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

WCC2003
March 24-28, 2003

Zongduo Dai
State Key Laboratory of Information Security,
Chinese Academy of Sciences, Beijing, China

Guang Gong
Dept. Electrical and Computer Engineering,
University of Waterloo, Waterloo, ON, Canada

Hong-Yeop Song
School of Electrical and Electronics Engineering,
Yonsei University, Seoul, Korea
hy.song@coding.yonsei.ac.kr

I. Introduction

◇ **In this presentation, we would like to announce that ...**

- We define binary e-th residue sequences $\mathbf{s} = \{s(t) | t \geq 0\}$ of period $p = 1 + ef$ that is constant on the cosets of F_p^* mod H_e.
- We try to give a general description on their
  1. defining pairs of the form $(g(x), \beta)$ such that $s(t) = g(\beta^t)$ for $t = 0, 1, 2, ...,$
  2. trace representations, and
  3. minimal polynomials, and hence, their linear complexities.
- For simplicity, we considered (and were able to give answers to) all e-th residue sequences for $e = 2$ and $e = 6$, and the e-th residue sequences that are characteristic sequences of e-th power residue cyclic difference sets for $e = 4$, 8, and 10 (as given in Baumert '71 or Storer '67 or Berndt, Evans, and Williams '98)
- The methodology will work for any e-th residue sequences whether they are characteristic sequences of some cyclic difference sets or not.

- A (v, k, λ) cyclic difference set D is a k-subset of $\mathbb{Z}_v \triangleq \mathbb{Z}/v\mathbb{Z}$ such that for all non-zero $d \in \mathbb{Z}_v$ the equation

$$x - y \equiv d \pmod{v}$$

has exactly λ solution pairs (x, y) with $x, y \in D$.

- A binary sequence $\mathbf{s} = \{s(t) | t \geq 0\}$ (or "the characteristic sequence") of a (v, k, λ)-CDS of period v, defined by $s(t) = 0$ iff $t \in D$, has 2-level autocorrelation values, given as

$$\phi(\tau) = \begin{cases} v & \tau \equiv 0 \pmod{v} \\ v - 4(k - \lambda) & \tau \not\equiv 0 \pmod{v}. \end{cases}$$

- A cyclic Hadamard difference set is a $(v, (v-1)/2, (v-3)/4)$-cyclic difference set, and known to be equivalent to a balanced binary sequence of period v with ideal autocorrelation: $\phi(\tau) = -1$ for all $\tau \not\equiv 0 \pmod{v}$. .

Conjecture 1 *If a cyclic Hadamard difference set of length v exists, then v must be either*

(i) a prime congruent to 3 mod 4,
(ii) a product of twin primes, or
(iii) one less than a power of 2.

- A series of computer search confirms the conjecture is true for $v < 10000$ except possibly for the following 13 cases: $\mathbf{3439}$, 4355, 4623, 5775, 7395, 7743, 8227, 8463, 8591, 8835, 9135, 9215, and 9423.

1. H. -Y. Song and S. W. Golomb, "On the existence of cyclic Hadamard difference sets," *IEEE Trans. Inform. Theory*, vol. 40, no. 4, pp. 1266-1268, July 1994.
2. 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.
3. J. -H. Kim, *On the Hadamard Sequences*, PhD Thesis, Dept Electronics Engineering, Yonsei University, Feb. 2002.

- For those three types of v, we have the following constructions:

1. $v = p \equiv 3 \pmod 4$ is a prime:
   (a) Quadratic residue construction works for all such p.
   (b) Hall's sextic residue construction works for $p = 4x^2 + 27$.

2. $v = p(p+2)$ is a product of twin primes:
   (a) Generalization of "Quadratic residue construction" works.

3. $v = 2^t - 1$ for $t = 1, 2, 3, ...$
   (a) m-sequence (or maximal LFSR sequence) for all such t.
   (b) GMW construction for all "composite" t.
   (c) 3-term trace sequences, 5-term trace sequences
   (d) hyperoval type (Segre Type, and Glyn Type I and Type II)

Example 1 *Binary sequences of period* $31 = 4 \cdot 1^2 + 27 = 1 + 6 \cdot 5$. *Note that* 3 *is a generator of* F_{31}^* *and we have*

Cosets	*Legendre*	*Hall's sextic*
$C_* = \{0\}$		
$C_0 = \{1, 2, 4, 8, 16\}$	x	x
$C_1 = \{3, 6, 12, 24, 17\}$		x
$C_2 = \{9, 18, 5, 10, 20\}$	x	
$C_3 = \{27, 23, 15, 30, 29\}$		x
$C_4 = \{19, 7, 14, 28, 25\}$	x	
$C_5 = \{26, 21, 11, 22, 13\}$		

$i:$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
$a(i):$	1	0	0	1	0	0	1	0	0	0	0	1	1	1	0	1	0	1	0	0	0	1	1	1	1	0	1	1	0	1	1
$b(i):$	1	0	0	0	0	1	0	1	0	1	1	1	0	1	1	0	0	0	1	1	1	1	1	0	0	1	1	0	1	0	0

- *The Hall's sextic residue sequence* $b(i)$ *turns out to be equivalent to m-sequence of period* $31 = 2^5 - 1$.

- Motivation of the current research

1. Those of length type (i) or type (ii) are originally constructed much differently from those of length type (iii) that can naturally be described using a trace function or a sum of trace functions.

2. So, what is the trace representation of those of length type (i) or (ii) ?

3. What are their minimal polynomials (and hence, the linear complexity) ?

4. Will it help to settle the conjecture ? — Well, not much yet...

- Historical Review on "Quadratic residue sequences"
  1. (Turyn '64) Linear generation of quadratic residue sequences
  2. (Pott, '92) Abelian difference set codes
  3. (No, Chung, Yang, Song, '96) Trace representation of Legendre sequences of Mersenne prime period
  4. (Ding, Helleseth, Shan, '98) Linear complexity of Legendre sequences
  5. (Kim, Song, '01) Trace representation of Legendre sequences

- on "Hall's sextic residue sequences"
  1. (Lee, No, Chung, Yang, Kim, Song, '97) Trace representation for Mersenne Prime periods:31, 127, and 131071.
  2. (Kim, Song, '01) Linear complexity of Hall's sextic residue sequences
  3. (Kim, Gong, Song, '02) Trace representation of HSR sequences of period $p \equiv 7 \pmod 8$.
  4. This paper completes "trace representation of HSR sequences" including the case $p \equiv 3 \pmod 8$

- on twin-prime sequences
  1. (Ding, '97) Linear complexity of generalized cyclotomic sequences of order 2
  2. (Kim, Song, '99) Linear complexity of binary Jacobi sequences (unpublished)
  3. (Dai, Gong, Song, '02) Trace representation of binary Jacobi sequences (submitted)

- The conjecture is still widely open !

II. e-th residue sequences and their trace representations

- p is an odd prime, and $p = ef + 1$ for some e, f
- $F_p^* = F_p \backslash \{0\}$ and $H_e = \{x^e \mid x \in F_p^*\}$
- α be a primitive p-th root of unity, and let $< \alpha >^* = < \alpha > \backslash \{1\}$
- n is the order of 2 mod p, $c = (p-1)/n$, $d = \gcd(c, e)$, $c_1 = c/d$, and $e_1 = e/d$ so that

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

- $LC(\mathbf{s})$ is the linear complexity of a binary sequence $\mathbf{s}$
- $w_H(\underline{\rho})$ is the Hamming weight of a tuple $\underline{\rho}$ over $\overline{F}$
- $\delta(x) = 1$ (or 0) if the integer x is odd (or even), respectively.

Definition 1 (e-th residue sequences) *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* $t_1 H_e = t_2 H_e$.

Example 2 (single coset sequences) *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.*

Example 3 *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

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

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 1 *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*

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

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

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

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

and define

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

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

3. *Keep the notations in the above items. Then*

$$LC(\mathbf{s_{a^*}}) = \delta(\rho_*) + w_H(\underline{\rho})f,$$

where

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

which is given in the item 2 above.

4. *Keep the notations in the above items. Let* $\mathbf{s_{a^*}} = \{s(t)|t \geq 0\}$. *With the knowledge of the defining pair of* $\mathbf{s_{a^*}}$ *as shown in the item 2 above, its a trace representation can be obtained immediately as follows:*

$$s(t) = \rho_* + \sum_{0 \leq i < e} \mathsf{Tr}_1^n \left(\rho_i \sum_{\substack{0 \leq j < c, \\ j = i \pmod e}} \beta^{u^j t} \right), \quad \forall t,$$

where $\mathsf{Tr}_1^n(x) = \sum_{0 \leq i < n} x^{2^i}$ *is the trace of* x *from* F_{2^n} *to* F_2.

Proof. The item 1 is obvious. For the item 2, we let $r(x) = \sum_{0\le k<p} r_k x^k \pmod{x^p - 1}$ be the defining polynomial of $\mathbf{b}_{u^i}$ corresponding to β, and take the inverse Fourier transform:

$$b_{u^i}(t) = r(\beta^t) = \sum_{0\le k<p} r_k \beta^{kt}, \text{ or } r_k = \sum_{0\le t<p} b_{u^i}(t)\beta^{-kt}.$$

For $k = 0$,

$$r_0 = \sum_{0\le t<p} b_{u^i}(t) = |u^i H_e| = f.$$

For $k \in F_p^*$, we have

$$r_k = \sum_{0\le t<p} b_{u^i}(t)\beta^{-kt} = \sum_{t\in u^i H_e} \beta^{-kt} = \sum_{t\in -ku^i H_e} \beta^t = c_{-ku^i}(\beta).$$

Note that if $kH_e = lH_e$ then $-ku^iH_e = -lu^iH_e$, and hence

$$r_k = c_{-ku^i}(\beta) = c_{-lu^i}(\beta) = r_l.$$

Therefore, r_k depends only on the coset of H_e in F_p^* to which k belongs. Denoting $k = u^j \in F_p^*$ for j with $0 \le j < p-1$, we obtain the following useful relation:

$$r_{u^j} = c_{-u^{i+j}}(\beta) = c_{-u^{i+j+em}}(\beta) = r_{u^{j+em}}, \quad \forall m.$$

Therefore,

$$\begin{aligned} r(x) &= f + \sum_{1\le k<p} r_k x^k = f + \sum_{0\le j<p-1} r_{u^j} x^{u^j} = f + \sum_{0\le j<e}\sum_{0\le k<f} r_{u^{j+ek}} x^{u^{j+ek}} \\ &= f + \sum_{0\le j<e} r_{u^j} \sum_{0\le k<f} x^{u^{j+ek}} = f + \sum_{0\le j<e} c_{-u^{i+j}}(\beta) c_{u^j}(x) \stackrel{\triangle}{=} g_{u^i}(x). \end{aligned}$$

Clearly, $(g_{\mathbf{1}}(x) = 1, \beta)$ is a defining pair of the all-1 sequence $\mathbf{1}$. Therefore,

$$\begin{aligned} g(x) &= a_* + \sum_{0\le i<e} a_i g_{u^i}(x) \\ &= a_* + \sum_{0\le i<e} a_i \left(f + \sum_{0\le j<e} c_{-u^{i+j}}(\beta) c_{u^j}(x) \right) \\ &= a_* + f \sum_{0\le i<e} a_i + \sum_{0\le j<e} \left(\sum_{0\le i<e} a_i c_{-u^{i+j}}(\beta) \right) c_{u^j}(x) \\ &= \rho_* + \sum_{0\le j<e} \rho_j c_{u^j}(x). \end{aligned}$$

The item 3 is obvious since LC is given as the number of non-zero terms in $g(x)$. For trace representation in the item 4, we first determine the trace representation of $\mathbf{b}_{u^i}$ as follows: Since it is a binary sequence, we have, using $r(x) = g_{u^i}(x) \pmod{x^p - 1}$,

$$\sum_{0 \le k < p} r_k^2 \beta^{2t} = r(\beta^t)^2 = b_{u^i}(t)^2 = b_{u^i}(t) = r(\beta^t) = \sum_{0 \le k < p} r_k \beta^t,$$

or

$$r_k^2 = r_{2k} \text{ or } r_k^{2^l} = r_{2^l k} \quad \forall l.$$

Since both 2 and u^c have order n, we have $< 2 >=< u^c >$ and

$$F_p^* = \bigcup_{0 \le i < c} u^i < u^c >= \bigcup_{0 \le i < c} u^i < 2 >.$$

Therefore, we have

$$\begin{aligned} b_{u^i}(t) &= r_0 + \sum_{0 \le j < p-1} r_{u^j} \beta^{u^j t} = r_0 + \sum_{\substack{0 \le j < c \\ 0 \le l < n}} r_{u^j 2^l} \beta^{u^j 2^l t} = r_0 + \sum_{\substack{0 \le j < c \\ 0 \le l < n}} \left(r_{u^j} \beta^{u^j t} \right)^{2^l} \\ &= r_0 + \sum_{0 \le j < c} \mathrm{Tr}_1^n \left(r_{u^j} \beta^{u^j t} \right) = f + \sum_{0 \le j < c} \mathrm{Tr}_1^n \left(c_{-u^{i+j}}(\beta) \beta^{u^j t} \right). \end{aligned}$$

Therefore, we have

$$
\begin{aligned}
s(t) &= a_* + \sum_{0 \le i < e} a_i b_{u^i}(t) \\
&= a_* + \sum_{0 \le i < e} a_i \left(f + \sum_{0 \le j < c} \mathsf{Tr}_1^n \left(c_{-u^{i+j}}(\beta) \beta^{u^j t} \right) \right) \\
&= a_* + f \sum_{0 \le i < e} a_i + \sum_{0 \le j < c} \mathsf{Tr}_1^n \left(\sum_{0 \le i < e} a_i c_{-u^{i+j}}(\beta) \beta^{u^j t} \right) \\
&= \rho_* + \sum_{0 \le j < c} \mathsf{Tr}_1^n \left(\rho_j \beta^{u^j t} \right) \\
&= \rho_* + \sum_{0 \le i < e} \mathsf{Tr}_1^n \left(\rho_i \sum_{\substack{0 \le j < c \\ j = i \pmod{e}}} \beta^{u^j t} \right).
\end{aligned}
$$

Theorem 2 *Let $p = ef + 1$, and let d be the d-parameter corresponding to the chosen (p, e). Keep the notation in* Theorem 1.

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*

$$N_{\varepsilon+ke_1f} = \binom{d}{k}(2^{e_1} - 1)^k.$$

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 Theorem 1, then*

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

where we use the notation $\mathbf{a} = (a_0, a_1, ..., a_{e-1})$.

III. e-tuples

Based on Theorem 1, it is enough to focus on the e-tuple of the form

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

for trace representation and minimal polynomials, etc.

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,

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

Then, it is an equivalence class under the group $G \triangleq \ < \{L, D_\lambda \mid \gcd(\lambda, e) = 1, \ 0 < \lambda < e \ \} >$ where

$$\begin{aligned} L\mathbf{x} &= (x_1, x_2, \cdots, x_{e-1}, x_0), \ \forall \mathbf{x} = (x_0, x_1, ..., x_{e-1}), \\ D_\lambda \mathbf{x} &= (x_0, x_\lambda, x_{2\lambda}, ..., x_{(e-1)\lambda}), \ \forall \mathbf{x} = (x_0, x_1, ..., x_{e-1}). \end{aligned}$$

Theorem 3 *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) $\sum_{0 \leq k < d} \epsilon_k = 1$,
   (c) *In case when* $d > 1$, *there exists at least one* k *in the range* $0 \leq k < d$ *such that* $\epsilon_k = 0$.

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

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

   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* $Tr_1^{e_1}(\theta) = 1$. ■

IV. Applications

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 $uH_2 = F_p^* \backslash H_2$ is the set of quadratic non-residues mod p. Let $\mathbf{s} = \{s(t) | t \geq 0\}$ be the Legendre sequence of period p defined by the following:

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

The item 1 of Theorem 1 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 1, 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 1 *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 1, 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 3, $(\epsilon_0, \epsilon_1) = (c_0, c_1) = (1, 0)$ 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 3, 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

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

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

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

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

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

Theorem 4 *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*

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

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 $D = H_6 \cup u^3 H_6 \cup u^i H_6$, 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*

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

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

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

(c) *The trace representation and linear complexity of* $\mathbf{s}$ *is given as follows:*

$$s(t) = \sum_{\substack{0 \le m < c \\ m \equiv 0 \pmod 6}} \mathsf{Tr}_1^n\left(\beta^{u^m t}\right) = \sum_{m=0}^{c/6-1} \mathsf{Tr}_1^n\left(\beta^{u^{6m} t}\right), \quad LC = (p-1)/6,$$

$$s(t) = \sum_{\substack{0 \le m < c \\ m \equiv 0 \pmod 6}} \mathsf{Tr}_1^n\left(\omega\beta^{u^m t}\right) + \sum_{\substack{0 \le m < c \\ m \equiv 3 \pmod 6}} \mathsf{Tr}_1^n\left(\omega^2\beta^{u^m t}\right) + \sum_{\substack{0 \le m < c \\ m \not\equiv 0 \pmod 3}} \mathsf{Tr}_1^n\left(\beta^{u^m t}\right), \quad LC = p-1.$$

Theorem 5 *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 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 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 6 *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*

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

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 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 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 7 *Let* $p = 31$, $e = 10$, *and let* $\mathbf{s}$ *be the characteristic sequence of the cyclic difference set* $D = H_{10} \cup 11H_{10} = \{i \pmod{31} \mid i = 1, 5, 11, 24, 25, 27\}$. *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* $\mathbf{s}$. ■

V. Concluding remarks

- Binary 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 $e \leq 12$ are studied in terms of
  - their defining pairs,
  - trace representations,
  - linear complexities.
- In particular, linear complexities of all the 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 ?
- **Open Problem**: Which one among the two values ρ and $\rho + 1$ the element θ in Theorem 4 or in Theorem 5 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 6.