Trace representation of binary e-th residue sequences of period p

2003 IEEE ISIT
June 29 - July 4, 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

Cyclic difference sets and characteristic sequences

- 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 $x, y \in D$.

- The set $\{1, 3, 4, 5, 9\} \subset Z_{11}$ is a $(11, 5, 2)$-CDS, since

$-$	1	3	4	5	9
1	0	9	8	7	3
3	2	0	10	9	5
4	3	1	0	10	6
5	4	2	1	0	7
9	8	6	5	4	0

- A binary sequence $\mathbf{s} = \{s(t) | t \geq 0\}$ (or "the characteristic sequence") of a (v, k, λ)-CDS of period v is defined by $s(t) = 0$ iff $t \in D$.

- An e-th power residue cyclic difference set mod $p = ef + 1$ is a $(v = p, k, \lambda)$ CDS which are some union of cosets of the subgroup H_e of e-th powers in F_p^*, with or without $\{0\}$.
- (Storer '67, Baumert '71, Berndt-Evans-Williams '98) The ONLY e-th power residue cyclic difference sets for $e \le 12$ are the following:

e	D	(v, k, λ)	when
2	H_2	$(p, \frac{p-1}{2}, \frac{p-3}{4})$	$p = 4z + 3$ [hadamard]
6	$H_6 \cup u^3 H_6 \cup u^1 H_6$	$(p, \frac{p-1}{2}, \frac{p-3}{4})$	$p = 4z^2 + 27 \quad (3 \in uH_6)$ [hadamard]
4	H_4	$(p, \frac{p-1}{4}, \frac{p-5}{16})$	$p = 1 + 4z^2$
	$H_4 \cup \{0\}$	$(p, \frac{p+3}{4}, \frac{p+3}{16})$	$p = 9 + 4z^2$
8	H_8	$(p, \frac{p-1}{8}, \frac{p-7}{64})$	$p = 1 + 8z^2 = 9 + 64y^2$ (odd z, y)
	$H_8 \cup \{0\}$	$(p, \frac{p+7}{8}, \frac{p+7}{64})$	$p = 49 + 8z^2 = 441 + 64y^2$ (odd z, y)
10	$H_{10} \cup uH_{10}$	$(31, 6, 1)$	$p = 31$ (use $u = 11$) [single case]

- A cyclic Hadamard difference set is a $(v, (v-1)/2, (v-3)/4)$-cyclic difference set and are equivalent to balanced binary sequences with the ideal autocorrelation.
- KNOWN three types of v for which a cyclic Hadamard difference set exists:
  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 $t = 1, 2, 3, \ldots$.
     (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)
     (e) what else ?? (conjecture: no more for odd t. Checked partially for $t \leq 17$ by Gong-Golomb '02, and completely for $t \leq 10$ by many others.)
- conjecture: no more v for CHDS. Checked for $v < 10000$ by Song-Golomb '94, Kim-Song '99.

- Cyclic Hadamard difference sets which are some union of cosets of sextic residues in F_{31}^*. (Example for $e = 6$)

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	
$C_5 = \{26, 21, 11, 22, 13\}$		

- Their characteristic sequences are:

$i:$	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 the m-sequence of period $31 = 2^5 - 1$.

e-th residue sequences and their trace representations

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 $t_1 H_e = t_2 H_e$.*

- $\underline{\mathbf{1}} = \{b(t) = 1|t \geq 0\}$
- $\mathbf{b}_* = \{b(t)|t \geq 0\}$, where $b(t) = \begin{cases} 1, & t = 0 \pmod{p} \\ 0, & \text{otherwise} \end{cases}$.
- $\mathbf{b}_{kH_e} \triangleq \mathbf{b}_k = \{b(t)|t \geq 0\}$, where $b(t) = \begin{cases} 1, & t \in kH_e \\ 0, & \text{otherwise} \end{cases}$.
- Legendre sequence: $\mathbf{s} = \underline{\mathbf{1}} + \mathbf{b}_1$.
- Hall's sextic residue sequence: $\mathbf{s} = \underline{\mathbf{1}} + \mathbf{b}_1 + \mathbf{b}_u + \mathbf{b}_{u^3}$.
- In general, we have $\underline{1} = \mathbf{b}_* + \sum_{0 \leq i < e} \mathbf{b}_{u^i}$.

Theorem 0

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

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

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

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* $t = 0, 1, 2, \ldots$, *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.*

Let the generating polynomial of a coset $u^j H_e$ be given as

$$c_{u^j H_e}(x) = c_{u^j}(x) = \sum_{i \in u^j H_e} x^i = \sum_{0 \leq i < f} x^{u^{j+ei}} \pmod{x^p - 1}$$

Theorem 1 *Let $p = ef + 1$ be a prime for some e and f.*

1. $\mathbf{s}_{\mathbf{a}^*} = a_* \underline{1} + \sum_{0 \le i < e} a_i \mathbf{b}_{u^i}$, *for some unique* $\mathbf{a}^* = (a_*, a_0, a_1, \ldots, a_i, \ldots, a_{e-1})$.

2. $\mathbf{s}_{\mathbf{a}^*}$ *has the defining pair* $(g(x), \beta)$ *where*
$$g(x) = \rho_* + \sum_{0 \le j < e} \rho_j c_{u^j}(x),$$
where $\rho_* = a_* + f \sum_{0 \le i < e} a_i$ *and* $\rho_j = \sum_{0 \le i < e} a_i c_{-u^{i+j}}(\beta)$.

3. $LC(\mathbf{s}_{\mathbf{a}^*}) = \delta(\rho_*) + w_H(\underline{\rho}) f$, *where* $\delta(\cdot) = 1$ *or* 0; $w_H(\ldots)$ *is the Hamming weight; and*
$$\underline{\rho} = (\rho_0, \rho_1, \cdots, \rho_i, \cdots, \rho_{e-1}).$$

4. *Finally, using* $c \triangleq (p-1)/n$ *where* n *is the order of* 2 mod p,
$$s(t) = \rho_* + \sum_{0 \le i < e} \mathrm{Tr}_1^n \left(\rho_i \sum_{\substack{0 \le j < c, \\ j = i \pmod{e}}} \beta^{u^j t} \right), \quad \forall t.$$

Two Examples

$\diamond$ **Case** $e = 2$ Let $p = 2f + 1$ be an odd prime and u be a generator of F_p^* and H_2 be the set of quadratic residues mod p. Then any quadratic residue sequence $\mathrm{s} = \{s(t) | t \geq 0\}$ of period p can be written uniquely as

$$\mathbf{s} = a_* \underline{1} + a_0 \mathbf{b}_{u^0} + a_1 \mathbf{b}_{u^1}.$$

It has the defining polynomial $g(x) = \rho_* + \rho_0 c_{u^0}(x) + \rho_1 c_{u^1}(x)$, where

$$\rho_* = a_* + (a_0 + a_1) f \quad \text{and} \quad \begin{cases} \rho_0 &= a_0 c_{-u^0}(\beta) + a_1 c_{-u^1}(\beta) \\ \rho_1 &= a_0 c_{-u^1}(\beta) + a_1 c_{-u^0}(\beta). \end{cases}$$

The linear complexity is given as $LC(\mathbf{s}_{\mathbf{a}^*}) = \delta(\rho_*) + w_H(\rho_0, \rho_1) f$, and, for all t,

$$s(t) = \rho_* + \mathrm{Tr}_1^n \left(\rho_0 \sum_{j=0}^{\frac{p-1}{2n}-1} \beta^{u^{2j}t} + \rho_1 \sum_{j=0}^{\frac{p-1}{2n}-1} \beta^{u^{2j+1}t} \right).$$

Now, we only need to determine the values of $(c_{u^0}(\beta), c_{u^1}(\beta)) \triangleq (c_0, c_1)$.

◇ **Case** $e = 6$ Let $p = 6f + 1$ be an odd prime and u be a generator of F_p^* and H_6 be the set of sextic residues mod p. Then any sextic residue sequence $\mathbf{s} = \{s(t)|t \geq 0\}$ of period p can be written uniquely as

$$\mathbf{s} = a_*\underline{1} + a_0\mathbf{b}_{u^0} + a_1\mathbf{b}_{u^1} + a_2\mathbf{b}_{u^2} + a_3\mathbf{b}_{u^3} + a_4\mathbf{b}_{u^4} + a_5\mathbf{b}_{u^5}.$$

It has the defining polynomial

$$g(x) = \rho_* + \rho_0 c_{u^0}(x) + \rho_1 c_{u^1}(x) + \rho_2 c_{u^2}(x) + \rho_3 c_{u^3}(x) + \rho_4 c_{u^4}(x) + \rho_5 c_{u^5}(x),$$

where $\rho_j = \sum_{0\leq i<e} a_i c_{-u^{i+j}}(\beta)$, i.e.,

$$\begin{cases} \rho_* &= a_* + (a_0 + a_1 + a_2 + a_3 + a_4 + a_5)f \\ \rho_0 &= a_0c_{-u^0}(\beta) + a_1c_{-u^1}(\beta) + a_2c_{-u^2}(\beta) + a_3c_{-u^3}(\beta) + a_4c_{-u^4}(\beta) + a_5c_{-u^5}(\beta) \\ \rho_1 &= a_0c_{-u^1}(\beta) + a_1c_{-u^2}(\beta) + a_2c_{-u^3}(\beta) + a_3c_{-u^4}(\beta) + a_4c_{-u^5}(\beta) + a_5c_{-u^0}(\beta) \\ \rho_2 &= a_0c_{-u^2}(\beta) + a_1c_{-u^3}(\beta) + a_2c_{-u^4}(\beta) + a_3c_{-u^5}(\beta) + a_4c_{-u^0}(\beta) + a_5c_{-u^1}(\beta) \\ \rho_3 &= a_0c_{-u^3}(\beta) + a_1c_{-u^4}(\beta) + a_2c_{-u^5}(\beta) + a_3c_{-u^0}(\beta) + a_4c_{-u^1}(\beta) + a_5c_{-u^2}(\beta) \\ \rho_4 &= a_0c_{-u^4}(\beta) + a_1c_{-u^5}(\beta) + a_2c_{-u^0}(\beta) + a_3c_{-u^1}(\beta) + a_4c_{-u^2}(\beta) + a_5c_{-u^3}(\beta) \\ \rho_5 &= a_0c_{-u^5}(\beta) + a_1c_{-u^0}(\beta) + a_2c_{-u^1}(\beta) + a_3c_{-u^2}(\beta) + a_4c_{-u^3}(\beta) + a_5c_{-u^4}(\beta) \end{cases}$$

The linear complexity is given as

$$LC(\mathbf{s}_{\mathbf{a}^*}) = \delta(\rho_*) + w_H(\rho_0, \rho_1, \rho_2, \rho_3, \rho_4, \rho_5) f,$$

and, for all t,

$$\begin{aligned} s(t) = \rho_* + \quad & \mathit{Tr}_1^n \left(\rho_0 \sum_{j=0}^{\frac{p-1}{6n}-1} \beta^{u^{6j}t} + \rho_1 \sum_{j=0}^{\frac{p-1}{6n}-1} \beta^{u^{6j+1}t} + \rho_2 \sum_{j=0}^{\frac{p-1}{6n}-1} \beta^{u^{6j+2}t} \right. \\ & \left. + \rho_3 \sum_{j=0}^{\frac{p-1}{6n}-1} \beta^{u^{6j+3}t} + \rho_4 \sum_{j=0}^{\frac{p-1}{6n}-1} \beta^{u^{6j+4}t} + \rho_5 \sum_{j=0}^{\frac{p-1}{6n}-1} \beta^{u^{6j+5}t} \right) \end{aligned}$$

Now, we only need to determine the values of

$$(c_{u^0}(\beta), c_{u^1}(\beta), c_{u^2}(\beta), c_{u^3}(\beta), c_{u^4}(\beta), c_{u^5}(\beta)) \triangleq (c_0, c_1, c_2, c_3, c_4, c_5).$$

e-tuples

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

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

in order to determine the trace representation of the sequence $\mathbf{s}_{\mathbf{a}^*}$.

We were able to find some necessary conditions for $\mathbf{c}_u(\beta)$, and thus, able to calculate these values for all the characteristic sequences of e-th power cyclic difference sets.

Applications

We use the following notations.

- $p = ef + 1$ is a given prime for some e and f,
- n is the order of 2 mod p,
- $c \triangleq \frac{p-1}{n}$, $d \triangleq \gcd(c, e)$, $c_1 \triangleq c/d$, and $e_1 \triangleq e/d$ so that

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

$\diamond$ $e = 2$**.** Legendre sequence picks up all the terms except for $t \in H_2$, therefore,

$$\mathbf{s}_{\text{Legendre}} \triangleq \underline{1} + \mathbf{b}_{u^0},$$

and hence, $\mathbf{a}^* = (a_*, a_0, a_1) = (1, 1, 0)$ in this case. Now, 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 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 s is given as

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

$\diamond$ $e = 6$. 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

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

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

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

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

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

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

$$s(t) = \sum_{\substack{0 \le m < c \\ m \equiv 0 \pmod 6}} Tr_1^n\left(\beta^{u^m t}\right) = \sum_{m=0}^{c/6-1} Tr_1^n\left(\beta^{u^{6m} t}\right), \quad LC = (p-1)/6,$$

$$s(t) = \sum_{\substack{0 \le m < c \\ m \equiv 0 \pmod 6}} Tr_1^n\left(\omega\beta^{u^m t}\right) + \sum_{\substack{0 \le m < c \\ m \equiv 3 \pmod 6}} Tr_1^n\left(\omega^2\beta^{u^m t}\right) + \sum_{\substack{0 \le m < c \\ m \not\equiv 0 \pmod 3}} Tr_1^n\left(\beta^{u^m t}\right), \quad LC = p-1.$$

Linear complexity of sextic residue sequences of period $p = 6f + 1$ with f odd and with $a_* = 0$ and $\mathbf{a} = (a_0, a_1, ..., a_5)$:

		Linear Complexity			
$w_H(\mathbf{a})$	$\mathbf{a} = (a_0 a_1 ... a_5)$	$d = 6$	$d = 3$	$d = 2$	$d = 1$
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)	$6f$	$6f$	$6f$	$6f$

† corresponds to Hall's sextic residue sequences, and ‡ to Legendre sequences.

$\diamond$ $e = 4$. 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, $LC(\mathbf{s}) = p$. ∎

◇ $e = 8$. 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 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. ■

$\diamond$ $e = 10$. Let $p = 31$, $e = 10$, and let $\mathbf{s}$ be the characteristic sequence of the cyclic difference set $D = H_{10} \cup 11H_{10} = \{i \pmod{31} \mid i = 1, 5, 11, 24, 25, 27\}$. 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 $c_{2j} = \beta^{-7 \cdot 2^{4j}}$, $c_{2j+1} = \beta^{-2^{4j}}$, $0 \leq j < 5$.
2. $\mathbf{s} = \underline{1} + \mathbf{b}_1 + \mathbf{b}_{11}$.
3. Let
$$g(x) = 1 + \sum_{0 \leq j < 5} \left(\beta^{11 \cdot 2^{4j}} c_{11^{2j}}(x) + \beta^{18 \cdot 2^{4j}} c_{11^{2j+1}}(x) \right).$$
Then $(g(x), \beta)$ is a defining pair of $\mathbf{s}$. ■

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 the cases $e = 4$ and $e = 6$ 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 the case $e = 8$.