Serdica J. Computing **2** (2008), 105–110

Serdica
Journal of Computing

Bulgarian Academy of Sciences
Institute of Mathematics and Informatics

ON THE WEIGHT DISTRIBUTION OF THE COSET LEADERS OF CONSTACYCLIC CODES

Evgeniya Velikova, Asen Bojilov

Abstract. Constacyclic codes with one and the same generator polynomial and distinct length are considered. We give a generalization of the previous result of the first author [4] for constacyclic codes. Suitable maps between vector spaces determined by the lengths of the codes are applied. It is proven that the weight distributions of the coset leaders don't depend on the word length, but on generator polynomials only. In particular, we prove that every constacyclic code has the same weight distribution of the coset leaders as a suitable cyclic code.

1. Introduction. Let C be an a-constacyclic code of length n over the finite field $F_q = GF(q)$, i. e., if whenever $(c_1, c_2, \ldots, c_n)$ is in C, so is $(ac_n, c_1, \ldots, c_{n-1})$ (a is a nonzero element of F_q). A leader of a coset $\mathbf{b} + C$ is the vector with the smallest Hamming weight in that coset and by $\mathrm{wt}(\mathbf{b}+C)$ we denote the weight of the coset's leader of $\mathbf{b} + C$, i.e., $\mathrm{wt}(\mathbf{b} + C) = \min\{\mathrm{wt}(x) \mid x \in \mathbf{b} + C\}$. Some applications of codes require knowledge of the spectrum of leaders of all

ACM Computing Classification System (1998): G.2.3.
Key words: covering radius, constacyclic codes, coset leaders.

cosets of a code. Let us denote by ω_e the number of cosets $\mathbf{b}+C$ for which $\mathrm{wt}(\mathbf{b}+C)=e$. It is clear that $\omega_0=1$; $\omega_0+\omega_1+\cdots+\omega_n=q^{n-k}$ and $\omega_t=0$, for every $t>n-k$. The spectrum of the coset leaders of the code C will be denoted $\omega(C)=(\omega_0,\omega_1,\ldots,\omega_{n-k})$.

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 $F_q[x]/(x^n-a)$, defined by

$$\mathbf{b}=(b_0,b_1,\ldots,b_{n-1})\leftrightarrow\mathbf{b}(x)=b_0+b_1x+\cdots+b_{n-1}x^{n-1}.$$

A generator polynomial $g(x)$ of the constacyclic code C is a nonzero polynomial of the smallest degree such that $\mathbf{b}\in C$ if and only if $g(x)|\mathbf{b}(x)$. Let C be a constacyclic $[n,k]$ code with the generator polynomial $g(x)$ where $g(x)\mid x^n-a$. Then the degree of $g(x)$ is $n-k$ and the number of cosets $\mathbf{b}+C$ of code C is equal to q^{n-k}.

In all known tables ([1], [2], [3], [5], [6], [7]) 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 the spectrum of coset leaders of constacyclic codes over a finite field $GF(q)$ with one and the same generator polynomials and different lengths.

2. Cosets of constacyclic codes with equal generator polynomial. Let C_0 be a a-constacyclic $[n_0,k]$ code over the finite field with q elements F_q. The generator polynomial $g(x)$ of C_0 has degree $\deg(g(x))=n-k$, $g(x)|(x^{n_0}-a)$ and $h(x)=\dfrac{x^{n_0}-a}{g(x)}$ is a parity check polynomial of the code C_0. If $n=n_0s$ it is clear that $x^{n_0}-a\mid x^n-a^s$. Then the $[n,n-\deg(g(x))]$-code C generated by $g(x)$ is a a^s-constacyclic code.

Theorem 2.1. *Let $a\in F_q$, $a\neq 0$, $n=n_0s$ and $g(x)\in F_q[x]$ be a polynomial of $\deg g(x)=m$ such that $g(x)\mid(x^{n_0}-a)$. Then the $[n,n-m]$ a^s-constacyclic code $C=\langle g(x)\rangle$ and the $[n_0,n_0-m]$ a-constacyclic code $C_0=\langle g(x)\rangle$ have equal spectra of coset leaders, i. e., $\omega(C)=\omega(C_0)$.*

P r o o f. Let $\mathbf{b_0}\in F_q^{n_0}$ and $\mathbf{b_0}\uparrow$ be the extended vector $\mathbf{b_0}\uparrow=(\mathbf{b_0},0,\ldots,0)$ from F_q^n. Note that $\mathbf{b_0}(x)=\mathbf{b_0}\uparrow(x)$ and $\mathrm{wt}(\mathbf{b_0})=\mathrm{wt}(\mathbf{b_0}\uparrow)$. It is clear that $\mathbf{b'_0}+C_0=\mathbf{b_0}+C_0$ iff $\mathbf{b'_0}\uparrow+C=\mathbf{b_0}\uparrow+C$. Therefore there exists a map

$$\varphi\colon\{\mathbf{b_0}+C_0\mid\mathbf{b_0}\in {F_q}^{n_0}\}\to\{\mathbf{b}+C\mid\mathbf{b}\in {F_q}^n\}$$

between the cosets of the codes C_0 and C defined by $\varphi(\mathbf{b_0} + C_0) = \mathbf{b_0}\uparrow + C$. Obviously, the map φ is injective. If $\mathbf{b_0}$ is one of the coset leaders of $\mathbf{b_0} + C_0$ then

$$\mathrm{wt}(\mathbf{b_0} + C_0) = \mathrm{wt}(\mathbf{b_0}) = \mathrm{wt}(\mathbf{b_0}\uparrow) \geq \mathrm{wt}(\mathbf{b_0}\uparrow + C) = \mathrm{wt}(\varphi(\mathbf{b_0} + C_0)).$$

For an arbitrary vector $\mathbf{z} = (z_0, \ldots, z_{n-1}) \in {F_q}^n$, let us consider the vector $\mathbf{z}\downarrow = (y_0, \ldots, y_{n_0-1}) \in {F_q}^{n_0}$, where $y_i = z_i + az_{i+n_0} + \cdots + a^{s-1}z_{i+(s-1)n_0}$ for all $i \in \{0, \ldots, n_0 - 1\}$. Note that the polynomial $\mathbf{z}\downarrow(x)$ is the remainder of the division of $\mathbf{z}(x)$ by $x^{n_0} - a$ and

$$\mathbf{z}(x) = \sum_{i=0}^{n-1} z_i x^i \equiv \sum_{i=0}^{n_0-1} (z_i + az_{i+n_0} + \cdots + a^{s-1}z_{i+(s-1)n_0})x^i = \\ = \sum_{i=0}^{n_0-1} y_i x^i = \mathbf{z}\downarrow(x) \pmod{x^{n_0} - a},$$

because

$$x^{n_0} \equiv a \pmod{x^{n_0} - a}.$$

From $g(x) \mid x^{n_0} - a$ we obtain that

$$\mathbf{z}(x) \equiv \mathbf{z}\downarrow(x) \pmod{g(x)}.$$

Therefore $\mathbf{z}' + C = \mathbf{z} + C$ iff $\mathbf{z}'\downarrow + C_0 = \mathbf{z}\downarrow + C_0$, and $(\mathbf{z}\downarrow)\uparrow + C = \mathbf{z} + C$. We obtain a map

$$\psi\colon \{\mathbf{z} + C \mid \mathbf{z} \in {F_q}^n\} \to \{\mathbf{y} + C_0 \mid \mathbf{y} \in {F_q}^{n_0}\}$$

between the cosets of the codes C and C_0 defined by $\psi(\mathbf{z} + C) = \mathbf{z}\downarrow + C_0$ and the map ψ is injective.

It is clear that if $y_i \neq 0$ then there exists $j = 0, 1, \ldots, s-1$ such that $z_{i+jn_0} \neq 0$ and $\mathrm{wt}(z_i) + \mathrm{wt}(z_{i+n_0}) + \cdots + \mathrm{wt}(z_{i+(s-1)n_0}) \geq 1$. Hence $\mathrm{wt}(\mathbf{z}\downarrow) \leq \mathrm{wt}(\mathbf{z})$.

If $\mathbf{z}$ is the coset leader of $\mathbf{z} + C$ then

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

Since $(\mathbf{b_0}\uparrow)\downarrow = \mathbf{b_0}$, $\mathbf{b_0} \in F_q^{n_0}$, we have

$$(\psi\varphi)(\mathbf{b_0} + C_0) = \psi\big(\varphi(\mathbf{b_0} + C_0)\big) = \psi(\mathbf{b_0}\uparrow + C) = (\mathbf{b_0}\uparrow)\downarrow + C_0 = \mathbf{b_0} + C_0$$

and therefore the map $\psi\varphi$ is the identity map over the cosets of the code C_0.

Similarly, we obtain the map $\varphi\psi$ is the identity map over the cosets of the code C, because

$$(\varphi\psi)(\mathbf{z}+C) = \varphi\big(\psi(\mathbf{z}+C)\big) = \varphi(\mathbf{z}\downarrow + C_0) = (\mathbf{z}\downarrow)\uparrow + C = \mathbf{z} + C.$$

Therefore the maps φ and ψ are bijections between the cosets of the codes C and C_0 and inverse to each other.

Finally, we have for every $\mathbf{b_0} \in F_q^{n_0}$

$$\mathrm{wt}(\mathbf{b_0}+C_0) \geq \mathrm{wt}(\varphi(\mathbf{b_0}+C_0)) \geq \mathrm{wt}(\psi\varphi(\mathbf{b_0}+C_0)) = \mathrm{wt}(\mathbf{b_0}+C_0)$$

and therefore $\mathrm{wt}(\mathbf{b_0}+C_0) = \mathrm{wt}(\varphi(\mathbf{b_0}+C_0))$ □

Corollary 2.2. *Let $a \in F_q$, $a^s = 1$ and $g(x) \in F_q[x]$ be a polynomial of $\deg g(x) = m$ such that $g(x) \mid (x^{n_0} - a)$. Then the $[n_0 s, n_0 s - m]$ cyclic code $C = \langle g(x)\rangle$ and the $[n_0, n_0 - m]$ a-constacyclic code $C_0 = \langle g(x)\rangle$ have equal spectra of coset leaders, i. e., $\omega(C) = \omega(C_0)$.*

Proof. It is clear that the code C is a^s-constacyclic ($a^s = 1$) $[n, k]$ code where $n = n_0 s$ and applying the Theorem 2.1 we complete the proof. □

Theorem 2.3. *Let a and b be nonzero constants from the field F_q and $g(x) \in F_q[x]$ be a polynomial of degree m such that $g(x) \mid (x^n - a)$ and $g(x) \mid (x^l - b)$. Then the $[n, n-m]$ a-constacyclic code $C_1 = \langle g(x)\rangle$ and the $[l, l-m]$ b-constacyclic code $C_2 = \langle g(x)\rangle$ have equal spectra of coset leaders, i. e., $\omega(C_1) = \omega(C_2)$.*

Proof. Suppose that $a^s = 1$ and $b^t = 1$ and denote $p = ts$. Then $x^n - a \mid x^{npl} - a^{npl} = x^{npl} - 1$ and $x^l - b \mid x^{npl} - b^{npl} = x^{npl} - 1$. Hence $g \mid x^{npl} - 1$ too. Let C be the cyclic code generated by $g(x)$ with length npl. We conclude from Corollary 2.2 that $\omega(C_1) = \omega(C)$ and $\omega(C_2) = \omega(C)$ and therefore $\omega(C_1) = \omega(C_2)$. □

From Theorem 2.3 we can conclude that if C_1 and C_2 are two constacyclic codes with different lengths but with one and the same generator polynomial $g(x)$, then $\omega(C_1) = \omega(C_2)$.

Let n_0 be the smallest integer such that $g(x) | (x^{n_0} - a_0)$ for some $a_0 \in F_q$ and C_0 is a a_0-constacyclic code with length n_0 and generator polynomial $g(x)$. It is clear that there exists a number s such that $n = s.n_0$, $a = a_0^s$ and the parity check polynomial of the code C is

$$h(x) = \frac{x^n - a}{g(x)} = \frac{x^{n_0.s} - a_0^s}{x^{n_0} - a_0}.h_0.$$

According to Theorem 2.1 we can find the spectra of coset leaders for code C if we know the spectra of coset leaders for code C_0.

3. Example. As an example we take the field with 7 elements F_7 ($q = 7$), $n_0 = 5$, $a = 3$, $g(x) = x^4 + 5x^3 + 4x^2 + 6x + 2$ ($g(x) \mid (x^5 - 3)$) and $C_0 = \langle g(x) \rangle$. Then the generator matrix of the code C is

$$G = \begin{pmatrix} 2 & 6 & 4 & 5 & 1 \end{pmatrix}$$

and the parity check matrix is

$$H = \begin{pmatrix} 1 & 0 & 0 & 0 & -2 \\ 0 & 1 & 0 & 0 & -6 \\ 0 & 0 & 1 & 0 & -4 \\ 0 & 0 & 0 & 1 & -5 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 5 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 3 \\ 0 & 0 & 0 & 1 & 2 \end{pmatrix}.$$

Hence, we obtain that C_0 is a $[5, 1, 5]_7$ 3-constacyclic code and each vector $\mathbf{b} \in F_7^5$ with weight less than 2 is a unique leader of the coset $\mathbf{b} + C_0$. There is only one coset with weight 0, so $w_0 = 1$. The number of the cosets with weight 1 is $\binom{5}{1}6 = 30$, i. e., $w_1 = 30$, while the number of those with weight 2 is $\binom{5}{2}6^2 = 360$, i. e., $w_2 = 360$. If the syndrome $\mathbf{s} = H\mathbf{b}$ of the coset $\mathbf{b} + C_0$ has weight $t \leq 3$, it can be expressed as a linear combination of t columns of identity matrix I (I is a part of the parity check matrix H) and the coset has a leader of weight less or equal than 3. Now, let us find the syndromes of weight 4 which can not be expressed as a linear combination of less than 4 columns of H. We have that syndrome $\mathbf{s} = \begin{pmatrix} s_1 & s_2 & s_3 & s_4 \end{pmatrix}^t$ satisfies this condition iff the vector $\begin{pmatrix} 3s_1 & s_2 & 5s_3 & 4s_4 \end{pmatrix}^t$ has distinct nonzero coordinates. The different nonzero elements of the field F_7 are 6 and the number of syndromes of weight 4 are $w_4 = 6.5.4.3 = 360$. Furthermore, the number of all cosets is $7^4 = 2403$ and there do not exist cosets with weight greater than 4. Hence, $w_3 = 2403 - 30 - 360 - 360 - 1 = 1652$. Therefore, the spectrum of the coset leaders of the code C_0 is $w(C_0) = (1, 30, 360, 1652, 360)$. According to Theorem 2.1 we have that

$C_2 = \langle g(x) \rangle$ is $[10, 6, 2]_7$ 2-constacyclic code for $s = 2$;
$C_3 = \langle g(x) \rangle$ is $[15, 11, 2]_7$ 6-constacyclic code for $s = 3$;
$C_4 = \langle g(x) \rangle$ is $[20, 16, 2]_7$ 4-constacyclic code for $s = 4$;
$C_5 = \langle g(x) \rangle$ is $[25, 21, 2]_7$ 5-constacyclic code for $s = 5$;

$C_6 = \langle g(x) \rangle$ is $[30, 26, 2]_7$ cyclic code for $s = 6$.

Note that the polynomial $x^5 - 3$ is a codeword and therefore the codes C_2, C_3, C_4, C_5 and C_6 have minimal distance 2.

All codes have spectra of coset leaders equal to $w(C_0) = (1, 30, 360, 1652, 360)$.

Acknowledgment. The authors are grateful to Prof. S. Dodunekov for pointing out this interesting problem.

REFERENCES

[1] Baicheva Ts. S. The covering radius of ternary cyclic codes with length up to 25. *Designs, Codes, and Cryptography* **13** (1998), no. 3, 223–227, MR 98i:94038.

[2] Baicheva Ts. S. On the covering radius of ternary negacyclic codes with length up to 26. *IEEE Transactions on Information Theory* **47** (2001), no. 1, 413–416.

[3] Dougherty R., H. Janwa. Covering radius computations for binary cyclic codes. with microfiche supplement. *Mathematics of Computation* **57** (1991), no. 195, 415–434, MR 91j:94029.

[4] Downie D. E., N. J. A. Sloane. The covering radius of cyclic codes of length up to 31. *IEEE Transactions on Information Theory* **31** (1985), no. 3, 446.

[5] Velikova E. The weight distribution of the coset leaders of ternary cyclic codes with generating polynomial of small degree. *Annuaire de L'Universite de Sofia* **97** (2005).

[6] Velikova E., K. Manev. The covering radius of cyclic codes of lengths 33, 35 and 39. *Annuaire de L'Universite de Sofia* **81** (1987).

[7] Manev K., E. Velikova. The covering radius and weight distribution of cyclic codes over GF(4) of lengths up to 13. Internat. Workshop on Algebraic and Combinatorial Coding Theory, Leningrad, 1990.

Faculty of Mathematics and Informatics
Sofia University
5 James Baucher blvd
Sofia, Bulgaria
e-mail: velikova@fmi.uni-sofia.bg
bojilov@fmi.uni-sofia.bg

Received January 31, 2008
Final Accepted May 15, 2008