ON THE WEIGHT DISTRIBUTION OF THE COSET LEADERS OF CYCLIC CODES

Evgeniya Velikova, Faculty of Mathematics and Informatics, Sofia University, 5 James Baucher blvd, Sofia, BULGARIA
velikova@fmi.uni-sofia.bg
Asen Bojilov, Faculty of Mathematics and Informatics, Sofia University, 5 James Baucher blvd, Sofia, BULGARIA
bojilov@fmi.uni-sofia.bg

1 Introduction

Let C be a cyclic code of length n over the finite field $F_q = GF(q)$. Leader of a coset $a + C$ is the vector with the smallest Hamming weight in that coset and by $wt(a + C)$ we denote the weight of the coset's leader of $a + C$, i.e. $wt(a + C) = min\{wt(x)|x \in a + C\}$. Some applications of codes require the knowledge of the spectrum of leaders of all cosets of a code. Let us denote by ω_e the number of cosets $a + C$ for which $wt(a + C) = e$. It is clear that $\omega_0 = 1$; $\omega_0 + \omega_1 + ... + \omega_n = q^{n-k}$ and $\omega_t = 0$, for every $t > n - k$. The spectrum of the of coset leaders of the code C is $\omega(C) = (\omega_0, \omega_1, ..., \omega_{n-k})$.

Let us consider the standard correspondence between vectors from the n - dimensional vector space ${F_q}^n$ and polynomials from the factor ring of the polynomials $F_q[x]/(x^n - 1)$, defined by

$$v = (a_0, a_1, \ldots, a_{n-1}) \leftrightarrow v(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}.$$

A generator polynomial $g(x)$ of the code C is a nonzero polynomial of the smallest degree such that $c \in C$ if and only if $g(x)|c(x)$. If C is a cyclic $[n, k]$ code with the generator polynomial $g(x)$, then the degree of $g(x)$ is $n - k$ and the number of cosets $a + C$ of code C is equal to q^{n-k}.

In all the known tables the cyclic codes are grouped by the code length and by

the roots of the generator polynomials. It is proved in this paper that there is a connection between spectrum of coset leaders of cyclic codes over a finite field $GF(q)$ with equal generator polynomial and non equal lengths.We suggest a method for efficient calculation of the complete coset weight distributions of cyclic codes, based on the cyclic structure of codes.

2 Cosets of cyclic codes with equal generator polynomial

Let C be a cyclic $[n, k]$ code over the finite field with q elements F_q. The generator polynomial $g(x)$ of C has degree $deg(g(x)) = n-k$, $g(x)|(x^n-1)$ and $h(x) = \frac{x^n-1}{g(x)}$ is parity check polynomial of the code C.

Let $n_0 = \mathrm{ord}\,(g(x))$ be the smallest integer such that $g(x)|(x^{n_0}-1)$ and C_0 is a cyclic code with length n_0 and generator polynomial $g(x)$. If $n = s.n_0$ then the parity check polynomial of the code C is

$$h(x) = \frac{x^n-1}{g(x)} = \frac{x^{n_0.s}-1}{x^{n_0}-1}.h_0$$

and the dual of the code C is s times repeated the dual of C_0.

Theorem 1. Let $a \in F_q$, $a \neq 0$, $n = n_0 s$ and $g(x) \in F_q[x]$ be a polynomial such that $g \mid (x^{n_0} - a)$. Then the $[n, k]$ a^s-constacyclic code $C = \langle g(x) \rangle$ and the $[n_0, k]$ a-constacyclic code $C_0 = \langle g(x) \rangle$ have equal spectra of coset leaders, i. e. $\omega(C) = \omega(C_0)$.

Proof. Let $\mathbf{c} \in {F_q}^{n_0}$ and $\mathbf{c}\uparrow$ be the extended vector $\mathbf{c}\uparrow = (\mathbf{c}, 0, \ldots, 0)$ from F_q^n. Let a correspondence $\varphi : \{\mathbf{c_0} + C_0 \mid \mathbf{c_0} \in {F_q}^{n_0}\} \to \{\mathbf{c} + C \mid \mathbf{c} \in {F_q}^n\}$ between the cosets of code C_0 and C be defined as $\varphi(\mathbf{c_0} + C_0) = \mathbf{c}\uparrow + C$. It is clear that $\mathbf{c'_0} + C_0 = \mathbf{c} + C_0 \Leftrightarrow \mathbf{c'_0}\uparrow + C = \mathbf{c}\uparrow + C$ and therefore the map φ is defined propriety and it is injective. The number of cosets of codes C and C_0 are equal then the correspondence φ is a bijection.

For $\mathbf{z} = (z_0, \ldots, z_{n-1}) \in {F_q}^n$, let us consider the vector $\mathbf{z}\downarrow = (y_0, \ldots, y_{n_0-1}) \in {F_q}^{n_0}$, where $y_i = z_i + a z_{i+n_0} + \cdots + a^{s-1} z_{i+(s-1)n_0}$ for all $i \in \{0, \ldots, n_0 - 1\}$. The polynomial $\mathbf{z}\downarrow(x)$ is the remainder of the division of $\mathbf{z}(x)$ by $x^{n_0} - a$. Therefore $(\mathbf{z}\downarrow)\uparrow \in \mathbf{z} + C$. It is clear that if $y_i \neq 0$ then $\mathrm{wt}(z_i) + \mathrm{wt}(z_{i+n_0}) + \cdots + \mathrm{wt}(z_{i+(s-1)n_0}) \geq 1$. Hence $\mathrm{wt}(\mathbf{z}\downarrow) \leq \mathrm{wt}(\mathbf{z})$.

If $\mathbf{z}$ is the leader of $\mathbf{c}\uparrow + C$ then $\mathbf{z}\downarrow \in \mathbf{c} + C_0$ and

$$\mathrm{wt}(\mathbf{c}\uparrow + C) = \mathrm{wt}(z) \geq \mathrm{wt}(\mathbf{z}\downarrow) \geq \mathrm{wt}(\mathbf{c} + C_0).$$

Let $\mathbf{c} \in {F_q}^{n_0}$ be the leader of the coset $\mathbf{c} + C_0$. Then

$$\mathrm{wt}(\mathbf{c}\uparrow + C) \leq \mathrm{wt}(\mathbf{c}\uparrow) = \mathrm{wt}(\mathbf{c}) = \mathrm{wt}(\mathbf{c} + C_0).$$

Therefore $\mathrm{wt}(\mathbf{c} + C_0) = \mathrm{wt}(\varphi(\mathbf{c} + C_0))$. □

3 The cyclic group action on the cosets of a cyclic code

By V we will denote the n-dimensional vector space over F_q. Then the map $\sigma_a : V \to V$ will be the constacyclic shift of the words of V

$$\sigma_a(c_0, c_1, c_2, \ldots, c_{n-1}) = (a c_{n-1}, c_0, c_1, \ldots, c_{n-2}).$$

The constacyclic shift σ_a is an automorphism of constacyclic $[n, k]$ code C and generates the cyclic group G of order divided by n.

Lemma 2. Let C be a cyclic $[n, k]$ code and $a \in V$. Let $B = \{\sigma(z) | z \in a + C\}$. Then B is a coset of the code C and $B = \sigma(a) + C$.

Proof. $\sigma(a + c_1) - \sigma(a + c_2) = \sigma(a) + \sigma(c_1) - \sigma(a) - \sigma(c_2) = \sigma(c_1 - c_2) = = \sigma(c_3) \in C$. □

It follows from this lemma that we can consider the action of G on the set of all cosets of the code C by $\sigma(a+C) = \sigma(a)+C$. In this way the set of all cosets is partitioned to non intersecting orbits $O(a+C) = \{\sigma^t(a)+C | t = 0, \ldots, n-1\}$. All cosets belonging to one and the same orbit have one and the same weight distribution.

Theorem 3. Let C be a cyclic $[n,k]$ code, $a \notin C$ and $d(x) = gcd(g(x), a(x))$. Then the length of the orbit $O(a+C)$ is m, where $m = \text{ord}\left(\frac{g(x)}{d(x)}\right)$.

Proof. The length of each orbit is a divisor of n_0 where $n_0 = \text{ord}\,(g(x))$ is the smallest integer such that $g(x)|(x^{n_0}-1)$.Let $a \notin C$. To calculate the length of the orbit $O(a+C)$ we have to find the smallest integer m such that $\sigma^m(a)+C = a+C$, which is equivalent to $g(x)|(x^m-1)a(x)$.

case 1. If $gcd(g(x), a(x)) = 1$ then $g(x)|(x^m-1)a(x)$ iff $g(x)|(x^m-1)$. Then $m = \text{ord}\,(g(x))$.

case 2. If $gcd(g(x), a(x)) = d(x) \neq 1$ and $t(x) = \frac{g(x)}{d(x)}$. Let $a_1(x) = \frac{a(x)}{d(x)}$. It is clear that $t(x)|a_1(x)(x^m-1)$, hence $t(x)|(x^m-1)$. Then $m = \text{ord}\,(t(x))$. □

The following has been proved in [2]:

Theorem 4. Let C be a cyclic $[n,k]$ code with a generator polynomial $g(x) = x^{n-k} + g_{n-k-1}x^{n-k-1} + \cdots + g_1x + g_0$ and let $a = (a_0, a_1, \ldots, a_{n-k-1}, 0, \ldots, 0)$ be a vector from the space V. Then the following two cosets coincide

$$\sigma(a) + C = r + C,$$

where $r = (0, a_0, a_1, \ldots, a_{n-k-2}, 0, \ldots, 0) - a_{n-k-1}(g_0, g_1, \ldots, g_{n-k-1}, 0, \ldots, 0)$.

For $a = (a_0, a_1, \ldots, a_{n-k-1}, 0, \ldots, 0)$ we define

$$\phi(a) = (0, a_0, a_1, \ldots, a_{n-k-2}, 0, \ldots, 0) - a_{n-k-1}(g_0, g_1, \ldots, g_{n-k-1}, 0, \ldots, 0).$$

We can obtain one representative from each coset of one and the same orbit by taking the vectors $a = (a_0, a_1, \ldots, a_{n-k-1}, 0, \ldots, 0)$, $\phi^2(a), \ldots, \phi^{n-1}(a)$. If the last k coordinates of the vectors a and b are zeroes then they belong to the cosets from one and the same orbit iff there exists s such that $b = \phi^s(a)$.

Let the parity check matrix of the code C be in the form $H = [I_{n-k}|B]$. If $a = (a_0, a_1, \ldots, a_{n-k-1}, 0, \ldots, 0)$ is a vector from V then its syndrome is $s(a) = Ha^t = (a_0, a_1, \ldots, a_{n-k-1})^t$. According to Theorem 4 we have $\sigma(a)+C = r+C$ and therefore

$$s(\sigma(a)) = (0, a_0, a_1, \ldots, a_{n-k-2}) - a_{n-k-1}(g_0, g_1, \ldots, g_{n-k-1}).$$

Therefore from the syndrome of a word of V we are able to compute the syndromes of all its cyclic shifts.

The covering radii of some ternary cyclic codes are determined in [1]. In [2] and [3] are given the weight distributions of the leaders of the cosets of some ternary cyclic codes.

As an illustration we present the table of ternary cyclic codes with generator polynomials of degree 5. Every such code has 243 cosets and in the table the number of orbits of the cosets for all codes is given. To calculate the coset leaders weight spectrum of a code it is sufficient to take only one coset from each orbit. The full table of all ternary codes with generator polynomials of degree less than 6 is given in [3]. In the table bellow, the polynomials are represented by their coefficients. Namely $g(x) = g_0 + g_1x + ... + g_mx^m$ is presented as the string $g_0g_1...g_m$.

TABLE 1. Coset leaders weight distributions of irreducible ternary cyclic codes with generator polynomial of degree 5

N	deg	polynomial	n	k	d	number of orbits	Spectrum
irreducible ternary cyclic codes							
1	5	221201; 201211	$11s$	$11s-5$	5 or 2	23	$(1, 22, 220, 0, 0, 0)$
2	5	122201; 102221	$22s$	$22s-5$	2	12	$(1, 22, 220, 0, 0, 0)$
3	5	220001;211001;210101; 201101;221101;211201; 202201;200011;210011; 221011;212111;220211; 202211;220021;202021; 212021;210121;211121 222121;200221;201221;	$121s$	$121s-5$	3 or 2	2	$(1, 242, 0, 0, 0, 0)$
4	5	120001;112001;110101; 102101;122101;112201; 120011;111011;121111; 101201;101011;110111; 100211;111211;102211; 100021;110021;111121; 112111;122021; 120221;101221	$242s$	$242s-5$	2	2	$(1, 242, 0, 0, 0, 0)$
ternary cyclic codes without multiple roots							
5	5	200001	$5s$	$5s-5$	2	51	$(1, 10, 40, 80, 80, 32)$
6	5	111201; 102111	$8s$	$8s-5$	5 or 2	36	$(1, 16, 112, 108, 6, 0)$
7	5	212201; 201121	$8s$	$8s-5$	5 or 2	35	$(1, 16, 112, 108, 6, 0)$
8	5	210021	$8s$	$8s-5$	4 or 2	33	$(1, 16, 82, 96, 48, 0)$
9	5	110011	$8s$	$8s-5$	4 or 2	32	$(1, 16, 82, 96, 48, 0)$
10	5	100001	$10s$	$10s-5$	2	26	$(1, 10, 40, 80, 80, 32)$
11	5	122221	$10s$	$10s-5$	4 or 2	34	$(1, 20, 132, 90, 0, 0)$
12	5	221211	$10s$	$10s-5$	4 or 2	28	$(1, 20, 132, 90, 0, 0)$
13	5	121221; 122121	$16s$	$16s-5$	3 or 2	18	$(1, 32, 210, 0, 0, 0)$
14	5	221111; 222211	$16s$	$16s-5$	3 or 2	17	$(1, 32, 210, 0, 0, 0)$
15	5	222201; 201111	$20s$	$20s-5$	4 or 2	15	$(1, 40, 202, 0, 0, 0)$
16	5	102121; 121201	$20s$	$20s-5$	4 or 2	14	$(1, 40, 202, 0, 0, 0)$
17	5	112101;121011; 101211;110121	$26s$	$26s-5$	3 or 2	18	$(1, 52, 184, 6, 0, 0)$
18	5	202221;222021; 211101;210111	$26s$	$26s-5$	3 or 2	15	$(1, 52, 184, 6, 0, 0)$
19	5	212001;221121; 200121;212211	$40s$	$40s-5$	3 or 2	9	$(1, 80, 162, 0, 0, 0)$
20	5	122111;100111; 111221;111001	$40s$	$40s-5$	3 or 2	8	$(1, 80, 162, 0, 0, 0)$
21	5	222001;210211; 200111;221021	$52s$	$52s-5$	3 or 2	9	$(1, 104, 138, 0, 0, 0)$
22	5	100121;110221; 121001;122011	$52s$	$52s-5$	3 or 2	8	$(1, 104, 138, 0, 0, 0)$

23	5	120111;111021 ;102021; 120201;101001; 110211; 112011;100101	$80s$	$80s-5$	3 or 2	6	$(1,160,82,0,0,0)$
24	5	220201; 201011;212011; 220121; 210221;211021; 200101; 202001	$80s$	$80s-5$	3 or 2	5	$(1,160,82,0,0,0)$
25	5	101111; 111101;121021; 120121; 112121;121211; 102001; 100201;220111; 222011; 212101;202121; 200201; 201001;222221; 211111	$104s$	$104s-5$	3 or 2	6	$(1,208,34,0,0,0)$
ternary cyclic codes with multiple roots							
26	5	212121	$6s$	$6s-5$	6 or 2	49	$(1,12,60,140,30,0)$
27	5	111111	$6s$	$6s-5$	6 or 2	46	$(1,12,60,140,30,0)$
28	5	222111	$9s$	$9s-5$	3 or 2	35	$(1,18,114,108,2,0)$
29	5	120021	$12s$	$12s-5$	3 or 2	40	$(1,24,74,96,48,0)$
30	5	220011	$12s$	$12s-5$	3 or 2	39	$(1,24,74,96,48,0)$
31	5	112211	$12s$	$12s-5$	3 or 2	26	$(1,24,134,72,12,0)$
32	5	211221	$12s$	$12s-5$	3 or 2	27	$(1,24,134,72,12,0)$
33	5	101101	$12s$	$12s-5$	4 or 2	28	$(1,24,146,72,0,0)$
34	5	202101	$12s$	$12s-5$	4 or 2	33	$(1,24,146,72,0,0)$
35	5	121121	$18s$	$18s-5$	2	18	$(1,18,114,108,2,0)$
36	5	102201	$18s$	$18s-5$	3 or 2	34	$(1,36,134,72,0,0)$
37	5	201201	$18s$	$18s-5$	3 or 2	27	$(1,36,134,72,0,0)$
38	5	122211; 112221	$24s$	$24s-5$	3 or 2	22	$(1,48,122,72,0,0)$
39	5	211211; 221221	$24s$	$24s-5$	3 or 2	17	$(1,48,122,72,0,0)$
40	5	221001; 200211	$24s$	$24s-5$	3 or 2	25	$(1,48,182,12,0,0)$
41	5	100221; 122001	$24s$	$24s-5$	3 or 2	24	$(1,48,182,12,0,0)$
42	5	202011; 220101	$24s$	$24s-5$	3 or 2	15	$(1,48,194,0,0,0)$
43	5	120101; 101021	$24s$	$24s-5$	3 or 2	14	$(1,48,194,0,0,0)$
44	5	211011; 220221	$39s$	$39s-5$	3 or 2	15	$(1,78,158,6,0,0)$
45	5	201021; 210201	$39s$	$39s-5$	3 or 2	15	$(1,78,158,6,0,0)$
46	5	112021; 120211	$78s$	$78s-5$	2	8	$(1,78,158,6,0,0)$
47	5	110201; 102011	$78s$	$78s-5$	2	8	$(1,78,158,6,0,0)$
48	5	200021; 210001	$78s$	$78s-5$	3 or 2	9	$(1,156,86,0,0,0)$
49	5	222101; 202111	$78s$	$78s-5$	3 or 2	9	$(1,156,86,0,0,0)$
50	5	100011; 110001	$78s$	$78s-5$	3 or 2	10	$(1,156,86,0,0,0)$
51	5	101121; 121101	$78s$	$78s-5$	3 or 2	10	$(1,156,86,0,0,0)$

REFERENCES

1. Baicheva T., The Covering Radius of Ternary Cyclic Codes with Length up to 25, *Designs, Codes and Cryptography*, vol.13, 1998, 223–227.
2. Velikova E. and Baicheva T. On the computation of weight distribution of the cosets of cyclic codes, to appear in*Ann. de L'Univ. de Sofia*
3. Velikova E. The weight distribution of the cosets leaders of ternary cyclic codes with generating polynomial of small degree, to appear in*Ann. de L'Univ. de Sofia*