ГОДИШНИК НА СОФИЙСКИЯ УНИВЕРСИТЕТ „СВ. КЛИМЕНТ ОХРИДСКИ“

ФАКУЛТЕТ ПО МАТЕМАТИКА И ИНФОРМАТИКА
Том 97

ANNUAIRE DE L'UNIVERSITE DE SOFIA „ST. KLIMENT OHRIDSKI“

FACULTE DE MATHEMATIQUES ET INFORMATIQUE
Tome 97

THE WEIGHT DISTRIBUTION OF THE COSET LEADERS OF TERNARY CYCLIC CODES WITH GENERATING POLYNOMIAL OF SMALL DEGREE

E. VELIKOVA

Using the algebraic structure of cyclic codes, it is proved that the cyclic codes with one and the same generating polynomial have equal weight distribution of cosets' leaders. As an illustration,the weight distribution of the leaders of the cosets of all ternary cyclic codes with generating polynomial of degree less than 6 is presented.

Keywords: cyclic codes, covering radius, coset weight distribution
2000 MSC: 94B15

1. INTRODUCTION

Let C be a cyclic code of length n over the finite field $F_q = GF(q)$. Let us consider the standard correspondence between a vector from $n-$dimensional vector space ${F_q}^n$ and a polynomial from the ring of the polynomials $F_q[x]$

$$v = (v_0, v_1, \dots, v_{n-1}) \to v(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}.$$

A generator polynomial $g(x)$ of code C is a nonzero polynomial of the smallest degree of code and $c \in C$ 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 $m = n - k$ and the number of cosets $a + C$ of code C is equal to q^m.

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 leader $a + C$, i.e.

$wt(a+C) = min\{wt(x)|x \in a+C\}$. The covering radius of the code is the weight of the leader with maximum weight. The covering radii of some binary and ternary cyclic codes are determined in [1], [2], [3], [4], [5], [6], [7].

Some applications of codes require the knowledge of not only the covering radius but also of 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 cosets leaders of the code C is $\omega(C) = (\omega_0, \omega_1, ..., \omega_{n-k})$. In [8] a method for computation of weight distribution of spectrum of coset leaders of an cyclic code is presented.

In all the known tables the cyclic codes are grouped by the code length and by the roots of the generating polynomials. It is proved in this paper that there is a connection between spectrum of coset leaders for cyclic codes over a finite field $GF(q)$ with equal generating polynomial and non equal lengths. As an illustration,the weight distribution of the leaders of the cosets of all ternary cyclic codes with generating polynomial with degree less than 6 is presented.

2. COSETS OF CYCLIC CODES WITH EQUAL GENERATING 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 is of degree $deg(g(x)) = n-k$, $g(x)|(x^n-1)$ and $h(x) = \frac{x^n-1}{g(x)}$ is a parity check polynomial of code C.

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

Theorem 2.1. *Let C be a cyclic $[n,k]$ code with the generator polynomial $g(x)$ and let n_0 is the small integer such that $g(x)|(x^{n_0}-1)$. If the $C_0 =< g(x) >$ is the cyclic code with length n_0 and the generator polynomial $g(x)$ then the spectra of cosets leaders for codes C and C_0 are equal $\omega(C) = \omega(C_0)$.*

Proof. Let $a \in {F_q}^{n_0}$ and $\breve{a}$ be the extended vector $\breve{a} = (a, 0, ..., 0)$ from F_q^n. Let a correspondence $\varphi : \{a + C_0 | a \in {F_q}^{n_0}\} \to \{a + C | a \in {F_q}^n\}$ between the cosets of code C_0 and C be defined as $\varphi(a + C_0) = \breve{a} + C$. Then it is clear that $b \in a + C_0 \Leftrightarrow \breve{b} \in \breve{a} + C$. Hence the correspondence φ is a bijection as the number of cosets of codes C and C_0 are equal.

For $z = (z_0, ..., z_{n-1}) \in {F_q}^n$, let us consider the vector $z^{(n_0)} = (y_0, ..., y_{n_0-1}) \in {F_q}^{n_0}$, where $y_i = z_i + z_{i+n_0} + ... + z_{i+(s-1)n_0}$ for all $i \in \{0, ..., n_0-1\}$. It is clear that if $y_i \neq 0$ then $wt(z_i) + wt(z_{i+n_0}) + ... + wt(z_{i+(s-1)n_0}) \geq 1$. Hence $wt(z^{(n_0)}) \leq wt(z)$. The polynomial $z^{(n_0)}(x)$ is the remainder of the division of $z(x)$ by $x^{n_0} - 1$. Therefore $\check{z}^{(n_0)} \in z + C$. If $a \in F_q^{n_0}$ is the leader of the coset $a + C_0$ then $wt(\varphi(a + C_0)) \leq wt(a)$. Let z be the leader of $\varphi(a + C_0)$ then $z^{(n_0)} \in a + C_0$ hence $wt(z) \geq wt(a + C_0)$. Therefore $wt(a + C_0) = wt(\varphi(a + C_0))$. □

From that theorem we can conclude that if C_1 and C_2 are two cyclic codes with different lengths but with one and the same generator polynomial $g(x)$ then $\omega(C_1) = \omega(C_2)$.

3. COSET LEADERS WEIGHT DISTRIBUTIONS OF SOME TERNARY CYCLIC CODES

As an illustration of the previous section we calculate the coset leaders weight distributions of some ternary cyclic codes with generator polynomial of degree≤ 5. For the calculations we have used mostly the definition of the spectrum of the coset leaders and the following methods:

Method 1. If the linear $[n, k]$ code C over F_q has a parity check matrix H and $a \in F_q{}^n, a \notin C$ then $wt(a + C)$ is the least integer e such that the syndrome $S(a) = Ha^t$ can be represented as a linear combination of the e from the columns of matrix H. So, we can calculate the coset leader's spectrum if for any nonzero syndrome S calculate the minimal number of columns of H that linear generate S.

Method 2. In [8] is considered the action of the cyclic group $G_n =< \sigma >$ (σ is a cyclic shift of coordinates) with n elements on the cosets of one cyclic $[n, k]$ code as $\sigma(a + C) = \sigma(a) + C$. This action splits the cosets in disjoint orbits and from [8] it is clear how to obtain one representative from each coset.Thus we calculate the weight of the coset leader only for one coset from each orbit.

Let C be a cyclic code with generator polynomial $g(x)$ and the minimum length of cyclic code with generator polynomial $g(x)$ be n_0. In the following tables are presented basic parameters of some cyclic codes . In the tables the polynomials are represented by their coefficients, namely $g(x) = g_0 + g_1x + ... + g_mx^m$ is given as a string $g_0g_1...g_m$. As the reciprocals polynomials generate equivalent codes, the table contains only one from any couple of such polynomials.

3.1. SPECTRUM OF COSET LEADERS FOR IRREDUCIBLE POLYNOMIALS

Let $g(x)$ be an irreducible polynomial over F_q of degree m. Then $g(x)|(x^{q^m-1} - 1)$ and if n_0 is the smallest integer such that $g(x)|x^{n_0} - 1$, then $n_0|(q^m - 1)$. Let α be a root of $g(x)$ and C_0 be the cyclic $[n_0, n_0 - m]$ code, with generator polynomial $g(x)$, then a parity check matrix of code C_0 is the following $H = (1, \alpha, \alpha^2, ..., \alpha^{n_0-1})$. A polynomial $g(x)$ for which is hold $n_0 = q^m - 1$ is called primitive polynomial and every parity check matrix for the code with length $q^m - 1$ consists of every nonzero vector column from F_q^m . Hence for that code spectrum of coset's leaders is $(1, q^m - 1, 0, ..., 0)$. If C_1 and C_2 are $[n, k]$ cyclic codes generated with irreducible polynomials of degree m the codes C_1 and C_2 are equivalent.

The table from [9] was used as a source for all irreducible polynomials over F_3.

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

N	deg	polynomial	n	k	d	R	Spectrum
1	1	21	n	$n-1$	2	1	$(1,2)$
2	1	11	$2s$	$2s-1$	2	1	$(1,2)$
3	2	101	$4s$	$4s-2$	2	2	$(1,4,4)$
4	2	211	$8s$	$8s-2$	2	1	$(1,8,0)$
5	3	2201; 2111	$13s$	$13s-3$	3 or 2	1	$(1,26,0,0)$
6	3	1201; 1211	$26s$	$26s-3$	2	1	$(1,26,0,0)$
7	4	11111	$5s$	$5s-4$	5 or 2	3	$(1,10,40,30,0)$
8	4	12121	$10s$	$10s-4$	2	3	$(1,10,40,30,0)$
9	4	20201	$16s$	$16s-4$	2	2	$(1,16,64,0,0)$
10	4	12011	$20s$	$20s-4$	2	2	$(1,20,60,0,0)$
11	4	10111; 12101	$40s$	$40s-4$	2	2	$(1,40,40,0,0)$
12	4	20021;22001; 22111;21121	$80s$	$80s-4$	2	1	$(1,80,0,0,0)$
13	5	221201	$11s$	$11s-5$	5 or 2	2	$(1,22,220,0,0,0)$
14	5	122201	$22s$	$22s-5$	2	2	$(1,22,220,0,0,0)$
15	5	220001;211001;210101; 201101;221101;211201; 210011;221011;212111; 212021;211121	$121s$	$121s-5$	3 or 2	1	$(1,242,0,0,0,0)$
16	5	120001;112001;110101; 102101;122101;112201; 120011;111011;121111; 112111;122021	$242s$	$242s-5$	2	1	$(1,242,0,0,0,0)$

3.2. SPECTRA FOR REDUCIBLE POLYNOMIALS WITHOUT MULTIPLE ROOTS

If $g(x)$ is a reducible polynomial over F_q and it does not have multiple roots then for the minimum integer n_0 for which $g(x)|(x^{n_0}-1)$ is hold $gcd(q,n_0)=1$. If α is a primitive $n-$th root of unity in some field F_{q^t} then all zeros of $g(x)$ will be $\alpha^{i_1},...,\alpha^{i_m}$. It is known that if C_1 and C_2 are cyclic $[n_0,n_0-m]$ codes and the sets of roots of the codes C_1 and C_2 are, respectively, $\alpha^{i_1},...,\alpha^{i_m}$ and $\alpha^{j_1},...,\alpha^{j_m}$ and there exists a integer v, such that $gcd(n_0,v)=1$ and $j_s=v,i_s$ for $s\in\{1,...,m\}$ then the codes C_1 and C_2 are equivalent. In that table we omit all equivalent codes, obtained by the upper procedure.

TABLE 2. Coset leaders weight distributions of ternary cyclic codes without multiple roots and generator polynomial of degree ≤ 5

No	deg	polynomial	n	k	d	R	Spectrum
1	2	201	$2s$	$2s-2$	2	2	$(1,4,4)$
2	3	1111; 2121	$4s$	$4s-3$	4 or 2	2	$(1,8,18,0)$
3	3	1101; 2021	$8s$	$8s-3$	3 or 2	2	$(1,16,10,0)$
4	4	20001	$4s$	$4s-4$	2	4	$(1,8,24,32,16)$
5	4	10001	$8s$	$8s-4$	2	4	$(1,8,24,32,16)$
6	4	12111	$8s$	$8s-4$	4 or 2	3	$(1,16,60,4,0)$
7	4	21011	$8s$	$8s-4$	4 or 2	3	$(1,16,60,4,0)$
8	4	10221; 11001	$13s$	$13s-4$	3 or 2	3	$(1,26,52,2,0)$
9	4	10211; 10021	$26s$	$26s-4$	2	3	$(1,26,52,2,0)$
10	4	21211; 20221; 22221; 22101	$26s$	$26s-4$	3 or 2	2	$(1,52,28,0,0)$
11	5	200001	$5s$	$5s-5$	2	5	$(1,10,40,80,80,32)$
12	5	111201; 201121	$8s$	$8s-5$	5 or 2	4	$(1,16,112,108,6,0)$
13	5	210021; 110011	$8s$	$8s-5$	4 or 2	4	$(1,16,82,96,48,0)$
14	5	100001	$10s$	$10s-5$	2	5	$(1,10,40,80,80,32)$
15	5	122221; 221211	$10s$	$10s-5$	4 or 2	3	$(1,20,132,90,0,0)$
16	5	121221; 222211	$16s$	$16s-5$	3 or 2	2	$(1,32,210,0,0,0)$
17	5	222201; 121201	$20s$	$20s-5$	4 or 2	2	$(1,40,202,0,0,0)$
18	5	112101;121011; 211101;210111	$26s$	$26s-5$	3 or 2	3	$(1,52,184,6,0,0)$
19	5	212001;221121; 111221;111001	$40s$	$40s-5$	3 or 2	2	$(1,80,162,0,0,0)$
20	5	222001;210211; 121001;122011	$52s$	$52s-5$	3 or 2	2	$(1,104,138,0,0,0)$
21	5	120111; 102021; 101001; 110211; 201011; 212011; 210221; 202001	$80s$	$80s-5$	3 or 2	2	$(1,160,82,0,0,0)$
22	5	111101; 212101	$104s$	$104s-5$	3 or 2	2	$(1,208,34,0,0,0)$
23	5	121021; 222011	$104s$	$104s-5$	3 or 2	2	$(1,208,34,0,0,0)$
24	5	102001; 201001	$104s$	$104s-5$	3 or 2	2	$(1,208,34,0,0,0)$
26	5	121211; 211111	$104s$	$104s-5$	3 or 2	2	$(1,208,34,0,0,0)$

3.3. SPECTRUM CODES GENERATED BY POLYNOMIALS WITH MULTIPLE ROOTS

If $x^{qn}-1=(x^n-1)^q$ over the field F_q and $g(x)$ has multiple roots then $g(x)|(x^n-1)$ where $q|n$. Very few is known about such a codes so in the following table may contain equivalent codes.

TABLE 3. Coset leaders weight distributions of ternary cyclic codes with multiple roots and generator polynomial of degree ≤ 5

N	deg	polynomial	n	k	d	R	Spectrum
1	2	111	$3s$	$3s-2$	3 or 2	2	$(1,6,2)$
2	2	121	$6s$	$6s-2$	2	2	$(1,6,2)$
3	3	2001	$3s$	$3s-3$	2	3	$(1,6,12,8)$
4	3	1001	$6s$	$6s-3$	2	3	$(1,6,12,8)$
5	3	2211	$6s$	$6s-3$	4 or 2	2	$(1,12,14,0)$
6	3	1221	$6s$	$6s-3$	3 or 2	2	$(1,12,14,0)$
7	4	10101	$6s$	$6s-4$	3 or 2	4	$(1,12,40,24,2)$
8	4	22011	$6s$	$6s-4$	4 or 2	3	$(1,12,44,24,0)$
9	4	21021	$6s$	$6s-4$	4 or 2	3	$(1,12,44,24,0)$
10	4	12021	$9s$	$9s-4$	3 or 2	3	$(1,18,38,24,0)$
11	4	10201	$12s$	$12s-4$	2	4	$(1,12,40,24,4)$
12	4	11211	$12s$	$12s-4$	3 or 2	2	$(1,24,56,0,0)$
13	4	12221	$12s$	$12s-4$	3 or 2	2	$(1,24,56,0,0)$
14	4	11011	$18s$	$18s-4$	2	3	$(1,18,38,24,0)$
15	4	20121	$24s$	$24s-4$	3 or 2	2	$(1,48,32,0,0)$
16	4	22201	$24s$	$24s-4$	3 or 2	2	$(1,48,32,0,0)$
17	4	11221	$24s$	$24s-4$	2	2	$(1,24,56,0,0)$
18	5	212121	$6s$	$6s-5$	6 or 2	4	$(1,12,60,140,30,0)$
19	5	111111	$6s$	$6s-5$	6 or 2	4	$(1,12,60,140,30,0)$
20	5	222111	$9s$	$9s-5$	3 or 2	4	$(1,18,114,108,2,0)$
21	5	120021	$12s$	$12s-5$	3 or 2	4	$(1,24,74,96,48,0)$
22	5	220011	$12s$	$12s-5$	3 or 2	4	$(1,24,74,96,48,0)$
23	5	112211	$12s$	$12s-5$	3 or 2	4	$(1,24,134,72,12,0)$
24	5	211221	$12s$	$12s-5$	3 or 2	4	$(1,24,134,72,12,0)$
25	5	101101	$12s$	$12s-5$	4 or 2	3	$(1,24,146,72,0,0)$
26	5	202101	$12s$	$12s-5$	4 or 2	3	$(1,24,146,72,0,0)$
27	5	121121	$18s$	$18s-5$	2	4	$(1,18,114,108,2,0)$
28	5	102201	$18s$	$18s-5$	3 or 2	3	$(1,36,134,72,0,0)$
29	5	201201	$18s$	$18s-5$	3 or 2	3	$(1,36,134,72,0,0)$
30	5	122211	$24s$	$24s-5$	3 or 2	3	$(1,48,122,72,0,0)$
31	5	211211	$24s$	$24s-5$	3 or 2	3	$(1,48,122,72,0,0)$
32	5	221001	$24s$	$24s-5$	3 or 2	3	$(1,48,182,12,0,0)$
33	5	100221	$24s$	$24s-5$	3 or 2	3	$(1,48,182,12,0,0)$
34	5	202011	$24s$	$24s-5$	3 or 2	2	$(1,48,194,0,0,0)$
35	5	120101	$24s$	$24s-5$	3 or 2	2	$(1,48,194,0,0,0)$
36	5	211011	$39s$	$39s-5$	3 or 2	3	$(1,78,158,6,0,0)$
37	5	201021	$39s$	$39s-5$	3 or 2	3	$(1,78,158,6,0,0)$

N	deg	polynomial	n	k	d	R	Spectrum
38	5	112021	$78s$	$78s-5$	2	3	$(1,78,158,6,0,0)$
39	5	110201	$78s$	$78s-5$	2	3	$(1,78,158,6,0,0)$
40	5	200021	$78s$	$78s-5$	3 or 2	2	$(1,156,86,0,0,0)$
41	5	222101	$78s$	$78s-5$	3 or 2	2	$(1,156,86,0,0,0)$
42	5	100011	$78s$	$78s-5$	3 or 2	2	$(1,156,86,0,0,0)$
43	5	101121	$78s$	$78s-5$	3 or 2	2	$(1,156,86,0,0,0)$

Acknowledgments The author would like to thank Assen Bojilov and Azniv Kasparian for their help in preparing of the paper.

4. REFERENCES

1. Downie D., Sloane N. J. A. The Covering Radius of Cyclic Codes of Length up to 31, *IEEE Trans. Inf. Theory*, **IT-31**, 1985, 446–447.
2. Velikova E. and Manev K. The Covering Radius of Cyclic Codes of Lengths 33, 35 and 39, *Annuaire de L'Universite de Sofia*, **81**, 1987, 215–223.
3. Velikova E., Covering radius of some cyclic codes, In: *Internat. Workshop on Algebraic and Combinatorial Coding Theory*, Varna, 1988, 165–169.
4. Manev K., Velikova E., The Covering Radius and weight distribution of cyclic codes over $GF(4)$ of lengths up to 13, In: *Internat. Workshop on Algebraic and Combinatorial Coding Theory*, Leningrad, 1990, 150–154.
5. Dougherty R. and Janwa H., Covering radius computation for binary cyclic codes, *Mathematics of Computation*, **57**, 1991, No. 195, 415–434.
6. Baicheva T., The Covering Radius of Ternary Cyclic Codes with Length up to 25, *Designs, Codes and Cryptography*, **13**, 1998, 223–227.
7. Baicheva T., On the covering radius of ternary negacyclic codes with length up to 26, *IEEE Trans. on Inform. Theory*, **47**, 2001, No. 1, 413–416.
8. Velikova E. and Baicheva T. On the computation of weight distribution of the cosets of cyclic codes submitted to*Annuaire de L'Universite de Sofia*
9. Lidl R. and Niederreiter H. Finite Fields, Addision-Wesley Publishing Company, 1983

Received September 30, 2004

Faculty of Mathematics and Informatics
"St. Kl. Ohridski" University of Sofia
5, J. Bourchier blvd., 1164 Sofia
BULGARIA
E-mail: velikova@fmi.uni-sofia.bg