Trace representation and linear complexity of binary e-th residue sequences

Zongduo Dai* Guang Gong† Hong-Yeop Song‡

November 12, 2004

Abstract

Let $p = ef + 1$ be an odd prime for some e and f. In this paper, e-th residue sequences of period p and their defining pairs are defined, and the problem of determining their trace representations is reduced to that of determining their defining pairs, and the latter is further reduced to that of evaluating the values of some e-tuples which are associated with e-th residue classes, and some properties of those e-tuples are discussed. Finally, trace representations and linear complexities of the binary characteristic sequences of all the e-th residue cyclic difference sets modulo p with $e \leq 12$ and some other e-th residue sequences are determined, based on the theory developed in this paper, and some open problems are proposed.

Key Words: Cyclic difference sets, e-th residue cyclic difference sets, Trace representations, Linear complexity, Defining pairs, Binary sequences with two-level autocorrelation, Binary Hadamard sequences.

1 Introduction

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 e-th powers in F_p^*. These are called e-th residue cyclic difference sets [1][2]. Existence and constructions for e-th residue cyclic difference sets are well summarized in [1][2]. The characteristic sequences of e-th residue cyclic difference sets are also called "cyclotomic sequences" due to their close relation with cyclotomic classes and/or cyclotomic numbers [3][5][6].

Quadratic residue difference set sequences (also called as Legendre sequences) is perhaps the most well-known class of e-th residue sequences. Its linear complexity has been determined earlier in [26] and [21], later independently in [4]. Trace representation of these sequences of period p which are Mersenne prime was determined in [20], and its full generalization in [16]. Some generalization

*Z. Dai is with State Key Laboratory of Information Security, Graduate School of Chinese Academy of Sciences, 100039, Beijing, China, E-mail: yangdai@public.bta.net.cn. Z. Dai is supported by Chinese Natural Science Foundation (Grant No. 60173016) and 973 Foundation (Grant No. 1999035804). She was visiting University of Waterloo, Canada, while she was working on this paper.

†G. Gong is with Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Ontario, Canada, Email: ggong@cacr.math.uwaterloo.ca. G. Gong's research is supported by NSERC grants RGPIN #227700-00 and RPEA.

‡H.-Y. Song is with School of Electrical and Electronics Engineering, Yonsei University, Seoul, Korea, E-mail: hy.song@coding.yonsei.ac.kr. He was visiting University of Waterloo, Canada, while he was working on this paper. He was supported in part by the Brain Korea 21 Project.

of Legendre sequences was given in [6] that gives some constructions for balanced binary sequence pairs with desirable cryptographic properties, including their 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 [18]. It is well known that there are only three such primes, namely, 31, 127, and 131071. Numerical computation was enough to check the trace representation of these three cases in [18]. Linear complexity of these sequences in general has been determined in [15]. It is a recent result that trace representation of these sequences of period $p \equiv 7 \pmod 8$ is determined [17], leaving the case where $p \equiv 3 \pmod 8$ open.

In this paper, trace representations and linear complexities of the binary characteristic sequences of all the e-th residue cyclic difference sets modulo p with $e \leq 12$ are determined. So are those of some other e-th residue sequences. Some of the results in this paper can be found elsewhere, due to partial overlap with others. For example, the results on Legendre sequences are simply a re-discovery based on the theory developed in this paper, and can be found in many earlier papers.

2 e-th residue sequences and their trace representations

At first, we make some notations for this paper. We fix a pair (p, e), where p is an odd prime, and e is a factor of $p-1$, *i.e.*, $p = ef + 1$ for some number f. We let $F_p^* = F_p \backslash \{0\}$ be the cyclic multiplicative group mod p, and let $H_e = \{x^e \mid x \in F_p^*\}$, which is a subgroup of F_p^* made of all the e-th powers in F_p^*. We let α be a primitive p-th root of unity, and let $< \alpha >^* = < \alpha > \backslash \{1\}$, where $< \alpha >$ denotes the group generated by α. We let n be the order of 2 mod p, and let $c = (p-1)/n$. We call $d \triangleq \gcd(c, e)$ the d-parameter corresponding to the chosen pair (p, e), and let $c_1 = c/d$, and $e_1 = e/d$. We know

$$ef = p - 1 = cn, \quad (p-1)/d = e_1 f = c_1 n, \quad \text{and} \quad (e_1, c_1) = 1. \tag{1}$$

We denote by $LC(\mathbf{s})$ the linear complexity of a binary sequence $\mathbf{s}$, and denote by $w_H(\underline{\rho})$ the Hamming weight of a tuple $\underline{\rho}$ over $\overline{F}$, here $\overline{F}$ is the algebraic closure of the binary field F_2. We also let $\delta(x)$ be 1 or 0 according to whether the integer x is odd or even, respectively.

Definition 1 *Let* $\mathbf{s} = \{s(t) | t \geq 0\}$ *be a binary sequence of period* $p = ef + 1$. *Then, we say* $\mathbf{s}$ *is* an e-th residue sequence *if* $s(t)$ *is constant on each of the cosets* $kH_e = \{ kx \mid x \in H_e \}$ *of* H_e *in* F_p^*, *that is, if* $s(t_1) = s(t_2)$ *whenever* $t_1 H_e = t_2 H_e$. ■

For examples, given any coset kH_e, let $\mathbf{b}_{kH_e} = \{b(t) | t \geq 0\}$, where $b(t) = 1$ for $t \in kH_e$ and $b(t) = 0$ otherwise, then $\mathbf{b}_{kH_e}$ is an e-th residue sequence. And two more examples: let $\underline{1} = \{b(t) | t \geq 0\}$, where $b(t) = 1$ for all t; and let $\mathbf{b}_* = \{b(t) | t \geq 0\}$, where $b(t) = 1$ if $t = 0 \pmod p$ and $b(t) = 0$ otherwise, then these two are also e-th residue sequences.

We will denote the sequence $\mathbf{b}_{kH_e}$ simply by $\mathbf{b}_k$ with $k \in F_p^*$. It is clear there are only e distinct sequences in the set $\{\mathbf{b}_k | k \in F_p^*\}$, and they can be represented by $\mathbf{b}_{u^i}$, for $0 \leq i < e$, where u is any given generator of the group F_p^*. It is clear that $\mathbf{b}_1 = \mathbf{b}_{u^0}$ for any u, and that

$$\underline{1} = \mathbf{b}_* + \sum_{0 \leq i < e} \mathbf{b}_{u^i}.$$

The generating polynomial of each coset kH_e is important in expressing the trace representations of e-th residue sequences, it is defined as

$$c_{kH_e}(x) = \sum_{i \in kH_e} x^i \pmod{x^p - 1}, \tag{2}$$

which will also be denoted simply by $c_k(x)$ where $k \in F_p^*$.

Definition 2 *Given a binary sequence* $\mathbf{s} = \{s(t)|t \geq 0\}$ *of period* p, *we say* $(g(x), \beta)$ *form a* defining pair *of* $\mathbf{s}$ *if* $s(t) = g(\beta^t)$ *for* $t = 0, 1, 2, ...$, *where* $g(x)$ *is a polynomial modulo* $x^p - 1$ *over* $\overline{F}$ *and* $\beta \in < \alpha >^*$. *We call* $g(x)$ the defining polynomial *of* $\mathbf{s}$, *and* β the corresponding defining element. ■

Theorem 3 *Let* $p = ef + 1$.

1. *Let* $\mathcal{L}$ *be the set of all* e*-th residue sequences of period* p. *Then* $\mathcal{L}$ *is a vector space over* F_2 *of dimension* $1 + e$, *and* $\{\mathbf{b}_{u^i}|0 \leq i < e\} \cup \{\underline{1}\}$ *is a basis of* $\mathcal{L}$ *over* F_2, *where* u *is any given generator of* F_p^*; *i.e., any* e*-th residue sequence in* $\mathcal{L}$ *can be expressed uniquely in the form of*

$$\mathbf{s}_{\mathbf{a}^*} = a_* \underline{1} + \sum_{0 \leq i < e} a_i \mathbf{b}_{u^i}, \tag{3}$$

for some binary $(1+e)$*-tuple* $\mathbf{a}^* = (a_*, \mathbf{a})$, $\mathbf{a} = (a_0, a_1, ..., a_i, ..., a_{e-1})$.

2. *Keep the notations in the above item, and let* $\beta \in < \alpha >^*$. *Corresponding to* $\mathbf{a}^*$ *and* β, *define*

$$\begin{cases} \rho_* = a_* + f \sum_{0 \leq k < e} a_k, \\ \rho_j = \sum_{0 \leq k < e} a_k c_{-u^k + j}(\beta) \end{cases}$$

and define

$$g(x) = \rho_* + \sum_{0 \leq j < e} \rho_j c_{u^j}(x). \tag{4}$$

Then $(g(x), \beta)$ *is a defining pair of* $\mathbf{s}_{\mathbf{a}^*}$.

3. *Keep the notations in the above items. Then* $LC(\mathbf{s}_{\mathbf{a}^*}) = \delta(\rho_*) + w_H(\underline{\rho})f$, *where*

$$\underline{\rho} = (\rho_0, \rho_1, \cdots, \rho_i, \cdots, \rho_{e-1}).$$

4. *Keep the notations in the above items. Let* $\mathbf{s}_{\mathbf{a}^*} = \{s(t)\}_{t \geq 0}$. *With the knowledge of the defining pair of* $\mathbf{s}_{\mathbf{a}^*}$ *as shown in* (4), *its a trace representation can be obtained immediately as follows:*

$$s(t) = \rho_* + \sum_{0 \leq i < e} Tr_1^n \left(\rho_i \sum_{\substack{0 \leq j < c_i \\ j = i \pmod e}} \beta^{u^j t} \right), \quad \forall t, \tag{5}$$

where $Tr_1^n(x) = \sum_{0 \leq i < n} x^{2^i}$ *is the trace of* x *from* F_{2^n} *to* F_2 [19]. ■

Theorem 4 *Let* $p = ef + 1$, *and let* d *be the* d*-parameter corresponding to the chosen* (p, e). *Keep the notation in* Theorem 3.

1. *The linear complexity of any* e*-th residue sequence of period* p *must be of the form* $\varepsilon + ke_1 f$ *for some* $k \in \{0, 1, 2, ..., d\}$ *and* $\varepsilon \in \{0, 1\}$. *Moreover, denote by* $N_{\varepsilon + ke_1 f}$ *the total number of the* e*-th residue sequences of period* p *with the linear complexity being equal to* $\varepsilon + ke_1 f$. *Then*

$$N_{\varepsilon + ke_1 f} = \binom{d}{k} (2^{e_1} - 1)^k.$$

2. *In the case when* $d = 1$, *we have* $N_{p-1} = N_p = 2^e - 1$, *and* $N_0 = N_1 = 1$; *moreover, let* $\mathbf{s}_{\mathbf{a}^*}$ *be the sequence as given in* (3), *then*

$$LC(\mathbf{s}_{\mathbf{a}^*}) = \begin{cases} p - 1 + \delta(a_* + fw_H(\mathbf{a})) & \text{if } \mathbf{a} \neq (0,0,...,0), \\ 1 & \text{if } \mathbf{a} = (0,0,...,0),\ a_* = 1, \\ 0 & \text{otherwise.} \end{cases}$$ ■

3 e-tuples

Based on Theorem 3, one can find explicitly trace representations of e-th residue sequences of period $p = ef + 1$, once an e-tuple of the form

$$\mathbf{c}_u(\beta) = (c_{u^0}(\beta), c_{u^1}(\beta), ..., c_{u^{e-1}}(\beta)) \tag{6}$$

is evaluated for some u which is a generator of the group F_p^* and $\beta \in < \alpha >^*$, where $c_{u^i}(\beta)$ is the value of $c_{u^i}(x)$ at $x = \beta$. In order to evaluate each component of these e-tuples, we need to study their properties. We consider the set $\mathcal{C}$ of the e-tuples $\mathbf{c}_u(\beta)$ over all possible generators u of F_p^* and all $\beta \in < \alpha >^*$. That is,

$$\mathcal{C} \triangleq \{\mathbf{c}_u(\beta) \mid \ < u >= F_p^*, \ \ \beta \in < \alpha >^*\}. \tag{7}$$

Let Ω be the set of all possible e-tuples over F_{2^n}. It is known that $\mathcal{C} \subseteq \Omega$. Define L to be the cyclically left-shift-by-1 operator, and D_λ for $1 \leq \lambda < e$ and $(\lambda, e) = 1$ to be the λ-decimation operator over Ω given as

$$L\mathbf{x} = (x_1, x_2, \cdots, x_{e-1}, x_0),\ \forall \mathbf{x} = (x_0, x_1, ..., x_{e-1}) \in \Omega, \tag{8}$$

$$D_\lambda \mathbf{x} = (x_0, x_\lambda, x_{2\lambda}, ..., x_{(e-1)\lambda}),\ \forall \mathbf{x} = (x_0, x_1, ..., x_{e-1}) \in \Omega. \tag{9}$$

Let $G \triangleq < \{L, D_\lambda \mid \gcd(\lambda, e) = 1,\ 0 < \lambda < e\ \} >$ be the group generated by L and those D_λ. It is well-known that for any i and λ with $(\lambda, e) = 1$, there exists j such that $D_\lambda L^i = L^j D_\lambda$ [27]. We say two elements $\mathbf{x}$ and $\mathbf{y}$ in Ω are equivalent under the group G (in short, G-equivalent) if there exists $\sigma \in G$ such that $\sigma(\mathbf{x}) = \mathbf{y}$, which will be denoted by $\mathbf{x} \sim \mathbf{y}$. This implies that the set $\mathcal{C}$ in (7) is an equivalent class under the group G.

Theorem 5 *Let* $\underline{c} = (c_0, c_1, \cdots, c_{e-1}) \in \mathcal{C}$, *then*

1. $c_i \in F_{2^{e_1}}$ *for all* i.

2. $\underline{c}$ *has* λ*-conjugate property for some integer* λ *which is coprime to* e_1 *in the sense that*

$$c_{i+dj} = c_i^{2^{\lambda j}} \quad \forall 0 \leq i < e, 0 \leq j < e_1.$$

Moreover, if $\underline{c}$ *has the* λ*-conjugate property, then* $D_\nu(\underline{c})$ *has the* 1*-conjugate property, where* $\nu\lambda = 1 \pmod{e_1}$.

3. *Let* $C = (c_{i,j})$ *be the square matrix of size* e *associated with the tuple* $\underline{c}$, *where* $c_{i,j} = c_{i+j}$, $0 \leq i, j < e$, *and the index* $i+j$ *are computed mod* e. *Then* C *is invertible. As a consequence, the* e*-tuple* $\underline{c}$ *has no smaller "period" than* e. *Let* $\epsilon_i = Tr_1^{e_1}(c_i) = \sum_{0 \leq j < e_1} c_i^{2^j}$, *then*

   (a) $\epsilon_i = \sum_{0 \leq j < e_1} c_{i+dj}$ *for all* i, *and hence* $\epsilon_{i+dj} = \epsilon_i$, *for all* $0 \leq i < d,\ \ 0 \leq j < e_1$.

(b) $\sum_{0\le k<d}\epsilon_k = 1$,

(c) *In case when* $d>1$, *there exists at least one* k *in the range* $0\le k<d$ *such that* $\epsilon_k = 0$.

4. *For all* $i = 0, 1, ..., e-1$,

$$\sum_{0\le j<e} c_j c_{j+i} = \begin{cases} f+1 \pmod 2 & \text{if } i \equiv \frac{e\delta(f)}{2} \pmod e \\ f \pmod 2 & \text{otherwise,} \end{cases}$$

where the subscripts $j+i$ *are computed mod* e.

5. *In the case when* $d=1$, *which is the* d*-parameter corresponding to the chosen* (p,e), *the* e*-tuple* $\underline{c}$ *is* G*-equivalent to an* e*-tuple of the form of* $\underline{\theta} = (\theta, \theta^2, \ldots, \theta^{2^{e-1}})$ *for some* θ, *where* θ *is a root of an irreducible polynomial* $p(x)$ *of degree* e_1 *over* F_2, *and* $Tr_1^{e_1}(\theta) = 1$. ■

Let $p = ef+1$, and let d be the d-parameter corresponding to the chosen pair (p,e) and $e_1 = e/d$. For any given generator u of F_p^*, let

$$\mathcal{P}_u \triangleq \{\rho_* + g_{\underline{\rho},u}(x) \mid \rho_* \in F_2,\ \underline{\rho} = (\theta_0, \theta_1, \cdots, \theta_{d-1}), \theta_i \in F_{2^{e_1}}\},$$

where

$$g_{\underline{\rho},u}(x) = \sum_{0\le i<d} \sum_{0\le j<e_1} \rho_i^{2^j} c_{u^i}(x)^{2^j}.$$

Then, for any given $\beta \in <\alpha>^*$, $(g(x), \beta)$ is a defining pair of an e-th residue sequence of period p if and only if $g(x) \in \mathcal{P}_u$. As a consequence, $\mathcal{P}_u = \mathcal{P}_v$ for any generators u and v of F_p^*.

4 Applications

Based on the theory developed above, we may determine e-tuples $\mathbf{c}_u(\beta)$ for some (p,e) with $e = 2, 4, 6, 8, 10$, and then defining pairs and trace representations of the characteristic sequences of some well-known e-th residue cyclic different sets modulo p can be determined based on these values.

Linear complexity and trace representation of Legendre sequence [25][1] of period p has been discussed in [26][21][20][4][3][6][16], which can also be obtained from the item 2(b) of the following Theorem together with the item 4 of Theorem 3.

Let $p = 2f+1$ be an odd prime and u be a generator of F_p^*. Then, $F_p^* = \{0\} \cup H_2 \cup uH_2$, where H_2 is the set of quadratic residues mod p and $uH_2 = F_p^* \setminus H_2$ is the set of quadratic non-residues mod p. Let $\mathbf{s} = \{s(t) | t \ge 0\}$ be the Legendre sequence of period p defined by the following:

$$s(t) = \begin{cases} 0 & \text{if } t \in H_2 \\ 1 & \text{otherwise.} \end{cases} \tag{10}$$

The item 1 of Theorem 3 implies that

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

where $\underline{1}$ is the all-1 sequence. Note that $\mathbf{a}^* = (a_*, a_0, a_1) = (1, 1, 0)$. Therefore, from the item 3 of Theorem 3, $\mathbf{s}$ has a defining pair $(g(x), \beta)$ where

$$g(x) = \rho_* + \rho_0 c_{u^0}(x) + \rho_1 c_{u^1}(x),$$

where

$$\rho_* = 1 + f, \quad \rho_j = c_{-u^j}(\beta), \quad j = 0, 1.$$

Now, we need to determine the value of $\mathbf{c}_u(\beta) = (c_{u^0}(\beta), c_{u^1}(\beta)) \triangleq (c_0, c_1)$. We need the following:

Lemma 6 *Keep the notations so far. Then, the parameter d is the maximum integer that divides e and that $x^d = 2$ has a solution in F_p.*

Now, we distinguish two cases where $2 \in H_2$ or $2 \notin H_2$.

Case 1 $(2 \in H_2)$**:** According to the quadratic reciprocity theorem, $2 \in H_2$ if and only if $p \equiv 1, 7 \pmod 8$, which are equivalent to $f \equiv 0, 3 \pmod 4$, respectively. This implies $d = 2$ from Lemma 6, and hence, $e_1 = 2/d = 1$. It implies that $c_i \in F_2$ for $i = 0, 1$. Therefore, from the item 3 of Theorem 5, $(\epsilon_0, \epsilon_1) = (c_0, c_1) = (1, 0)$ or $(0, 1)$ according to the choice of u and β. That is, $\mathcal{C} = \{(1, 0), (0, 1)\}$.

Case 2. $(2 \in uH_2)$**:** This case corresponds to $p \equiv 3, 5 \pmod 8$, which are equivalent to $f \equiv 1, 2 \pmod 4$, respectively. We have $d = (2, c) = 1$, and $e_1 = 2/d = 2$, and hence, $F_2 \subset F_4 = F_{2^{e_1}} \subset F_{2^n}$, and $c_i \in F_4 = \{0, 1, \omega, \omega^2\}$ for $i = 0, 1$, where ω is a primitive 3-rd root of unity. From Theorem 5, the fact that $d = 1$ implies $\epsilon_0 = 1 = c_0 + c_1$. Therefore, $c_i \in F_4 \backslash F_2$ for $i = 0, 1$, and we have $\mathcal{C} = \{(\omega^2, \omega), (\omega, \omega^2)\}$.

In conclusion, we may choose $\beta \in < \alpha >^*$ such that for any given generator u of F_p^*, we have

$$(c_{u^0}(\beta), c_u(\beta)) = \begin{cases} (1, 0) & if\ p = 1 \pmod 8 \\ (0, 1) & if\ p = 7 \pmod 8 \\ (w^2, w) & if\ p = 3 \pmod 8 \\ (w, w^2) & if\ p = 5 \pmod 8, \end{cases}$$

where $\omega \in F_4$ is a primitive 3-rd root of unity. With β and ω chosen as in the above, $(g(x), \beta)$ is a defining pair of $\mathbf{s}$, where

$$g(x) = \frac{p+1}{2} + \begin{cases} c_{u^0}(x) & \text{if } p = \pm 1 \pmod 8 \\ w c_{u^0}(x) + w^2 c_{u^1}(x) & \text{if } p = \pm 3 \pmod 8. \end{cases}$$

The linear complexity of $\mathbf{s}$ is given as

$$LC(\mathbf{s}) = \delta(\frac{p+1}{2}) + \begin{cases} \frac{p-1}{2} & \text{if } p = \pm 1 \pmod 8 \\ p - 1 & \text{if } p = \pm 3 \pmod 8. \end{cases}$$

Trace representation and linear complexity of Hall's sextic residue difference set sequences [25][1] of period p have been discussed in [18][15][17] (except the trace representation for the case $p \equiv 3 \pmod 8$), which can be obtained from the item 2(b) of the following Theorem together with the item 4 of Theorem 3, including the unsolved case $p \equiv 3 \pmod 8$.

Theorem 7 *Let $p = ef + 1$ be a prime with $e = 6$ and f odd. Let d be the d-parameter corresponding to the chosen $(p, 6)$. Then*

1. (Sextic residue sequences in general) *There exist a generator u of F_p^* and $\beta \in < \alpha >^*$ such that*

$$\mathbf{c}_u(\beta) = \begin{cases} (0, 1, 1, 0, 1, 0) & if\ d = 6, \\ (1, 0, w, 1, 0, w^2) & if\ d = 3, \\ (\gamma, \gamma^3, \gamma^2, \gamma^6, \gamma^4, \gamma^5) & if\ d = 2, \\ (\theta, \theta^2, \theta^4, \theta^8, \theta^{16}, \theta^{32}) & if\ d = 1, \end{cases}$$

where w is a root of $x^2 + x + 1$, γ is a root of $x^3 + x + 1$, and $\theta = \rho$ or $\theta = \rho + 1$ where ρ is a root of $x^6 + x^5 + 1$ (and hence, $\rho + 1$ is a root of $x^6 + x^5 + x^2 + x + 1$).

2. (Hall's sextic residue sequences) *In the case when* $p = 6f + 1 = 4z^2 + 27$ *for some integer* z, *let* $\mathbf{s}$ *be the Hall's sextic residue sequence of period* p *which is defined as the characteristic sequence of the Hall's sextic residue different set* [10] $D = H_6 \cup u^3 H_6 \cup u^i H_6$, *where* $u^i H_6$ *is the coset containing* 3. *Then*

   (a) *There exists a generator* u *of* F_p^* *and* $\beta \in < \alpha >^*$ *such that*

$$\mathbf{c}_u(\beta) = \begin{cases} (0,1,1,0,1,0) & \text{if } p = 7 \pmod 8 \\ (1,0,w,1,0,w^2) & \text{if } p = 3 \pmod 8 \end{cases}$$

   (b) *With the choice of* u *and* β *as in the above item,* $(g(x), \beta)$ *is a defining pair of* $\mathbf{s}$, *where*

$$g(x) = \begin{cases} c_{u^0}(x) & \text{if } p = 7 \pmod 8 \\ w c_{u^0}(x) + w^2 c_{u^3}(x) + \sum_{i=1,2,4,5} c_{u^i}(x) & \text{if } p = 3 \pmod 8 \end{cases}$$

   (c) *The linear complexity of* $\mathbf{s}$ *is given as*

$$LC(\mathbf{s}) = \begin{cases} \frac{p-1}{6} & \text{if } p = 7 \pmod 8 \\ p - 1 & \text{if } p = 3 \pmod 8. \end{cases}$$

■

Theorem 8 *Let* $p = ef + 1$ *with* $e = 4$ *and* f *odd. Then*

1. *There exists a generator* u *of* F_p^* *with* $2 \in uH_4$ *and* $\beta \in < \alpha >^*$, *such that* $c_{u^i}(\beta) = (\theta, \theta^2, \theta^4, \theta^8)$, *where* $\theta = \rho$ *or* $\rho + 1$, *and* ρ *is a root of the polynomial* $x^4 + x^3 + 1$ *and is a primitive* 15*-th root of unity, and hence,* $\rho + 1$ *is a root of the polynomial* $\sum_{0 \le i \le 4} x^i$ *and is a primitive* 5*-th root of unity.*

2. *In case when* $p = 4f + 1 = 1 + 4z^2$ *for some integer* z (for this case, it is known [25][1][2] that H_4 is a $(p, (p-1)/4, (p-5)/16)$-cyclic difference set mod p), *let* $\mathbf{s}$ *be the characteristic sequence of* H_4. *Then* $\mathbf{s} = \underline{1} + \mathbf{b}_{u^0}$, *and it has a defining pair* $(g(x), \beta)$, *where*

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

   and θ *is described as in the* item 1 *above. As a consequence,* $LC(\mathbf{s}) = p - 1$.

3. *In case when* $p = 9 + 4z^2$ *for some integer* z (for this case, it is known [25][1][2] that $H_4 \cup \{0\}$ is a $(p, (p+3)/4, (p+3)/16)$- cyclic difference set mod p), *let* $\mathbf{s}$ *be the characteristic sequence of the difference set* $H_4 \cup \{0\}$. *Then* $\mathbf{s} = \underline{1} + \mathbf{b}_* + \mathbf{b}_{u^0}$, *and it has a defining pair* $(g(x), \beta)$, *where*

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

   and θ *is described as in the* item 1 *above. As a consequence,* $LC(\mathbf{s}) = p$. ■

Theorem 9 *Let* $p = ef + 1$ *with* $e = 8$ *and* f *odd, and assume* $d = 8$, *where* d *is the* d*-parameter corresponding to* (p, e). *Then*

1. *There exist* u *and* $\beta \in < \alpha >^*$ *such that* $\mathbf{c}_u(\beta) = (c_0, c_1, \cdots, c_7)$, *where*

$$(c_0, c_1, \cdots, c_7) = (1,1,0,1,0,0,0,0), \quad \text{or its complement} \quad (0,0,1,0,1,1,1,1).$$

2. *In the case when* $p = 1 + 8z^2 = 9 + 64y^2$ *for some odd integers* z *and* y (for this case, it is known [25][1][2] that H_8 is a $(p, (p-1)/8, (p-7)/64)$-cyclic difference set mod p), *let* $\mathbf{s}$ *be the characteristic sequence of* H_8. *Then* $\mathbf{s} = \underline{1} + \mathbf{b}_{u^0}$, *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 indexes $4 + i$ *is modulo* 8, *and* c_i *is described as in the* item 1 *above.*

3. *In the case when* $p = 49 + 8z^2 = 441 + 64y^2$ *for some odd integers* z *and* y (for this case, it is known [25][1][2] that $D = H_8 \cup \{0\}$ is a $(p, (p+7)/8, (p+7)/64)$-cyclic difference set mod p), *let* $\mathbf{s}$ *be the characteristic sequence of* $D = H_8 \cup \{0\}$. *Then* $\mathbf{s} = \underline{1} + \mathbf{b}_* + \mathbf{b}_{u^0}$, *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 subscript $4 + i$ *is computed mod* 8, *and* c_i *is described as in the* item 1 *above.* ■

Theorem 10 *Let* $p = 31$, $e = 10$, *and let* $\mathbf{s}$ *be the characteristic sequence of the cyclic difference set* $D = H_{10} \cup 11H_{10} = \{i \pmod{31} \mid i = 1, 5, 11, 24, 25, 27\}$ [25][1]. *Let* β *be a root of the polynomial* $x^5 + x^2 + 1$. *Then*

1. $\mathbf{c}_{11}(\beta) = (c_0, c_1, \cdots, c_9)$, *where* $c_{2j} = \beta^{-7 \cdot 2^{4j}}$, $c_{2j+1} = \beta^{-2^{4j}}$, $0 \le j < 5$.
2. $\mathbf{s} = \underline{1} + \mathbf{b}_1 + \mathbf{b}_{11}$.
3. *Let*

$$g(x) = 1 + \sum_{0 \le j < 5} \left(\beta^{11 \cdot 2^{4j}} c_{11^{2j}}(x) + \beta^{18 \cdot 2^{4j}} c_{11^{2j+1}}(x) \right).$$

Then $(g(x), \beta)$ *is a defining pair of* $\mathbf{s}$. ■

5 Concluding remarks

In this paper, for the binary characteristic sequences (of period p) of all the cyclic difference sets D which are some union of cosets of e-th powers in F_p^* for $e \le 12$, including the Hall's sextic residue sequences for $p \equiv 3 \pmod 8$, their defining pairs, and then trace representations and linear complexities are determined based on the evaluation of the e-tuples $\mathbf{c}_u(\beta)$. In particular, linear complexities of all e-th residue sequences are determined whenever $d = \gcd(e, (p-1)/n) = 1$, where n is the order of 2 mod p.

How to evaluate the e-tuple $(c_{u^0}(\beta), ..., c_{u^{e-1}}(\beta))$ for some u and β whenever a prime $p = ef + 1$ is given seems to be an interesting problem. Theory provided in this paper has given some way to do it, as we do for all the characteristic sequences of the e-th residue cyclic difference sets for $e \le 12$ including the Legendre sequences and the Hall's sextic residue sequences, and many others. However, how to develop the theory for the general e with $p = ef + 1$ is worth of studying further.

Open Problem: Which one among the two values ρ and $\rho + 1$ the element θ in Theorem 7 or in Theorem 8 takes has not been determined yet, and we do not know whether both values will be taken when p changes; and the same problem for the tuple $(c_0, c_1, \cdots, c_7)$ in Theorem 9.

References

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

[2] B. C. Berndt, R. J. Evans and K. S. Williams, *Gauss and Jacobi Sums*, Canadian Mathematical Society Series of Monographs and Advanced Texts, vol 21., John-Wiley and Sons, New York, 1998.

[3] T. Cusick, C. Ding, A. Renvall, *Steam Ciphers and Number Theory*, North-Holland Mathematical Library, vol. 50, North-Holland/Elsevier, 1998.

[4] C. Ding, T. Helleseth, and W. Shan, "On the linear complexity of Legendre sequences," *IEEE Trans. Inform. Theory*, vol. 44, no. 3, pp. 1276-1278, 1998.

[5] C. Ding, T. Helleseth, K.Y. Lam, Several classes of binary sequences with three-level autocorrelation, *IEEE Trans. Inform. Theory*, vol. 45, no. 7, pp. 2606–2612, 1999.

[6] C. Ding, T. Helleseth, K.Y. Lam, Duadic sequences of prime lengths, *Discrete Mathematics*, vol. 218, no. 1-3, pp. 33-49, 2000.

[7] S. W. Golomb, *Shift Register Sequences*, Holden-Day, San Francisco, CA, 1967; Revised Edition, Aegean Park Press, Laguna Hills, CA, 1982.

[8] S. W. Golomb, "Construction of signals with favourable correlation properties," in *Survey in Combinatorics*, A. D. Keedwell, Editor; LMS Lecture Note Series 166, Cambridge University Press, pp. 1-40, 1991.

[9] G. Gong, *Lecture Notes on Sequence Design and Analysis*, pre-print, on the webpage of `http://calliope.uwaterloo.ca/~ggong`, 2000.

[10] M. Hall Jr., "A Survey of Difference Sets," *Proc. Amer. Math. Soc.*, vol. 7, pp. 975-986, 1956.

[11] D. Jungnickel, "Difference Sets," in *Contemporary Design Theory* edited by J. H. Dinitz and D. R. Stinson, pp. 241-324, John Wiley & Sons, Inc., New York, 1992.

[12] J. -H. Kim, *On the Hadamard Sequences*, PhD Thesis, Dept. of Electronics Engineering, Yonsei University, Feb. 2002.

[13] J. -H. Kim, M. Shin, and H. -Y. Song, "Linear complexity of Jacobi sequences," pre-print, 1999.

[14] J. -H. Kim and H. -Y. Song, "Existence of Cyclic Hadamard Difference Sets and its Relation to Binary Sequences with Ideal Autocorrelation," *Journal of Communications and Networks*, vol. 1, no.1, pp. 14-18, March 1999.

[15] J. -H. Kim and H. -Y. Song, "On the linear complexity of hall's sextic residue sequences," *IEEE Trans. Inform. Theory*, vol. 47, no. 5, pp. 2094–2096, June 2001.

[16] J. -H. Kim and H. -Y. Song, "Trace Representation of Legendre Sequences," *Designs, Codes and Cryptography*, vol. 24, no. 3, pp. 343-348, December 2001.

[17] J. -H. Kim, H. -Y. Song, and G. Gong, "Trace Function Representation of Hall's Sextic Residue Sequences of Period $p \equiv 7 \pmod 8$)," to appear in *Mathematical Properties of Sequences and Other Related Structures*, edited by J. -S. No, H. -Y. Song, T. Helleseth, and V. Kumar, Kluwer, New York.

[18] 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 *Proceedings of APCC'97*. APCC, Dec. 1997, pp. 536–540.

[19] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and Its Applications, vol. 20, Addison-Wesley, Reading, MA, 1983.

[20] 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. Inform. Theory*, vol. 42, no. 6, pp. 2254-2255, Nov. 1996.

[21] A. Pott, "On Abelian Difference Set Codes," *Designs, Codes and Cyptography*, vol. 2, pp. 263-271, 1992.

[22] R. A. Scholtz and L. R. Welch, "GMW Sequences," *IEEE Trans. Inform. Theory*, vol. 30, no. 3, pp. 548-553, 1984.

[23] M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt, *Spread Spectrum Communications Handbook*, Computer Science Press, Rockville, MD, 1985; revised edition, McGraw-Hill, 1994.

[24] J. Singer, "A Theorem in Finite Projective Geometry and Some Applications to Number Theory," *Trans. Amer. Math. Soc.*, vol. 43, pp. 377-385, 1938.

[25] T. Storer, *Cyclotomy and Difference Sets*, Markham Publishing Co., Chicago, 1967.

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

[27] N. Zierler, "Linear recurring sequences," *J. Soc. Indust. Appl. Math.*, vol. 7, pp. 31-48, 1959.