Southeast Asian Journal of Sciences: Vol 5, No. 2 (2017) pp. 153-161

ON REPEATED-ROOT CONSTACYCLIC CODES OF LENGTH 100 OVER $\mathbb{F}_{25}$

Nguyen Trong Bac

Department of Basic Sciences
University of Economics and Business Administration
Thai Nguyen University, Thai Nguyen 250000, Vietnam
e-mail: bacnt2008@gmail.com

Abstract

A classification of all constacyclic codes of length 100 over $\mathbb{F}_{25}$ is obtained, which establishes the algebraic structure in term of specified polynomial generators of such codes. Among other results, all self-dual and LCD cyclic and negacylic codes of length 100 are obtained.

1. Introduction

The constacyclic codes play a very significant role in the theory of error-correcting codes as they are a direct generalization of the important family of cyclic codes. Cyclic codes have been the most studied of all codes. Many well known codes, such as BCH, Kerdock, Golay, Reed-Muller, Preparata, Justesen, and binary Hamming codes, are either cyclic codes or constructed from cyclic codes. The classes of cyclic codes in particular provide a very significant role in the theory of error-correcting codes. Due to their rich algebraic structure, constacyclic codes can be efficiently encoded using shift registers, which explains their preferred role in engineering. Given a nonzero element λ of the finite field F, λ-constacyclic codes of length n are classified as ideals as the ideals $\langle f(x)\rangle$ of the quotient ring $\frac{F[x]}{\langle x^n-\lambda\rangle}$, where $f(x)$ is a divisor of $x^n - \lambda$. In the early

Key words: Finite fields, constacyclic codes, dual codes, LCD codes, repeated-root codes.

history of error-correcting codes, most of the research was concentrated on the situation when the code length n is relatively prime to the characteristic of the field F. The case when the code length n is divisible by the characteristic p of the field yields the so-called repeated-root codes, which were first studied since 1967 by Berman [1], and then in the 1970's and 1980's by several authors such as Massey *et al.* [10], Falkner *et al.* [6], Roth and Seroussi [12]. Repeated-root codes were first investigated in the most generality in the 1990's by Castagnoli *et al.* [2], and van Lint [14], where they showed that repeated-root cyclic codes have a concatenated construction, and are asymptotically bad. Nevertheless, such codes are optimal in a few cases, that motivates researchers to further study this class of codes.

In a recently papers, we established the algebraic structure in term of polynomial generators of all repeated-root constacyclic codes of length $2p^s$ over $\mathbb{F}_{25}$ [4]. In particular, all self-dual negacyclic codes of length $2p^s$, where $p^m \equiv 1 \pmod 4$ were obtained. It was also shown the non-existence of self-dual negacyclic codes of length $2p^s$, where $p^m \equiv 3 \pmod 4$, and self-dual cyclic codes of length $2p^s$, for any odd prime p. In this paper, The line of research to study repeated-root constacyclic codes of length 100 over finite field $\mathbb{F}_{25}$.

The purpose of this paper is to give the algebraic structure in term of polynomial generators of all repeated-root constacyclic codes of length 100 over $\mathbb{F}_{25}$. We start in Section 2 by recalling some preliminary concepts about constacyclic codes of any length in general. In Section 3, we give the structures of cyclic and negacylic codes of length 100. These structures allow us to identify all self-dual and LCD codes among them.

2. Preliminaries

Let F be a finite field. Given an n-tuple $(x_0, x_1, \ldots, x_{n-1}) \in F^n$, the *cyclic shift* τ and *negashift* ν on F^n are defined as usual, i.e.,

$$\tau(x_0, x_1, \ldots, x_{n-1}) = (x_{n-1}, x_0, x_1, \cdots, x_{n-2}),$$

and

$$\nu(x_0, x_1, \ldots, x_{n-1}) = (-x_{n-1}, x_0, x_1, \cdots, x_{n-2}).$$

A code C is called *cyclic* if $\tau(C) = C$, and C is called *negacyclic* if $\nu(C) = C$. More generally, if λ is a nonzero element of F, then the λ-*constacyclic* (λ-twisted) *shift* τ_λ on F^n is the shift

$$\tau_\lambda(x_0, x_1, \ldots, x_{n-1}) = (\lambda x_{n-1}, x_0, x_1, \cdots, x_{n-2}),$$

and a code C is said to be λ-*constacyclic* if $\tau_\lambda(C) = C$, i.e., if C is closed under the λ-constacyclic shift τ_λ. In light of this definition, when $\lambda = 1$, λ-constacyclic codes are cyclic codes, and when $\lambda = -1$, λ-constacyclic codes are just negacyclic codes.

Each codeword $c = (c_0, c_1, \dots, c_{n-1})$ is customarily identified with its polynomial representation $c(x) = c_0 + c_1x + \cdots + c_{n-1}x^{n-1}$, and the code C is in turn identified with the set of all polynomial representations of its codewords. Then in the ring $\frac{F[x]}{\langle x^n-\lambda\rangle}$, $xc(x)$ corresponds to a λ-constacyclic shift of $c(x)$. From that, the following fact is well known and straightforward (cf. [7, 8]).

Proposition 2.1. *A linear code C of length n is λ-constacyclic over F if and only if C is an ideal of $\frac{F[x]}{\langle x^n-\lambda\rangle}$. Moreover, $\frac{F[x]}{\langle x^n-\lambda\rangle}$ is a principal ideal ring, whose ideals are generated by factors of $x^n - \lambda$.*

The dual of a cyclic code is a cyclic code, and the dual of a negacyclic code is a negacyclic code. In general, for any λ-constacyclic code length n over F, and arbitrary elements $x \in C^\perp$, and $y \in C$, $\tau_\lambda^{n-1}(y) \in C$, and hence,

$$0 = x \cdot \tau_\lambda^{n-1}(y) = \lambda\tau_{\lambda^{-1}}(x) \cdot y = \tau_{\lambda^{-1}}(x) \cdot y.$$

That means, $C^\perp$ is closed under the $\tau_{\lambda^{-1}}$-shift, i.e., $C^\perp$ is a λ^{-1}-constacyclic code.

Proposition 2.2. *The dual of a λ-constacyclic code is a λ^{-1}-constacyclic code.*

Proposition 2.3. *Let λ be a nonzero element of F and*

$$a(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1},\ b(x) = b_0 + b_1x + \cdots + b_{n-1}x^{n-1} \in F[x].$$

Then $a(x)b(x) = 0$ in $\frac{F[x]}{\langle x^n-\lambda\rangle}$ if and only if $(a_0, a_1, \dots, a_{n-1})$ is orthogonal to $(b_{n-1}, b_{n-2}, \dots, b_0)$ and all its λ^{-1}-constacyclic shifts.

Proof. Let $\tau_{\lambda^{-1}}$ denote the λ^{-1}-constacyclic shift for codewords of length n, i.e., for each $(x_0, x_1, \dots, x_{n-1}) \in F^n$,

$$\tau_{\lambda^{-1}}(x_0, x_1, \dots, x_{n-1}) = (\lambda^{-1}x_{n-1}, x_0, \dots, x_{n-2}).$$

Let L be the smallest positive integer such that $\lambda^L = 1$. Note that, for $1 \le j \le n$, $0 \le l \le L-1$,

$$\begin{aligned}\tau_{\lambda^{-1}}^{j+ln}(b_{n-1}, b_{n-2}, \dots, b_0) &= \lambda^{-l}\tau_{\lambda^{-1}}^{j}(b_{n-1}, b_{n-2}, \dots, b_0)\\ &= \lambda^{-l}(\lambda^{-1}b_{j-1}, \dots, \lambda^{-1}b_0, b_{n-1}, \dots, b_j).\end{aligned}$$

Thus, $\tau^i_{\lambda^{-1}}(b_{n-1}, b_{n-2}, \dots, b_0)$, $i = 1, 2, \dots, nL$, are all λ^{-1}-constacyclic shifts of $(b_{n-1}, b_{n-2}, \dots, b_0)$. Let

$$c(x) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1} = a(x)b(x) \in \frac{F[x]}{\langle x^n - \lambda\rangle}.$$

Then for $k = 0, 1, \dots, n-1$,

$$\begin{aligned}
c_k &= \sum_{\substack{i+j=k\\ 0\le i\le n-1\\ 0\le j\le n-1}} a_i b_j + \sum_{\substack{i+j=n+k\\ 0\le i\le n-1\\ 0\le j\le n-1}} \lambda a_i b_j\\
&= (a_0, a_1, \dots, a_k, a_{k+1}, \dots, a_{n-1}) \cdot (b_k, b_{k-1}, \dots, b_0, \lambda b_{n-1}, \dots, \lambda b_{k+1})\\
&= (a_0, a_1, \dots, a_k, a_{k+1}, \dots, a_{n-1}) \cdot (\lambda^{-1} b_k, \lambda^{-1} b_{k-1}, \dots, \lambda^{-1} b_0, b_{n-1}, \dots, b_{k+1}) \cdot \lambda\\
&= (a_0, a_1, \dots, a_{n-1}) \cdot \tau^{k+1}_{\lambda^{-1}}(b_{n-1}, b_{n-2}, \dots, b_0) \cdot \lambda.
\end{aligned}$$

Therefore, $c(x) = 0$ if and only if $c_k = 0$ for $k = 0, 1 \dots, n-1$ if and only if

$$(a_0, a_1, \dots, a_{n-1}) \cdot \tau^{k+1}_{\lambda^{-1}}(b_{n-1}, b_{n-2}, \dots, b_0) = 0$$

for $k = 0, 1 \dots, n-1$ if and only if $(a_0, a_1, \dots, a_{n-1})$ is orthogonal to $(b_{n-1}, b_{n-2}, \dots, b_0)$ and all its λ^{-1}-constacyclic shifts, as desired. □

Given a commutative ring R, for a nonempty subset S of R, the *annihilator* of S, denoted by $\mathrm{ann}(S)$, is the set

$$\mathrm{ann}(S) = \{f \mid fg = 0, \text{ for all } g \in S\}.$$

It is easy to see that $\mathrm{ann}(S)$ is an ideal of R.

Customarily, for a polynomial f of degree k, its reciprocal polynomial $x^k f(x^{-1})$ will be denoted by f^*. Thus, for example, if

$$f(x) = a_0 + a_1 x + \cdots + a_{k-1}x^{k-1} + a_k x^k,$$

then

$$\begin{aligned}
f^*(x) &= x^k(a_0 + a_1 x^{-1} + \cdots + a_{k-1}x^{-(k-1)} + a_k x^{-k})\\
&= a_k + a_{k-1}x + \cdots + a_1 x^{k-1} + a_0 x^k.
\end{aligned}$$

Note that $(f^*)^* = f$ if and only if the constant term of f is nonzero, if and only if $\deg(f) = \deg(f^*)$. Furthermore, by definition, it is easy to see that $(fg)^* = f^*g^*$. We denote $A^* = \{f^*(x) \mid f(x) \in A\}$. It is easy to see that if A is an ideal, then A^* is also an ideal.

Proposition 2.4. *Let λ be a unit of F such that $\lambda^2 = 1$, i.e., $\lambda = 1$ or $\lambda = -1$. Assume that C is a λ-constacyclic code of length n over F. Then the dual $C^\perp$ of C is* $\mathrm{ann}^*(C)$.

Proof. Since $\lambda^2 = 1$, $\lambda = \lambda^{-1}$. In light of Propositions 2.2, $C^\perp$ is a λ-constacyclic codes of length n over F, and hence, by Proposition 2.1, both C and $C^\perp$ are ideals of the ring $\frac{F[x]}{\langle x^n-\lambda\rangle}$. The assertion now follows from Proposition 2.3. $\square$

Proposition 2.5. *Let α, β be distinct nonzero elements of the field F. Then a linear code C of length n over F is both α- and β-constacyclic if and only if $C = \{\mathbf{0}\}$ or $C = F^n$.*

Proof. ($\Leftarrow$) is obvious. To prove ($\Rightarrow$), assume that C is a nonzero code of length n over F, and C is both α- and β-constacyclic. As C is nonzero, there exists a codeword with a nonzero entry in C, without loss of generality, we can assume that $(c_0, \dots, c_{n-1}) \in C$ where $c_{n-1} \neq 0$. It follows that both $(\alpha c_{n-1}, c_0, \dots, c_{n-1})$ and $(\beta c_{n-1}, c_0, \dots, c_{n-1})$ belong to C, and hence,

$$(1, 0, \cdots, 0) = (\alpha-\beta)^{-1} c_{n-1}^{-1} \left[(\alpha c_{n-1}, c_0, \dots, c_{n-1}) - (\beta c_{n-1}, c_0, \dots, c_{n-1})\right] \in C.$$

As $(1, 0, \dots, 0)$ and all its cyclic shifts give a basis for F^n, it follows that $C = F^n$. $\square$

By Proposition 2.2, if C is a λ-constacyclic code, then $C^\perp$ is a λ^{-1} constacyclic code. So if $\lambda^2 \neq 1$, then $\lambda \neq \lambda^{-1}$, and thus, in light of Proposition 3, $C \neq C^\perp$. That means, among constacyclic codes, we can only have self-dual negacyclic or self-dual cyclic codes.

Proposition 2.6. *If $\lambda^2 \neq 1$, then there is no self-dual λ-constacyclic codes of any length n over F.*

Massey [9] introduced the concept of *linear codes with complementary duals* in 1992. A linear code with complementary dual, or an LCD code, is a linear code C with the dual $C^\perp$ such that $C \cap C^\perp = \{\mathbf{0}\}$. It is shown that asymptotically good LCD codes exist, and there are applications of LCD codes such as they provide an optimum linear coding solution for the two-user binary adder channel. It was proven by Sendrier [13] that LCD codes meet the Gilbert-Varshamov bound. Necessary and sufficient conditions for cyclic codes [15] and certain class of quasi-cyclic codes [5] to be LCD codes were provided.

In the class of constacyclic codes of length n over F, Propositions 2.5 and 2.2 imply that all λ-constacyclic codes with $\lambda^2 \neq 1$ are LCD codes. Indeed, if C is a λ-constacyclic code then $C^\perp$ is a λ^{-1}-constacyclic code, and hence $C \cap C^\perp$ is both λ- and λ^{-1}-constacyclic. When $\lambda^2 \neq 1$, as $C \cap C^\perp$ can not be F^n, by Proposition 3.1, $C \cap C^\perp = \{\mathbf{0}\}$.

Corollary 2.7. *If $\lambda^2 \neq 1$, then any λ-constacyclic code C of length n over F*

is a LCD code.

Proposition 2.6 tells us that, among all classes of λ-constacyclic codes, we may only have self-dual codes in the classes of cyclic and negacyclic codes. By Corollary 2.7, when $\lambda \notin \{-1, 1\}$, any λ-constacyclic code C is a LCD code. Thus, in order to obtain all LCD λ-constacyclic codes, we only need to look at the classes of cyclic and negacyclic codes.

In Sections 3 and 4, we will concentrate on the situation when $\lambda = 1$ (cyclic codes) and $\lambda = -1$ (negacyclic codes). We will obtain structures of all cyclic and and negacyclic codes of length $n = 100$, and use that to establish all self-dual and LCD cyclic and negacylic codes of length 100.

3. Cyclic Codes of length 100 over $\mathbb{F}_{25}$

As mentioned in Section 2, cyclic codes of length 100 over $\mathbb{F}_{25}$ are precisely ideals of the ring

$$\mathcal{R}_1 = \frac{\mathbb{F}_{p^m}[x]}{\langle x^{100} - 1\rangle}.$$

It is shown that $\mathcal{R}_1$ is a pricipal ideal ring, whose ideals are generated by factors of $x^{100} - 1$ (cf. [7]). Therefore, we first obtain the factorization of $x^{100} - 1$ into irreducible factors in $\mathbb{F}_{p^m}[x]$. Since $\mathbb{F}_{25}$ is a finite field with characteristic 5, we can see that

$$x^{100} - 1 = (x^4 - 1)^{25} = (x - 1)^{25}(x + 1)^{25}(x^2 + 1)^{25}.$$

Let ξ be a primitive 24th root of identity, then $\mathbb{F}_25$ can be expressed as follows.

$$\mathbb{F}_{24} = \left\{0, \xi, \ldots, \xi^{23}, \xi^{24} = \xi^0 = 1\right\}.$$

Clearly, $\xi^{\frac{24}{2}} = -1$. Then $\left(\xi^{\frac{24}{4}}\right)^2 = -1$. On the other hand, there is no element γ in $\mathbb{F}_{25}$ such that $\gamma^2 = -1$, i.e., $x^2 + 1$ is irreducible in $\mathbb{F}_{25}[x]$. We summarize this in the following proposition.

Proposition 3.1. *There exists $\gamma \in \mathbb{F}_{25}$ such that $\gamma^2 = -1$, and the factorization of $x^{100} + 1$ into irreducible factors in $\mathbb{F}_{25}[x]$ is*

$$x^{100} + 1 = (x - 1)^{25}(x + 1)^{25}(x - \gamma)^{25}(x + \gamma)^{25}.$$

Now, we can list all cyclic codes of length 100 over $\mathbb{F}_{25}$, i.e., ideals of $\mathcal{R}_1$, their sizes, and duals:

Theorem 3.2. *Cyclic codes of length* 100 *over* $\mathbb{F}_{25}$ *are* $\langle (x-1)^i(x+1)^j(x-\gamma)^k(x+\gamma)^l\rangle \subseteq \mathcal{R}_1$*, where* $0 \le i,j,k,l \le 25$*. Each code* $C_{i,j,k,l} = \langle (x-1)^i(x+1)^j(x-\gamma)^k(x+\gamma)^l\rangle$ *contains* $5^{2(100-i-j)}$ *codewords, its dual* $C^{\perp}_{i,j,k,l}$ *is the cyclic code* $C_{25-i,25-j,25-l,25-k} = \langle (x-1)^{25-i}(x+1)^{25-j}(x-\gamma)^{25-l}(x+\gamma)^{25-k}\rangle$.

Proof. The list of cyclic codes follows from the factorization of $x^{100}+1$ into procduct of irreducible factors in Proposition 3.1. For the dual codes, we first observe that $\operatorname{ann}(C_{i,j,k,l}) = \langle (x-1)^{25-i}(x+1)^{25-j}(x-\gamma)^{25-k}(x+\gamma)^{25-l}\rangle$, and $\operatorname{ann}(C_{i,j,k}) = \langle (x-1)^{25-i}(x+1)^{25-j}(x^2+1)^{25-k}\rangle$. On the other hand, $(x-1)^* = -x+1 = -(x-1)$, $(x+1)^* = x+1$, $(x-\gamma)^* = -\gamma x+1 = -\gamma(x+\gamma)$; $(x+\gamma)^* = \gamma x+1 = \gamma(x-\gamma)$; and $(x^2+1)^* = x^2+1$. Thus,

$$\begin{aligned}
C^{\perp}_{i,j,k,l} &= \operatorname{ann}^*(C_{i,j,k,l})\\
&= \left\langle (x-1)^{25-i}(x+1)^{p^s-j}(x-\gamma)^{25-k}(x+\gamma)^{25-l}\right\rangle^*\\
&= \left\langle \left[(x-1)^{p^s-i}\right]^* \left[(x+1)^{25-j}\right]^* \left[(x-\gamma)^{25-k}\right]^* \left[(x+\gamma)^{25-l}\right]^*\right\rangle\\
&= \left\langle \left[(x-1)^*\right]^{25-i} \left[(x+1)^*\right]^{25-j} \left[(x-\gamma)^*\right]^{25-k} \left[(x+\gamma)^*\right]^{25-l}\right\rangle\\
&= \left\langle (x-1)^{25-i}(x+1)^{25-j}(x-\gamma)^{25-l}(x+\gamma)^{25-k}\right\rangle\\
&= C_{25-i,25-j,25-l,25-k};
\end{aligned}$$

and for $p^m \equiv 3 \pmod 4$,

$$\begin{aligned}
C^{\perp}_{i,j,k} &= \operatorname{ann}^*(C_{i,j,k})\\
&= \left\langle (x-1)^{25-i}(x+1)^{25-j}(x^2+1)^{25-k}\right\rangle^*\\
&= \left\langle \left[(x-1)^{25-i}\right]^* \left[(x+1)^{25-j}\right]^* \left[(x^2+1)^{25-k}\right]^*\right\rangle\\
&= \left\langle \left[(x-1)^*\right]^{25-i} \left[(x+1)^*\right]^{25-j} \left[(x^2+1)^*\right]^{25-k}\right\rangle\\
&= \left\langle (x-1)^{25-i}(x+1)^{25-j}(x^2+1)^{25-k}\right\rangle\\
&= C_{25-i,25-j,25-k}.
\end{aligned}$$

Comparing the cyclic codes $C_{i,j,k,l}$, $C_{i,j,k}$ and their duals $C^{\perp}_{i,j,k,l}$, $C^{\perp}_{i,j,k}$, we see that $C_{i,j,k,l} = C^{\perp}_{i,j,k,l}$ if and only if $25 = 2i = 2j = k+l$, and $C_{i,j,k} = C^{\perp}_{i,j,k}$ if and only if $25 = 2i = 2j = 2k$, which is impossible. Thus, self-dual cyclic codes of length 100 do not exist.

Corollary 3.3. *For any odd prime p, there are no self-dual cyclic codes of length* 100 *over* $\mathbb{F}_{25}$.

The structure of cyclic codes of length 100 in Theorem 3.2 also help us to find all LCD cyclic codes.

Corollary 3.4. *There are precisely* 6 *LCD cyclic codes of length* 100 *over* $\mathbb{F}_{25}$*, namely,* $\langle 0\rangle$, $\langle (x-1)^{25}\rangle$, $\langle (x+1)^{25}\rangle$, $\langle (x-1)^{25}(x+1)^{25}\rangle$, $\langle (x-1)^{25}(x-\gamma)^{25}(x+\gamma)^{25}\rangle$, $\langle (x+1)^{25}(x-\gamma)^{25}(x+\gamma)^{25}\rangle$, $\langle 1\rangle$.

Proof. By Theorem 3.2, a cyclic code of length 100 over $\mathbb{F}_{25}$ is of the form $C_{i,j,k,l} = \langle (x-1)^i(x+1)^j(x-\gamma)^k(x+\gamma)^l\rangle \subseteq \mathcal{R}_1$, where $0 \le i,j,k,l \le p^s$, and its dual is the cyclic code $C^{\perp}_{i,j,k,l} = C_{25-i,25-j,p^s-l,25-k} = \langle (x-1)^{25-i}(x+1)^{25-j}(x-\gamma)^{25-l}(x+\gamma)^{25-k}\rangle$. Hence,

$$C\cap C^{\perp} = \left\langle (x-1)^{\max\{i,25-i\}}(x+1)^{\max\{j,p^s-j\}}(x-\gamma)^{\max\{k,25-l\}}(x+\gamma)^{\max\{l,25-k\}}\right\rangle.$$

It follows that C is a LCD code, i.e. $C\cap C^{\perp} = \{\mathbf{0}\}$, if and only if

$$\max\{i,25-i\} = \max\{j,25-j\} = \max\{k,25-l\} = \max\{l,25-k\},$$

which means $i,j \in \{0,25\}$, and $k=l=0$, or $k=l=25$. $\square$

References

[1] S.D. Berman, *Semisimple cyclic and Abelian codes. II*, Kibernetika (Kiev) **3** (1967), 21-30 (Russian). English translation: Cybernetics **3** (1967), 17-23.

[2] 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.

[3] H.Q. Dinh, *Constacyclic codes of length* 2^s *over Galois extension rings of* $\mathbb{F}_2 + u\mathbb{F}_2$, IEEE Trans. Inform. Theory **55** (2009), 1730-1740.

[4] H.Q. Dinh, *Repeated-root constacyclic codes of length* $2p^s$, Finite Fields & Appl. **18** (2012), 133-143.

[5] M. Esmaeili and S. Yari, *On complementary-dual quasi-cyclic codes*, Finite Fields Appl. **15** (2009), 375-386.

[6] G. Falkner, B. Kowol, W. Heise, E. Zehendner, *On the existence of cyclic optimal codes*, Atti Sem. Mat. Fis. Univ. Modena **28** (1979), 326-341.

[7] W.C. Huffman and V. Pless, *Fundamentals of error-correcting codes*, Cambridge University Press, Cambridge, 2003.

[8] F.J. MacWilliams and N.J.A. Sloane, *The theory of error-correcting codes*, 10^{th} impression, North-Holland, Amsterdam, 1998.

[9] J.L. Massey, *Linear codes with complementary duals*, Discrete Math. **106/107** (1992), 337-342.

[10] J.L. Massey, D.J. Costello, and J. Justesen, *Polynomial weights and code constructions*, IEEE Trans. Information Theory **19** (1973), 101-110.

[11] B.R. McDonald, *Finite rings with identity*, Pure and Applied Mathematics, Vol. **28**, Marcel Dekker, New York, 1974.

[12] R.M. Roth and G. Seroussi, *On cyclic MDS codes of length q over* GF(q)*,* IEEE Trans. Inform. Theory **32** (1986), 284-285.

[13] N. Sendrier, *Linear codes with complementary duals meet the Gilbert-Varshamov bound*, Discrete Math. **285** (2004), 345-347.

[14] J.H. van Lint, *Repeated-root cyclic codes*, IEEE Trans. Inform. Theory **37** (1991), 343-345.

[15] X. Yang and J.L. Massey, *The condition for a cyclic code to have a complementary dual*, Discrete Math. **126**(1994), 391-393.