Southeast Asian J. of Sciences: Vol. 6, No. 1 (2018) pp.17-27

A NOTE ON THE SYMBOL-PAIR DISTANCE OF REPEATED-ROOT NEGACYCLIC CODES OF LENGTH 14

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

In this paper, the symbol-pair distances of all repeated-root negacyclic codes of length 14 are obtained. As an application, all MDS symbol-pair negacyclic codes of length 14 over finite field $\mathbb{F}_{7^m}$ are established.

1. Introduction

In [1], Shannon showed that good codes exist, gave birth to information theory and coding theory. Although its origins is to solve the problem about reliable communication in an engineering problem, the subject has developed by using more and more mathematical techniques. Cyclic codes are the most studied of all codes, since their rich algebraic structures and practical implementations. Moreover, cyclic codes can build blocks for many other codes, such as BCH, Kerdock, Preparata and Justesen codes. Negacyclic codes as a direct generalization of cyclic codes, they also have rich algebraic structure and can be efficiently encoded using shift registers, have attracted remarkable attention for the last half of the century.

Let $\mathbb{F}_{p^m}$ be the finite field of order p^m, where p is an odd prime. Negacyclic codes of length n over $\mathbb{F}_{p^m}$ are defined by the ideals$\langle g(x)\rangle$ of quotient

Key words: Negacyclic codes, repeated-root codes, dual codes, Hamming distance, symbol-pair distance, MDS codes.

ring $\frac{\mathbb{F}_{p^m}}{\langle x^n+1\rangle}$, where the generator polynomial $\langle g(x)\rangle$ is the monic polynomial of least degree in the code, and is a divisor of x^n+1. In fact, all previous studies, most researcher focus their attention on the situation that $\gcd(n,p)=1$. This is equivalent to say that generator polynomial $g(x)$ has no repeated irreducible factors, these codes are called simple-root negacyclic codes. Instead, when $\gcd(n,p)=n$, i.e., generator polynomial $g(x)$ has repeated roots in an extension filed. We called these codes are repeated-root codes, which were first investigated in the 1990s by Castagnoli in [7] and Van Lint in [37]. In these papers, the authors have shown that repeated-root cyclic codes cannot be asymptotically better than simple-root cyclic codes. But, there still exist a few optimal such codes (see, for example, [12 14]), which encourages many researchers to study the class of codes. The reader can refer to [16, 17, 18, 5, 24, 11, 12].

Let Σ be an alphabet of size q, whose elements are called symbols. Suppose that $\mathbf{x}=(x_0,x_1,\cdots,x_{n-1})$ is a vector in Σ^n, in [8], Cassuto and Blaum defined the symbol-pair vector of $\mathbf{x}$ as

$$\pi_{\mathrm{sp}}(\mathbf{x})=[(x_0,x_1),(x_1,x_2),\cdots,(x_{n-2},x_{n-1}),(x_{n-1},x_0)]\in(\Sigma^2)^n. \qquad (1)$$

Two pairs (c,d) and (e,f) are distinct if $c\neq e$ or $d\neq f$, or both. For any two vectors $\mathbf{x}$ and $\mathbf{y}$, the symbol-pair distance between $\mathbf{x}$ and $\mathbf{y}$ is defined as $\mathrm{d_{sp}}(\mathbf{x},\mathbf{y})=\mathrm{d_H}(\pi_{\mathrm{sp}}(\mathbf{x}),\pi_{\mathrm{sp}}(\mathbf{y}))$, where $\mathrm{d_H}$ denotes the usual Hamming distance. Accordingly, if the pair $(c,d)\neq(0,0)$, we say $\mathrm{wt_H}(c,d)=1$, otherwise, $\mathrm{wt_H}(c,d)=0$. Then the symbol-pair weight of a vector $\mathbf{x}$ is defined as

$$\mathrm{wt_{sp}}(\mathbf{x})=\mathrm{wt_H}(\pi_{\mathrm{sp}}(\mathbf{x}))=\Big|\{i\,|\,(x_i,x_{i+1})\neq(0,0),0\leq i\leq n-1,x_n=x_0\}\Big|.$$

A *q-ary* code C of length n over Σ can be regard as a nonempty subset of Σ^n. Then the minimum symbol-pair distance of a code C is defined to be $\mathrm{d_{sp}}(C)=min(\mathrm{d_{sp}}(\mathbf{c}_1,\mathbf{c_2})\mid\mathbf{c}_1,\mathbf{c_2}\in C,\mathbf{c}_1\neq\mathbf{c}_2)$. Clearly, if C is a linear pair code, the symbol-pair weight and minimum symbol-pair distance are the same, that is to say, $\mathrm{d_{sp}}(C)=min(\mathrm{wt_{sp}}(\mathbf{c})|\mathbf{c}\neq 0,\mathbf{c}\in C)$.

In [8, 9], Cassuto and Blaum has shown that the symbol-pair codes are designed to protect against pair errors in symbol-pair read channels, and a symbol-pair code C can correct t pair-errors if and only if $\mathrm{d_{sp}}>2t+1$, where $\mathrm{d_{sp}}$ is the minimum pair-distance of C. So the minimum pair-distance is one of the important parameters of a symbol-pair code. For any code C of length n with $0<\mathrm{d_H}<n$, a simple but important connection between $\mathrm{d_H}$ and $\mathrm{d_{sp}}$ is given in [8]: $\mathrm{d_H}+1\leq\mathrm{d_{sp}}\leq 2\mathrm{d_H}$. Later on, in [10], Cassuto and Litsyn have shown that for any cyclic code C of length n with Hamming distance $\mathrm{d_H}$, if the generator polynomial $g(x)$ of C has at least $\mathrm{d_H}$ roots in the splitting field of x^n-1, then the symbol-pair distance of C is at least $\mathrm{d_H}+2$. In addition, in [10], they proved that if the length n of cyclic code is prime, and

the generator polynomial $g(x)$ of C has at least m roots in the splitting field of $x^n - 1$, and $\mathrm{d_H} \leq min\{2m - n + 2, m - 1\}$, then the symbol-pair distance of C is at least $\mathrm{d_H} + 3$. Recently, in [38], Yaakobi *et al.* considered the lower bound of binary cyclic code and showed the result: for any linear cyclic code of dimension greater than one with a minimum Hamming distance $\mathrm{d_H}$, the symbol-pair distance is at least $\mathrm{d_H} + \lceil \frac{\mathrm{d_H}}{2} \rceil$.

It is well known for any fixed code length n and dimension k, maximum distance separable(MDS) code has the largest minimum distance, i.e., they have the best possible error-correction capability. Thus, how to construct MDS code always a hot topic in coding theory. As a generalization of MDS codes, MDS symbol-pair codes also have the best possible error-correction capability. More recently, in[15], Chee *et al.* established singleton Bound for symbol-pair codes as follows: Let $2 \leq \mathrm{d_{sp}} \leq n$, then for any symbol-pair code C of length n with size M and minimum pair-distance $\mathrm{d_{sp}}$ over $\mathbb{F}_q$, $M \leq q^{n-\mathrm{d_{sp}}+2}$. If the equality hold then the symbol-pair code C is called an optimal code with respect to Singleton bound, or MDS symbol-pair code. After establishing the Singleton Bound, a lot of work focus on how to construct MDS symbol-pair codes(see, for example, [15, 14]). But a few work has been done on how to determine the symbol-pair distance of some classes of linear code as it is generality difficult to determine. In [4], Dinh *et al.* computed the symbol-pair distance of all constacyclic codes of length 5 over $\mathbb{F}_{7^m}$. As an application, they obtained a lot of MDS symbol-pair codes. Motivated by [4], in this paper, we get the symbol-pair distance of all negacyclic codes of length 14 over $\mathbb{F}_{7^m}$ and obtained numerous symbol-pair codes. Moreover, we find that our result are also suitable for all constacyclic codes of length 14 over $\mathbb{F}_{7^m}$.

The remainder of the paper is organized as follows. Section 2 recalls some preliminary results. In Section 3, we study the symbol-pair distance of negacyclic codes of length 14. In Section 4, we give the all MDS symbol-pair codes of length 14.

2. Preliminaries

In this Section, we state some basic fact about finite ring and constacyclic codes. A principal ring is a ring in which each ideal generated by a single element. A chain ring is a principal ring such that the ideals are linearly orders under set theoretic containments. Let R be a finite ring. An element $r \in R$ is said to be nilpotent with nilpotency index l if $r^l = 0$ and l is the least positive integer with respect to this property. It follows that if R is a finite commutative chain ring, then there is an element γ such that γ generator of the unique maximal ideal of R. Hence, the ideals of R are $\langle\gamma^i\rangle$ and they form a chain:

$$R = \langle\gamma^0\rangle \supsetneq \langle\gamma^1\rangle \supsetneq \cdots \supsetneq \langle\gamma^{l-1}\rangle \supsetneq \langle\gamma^l\rangle = \langle 0\rangle.$$

Let p be an odd prime, m be a positive integer, and $\mathbb{F}_{p^m}$ be a finite field. A code C of length n over $\mathbb{F}_{p^m}$ is a nonempty subset of $\mathbb{F}_{p^m}^n$. An $[n,k]$-linear code C over the finite field $\mathbb{F}_{7^m}$ is a k-dimensional linear subspace of $\mathbb{F}_{p^m}^n$. Moreover, For a nonzero element λ of $\mathbb{F}_{7^m}$, if $(c_0, c_1, \cdots, c_{n-1}) \in C$ implies $(\lambda c_{n-1}, c_0, \cdots, c_{n-2}) \in C$, then C is called a λ-constacyclic code. It is well known that any constacyclic code C of length n over $\mathbb{F}_{7^m}$ corresponds to an ideal of $\mathbb{F}_{p^m}[x]/(x^n + \lambda)$ and it can be expressed as $C = (g(x))$, where $g(x)$ is monic and has least degree in the code. In the case $\lambda = -1$, those λ-constacyclic codes are called cyclic codes, and when $\lambda = 1$, such λ-constacyclic codes are called negacyclic codes. From that, negacyclic codes of length 14 over $\mathbb{F}_{7^m}$ correspond to the ideals of the finite ring

$$\mathcal{R}_1 = \frac{\mathbb{F}_{p^m}[x]}{\langle x^{10}+1\rangle}.$$

Clearly, $\mathcal{R}_1$ is a principal ideal ring, whose ideals are generated by factors of $x^{10}+1$. In [3], the authors have shown that the polynomial $x^2+1 \in \mathbb{F}_{p^m}[x]$ is irreducible if and only if $p^m \equiv 4k+3$ for some integer positive m (see Lemma 7.8). Hence, if $p^m \equiv 3 \pmod 4$, then the monic divisors of $x^{10}+1 = (x^2+1)^{p^s}$ are the set $\{x^2+1)^i : 0 \leq i \leq p^s\}$. Therefore, $\mathcal{R}_1$ is a chain ring, whose maximal ideal is (x^2+1). Similarly, If $p^m \equiv 1 \pmod 4$, then the monic divisors of $x^{10}+1 = (x-\gamma)^{p^s}(x+\gamma)^{p^s}$ are the set $\{(x-\gamma)^i(x+\gamma)^j : 0 \leq i,j \leq p^s\}$, where $\gamma \in \mathbb{F}_{p^m}$ such that $\gamma^2 = -1$. Therefore, $\mathcal{R}_1$ is a principal ideal ring, but not a chain ring, whose maximal ideal is $(x-\gamma)$ or $(x+\gamma)$.

The following is well known fact about $\mathcal{R}_1$.

Proposition 1. *(Theorem 3.2 of [16]) Let p be an odd prime, and m be a positive integer.*

- *(a) If $p^m \equiv 1 \pmod 4$, negacyclic codes of length 14 over $\mathbb{F}_{7^m}$ are $\langle (x-\gamma)^i(x+\gamma)^j\rangle \subseteq \mathcal{R}_1$, where $0 \leq i,j \leq p^s$. Each code $\mathcal{C}_{i,j} = \langle (x-\gamma)^i(x+\gamma)^j\rangle$ contains $p^{m(10-i-j)}$ codewords, its dual is $\mathcal{C}_{i,j}^{\perp} = \langle (x-\gamma)^{p^s-i}(x+\gamma)^{p^s-j}\rangle$.*
- *(b) If $p^m \equiv 3 \pmod 4$, negacyclic codes of length 14 over $\mathbb{F}_{7^m}$ are $\langle (x^2+1)^i\rangle \subseteq \mathcal{R}_1$, where $0 \leq i \leq p^s$. Each code $\mathcal{C}_i = \langle (x^2+1)^i\rangle$ contains $p^{2m(p^s-i)}$ codewords, its dual is $\mathcal{C}_i^{\perp} = \mathcal{C}_{p^s-i} = \langle (x^2+1)^{p^s-i}\rangle$.*

Given two codewords $\mathbf{x} = (x_0, x_1, \ldots, x_{n-1}), \mathbf{y} = (y_0, y_1, \ldots, y_{n-1}) \in \mathbb{F}_{p^m}^n$, their inner product is defined as:

$$\mathbf{x}\cdot\mathbf{y} = x_0y_0 + x_1y_1 + \cdots + x_{n-1}y_{n-1}.$$

Then $\mathbf{x}, \mathbf{y}$ are called *orthogonal* if $\mathbf{x} \cdot \mathbf{y} = 0$. For a linear code C over $\mathbb{F}_{p^m}$, its *dual code* $C^\perp$ is the set of n-tuples over $\mathbb{F}_{p^m}$ that are orthogonal to all codewords of C, i.e.,

$$C^\perp = \{\mathbf{x} \in \mathbb{F}_{p^m}^n \mid \mathbf{x} \cdot \mathbf{y} = 0, \forall \mathbf{y} \in C\}.$$

In particular, a code C is called *self-orthogonal* if $C \subseteq C^\perp$ and it is called *dual-containing* if $C^\perp \subseteq C$. Moreover, it is called *self-dual* if $C = C^\perp$.

Then, making use of Proposition 1, it is straightforward for us to get the necessary and sufficient conditions for negacyclic codes of length 14 over $\mathbb{F}_{p^m}$ to be self-dual, self-orthogonal, dual containing.

Corollary 2. *Let C be a nonzero negacyclic code of length 14 over $\mathbb{F}_{p^m}$. Then $C = \langle (x^2+1)^i \rangle \subseteq \mathcal{R}_1$ for $i \in \{0, 1, \ldots, 7\}$,*

(*a*) *C is dual containing if and only if and $0 \leq i \leq 7/2$.*

(*b*) *C is self-orthogonal if and only if $p^s/2 \leq i \leq 7$.*

(*c*) *C is self-orthogonal do not exist.*

If $p^m \equiv 1 \pmod 4$, i.e., $C = \langle (x-\gamma)^i (x+\gamma)^j \rangle \subseteq \mathcal{R}_1$ for $0 \leq i, j \leq 7$,

(*a*) *C is dual containing if and only if $0 \leq i, j \leq 7/2$.*

(*b*) *C is self-orthogonal if and only if $7/2 \leq i, j \leq 7$.*

(*c*) *C is self-dual if and only if $i + j = 7$.*

In the next section, we will use the concept of *coefficient weight* of polynomials, which was given in [19]: Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ be a polynomial with degree n, the coefficient weight of f, is defined as

$$\mathrm{cw}(f) = \begin{cases} 0, & \text{if } f \text{ is a monomial} \\ \min\{|i-j| : a_i \neq 0,\ a_j \neq 0,\ i \neq j\}, & \text{otherwise.} \end{cases}$$

Obviously, $\mathrm{cw}(f)$ is the smallest distance among exponents of nonzero terms of $f(x)$. Base on this fact, we have the following lemma.

Lemma 3. *For any two nonzero polynomial $f(x)$ and $g(x)$, if $f(x)$ and $g(x)$ satisfied one of the following condition*

- $0 \leq \deg(g(x)) \leq \mathrm{cw}(f(x)) - 2$, *and* $\deg(f(x)) + \deg(g(x)) \leq n - 2$*;*
- $0 \leq \deg(g(x)) = \mathrm{cw}(f(x)) - 1$, *and* $\deg(f(x)) + \deg(g(x)) = n - 1$*.*

Then, by definition,

$$\mathrm{wt}_{\mathrm{sp}}(f(x)\, g(x)) = \mathrm{wt}_{\mathrm{H}}(f(x)) \cdot \mathrm{wt}_{\mathrm{sp}}(g(x)).$$

The condition $\deg(f(x)) + \deg(g(x)) \leq n-2$ ensures that $f(x)g(x)$ does not represent a codeword of length n that has the first and last entries being nonzero, otherwise, $\mathrm{wt}_{\mathrm{H}}(f(x)) \cdot \mathrm{wt}_{\mathrm{sp}}(g(x))$ may be greater than $\mathrm{wt}_{\mathrm{sp}}(f(x)\, g(x))$. The conditions $0 \leq \deg(g(x)) = \mathrm{cw}(f(x)) - 1$, and $\deg(f(x)) + \deg(g(x)) = n-1$ ensures that a codeword of length n can be partition into some same short codes, otherwise, $\mathrm{wt}_{\mathrm{H}}(f(x)) \cdot \mathrm{wt}_{\mathrm{sp}}(g(x))$ may be less than $\mathrm{wt}_{\mathrm{sp}}(f(x)\, g(x))$. This can be explained by the following two examples.

Example 4. *Let* $f(x) = x^6 + 1$, *and* $g(x) = x^4 + x^2 + 1$. *Then* $\mathrm{cw}(f(x)) = 6$, $\deg(g(x)) = 4$, $\mathrm{wt}_{\mathrm{H}}(f(x)) = 2$, $\mathrm{wt}_{\mathrm{sp}}(g(x)) = 6$, *and* $f(x)g(x) = x^{10} + x^8 + x^6 + x^4 + x^2 + 1$. *If the code of length is* $n = 11$, *then* $f(x)g(x)$ *represents the codeword* $(1,0,1,0,1,0,1,0,1,0,1)$, *and* $\mathrm{wt}_{\mathrm{sp}}(f(x)g(x)) = 11 < \mathrm{wt}_{\mathrm{H}}(f(x)) \cdot \mathrm{wt}_{\mathrm{sp}}(g(x))$.

Example 5. *Let* $f(x) = x^6 + 1$, *and* $g(x) = x^5 + x^2 + 1$. *Then* $\mathrm{cw}(f(x)) = 6$, $\deg(g(x)) = 5$, $\mathrm{wt}_{\mathrm{H}}(f(x)) = 2$, $\mathrm{wt}_{\mathrm{sp}}(g(x)) = 5$, *and* $f(x)g(x) = x^{11} + x^8 + x^6 + x^5 + x^2 + 1$. *If the code of length is* $n = 13$, *then* $f(x)g(x)$ *represents the codeword* $(1,0,1,0,0,1,1,0,1,0,0,1,0)$, *and* $\mathrm{wt}_{\mathrm{sp}}(f(x)g(x)) = 11 > \mathrm{wt}_{\mathrm{H}}(f(x)) \cdot \mathrm{wt}_{\mathrm{sp}}(g(x))$.

3. Symbol-pair distance of negacyclic codes of length 14 over $\mathbb{F}_{7^m}$

As discussed in Section 3, for the sake of narrative convenience, we denote negacyclic code $\langle (x^2+1)^i \rangle$ by $\mathcal{C}_i$ for $i = 0, 1, \ldots, p^s$, and $\langle (x+\gamma)^i (x-\gamma)^j \rangle$ by $\mathcal{C}_{i,j}$ for $i, j \in \{0, 1, \ldots, 7\}$. Their symbol-pair distance are denoted by $\mathrm{d}_{\mathrm{sp}}(\mathcal{C}_i)$ and $\mathrm{d}_{\mathrm{sp}}(\mathcal{C}_{i,j})$, respectively. For any codeword $c(x) \in \mathcal{C}_i$ or $\mathcal{C}_{i,j}$, the Hamming weight and symbol-pair weight are denoted by $\mathrm{wt}_{\mathrm{H}}(c(x))$ and $\mathrm{wt}_{\mathrm{sp}}(c(x))$, respectively. In [3], the author have considered the Hamming distance of $\mathcal{C}_i$.

Proposition 6. *(Theorem* 7.9 *of [3]) The negacyclic codes of length* 14 *over* $\mathbb{F}_{7^m}$ *are of the form* $\mathcal{C}_i = \langle (x^2+1)^i \rangle$ *for* $i = 0, 1, \cdots, p^s$. *Moreover, its Hamming distance* $\mathrm{d}_{\mathrm{H}}(\mathcal{C}_i)$ *is determined by:*

$$\mathrm{d}_{\mathrm{H}}(\mathcal{C}_i) = \begin{cases} 1, & \text{if } \ i = 0 \\ (\beta+1)p^{k_1}, & \text{if } \ 7 - 7^{1-k_1} + \beta 7^{-k_1} + 1 \leq i \leq 7 - 7^{1-k_1} + (\beta+1)7^{-k_1} \\ & \qquad \text{where } \ 0 \leq \beta \leq 7, \ \text{ and } \ 0 \leq k_1 \\ 0, & \text{if } \ i = 7. \end{cases}$$

Base on the Hamming distance, we can show the symbol-pair distance of $\mathcal{C}_i$ as follows.

Theorem 7. *The symbols defined as Proposition 6. Then symbol-pair distance of $\mathcal{C}_i$ is determined by:*

$$\mathrm{d}_{\mathrm{sp}}(\mathcal{C}_i) = \begin{cases} 2, & \textit{if} \ \ i = 0 \\ 2(\beta+1)7^{k_1}, & \textit{if} \ \ 7 - 7^{1-k_1} + \beta 7^{-k_1} + 1 \le i \le 7 - 7^{1-k_1} + (\beta+1)7^{-k_1} \\ & \quad \textit{where} \ \ 0 \le \beta \le 5, \ \ \textit{and} \ \ 0 \le k_1 \\ 0, & \textit{if} \ \ i = 7. \end{cases}$$

Proof. Recall that

$$\mathcal{R}_1 = \mathcal{C}_0 \supset \mathcal{C}_1 \supset \cdots \supset \mathcal{C}_6 \supset \mathcal{C}_7 = \langle 0 \rangle.$$

Clearly, $\mathrm{d}_{\mathrm{sp}}(\mathcal{C}_7) = 0$, and $\mathrm{d}_{\mathrm{sp}}(\mathcal{C}_0) = 2$. Furthermore, $2 = \mathrm{d}_{\mathrm{sp}}(\mathcal{C}_0) \le \mathrm{d}_{\mathrm{sp}}(\mathcal{C}_1) \le \mathrm{d}_{\mathrm{sp}}(\mathcal{C}_2) \le \cdots \le \mathrm{d}_{\mathrm{sp}}(\mathcal{C}_6)$. Now, we consider the other cases.

Let $c(x)$ be an arbitrary nonzero element of $\mathcal{C}_i$. Then there exist a nonzero element $f(x) \in \mathcal{R}_1$ such that $c(x) = (x^2+1)^i f(x)$. By the Division Algorithm, we can assume that $\deg(f) < 14 - 2i - 1$. Let $f(x)$ be expressed as

$$f(x) = f_0 + f_1 x + \cdots + f_\ell x^\ell,$$

where $f_0, f_1, \ldots, f_\ell \in \mathbb{F}_{p^m}$, and $\ell = 14 - 2i - 1$. Partition $f(x)$ into two polynomials $f_0(x)$ and $f_1(x)$, i.e., $f(x) = f_0(x) + f_1(x)$, where $f_0(x)$ only contains terms of even exponents $f_{2l}x^{2l}$, and $f_1(x)$ only contains terms of odd exponents $f_{2l+1}x^{2l+1}$, where $l = 0, 1, \cdots, 6 - i$.

We consider the following 3 cases.

Case 1: $f_0(x) = 0$. Then there are exactly coefficients f_{2j+1} is nonzero. We have

$$\mathrm{wt}_{\mathrm{H}}(c(x)) = \mathrm{wt}_{\mathrm{H}}((x^2+1)^i f(x)) = \mathrm{wt}_{\mathrm{H}}\left(\left[\sum_{h=0}^{i} \binom{i}{h} x^{2h}\right] f_1(x)\right).$$

Thus, the nonzero terms of $c(x)$ are $2h+1$ positions apart for $h = 0, 1, \cdots, p^s - 1$. It follows that $\mathrm{wt}_{\mathrm{sp}}(c(x)) = 2\,\mathrm{wt}_{\mathrm{H}}(c(x)) \ge 2\,\mathrm{d}_{\mathrm{H}}(\mathcal{C}_i)$.

Case 2: $f_1(x) = 0$. Then there are exactly coefficients f_{2j} is nonzero. Then

$$\mathrm{wt}_{\mathrm{H}}(c(x)) = \mathrm{wt}_{\mathrm{H}}((x^2+1)^i f(x)) = \mathrm{wt}_{\mathrm{H}}\left(\left[\sum_{h=0}^{i} \binom{i}{h} x^{2h}\right] f_0(x)\right).$$

So the nonzero terms of $c(x)$ are $2h$ positions apart for $h = 0, 1, \cdots, p^s - 1$. Therefore, $\mathrm{wt}_{\mathrm{sp}}(c(x)) = 2\,\mathrm{wt}_{\mathrm{H}}(c(x)) \ge 2\,\mathrm{d}_{\mathrm{H}}(\mathcal{C}_i)$.

Case 3: $f_0(x) \neq 0$ and $f_1(x) \neq 0$. Then

$$(x^2+1)^i f(x) = (x^2+1)^i f_0(x) + (x^2+1)^i f_1(x).$$

Because the nonzero terms of $(x^2+1)^i f_0(x)$ are $2k$ positions apart and the nonzero terms of $(x^2+\gamma)^i f_1(x)$ are $2k+1$ positions apart for $k = 0, 1, \cdots, p^s - 1$, then $(x^2+1)^i f_0(x)$ and $(x^2+1)^i f_1(x)$ do not contain any term with same power of x. Therefore,

$$\mathrm{wt_H}((x^2+1)^i f(x)) = \mathrm{wt_H}((x^2+1)^i f_0(x)) + \mathrm{wt_H}((x^2+1)^i f_1(x)).$$

Since $(x^2+1)^i f_0(x)$ and $(x^2+1)^i f_1(x)$ are nonzero element in $\mathcal{C}_i$,

$$\mathrm{wt_H}((x^2+1)^i f_0(x)) \geq d_H(\mathcal{C}_i) \text{ and } \mathrm{wt_H}((x^2+1)^i f_1(x)) \geq d_H(\mathcal{C}_i).$$

Hence, $\mathrm{wt_{sp}}(c(x)) \geq \mathrm{wt_H}((x^2+1)^i f(x)) \geq 2\,\mathrm{d_H}(\mathcal{C}_i)$.

Theorefore, for any $c(x) \in \mathcal{C}_i$, $\mathrm{wt_{sp}}(c(x)) \geq 2\,\mathrm{d_H}(\mathcal{C}_i)$, implying $\mathrm{d_{sp}}(\mathcal{C}_i) \geq 2\,\mathrm{d_H}(\mathcal{C}_i)$. As $\mathrm{d_{sp}}(\mathcal{C}_i) \leq 2\,\mathrm{d_H}(\mathcal{C}_i)$, making use of Proposition 6, the result follows. □

Now, we consider the symbol-pair distance of negacyclic code $\mathcal{C}_{i,j}$ for $i, j \in \{0, 1, \ldots, p^s\}$. Obviously, if $i = j = 0$, then $\mathcal{C}_{0,0} = \mathcal{R}_1$, and if $i = j = p^s$, then $\mathcal{C}_{p^s,p^s} = \{0\}$. For the remaining values of i, j, as the symmetries of all the cases, without loss of generality, in the following of this section, we always assume $i \geq j$. If $i = j$, clearly, $\mathcal{C}_{i,j} = \langle (x+\gamma)^i (x-\gamma)^j \rangle = \langle (x^2+1)^i \rangle$. In fact, Theorem 7 gives the symbol-pair distance of $\mathcal{C}_{i,j}$.

Proposition 8. *If $i = j$ for $i \in \{0, 1, \cdots, 7\}$. Then symbol-pair distance of $\mathcal{C}_{i,j}$ is determined by:*

$$\mathrm{d_{sp}}(\mathcal{C}_{i,j}) = \begin{cases} 2, & if \;\; i = 0 \\ 2(\beta+1)7^{k_1}, & if \;\; 7 - 7^{1-k_1} + \beta 7^{-k_1} + 1 \leq i \leq 7 - 7^{1-k_1} + (\beta+1)7^{-k_1} \\ & \qquad where \;\; 0 \leq \beta \leq 5, \;\; and \;\; 0 \leq k_1 \\ 0, & if \;\; i = 7. \end{cases}$$

4. Symbol-Pair negacyclic Codes of Length 14 over $\mathbb{F}_{7^m}$

In [15], the authors introduced that the parameters of an $[n, k, \mathrm{d_{sp}}]$ linear code C over $\mathbb{F}_{7^m}$ satisfying $\mathrm{d_{sp}} \leq n - k + 2$, and if the equality hold then a symbol-pair code C is called an optimal code with respect to Singleton bound, or a *maximum distance separable* (MDS) symbol-pair code. For any fixed symbol-pair code length n and dimension k, MDS symbol-pair code has the largest minimum distance, i.e., they have the best possible error-correction capability. Hence, constructing MDS symbol-pair codes is significance in theory and practice.

In this section, we will determine all MDS symbol-pair negacyclic codes of length 14. First of all, we consider the case $p^m \equiv 3 \pmod 4$.

Theorem 9. *Let p be an odd prime, m be an interger, $p^m \equiv 3 \pmod 4$, then the negacyclic codes of length 14 over $\mathbb{F}_{7^m}$ are of the form $\mathcal{C}_i = \langle (x^2+1)^i \rangle$ for $i = 0, 1, \cdots, 7$. Moreover, $\mathcal{C}_i$ is a MDS symbol-pair code if and only if one of the following conditions holds:*

- *If $s = 1$, then $i = \beta + 1$, for $0 \leq \beta \leq 7$, in such case, $\mathrm{d}_{\mathrm{sp}}(\mathcal{C}_i) = 2(\beta + 2)$.*

Proof. For $0 \leq i, j \leq 7$, by Proposition 1, we have $|\mathcal{C}_i| = p^{m(7-i-j)}$, implying the dimension of symbol-pair code $\mathcal{C}_i$ is $7 - i - j$. By Singleton bound, $\mathcal{C}_i$ is a MDS symbol-pair code if and only if $i + j = \mathrm{d}_{\mathrm{sp}}(\mathcal{C}_i) - 2$.

When $i = j$, the conditions for $\mathcal{C}_{i,j}$ is a MDS symbol-pair code have been given by Theorem 9. So, we can give the result, directly.

- If $s = 1$, then $i = j = \beta + 1$, for $0 \leq \beta \leq 7$, in such case, $\mathrm{d}_{\mathrm{sp}}(\mathcal{C}_i) = 2(\beta + 2)$.

References

[1] C. E. Shannon, *A mathematical theory of communication*, The Bell System Technical Journal, **27** (1948) 379-423.

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

[3] S.R. Lopez-Permouth, H. Ozadam, F. Ozbudak, S.Szabo, *Polycyclic codes over Galois rings with applications to repeated-root constacyclic codes*, Finite Fields Appl. **19** (2013), 16-38.

[4] H.Q.Dinh, B.T. Nguyen, A.K. Singh, and S. Sriboonchitta *On the Symbol-Pair Distance of Repeated-Root Constacyclic codes of Prime Power Lenrths* , IEEE Trans. Inform. Theory

[5] G.K. Bakshi, M. Raka, *A class of constacyclic codes over a finite field*, Finite Fields & Appl. **18** (2012) 362-377.

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

[7] 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.

[8] Y. Cassuto and M. Blaum, *Codes for symbol-pair read channels*, Conference in Proc. IEEE Int. Symp. Inf. Theory, Austin, TX, USA, Jun, (2010), 988-992.

[9] Y. Cassuto and M. Blaum, *Codes for symbol-pair read channels*, IEEE Trans. Inf. Theory, 57 **12** (2011), 8011-8020.

[10] Y. Cassuto and S. Litsyn, *Symbol-pair codes: algebraic constructions and asymptotic bounds*, Conference in Proc. IEEE Int. Symp. Inf. Theory, St. Petersburg, Russia, Jul-Aug. (2011) 2348-2352.

[11] B. Chen, H.Q. Dinh, and H. Liu, *Repeated-root constacyclic codes of length ℓp^s and their duals*, Discrete Appl. Math. **177** (2014), 60-70.

[12] B. Chen, H.Q. Dinh, and H. Liu, *Repeated-root constacyclic codes of length $2\ell^m p^n$*, Finite Fields & Appl. **33** (2015), 137-159.

[13] B. Chen and H.Q. Dinh, *Equivalence classes and structures of constacyclic codes over finite fields*, AMS Contemporary Mathematics **642** (2015), 181-223.

[14] B. Chen, L. Lin, and H. Liu. *Constacyclic symbol-pair codes: lower bounds and optimal constructions*, preprint arXiv:1605.03460, (2016).

[15] Y. M. Chee, L. Ji, H. M. Kiah, C. Wang and J. Yin, *Maximum distance separable codes for symbol-pair read channels*, IEEE Trans. Inf. Theory, 59 **11** (2013), 7259-7267.

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

[17] H.Q. Dinh, *Structure of repeated-root constacyclic codes of length $3p^s$ and their duals*, Discrete Math. **313** (2013) 983-991.

[18] H.Q. Dinh, *Structure of repeated-root cyclic codes and negacyclic codes of length $6p^s$ and their duals*, Contemp. Math. **609** (2014) 69-87.

[19] 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.

[20] 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.

[21] H.Q. Dinh, *Repeated-root constacyclic codes of prime power length*, AMS Contemporary Mathematics **480** (2009), 87-100.

[22] 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.

[23] H.Q. Dinh, *Constacyclic codes of length p^s over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$*, J. Algebra **324** (2010), 940-950.

[24] H.Q. Dinh, *On repeated-root constacyclic codes of length $4p^s$*, Asian European J. Math **6** (2013), 1-25.

[25] H.Q. Dinh and S.R. López-Permouth, *Cyclic and Negacyclic Codes over Finite Chain Rings*, IEEE Trans. Inform. Theory **50** (2004), 1728-1744.

[26] 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.

[27] M. Hirotomo, M. Takita and M. Morii, *Syndrome decoding of symbol-pair codes*, Conference in Proc. IEEE Inf. Theory Workshop, Hobart, TAS, Australia, (2014), 162-166.

[28] X. Kai, S. Zhu and P. Li, *A Construction of New MDS Symbol-Pair Codes*, IEEE Trans. Inf. Theory, 61 **11** (2015), 5828-5834.

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

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

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

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

[33] C.-S. Nedeloaia, *Weight distributions of cyclic self-dual codes*, IEEE Trans. Inform. Theory **49** (2003), 1582-1591.

[34] V. Pless and W.C. Huffman, *Handbook of Coding Theory*, Elsevier, Amsterdam, 1998.

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

[36] L.-z. Tang, C.B. Soh and E. Gunawan, *A note on the q-ary image of a q^m-ary repeated-root cyclic code*, IEEE Trans. Inform. Theory **43** (1997), 732-737.

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

[38] E. Yaakobi, J. Bruck and P. H. Siegel. *Decoding of cyclic codes over symbol-pair read channels*, Conference in Proc. Int. Symp. Inf. Theory, Cambridge, MA, USA, (2012), 2891-2895.

[39] E. Yaakobi, J. Bruck, P. H. Siegel, *Constructions and decoding of cyclic codes over b-symbol read channels*, IEEE Trans. Inf. Theory, 62 **4** (2016), 1541-1551.