Advances in Mathematics of Communications
Volume 3, No. 3, 2009, 265–271
doi:10.3934/amc.2009.3.265

A NOTE ON NEGACYCLIC AND CYCLIC CODES OF LENGTH p^s OVER A FINITE FIELD OF CHARACTERISTIC p

Hakan Özadam and Ferruh Özbudak

Department of Mathematics and Institute of Applied Mathematics
Middle East Technical University, İnönü Bulvarı, 06531
Ankara, Turkey

(Communicated by Sergio López-Permouth)

Abstract. Recently, the minimum Hamming weights of negacyclic and cyclic codes of length p^s over a finite field of characteristic p are determined in [4]. We show that the minimum Hamming weights of such codes can also be obtained immediately using the results of [1].

1. Introduction

Recently, negacyclic codes of length 2^s over Galois rings of characteristic 2^m have been studied by Dinh and López-Permouth in [5] and by Dinh in [2, 3] . Later in [4], using similar techniques and detailed computations, Dinh has studied cyclic and negacyclic codes of length p^s over a finite field of characteristic p, where s is an arbitrary positive integer. More precisely, Dinh determined the ideal structure and the minimum Hamming weights of all such codes. Additionally, he gave the Hamming distance distribution of some of these codes.

In 1991, G. Castagnoli, J. L. Massey, P. A. Schoeller and N. von Seemann obtained general results on repeated-root cyclic codes over finite fields [1]. For a combinatorial treatment of this topic, we refer to [8]. In this study, as a simpler and more direct method compared to that of [4], we show that the minimum Hamming weights of all negacyclic and cyclic codes of length p^s over a finite field of characteristic p can be obtained immediately using the results of [1]. We also point out that the ideal structure of such codes can be obtained directly using a well-known result of algebraic coding theory (see Remark 1).

This note is organized as follows. In Section 2, we recall some preliminaries. In Section 3, we obtain the minimum Hamming weights of all cyclic and negacyclic codes of length p^s over finite fields of characteristic p using Lemma 1 and Theorem 1 of [1]. We recall the definitions and the results of [1] that we use in Appendix for convenience.

2. Preliminaries

Let $\mathbb{F}_q$ be a finite field of characteristic p. Let n be a positive integer. Throughout the paper we identify a codeword $(a_0, a_1, \ldots, a_{n-1})$ of length n over $\mathbb{F}_q$ with the polynomial $a(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} \in \mathbb{F}_q[x]$. Let $w_H(a(x))$ denote the Hamming weight of the codeword $a(x)$. The minimum Hamming weight of a code C is denoted by $d_H(C)$.

2000 *Mathematics Subject Classification:* Primary: 11T71, 94B15; Secondary: 94B05.
Key words and phrases: Cyclic code, negacyclic code, repeated-root cyclic code.

Let $\mathfrak{a} = \langle x^n - 1 \rangle$ and $\mathfrak{b} = \langle x^n + 1 \rangle$ be the ideals in $\mathbb{F}_q[x]$. Let $R_\mathfrak{a}$ and $R_\mathfrak{b}$ be the finite rings given by

$$R_\mathfrak{a} = \mathbb{F}_q[x]/\mathfrak{a}, \quad \text{and} \quad R_\mathfrak{b} = \mathbb{F}_q[x]/\mathfrak{b}.$$

It is well known that *cyclic codes of length* n *over* $\mathbb{F}_q$ are ideals of $R_\mathfrak{a}$ and *negacyclic codes of length* n *over* $\mathbb{F}_q$ are ideals of $R_\mathfrak{b}$ (cf. Chapter 7 of [7], see also [9]). Any element of $R_\mathfrak{a}$ (resp. $R_\mathfrak{b}$) can be represented as $f(x) + \mathfrak{a}$ (resp. $f(x) + \mathfrak{b}$), where $f(x) \in \mathbb{F}_q[x]$ is the uniquely determined representative of $f(x) + \mathfrak{a}$ such that $\deg(f(x)) < n$. The codeword corresponding to $f(x) + \mathfrak{a}$ (resp. $f(x) + \mathfrak{b}$) is $(f_0, f_1, \dots, f_{n-1}) \in \mathbb{F}_q^n$, where $f(x) = f_0 + f_1 x + \cdots + f_{n-1}x^{n-1}$. For any ideal I of $R_\mathfrak{a}$ (resp. $R_\mathfrak{b}$), there exists a uniquely determined monic polynomial $g(x) \in \mathbb{F}_q[x]$ such that $\deg(g(x)) < n$ and $I = \langle g(x) + \mathfrak{a} \rangle$ (resp. $I = \langle g(x) + \mathfrak{b} \rangle$). The polynomial $g(x)$ is called the *generator* of the cyclic code (resp. negacyclic code) I.

Let $n = p^s$ for some positive integer s, and let $\mathcal{R}_\mathfrak{a}, \mathcal{R}_\mathfrak{b}$ be as above, i.e., $\mathcal{R}_\mathfrak{a} = \mathbb{F}_q[x]/\langle x^{p^s} - 1 \rangle$ and $\mathcal{R}_\mathfrak{b} = \mathbb{F}_q[x]/\langle x^{p^s} + 1 \rangle$. The map

$$\begin{array}{rccc} \xi : & R_\mathfrak{a} & \to & R_\mathfrak{b} \\ & f(x) + \mathfrak{a} & \mapsto & f(-x) + \mathfrak{b} \end{array} \tag{1}$$

is a ring isomorphism between $R_\mathfrak{a}$ and $R_\mathfrak{b}$. Hence ξ gives a one-to-one correspondence between the cyclic codes of length p^s over $\mathbb{F}_q$ and the negacyclic codes of length p^s over $\mathbb{F}_q$. Moreover for $f(x) + \mathfrak{a} \in R_\mathfrak{a}$ we have

$$w_H(f(x)) = w_H(f(-x)).$$

Therefore if C is a cyclic code of length n over $\mathbb{F}_q$, then we have $d_H(C) = d_H(\xi(C))$, where $\xi(C)$ is the negacyclic code obtained by the isomorphism (1).

3. Negacyclic and cyclic codes of length p^s over $\mathbb{F}_q$

In this section we determine the ideal structure and the minimum Hamming weights of all negacyclic and cyclic codes of length p^s over $\mathbb{F}_q$, where s is an arbitrary positive integer.

It is well-known (see, for example, [7]) that the ideals of $\mathcal{R}_\mathfrak{a} = \mathbb{F}_q[x]/\langle x^{p^s} - 1 \rangle$ are exactly those generated by the divisors of the polynomial $x^{p^s} - 1 = (x-1)^{p^s}$. Therefore all of the ideals of $\mathcal{R}_\mathfrak{a}$ are of the form $\langle (x-1)^i + \mathfrak{a} \rangle$, where $0 \le i \le p^s$. Obviously, $\langle (x-1)^i + \mathfrak{a} \rangle \subsetneq \langle (x-1)^j + \mathfrak{a} \rangle$ if and only if $i > j$. Hence the ideals of $\mathcal{R}_\mathfrak{a}$ are linearly ordered as

$$\begin{aligned} \mathcal{R}_\mathfrak{a} &= \langle (x-1)^0 + \mathfrak{a} \rangle \supsetneq \langle (x-1) + \mathfrak{a} \rangle \supsetneq \cdots \\ &\supsetneq \langle (x-1)^{p^s-1} + \mathfrak{a} \rangle \supsetneq \langle (x-1)^{p^s} + \mathfrak{a} \rangle = \langle 0 + \mathfrak{a} \rangle. \end{aligned}$$

Similarly, the ideals of the ring $\mathcal{R}_\mathfrak{b} = \mathbb{F}_q[x]/\langle x^{p^s} + 1 \rangle$ are of the form $\langle (x+1)^i + \mathfrak{b} \rangle$, where $0 \le i \le p^s$, and they are linearly ordered as

$$\begin{aligned} \mathcal{R}_\mathfrak{b} &= \langle (x+1)^0 + \mathfrak{b} \rangle \supsetneq \langle (x+1) + \mathfrak{b} \rangle \supsetneq \cdots \\ &\supsetneq \langle (x+1)^{p^s-1} + \mathfrak{b} \rangle \supsetneq \langle (x+1)^{p^s} + \mathfrak{b} \rangle = \langle 0 + \mathfrak{b} \rangle. \end{aligned}$$

$C[i]$ (resp. $D[i]$) denotes the cyclic (resp. negacyclic) code, over $\mathbb{F}_q$, of length p^s, generated by the polynomial $(x-1)^i$ (resp. $(x+1)^i$) throughout .

Remark 1. We note that the arguments above give the ideal structure of the cyclic codes of length p^s over $\mathbb{F}_q$ directly. Hence we prove [4, Proposition 3.2 and Theorem 3.3] in a simpler way.

The minimum Hamming weights of some cyclic (and negacyclic) codes of length p^s are obvious.

Lemma 1 ([4, Proposition 4.1])**.** *For $1 \le i \le p^{s-1}$, the minimum Hamming weight $d_H(C[i])$ of $C[i]$ is 2.*

Let $f(x) \in \mathbb{F}_q[x]$ and $f(0) \neq 0$. Recall that (see, for example, Chapter 3 of [6]) the order of $f(x)$ is the least positive integer e such that $f(x)\,|x^e - 1$. Assume that $p^{s-1} \le i \le p^s - 1$. Then using [6, Theorem 3.6] we obtain that the order of $(x-1)^i$ is equal to p^s. Therefore the order of the generator polynomial $(x-1)^i$ is equal to the length of the cyclic code $C[i]$. This implies that for $p^{s-1}+1 \le i \le p^s - 1$, we can use the results of [1].

Let $\langle x-1 \rangle$ be the ideal in $\mathbb{F}_q[x]$. Let R be the finite ring $R = \mathbb{F}_q[x]/\langle x-1\rangle$. The zero ideal $\mathbf{0}$ and R constitute all ideals of R. For $C \in \{\mathbf{0}, R\}$, using the convention in [1] we denote the minimum Hamming weight $d_H(C)$ of the cyclic code C of length 1 over $\mathbb{F}_q$ as

$$d_H(C) = \begin{cases} \infty & \text{if } C = \mathbf{0}, \\ 1 & \text{if } C = R. \end{cases}$$

Assume that $p^{s-1}+1 \le i \le p^s - 1$. For $0 \le t \le p^s - 1$, let $\bar{C}_t[i]$ be the ideal of R defined by

$$\bar{C}_t[i] = \begin{cases} \mathbf{0} & \text{if } 0 \le t \le i-1, \\ R & \text{if } i \le t \le p^s - 1. \end{cases}$$

For $0 \le t \le p^s - 1$, let $0 \le t_0, t_1, \ldots, t_{s-1} \le p-1$ be the uniquely determined integers such that $t = t_0 + t_1 p + \cdots + t_{s-1}p^{s-1}$, and P_t be the positive integer given by

$$P_t = \prod_{i=0}^{s-1}(t_i + 1) \in \mathbb{Z}. \tag{2}$$

We define the sets (cf. [1, page 339])

$$T^* = \{t \quad : \quad t = (p-1)p^{s-1} + (p-1)p^{s-2} + \cdots + (p-1)p^{s-(j-1)} + rp^{s-j}, \\ 1 \le j \le s,\ 1 \le r \le p-1\}$$

and

$$T = T^* \cup \{0\}. \tag{3}$$

Note that if i is an integer satisfying $p^{s-1}+1 \le i \le (p-1)p^{s-1}$ and p is an odd prime, then there exists a uniquely determined integer β such that $1 \le \beta \le p-2$ and $\beta p^{s-1} + 1 \le i \le (\beta+1)p^{s-1}$.

Lemma 2. *Let p be an odd prime. Assume that β is an integer with $1 \le \beta \le p-2$. Then*

$$\min\{P_\ell : \quad \beta p^{s-1} + 1 \le \ell \le (\beta+1)p^{s-1}, \quad \textit{and} \quad \ell \in T^*\} = \beta + 2.$$

Proof. Since $\beta p^{s-1} + 1 \le \ell \le (\beta+1)p^{s-1}$ and $\ell \in T^*$, for some τ with $\beta + 1 \le \tau \le p-1$, we have

$$\ell = \tau p^{s-1}.$$

So $P_\ell = \tau + 1 \ge \beta + 2$. Clearly for $\ell = (\beta+1)p^{s-1}$ we get $P_\ell = \beta + 2$. □

For $s > 1$, we have

$$p^s - p^{s-1} < p^s - p^{s-2} < \cdots < p^s - p^{s-s} = p^s - 1.$$

Hence for an integer i satisfying $p^s - p^{s-1} + 1 \leq i \leq p^s - 1$, there exists a uniquely determined integer k such that $1 \leq k \leq s-1$ and

$$p^s - p^{s-k} + 1 \leq i \leq p^s - p^{s-k-1}. \tag{4}$$

Moreover if i is an integer as above and k is the integer satisfying $1 \leq k \leq s-1$ and (4), then we have

$$\begin{aligned} p^s - p^{s-k} &< p^s - p^{s-k} + p^{s-k-1} < p^s - p^{s-k} + 2p^{s-k-1} < \cdots \\ &< p^s - p^{s-k} + (p-1)p^{s-k-1} \end{aligned}$$

and $p^s - p^{s-k} + (p-1)p^{s-k-1} = p^s - p^{s-k-1}$. Therefore for such integers i and k, there exists a uniquely determined integer τ with $1 \leq \tau \leq p-1$ such that

$$p^s - p^{s-k} + (\tau - 1)p^{s-k-1} + 1 \leq i \leq p^s - p^{s-k} + \tau p^{s-k-1}.$$

Lemma 3. *Let p be any prime number. Assume that $s > 1$, τ and k are integers with $1 \leq \tau \leq p-1$ and $1 \leq k \leq s-1$. If $p^s - p^{s-k} + (\tau-1)p^{s-k-1} + 1 \leq \ell \leq p^s - p^{s-k} + \tau p^{s-k-1}$ and $\ell \in T^*$, then $P_\ell = (\tau+1)p^k$.*

Proof. For $0 \leq \alpha \leq p-1$, we have

$$\begin{aligned} &p^s - p^{s-k} + \alpha p^{s-k-1} \\ &= (p-1)p^{s-1} + (p-1)p^{s-2} + \cdots + (p-1)p^{s-k} + \alpha p^{s-k-1}. \end{aligned}$$

So we get

$$\begin{aligned} &(p-1)p^{s-1} + (p-1)p^{s-2} + \cdots + (p-1)p^{s-k} + (\tau-1)p^{s-k-1} + 1 \leq \ell \\ &\leq (p-1)p^{s-1} + (p-1)p^{s-2} + \cdots + (p-1)p^{s-k} + \tau p^{s-k-1}. \end{aligned} \tag{5}$$

As $\ell \in T^*$, using (5) we get

$$\ell = (p-1)p^{s-1} + (p-1)p^{s-2} + \cdots + (p-1)p^{s-k} + \tau p^{s-k-1}.$$

Therefore $P_\ell = (\tau+1)p^k$. □

If $i = 0$, then $d_H(C[i]) = 1$ trivially. For $1 \leq i \leq p^{s-1}$, we have $d_H(C[i]) = 2$ by Lemma 1. Let $p^{s-1} + 1 \leq i \leq p^s - 1$. Since $d_H(\bar{C}_t[i]) = 1$ for $i \leq t \leq p^s - 1$ and $d_H(\bar{C}_t[i]) = \infty$ for $0 \leq t \leq i-1$, using Lemma 1 of [1] (see Lemma 4 in Appendix) we obtain

$$d_H(C[i]) \leq min\{P_t : i \leq t \leq p^s - 1\}. \tag{6}$$

Moreover, using the fact that $d_H(C[i]) \neq \infty$, by Theorem 1 of [1] (see Theorem 2 in Appendix) we have

$$d_H(C[i]) \in \{P_t : t \in T^* \quad \text{and} \quad i \leq t \leq p^s - 1\}. \tag{7}$$

It follows from (6) and (7) that

$$d_H(C[i]) = min\{P_t : t \in T^* \quad \text{and} \quad i \leq t \leq p^s - 1\}. \tag{8}$$

Assume first that $p^{s-1} + 1 \leq i \leq (p-1)p^{s-1}$. Let p be an odd prime and β be the integer such that $1 \leq \beta \leq p-2$ and $\beta p^{s-1} + 1 \leq i \leq (\beta+1)p^{s-1}$. As $\beta + 2 \leq p < (\tau+1)p^k$ for integers $1 \leq \tau \leq p-1$ and $1 \leq k \leq s-1$, using Lemma 2, Lemma 3 and (8) we get

$$d_H(C[i]) = \beta + 2.$$

Assume next that $(p-1)p^{s-1}+1 \le i \le p^s-1$, where p is any prime number. Let $1 \le \tau \le p-1$ and $1 \le k \le s-1$ be the uniquely determined integers such that

$$p^s - p^{s-k} + (\tau-1)p^{s-k-1} + 1 \le i \le p^s - p^{s-k} + \tau p^{s-k-1}.$$

Note that

$$(\tau+1)p^k < (\tau^{'}+1)p^{k^{'}} \tag{9}$$

for $\tau < \tau^{'}$ and $k = k^{'}$, or $k < k^{'}$. Then using Lemma 3, (8) and (9) we obtain that

$$d_H(C[i]) = (\tau+1)p^k.$$

Using also the isomorphism (1) we have determined the minimum Hamming weights of all negacyclic and cyclic codes of length p^s over $\mathbb{F}_q$. We summarize our results in the following theorem (cf. [4, Theorems 4.11 and 6.4]).

Theorem 1 (See also Remark 2)**.** *Let $s > 1$ and $0 \le i \le p^s - 1$ be integers. Let $C[i]$ and $D[i]$ be the cyclic and negacyclic codes of length p^s over $\mathbb{F}_q$ generated by $(x-1)^i$ and $(x+1)^i$, respectively. If $p = 2$, then the minimum Hamming weights of $C[i]$ and $D[i]$ are*

$$d_H(C[i]) = d_H(D[i]) = \begin{cases} 1, & \text{if } \ i = 0, \\ 2, & \text{if } \ 1 \le i \le 2^{s-1}, \\ 2^{k+1}, & \text{if } \ 2^s - 2^{s-k} + 1 \le i \le 2^s - 2^{s-k} + 2^{s-k-1} \\ & \text{where } \ 1 \le k \le s-1. \end{cases}$$

If p is an odd prime, then the minimum Hamming weights of $C[i]$ and $D[i]$ are

$$\begin{aligned} &d_H(C[i]) = d_H(D[i]) \\ &= \begin{cases} 1, & \text{if } \ i = 0, \\ 2, & \text{if } \ 1 \le i \le p^{s-1}, \\ \beta+2, & \text{if } \ \beta p^{s-1} + 1 \le i \le (\beta+1)p^{s-1} \ \text{where } \ 1 \le \beta \le p-2 \\ (\tau+1)p^k, & \text{if } \ p^s - p^{s-k} + (\tau-1)p^{s-k-1} + 1 \le i \le p^s - p^{s-k} + \tau p^{s-k-1} \\ & \text{where } \ 1 \le \tau \le p-1 \ \text{ and } \ 1 \le k \le s-1. \end{cases} \end{aligned}$$

Remark 2. In the setup of Theorem 1, if $s = 1$, then the Hamming distances of $C[i]$ and $D[i]$ are as above with the exception that there are no $C[i] = D[i] = (\tau+1)p^k$ and $C[i] = D[i] = 2^{k+1}$ cases.

Remark 3. In [11], the authors have observed that the results of Theorem 1 also hold for constacyclic codes of length p^s. Let $\gamma, \lambda \in \mathbb{F}_q \setminus \{0\}$ such that $\gamma^{p^s} = -\lambda$. The λ-cyclic codes, of length p^s, over $\mathbb{F}_q$ correspond to the ideals of the ring

$$\mathcal{R} = \frac{\mathbb{F}_q[x]}{\langle x^{p^s} - \lambda \rangle}.$$

So λ-cyclic codes, of length p^s, over $\mathbb{F}_q$, are exactly those generated by the elements of the set $\{(x+\gamma)^i : \quad 0 \le i \le p^s\}$. Let $C[i]$ be the λ-cyclic code generated by $(x+\gamma)^i$. Then the minimum Hamming distance of $C[i]$ is exactly as in Theorem 1.

4. Concluding remarks and comparisons

In [4], Dinh has studied cyclic and negacyclic codes of length p^s over a finite field of characteristic p, where s is an arbitrary positive integer. The minimum Hamming weights of all such codes are given in [4], which is one of the main results of [4]. In this note, as a simpler and more direct method compared to that of [4], we have shown that the minimum Hamming weights of all such negacyclic and cyclic codes can be obtained immediately using the results of G. Castagnoli, J. L. Massey, P. A. Schoeller and N. von Seemann in [1]. The ideal structure of such codes is obtained in [4] using arguments from ring theory (see [4, Proposition 3.2 and Theorem 3.3]). We have also shown that the ideal structure of these codes can be determined easily using a classical result of algebraic coding theory (see Remark 1).

Recently, we have observed, in [10], that the methods presented in this paper can be extended to compute the Hamming weight of cyclic codes, of length $2p^s$, where p is an odd prime. Moreover, we believe that the ideas and techniques, introduced in this paper and in [10], can provide valuable insight into the more general problem of determining the minimum Hamming distance of repeated-root cyclic codes over finite fields.

Acknowledgements

The authors would like to thank the editor and the anonymous referees for their useful and detailed comments which improved the paper.

The authors were partially supported by TÜBİTAK under Grant No. TBAG-107T826.

Appendix

In the appendix we recall the definitions and the results that we use from [1] for convenience. Let

$$g(x) = \prod_{j=1}^{l} m_j(x)^{e_j}$$

be a monic polynomial over $\mathbb{F}_q$ having order $n = p^s\bar{n}$ with $gcd(p, \bar{n}) = 1$ where $m_j(x)$ are all irreducible over $\mathbb{F}_q$. Define

$$\bar{g}_t(x) = \begin{cases} 1, & \text{if } t \geq e_j \quad \text{for all } j, \\ \prod\limits_{e_j > t} m_j(x), & \text{otherwise.} \end{cases}$$

Let $C \subseteq \mathbb{F}_q^n$ be the cyclic code generated by $g(x)$ and $\bar{C}_t \subseteq \mathbb{F}_q^{\bar{n}}$ be the cyclic code generated by $\bar{g}_t(x)$. Recall that for $1 \leq t \leq p^s$, the integer $P_t \in \mathbb{Z}$ is defined in (2).

Lemma 4 (Lemma 1 of [1]). *The minimum weight of the cyclic code C defined above satisfies*

$$d_H(C) \leq P_t \cdot d_H(\bar{C}_t) \quad \textit{where} \quad 0 \leq t \leq p^s - 1.$$

Theorem 2 (Theorem 1 of [1]).

$$d_H(C) = P_t \cdot d_H(\bar{C}_t)$$

for some $t \in T$, where T is as in (3).

References

[1] G. Castagnoli, J. L. Massey, P. A. Schoeller and N. von Seemann, *On repeated-root cyclic codes*, IEEE Trans. Inform. Theory, **37** (1991), 337–342.

[2] H. Q. Dinh, *Negacyclic codes of length 2^s over Galois rings*, IEEE Trans. Inform. Theory, **51** (2005), 4252–4262.

[3] H. Q. Dinh, *Complete distances of all negacyclic codes of length 2^s over $\mathbb{Z}_{2^a}$*, IEEE Trans. Inform. Theory, **53** (2007), 147–161.

[4] H. Q. Dinh, *On the linear ordering of some classes of negacyclic and cyclic codes and their distance distributions*, Finite Fields Appl., **14** (2008), 22–40.
[5] H. Q. Dinh and S. R. López-Permouth, *Cyclic and negacyclic codes over finite chain rings*, IEEE Trans. Inform. Theory, **50** (2004), 1728–1744.
[6] R. Lidl and H. Niederreiter, "Finite Fields," Cambridge University Press, Cambridge, 1997.
[7] S. Ling and C. Xing, "Coding Theory A First Course," Cambridge University Press, 2004.
[8] J. H. van Lint, *Repeated-root cyclic codes*, IEEE Trans. Inform. Theory, **37** (1991), 343–345.
[9] F. J. MacWilliams and N. J. A. Sloane, "The Theory Of Error Correcting Codes," North Holland, Amsterdam, 1978.
[10] H. Özadam and F. Özbudak, *The minimum Hamming distance of cyclic codes of length* $2p^s$, in "Proceedings of AAECC 18," (2009), 92–100.
[11] H. Özadam and F. Özbudak, *Two generalizations on the minimum Hamming distance of repeated-root constacyclic codes*, preprint, arXiv:0906.4008v1.

Received March 2009; revised June 2009.

E-mail address: ozhakan@metu.edu.tr
E-mail address: ozbudak@metu.edu.tr