On the p-Ranks and Characteristic Polynomials of Cyclic Difference Sets

Jong-Seon No
School of EECS
Seoul Nat'l Univ., Seoul, Korea
e-mail: jsno@snu.ac.kr

Dong-Joon Shin
Division of ECE
Hanyang Univ., Seoul, Korea
e-mail: djshin@hanyang.ac.kr

Tor Helleseth
Dept. of Informatics
Univ. of Bergen, Bergen, Norway
e-mail: torh@ii.uib.no

Abstract — **In this paper, the p-ranks and characteristic polynomials of cyclic difference sets are derived by expanding the trace expressions of their characteristic sequences. The 3-ranks and characteristic polynomials of Helleseth-Kumar-Martinsen (HKM) and Lin difference sets are obtained, and the characteristic polynomial of Singer difference set is calculated.**

I. p-Ranks and Characteristic Polynomials of Cyclic Difference Sets

Let D be a cyclic difference set and $\overline{D}$ its complementary difference set. The *characteristic sequence* of D is defined as

$$s(t) = \begin{cases} 1, & \text{if } t \in D \\ 0, & \text{if } t \notin D. \end{cases}$$

The *characteristic polynomial* of D is a least-degree linear recursion over F_p of $s(t)$ and the p-rank of D is its degree.

Theorem 1 : Let D be the (v, k, λ) cyclic difference set defined by

$$D = \{t \mid f(\alpha^t) = 0,\ 0 \le t < v\}$$

where $v \mid p^n - 1$ and $f(\alpha^t)$ is a function from F_{p^n} to its subfield F_{p^m}. Suppose that the characteristic sequence $s_c(t)$ of $\overline{D}$ can be expanded as

$$s_c(t) = [f(\alpha^t)]^{p^m-1} = \sum_{j \in J} c_j \alpha^{jt} = \sum_{k|n,k>1} \sum_{a_k \in J_k} c_{a_k} tr_1^k(\alpha_k^{a_k t}),$$

where $c_j, c_{a_k} \in F_p^*$. Then if $p \mid v - k$, the p-ranks of $\overline{D}$ and D are $|J|$ and $|J| + 1$, respectively, and the characteristic polynomials are given as:

$$\begin{aligned} g(x) &= (x-1) \cdot g_c(x) \\ g_c(x) &= \prod_{k|n,k>1} \prod_{a_k \in J_k} M_{a_k}(x), \end{aligned}$$

where $M_{a_k}(x)$ is the minimal polynomial of $\alpha_k^{a_k}$.

II. 3-Ranks and Characteristic Polynomials of HKM, Lin and Singer Difference Sets

Theorem 2 [1]: HKM difference set with parameter $\left(\frac{3^n-1}{3-1}, \frac{3^{n-1}-1}{3-1}, \frac{3^{n-2}-1}{3-1}\right)$ is defined by

$$D = \left\{ t \mid tr_1^n(\alpha^t) + tr_1^n(\alpha^{dt}) = 0,\ 0 \le t < \frac{3^n-1}{3-1} \right\},$$

where $n = 3k$, $d = 3^{2k} - 3^k + 1$. Then the 3-ranks of D and $\overline{D}$ are given as $2n^2 - 2n + 1$ and $2n^2 - 2n$. Also, the characteristic polynomials are:
For $n = 2m + 1$:

$$\begin{aligned} g_c(x) &= M_{2d}(x) M_{1+3^k}(x) \prod_{i=1, i\neq k}^{m} M_{1+3^i}(x) \\ &\quad \prod_{i=1, i\neq k}^{m} M_{(1+3^i)d}(x) \prod_{i=0, i\neq k}^{n-1} M_{d+3^i}(x). \end{aligned}$$

For $n = 2m$:

$$\begin{aligned} g_c(x) &= M_{2d}(x) M_{1+3^m}(x) M_{(1+3^m)d}(x) M_{1+3^k}(x) \\ &\quad \prod_{i=1, i\neq k}^{m-1} M_{1+3^i}(x) \prod_{i=1, i\neq k}^{m-1} M_{(1+3^i)d}(x) \prod_{i=0, i\neq k}^{n-1} M_{d+3^i}(x). \end{aligned}$$

Theorem 3 [2]: Lin difference set with parameter $\left(\frac{3^n-1}{3-1}, \frac{3^{n-1}-1}{3-1}, \frac{3^{n-2}-1}{3-1}\right)$ is defined by

$$D = \left\{ t \mid tr_1^n(\alpha^t) + tr_1^n(\alpha^{dt}) = 0,\ 0 \le t < \frac{3^n-1}{3-1} \right\},$$

where $n = 2m + 1$, $d = 2 \cdot 3^m + 1$. Then the 3-ranks of D and $\overline{D}$ are given as $2n^2 - 2n + 1$ and $2n^2 - 2n$. Also, the characteristic polynomials are:

$$\begin{aligned} g_c(x) = \quad & M_2(x) M_{1+3^m}(x) \prod_{i=1}^{m-1} M_{1+3^i}(x) \prod_{i=1}^{m} M_{(1+3^i)d}(x) \\ & \prod_{i=0, i\neq m}^{n-2} M_{d+3^i}(x). \end{aligned}$$

Theorem 4 : Singer difference set with parameter $\left(\frac{q^n-1}{q-1}, \frac{q^{n-1}-1}{q-1}, \frac{q^{n-2}-1}{q-1}\right)$, where $q = p^s$, is defined by

$$D = \left\{ t \mid tr_s^{ns}(\alpha^t) = 0,\ 0 \le t < \frac{q^n-1}{q-1} \right\}.$$

Then the characteristic polynomials are given as:

$$\begin{aligned} g_c(x) &= \prod_{\substack{c(l):\ \text{coset leader} \\ \text{where } c(l) = \sum_{i=0}^{s-1} \sum_{j=0}^{n-1} l_{i,j} p^{i+js} \\ \text{and } \sum_{j=0}^{n-1} l_{i,j} = p-1, 0 \le i < s}} M_{c(l)}(x). \end{aligned}$$

[1] This work was supported in part by BK21 and ITRC program of the Korean Ministry of Information and Communications.

References

[1] T. Helleseth, P.V. Kumar, and H.M. Martinsen, "A new family of ternary sequences with ideal two-level autcorrelation," *Proceedings of International Symposium on Information Theory*, pp. 3289, Jun. 2000.

[2] H.A. Lin, "From cyclic Hadamard difference sets to perfectly balanced sequences," Ph.D. Dissertation, University of Southern California, May, 1998.

0-7803-7501-7/02/$17.00©2002 IEEE.