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

Zongduo Dai
State Key Lab of Information Security
Chinese Academy of Sciences, China
yangdai@public.bta.net.cn

Guang Gong
Dept. of Electrical & Computer Eng.
University of Waterloo, Canada
ggong@acr.math.uwaterloo.ca

Hong-You Song
Dept. of Electrical & Electronics Eng.
Yonsei University, Korea
by.song@coding.yonsei.ac.kr

I. INTRODUCTION

Let $p = ef + 1$ be an odd prime for some $e$ and $f$. In this presentation, binary $e$-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. Due to the space limitation, most of the application of the basic theory is omitted.

II. LINEAR SPACE OF $e$-TH RESIDUE SEQUENCES

Let $p = ef + 1$ be an odd prime for some $e$ and $f$. We let $a$ be a primitive $p$-th root of unity, and let $< a > = \{ a, a^2, \ldots, a^{p-1} \}$. We define $n$ to be the order of $p$, $c = (p - 1)/n$, $d = \gcd(c, e)$, $\gamma = \gamma(p)$, and $\mathbf{e}_i = e/d$. We denote by $Lc(s)$ the linear complexity of a binary sequence $s$, and denote by $\mathbf{w}(p)$ the Hamming weight of a tuple $p$. We also let $\delta(x)$ be $1$ or $0$ according to whether the integer $x$ is odd or even, respectively.

Definition 1 (i) Let $s = \{ s(t) \}_{t \geq 0}$ be a binary sequence of period $p = ef + 1$. Then, we say $s$ is an $e$-th residue sequence if $s(t) = 0$ is constant on each of the cosets $kH_e = \{ k \times x \in H_e \}$ of $H_e$ in $F_p^*$, that is, if $s(t_1) = s(t_2)$ whenever $t_1H_e = t_2H_e$.

(ii) Given a binary sequence $s = \{ s(t) \}_{t \geq 0}$ of period $p$, we say $(g(x), \beta)$ form a $e$ defining pair of $s$ if $s(t) = g(t \beta)$ for all $t = 0, 1, 2, \ldots$, where $g(x)$ is a polynomial modulo $x^e - 1$ over $\mathbb{F}$ and $\beta \in < a > ^*$. We call $g(x)$ the defining polynomial of $s$, and $\beta$ the corresponding defining element.

(iii) The generating polynomial of each coset $kH_e$ is important in expressing the trace representations of $e$-th residue sequences, it is defined as $c_{kH_e}(x) = \sum_{k \in kH_e} x^k \pmod{x^p - 1}$, which will be denoted simply by $c_k(x)$ where $k \in F_p^*$.

Theorem 1 (i) Let $Lc$ be the set of all $e$-th residue sequences of period $p$. Then $Lc$ is a vector space over $F_2$ of dimension $1 + e$, and $\{|b_i|, 0 \leq i < e\} \cup \{1\}$ is a basis of $Lc$ over $F_2$, where $u$ is any generator of $F_p^*$, i.e., any $e$-th residue sequence in $Lc$ can be expressed uniquely in the form of $s_u = a_1 + \sum_{0 \leq k < e} a_k b_k$, for some binary $(1 + e)$-tuple $a^* = (a_0, a_1, \ldots, a_{e-1})$.

(ii) Keep the notations in the above item, and let $\beta \in < a > ^*$. Corresponding to $a^*$ and $\beta$, define $\rho_s = a_0 + \sum_{0 \leq k < e} a_k \beta^k$, and $\beta_j = \sum_{0 \leq k < e} a_k \beta^{k+j}$ for $0 \leq j < e$, and define $g(x) = \rho_s + \sum_{0 \leq k < e} \beta_j c_k(x)$. Then $(g(x), \beta)$ is a defining pair of $s_u^*$.

(iii) Keep the notations in the above items. Then $Lc(s_u^*) = \delta(\rho_s) + \mathbf{w}(p)f$, where $p = (\rho_0, \rho_1, \ldots, \rho_e, \rho_{e+1})$.

(iv) Keep the notations in the above items. Let $s_u^* = \{ s(t) \}_{t \geq 0}$. With the knowledge of the defining pair of $s_u^*$ as shown above, we have

$$s(t) = \rho_s + \sum_{0 \leq k < e} \beta^k c_k(x), \forall t,$$

where $\mathbf{Tr}_n(x) = \sum_{0 \leq k < e} x^k$ is the trace of $x$ from $F_{p^n}$ to $F_2$.

Based on Theorem 1, one can find explicitly trace representations of $e$-th residue sequences of period $p = ef + 1$, once an $e$-tuple of the form $c_u(\beta) = \{ c_u(\beta), c_{u+1}(\beta), \ldots, c_{u+e-1}(\beta) \}$ is evaluated for some $u$ which is a generator of the group $F_p^*$ and $0 \leq \beta < e$, where $c_u(\beta)$ is the value of $c_u^*(x)$ at $x = \beta$. We were able to determine these $e$-tuples for all $e \leq 12$ such that some union of cosets of the $e$-th powers mod $p$ form a cyclic difference set. Following is the example for $e = 6$. Let $p = ef + 1$ be a prime and $f$ odd. Then there exist a generator $u$ of $F_p^*$ and $\beta \in < a > ^*$ such that

$$c_u(\beta) = \{(0, 1, 1, 0, 1, 0) \text{ if } d = 6, (1, 0, w, 1, 0, 2) \text{ if } d = 3,$$

where $w$ is a root of $x^2 + x + 1$. For the general sextic residue sequences (when $f$ is odd), we have the following: There exist a generator $u$ of $F_p^*$ and $\beta \in < a > ^*$ such that

$$c_u(\beta) = \{(e_1, \gamma, \gamma^2, \gamma^3, \gamma^4, \gamma^5) \text{ if } d = 2, (\theta, \theta^2, \theta^3, \theta^4, \theta^5, \theta^6) \text{ if } d = 1,$$

where $\gamma$ is a root of $x^2 + x + 1$, and $\theta = \rho \text{ or } \theta = \rho + 1$ where $\rho$ is a root of $x^2 + x + 1$ (and hence, $\rho + 1$ is a root of $x^2 + x + 2$ and $x + 1$).

Open Problem: Which one among the two values $\rho$ and $\rho + 1$ the element $\theta$ above takes has not been determined yet, and we do not know whether both values will be taken when $p$ changes.

REFERENCES

学霸图书馆
www.xuebalib.com

本文献由“学霸图书馆-文献云下载”收集自网络，仅供学习交流使用。

学霸图书馆（www.xuebalib.com）是一个“整合众多图书馆数据库资源，
提供一站式文献检索和下载服务”的24小时在线不限IP图书馆。

图书馆致力于便利、促进学习与科研，提供最强文献下载服务。

图书馆导航：
图书馆首页 文献云下载 图书馆入口 外文数据库大全 疑难文献辅助工具