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

ON THE COMPUTATION OF WEIGHT DISTRIBUTION OF THE COSETS OF CYCLIC CODES

E. VELIKOVA, T. BAICHEVA

Using the algebraic structure of cyclic codes an efficient method for the determination of the weight distribution of the cosets of cyclic codes is presented. As an illustration of the method weight distributions of the coset leaders of all ternary cyclic codes of lengths up to 14 are calculated.

Keywords: cyclic codes, covering radius, coset weight distribution

2000 MSC: main 11T71, secondary 15A03, 68R05

1. INTRODUCTION

Cyclic codes form an important subclass of linear codes. These codes are attractive by two reasons: first, encoding and syndrome computation can be implemented easily by employing shift registers with feedback connections and second, because they have well known algebraic structure, it is possible to find various methods for decoding them. To be able to evaluate the performance of a cyclic code for some application we have to know the exact values of all its basic characteristics among them covering radius, coset leaders and coset weight distributions.

Using an exhaustive search covering radii of some binary and ternary cyclic codes are determined in [1], [2], [3], [4], [5], [6], [7]. In this work we suggest a method for efficient calculation of the complete coset weight distributions of cyclic codes.

2. COSETS OF CYCLIC CODES

Let C be a cyclic $[n, k]$ code over the finite field of q elements $F_q = GF(q)$ and let the generator polynomial of C be $g(x)$ with the degree $deg(g(x)) = n - k$. By V we will denote the n-dimensional vector space over F_q. Then the map $\sigma : V \to V$ will be the cyclic shift of the words of V

$$\sigma(a_0, a_1, a_2, \dots, a_{n-1}) = (a_{n-1}, a_0, a_1, \dots, a_{n-2}).$$

Theorem 2.1. *Let C be a cyclic $[n, k]$ code with the generator polynomial $g(x) = x^{n-k}+g_{n-k-1}x^{n-k-1}+\ldots+g_1x+g_0$ and let $a = (a_0, a_1, \dots, a_{n-k-1}, 0, \dots, 0)$ be a vector from the space V. Then the following two cosets coincide:*

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

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

Proof. Let us consider the standard correspondence between a vector from V and a polynomial from the ring of the polynomials $F_q[x]$

$$v = (v_0, v_1, \dots, v_{n-1}) \to v(x) = v_0 + v_1x + \ldots + v_{n-1}x^{n-1}.$$

If C is a cyclic code with the generator polynomial $g(x)$ of degree $m = n - k$, then it is well known that

$$b \in a + C \Leftrightarrow g(x)|(b(x) - a(x)).$$

Let $a = (a_0, a_1, \dots, a_{n-k-1}, 0, \dots, 0)$ be a vector of V. Then

$$b = \sigma(a) = (0, a_0, a_1, \dots, a_{n-k-1}, 0, \dots, 0)$$

and its corresponding polynomial is

$$b(x) = \sigma(a)(x) = xa(x) = a_0x + a_1x^2 + \ldots + a_{n-k-1}x^{n-k}.$$

The remainder of the division of $b(x)$ by $g(x) = x^{n-k}+g_{n-k-1}x^{n-k-1}+\ldots+g_1x+g_0$ is

$$r(x) = b(x) - a_{n-k-1}g(x) =$$
$$= a_0x + a_1x^2 + \ldots + a_{n-k-2}x^{n-k-1} - a_{n-k-1}(g_{n-k-1}x^{n-k-1} + \ldots + g_1x + g_0)$$

and its corresponding vector is

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

From the well known fact that if two vectors a and b belong to one and the same coset of the code C then their corresponding polynomials have the same remainders by division by $g(x)$ we can conclude that we will get one representative from each coset if we take all vectors of the type

$$a = (a_0, a_1, \dots, a_{n-k-1}, 0, \dots, 0).$$

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 2.1 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.

3. ACTING OF THE CYCLIC GROUP ON THE COSETS OF A CYCLIC CODE

Let $G =< \sigma >$ be a cyclic group generated by σ. The group has n elements.

Lemma 3.1. *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 for 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 over the set of all cosets of the code C in the following way $\sigma(a + C) = \sigma(a) + C$. By this action the set of all cosets is partitioned to non intersecting orbits $O(a + C) = \{\sigma^t(a) + C|t = 0, \ldots n - 1\}$ and the length of each orbit (i.e. the number of the different cosets) is a divisor of n. All cosets belonging to one and the same orbit have one and the same weight distribution. We can obtain one representative from each coset of one orbit by taking the vectors $a = (a_0, a_1, \ldots, a_{n-k-1}, 0, \ldots, 0)$; $\phi(a) = (0, a_0, a_1, \ldots, a_{n-k-2}, 0, \ldots, 0) - a_{n-k-1}(g_0, g_1, \ldots, g_{n-k-1}, 0, \ldots, 0)$ and $\phi^2(a), \ldots, \phi^{n-1}(a)$. 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 $b = \phi^s(a)$.

4. COSET LEADERS WEIGHT DISTRIBUTIONS OF TERNARY CYCLIC CODES WITH $N \leq 14$

Using the results from the previous sections we have calculated the coset leaders weight distributions of some ternary cyclic codes of small lengths. For the calculations we have used the definition of the covering radius of a code as the weight of the coset leader of greatest weight. For a code in a standard form a vector of each coset can be found by generating all the vectors of the form $(a, \underbrace{0, \ldots, 0}_{k})$, $a \in GF(3^{n-k})$. Then the number of steps required to find $R(C)$ by an exhaustive search is proportional to $n3^n$. If we check only one coset from each orbit we can considerably reduce the required time. More precisely, if we have s different orbits the number of steps will be $n3^{k+s}$ and this number is less then $n3^n$ because $s < n - k$. .The time complexity can be additionally decreased if we take into the consideration the fact that all vectors of weight less than or equal to $t = \left\lfloor \frac{d-1}{2} \right\rfloor$ are unique coset leaders. So, we have to check only vectors of greater than t weights.

The classification from [6] was used as source for all ternary cyclic codes of lengths up to 14. The results (a list of the nonequivalent ternary cyclic codes of length up to 14, the roots of the generator polynomials and the coset leaders weight distributions) are presented in the Table below.

Table 1. Coset leaders weight distributions of ternary cyclic codes of length ≤ 14

No	n	k	d	Roots	Coset leaders weight distribution
1.	4	3	2	2	$\alpha_1 = 2$
2.	4	2	2	1	$\alpha_1 = 4, \alpha_2 = 4$
3.	4	1	4	0,1	$\alpha_1 = 8, \alpha_2 = 18$
4.	8	7	2	4	$\alpha_1 = 2$
5.	8	6	2	1	$\alpha_1 = 8$
6.	8	6	2	2	$\alpha_1 = 4, \alpha_2 = 4$
7.	8	5	3	0,1	$\alpha_1 = 16, \alpha_2 = 10$
8.	8	5	2	0,2	$\alpha_1 = 8, \alpha_2 = 18$
9.	8	4	4	1,2	$\alpha_1 = 16, \alpha_2 = 60, \alpha_3 = 4$
10.	8	4	2	1,5	$\alpha_1 = 8, \alpha_2 = 24, \alpha_3 = 32, \alpha_4 = 16$
11.	8	3	5	0,1,2	$\alpha_1 = 16, \alpha_2 = 112, \alpha_3 = 108, \alpha_4 = 6$
12.	8	3	4	0,1,5	$\alpha_1 = 16, \alpha_2 = 82, \alpha_3 = 96, \alpha_4 = 48$
13.	8	2	6	0,1,2,4	$\alpha_1 = 16, \alpha_2 = 112, \alpha_3 = 368, \alpha_4 = 216, \alpha_5 = 16$
14.	8	2	4	0,1,4,5	$\alpha_1 = 16, \alpha_2 = 100, \alpha_3 = 288, \alpha_4 = 324$
15.	8	1	8	0,1,2,5	$\alpha_1 = 16, \alpha_2 = 112, \alpha_3 = 448, \alpha_4 = 1050, \alpha_5 = 560$
16.	10	9	2	5	$\alpha_1 = 2$
17.	10	8	2	0,5	$\alpha_1 = 4, \alpha_2 = 4$
18.	10	6	2	1	$\alpha_1 = 10, \alpha_2 = 40, \alpha_3 = 30$
19.	10	5	4	0,1	$\alpha_1 = 20, \alpha_2 = 132, \alpha_3 = 90$
20.	10	5	2	0,2	$\alpha_1 = 10, \alpha_2 = 40, \alpha_3 = 80, \alpha_4 = 80, \alpha_5 = 32$
21.	10	4	4	0,1,5	$\alpha_1 = 20, \alpha_2 = 132, \alpha_3 = 240, \alpha_4 = 240,$ $\alpha_5 = 96$
22.	10	2	5	1,2	$\alpha_1 = 20, \alpha_2 = 180, \alpha_3 = 860, \alpha_4 = 2200, \alpha_5 = 2400,$ $\alpha_6 = 900$
23.	10	1	10	0,1,2	$\alpha_1 = 20, \alpha_2 = 180, \alpha_3 = 960, \alpha_4 = 3360, \alpha_5 = 7812,$ $\alpha_6 = 7350$
24.	11	6	5	1	$\alpha_1 = 22, \alpha_2 = 220$
25.	11	5	6	0,1	$\alpha_1 = 22, \alpha_2 = 220, \alpha_3 = 440, \alpha_4 = 44, \alpha_5 = 2$
26.	11	1	11	1,2	$\alpha_1 = 22, \alpha_2 = 220, \alpha_3 = 1320, \alpha_4 = 5280,$ $\alpha_5 = 14784, \alpha_6 = 25872, \alpha_7 = 11550$

No	n	k	d	Roots	Coset leaders weight distribution
27.	13	10	3	1	$\alpha_1 = 26$
28.	13	9	3	0,1	$\alpha_1 = 26, \alpha_2 = 52, \alpha_3 = 2$
29.	13	7	5	1,4	$\alpha_1 = 41, \alpha_2 = 362, \alpha_3 = 324$
30.	13	7	4	1,2	$\alpha_1 = 41, \alpha_2 = 302, \alpha_3 = 384$
31.	13	6	6	0,1,4	$\alpha_1 = 29, \alpha_2 = 348, \alpha_3 = 1274, \alpha_4 = 32, \alpha_5 = 3$
32.	13	6	6	0,1,2	$\alpha_1 = 29, \alpha_2 = 352, \alpha_3 = 1432, \alpha_4 = 373$
33.	13	4	7	1,2,4	$\alpha_1 = 26, \alpha_2 = 312, \alpha_3 = 2288, \alpha_4 = 8788,$ $\alpha_5 = 8060, \alpha_6 = 208$
34.	13	3	9	0,1,2,4	$\alpha_1 = 26, \alpha_2 = 312, \alpha_3 = 2288, \alpha_4 = 11440,$ $\alpha_5 = 30342, \alpha_6 = 14352, \alpha_7 = 288$
35.	13	1	13	1,2,4,7	$\alpha_1 = 26, \alpha_2 = 312, \alpha_3 = 2288, \alpha_4 = 11440,$ $\alpha_5 = 41184, \alpha_6 = 109824, \alpha_7 = 204204,$ $\alpha_8 = 162162$
36.	14	13	2	7	$\alpha_1 = 2$
37.	14	12	2	0,7	$\alpha_1 = 4, \alpha_2 = 4$
38.	14	8	2	1	$\alpha_1 = 14, \alpha_2 = 84, \alpha_3 = 280, \alpha_4 = 350$
39.	14	7	4	0,1	$\alpha_1 = 30, \alpha_2 = 300, \alpha_3 = 1015, \alpha_4 = 841$
40.	14	7	2	0,2	$\alpha_1 = 14, \alpha_2 = 84, \alpha_3 = 280, \alpha_4 = 560,$ $\alpha_5 = 672, \alpha_6 = 448, \alpha_7 = 128$
41.	14	6	4	0,1,7	$\alpha_1 = 44, \alpha_2 = 343, \alpha_3 = 1102, \alpha_4 = 1930,$ $\alpha_5 = 1935, \alpha_6 = 1003, \alpha_7 = 202$
42.	14	2	7	1,2	$\alpha_1 = 28, \alpha_2 = 364, \alpha_3 = 2912, \alpha_4 = 15596,$ $\alpha_5 = 56840, \alpha_6 = 137200, \alpha_7 = 196000,$ $\alpha_8 = 122500$
43.	14	1	14	0,1,2	$\alpha_1 = 28, \alpha_2 = 364, \alpha_3 = 2912, \alpha_4 = 16016,$ $\alpha_5 = 64064, \alpha_6 = 192192, \alpha_7 = 435864,$ $\alpha_8 = 630630, \alpha_9 = 252252$

Acknowledgements. Partially supported by the Bulgarian National Science Fund under Contract MM1405/2004. Part of this work was completed during the visit of the second author to Rényi Institute of Mathematics, Budapest. She would like to thank Prof. Ervin Győri for his hospitality.

REFERENCES

1. Downie D., Sloane N. J. A. The Covering Radius of Cyclic Codes of Length up to 31, *IEEE Trans. Inf. Theory*, **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.

Received September 14, 2004

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

Tsonka Baicheva
Institute of Mathematics and Informatics
Bulgarian Academy of Sciences
P.O. Box 323, Veliko Turnovo 5000
BULGARIA
E-mail: tsonka@moi.math.bas.bg