication, Cryptography and Radar* (Cambridge, U.K.: Cambridge Univ. Press, 2005).

Dr. Gong serves/served as Associate Editors for several journals including Associate Editor for Sequences for IEEE TRANSACTIONS ON INFORMATION THEORY, and served on a number of technical program committees and conferences. She has received several awards including the Best Paper Award from the Chinese Institute of Electronics in 1984, Outstanding Doctorate Faculty Award of Sichuan Province, China, in 1991, the Premiera's Research Excellence Award, Ontario, Canada, in 2001, NSERC Discovery Accelerator Supplement Award, 2009, Canada, and ORF-RE Award, 2010, Ontario, Canada.

Hong-Yeop Song (S'88–M'93–SM'08) received the B.S. degree in electronic engineering from Yonsei University, Seoul, Korea, in 1984, M.S.E.E. and Ph.D. degrees from the University of Southern California (USC), Los Angeles, in 1986 and 1991, respectively, specializing in the area of communication theory and coding.

After spending two years as a Research Staff Member with the Communication Sciences Institute at USC, and while working with Dr. S. W. Golomb, he joined Qualcomm Inc., San Diego, CA, in 1994 as a Senior Engineer and worked on a team researching and developing North American CDMA Standards for PCS and cellular air–interface systems. Finally, he joined the Department of Electrical and Electronics Engineering, Yonsei University, in 1995, and is currently working as a full professor. He visited Dr. G. Gong at the University of Waterloo, Canada, in 2002 for one year of his sabbatical leave, and every summer from 2003 to 2006. His area of research interest includes spread spectrum communication and the application of discrete mathematics into various communication and coding problems.

Dr. Song is a member of Mathematical Association of America (MAA), IEEK, KICS, and KIISC.

Dingfeng Ye received the B.S. degree from the University of Science and Technology of China (USTC) in 1988, the M.S. degree from the Institute of Mathematics, Chinese Academy of Sciences (CAS), in 1991, and the Ph.D. degree from the Graduate School, Chinese Academy of Sciences, in 1996, all in mathematics.

He is now a Professor with the Graduate School, CAS. His research interests include cryptography and information security.