THE UNITS OF THE CHAIN RING $\frac{\mathbb{F}_{2}m[u]}{\langle u^4\rangle}$ AND AN APPLICATION

Huong T. T. Nguyen*, Phuc T. Do, Hoa Q. Nguyen, Hai T. Hoang, Linh M. T. Tran

College of Economics and Business Administration - TNU

ABSTRACT

The units of the chain ring $\mathcal{R}_4 = \frac{\mathbb{F}_{2^m}[u]}{\langle u^4\rangle} = \mathbb{F}_{2^m} + u\mathbb{F}_{2^m} + u^2\mathbb{F}_{2^m} + u^3\mathbb{F}_{2^m}$ are partitioned into 4 distinct types. It is shown that for any unit α of Type k, a unit α^* of Type k^* can be constructed for all $k = 0, 1, 2, 3$. The units of $\mathcal{R}_4$ of the form $\alpha = \alpha_0 + u\alpha_1 + u^2\alpha_2 + u^3\alpha_3$, where $\alpha_0, \alpha_1, \alpha_2, \alpha_3 \in \mathbb{F}_{2^m}$, $\alpha_0 \neq 0$, $\alpha_1 \neq 0$, are considered in details. As an application, it is shown that self-dual α-constacyclic codes of length 2^s over $\mathcal{R}_4$ exist. We can also prove that it is unique.

Keywords: *Constacyclic codes, cyclic codes, dual codes, chain rings.*

1. INTRODUCTION

The classes of cyclic and negacyclic codes in particular, and constacyclic codes in general, play a very significant role in the theory of error-correcting codes. Let $\mathbb{F}$ be a finite field of characteristic p and α be a nonzero element of $\mathbb{F}$. α-constacyclic codes of length n over $\mathbb{F}$ are classified as the ideals $\langle g(x)\rangle$ of the quotient ring $\mathbb{F}[x]/\langle x^n - \alpha\rangle$, where the generator polynomial $g(x)$ is the unique monic polynimial of minimum degree in the code, which is a divisor of $x^n - \alpha$.

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. Cyclic codes over finite fields were first studied in the late 1950s by Prange [25], while negacyclic codes over finite fields were initiated by Berlekamp in the late 1960s [2].

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 [3], and then in the 1970's and 1980's by several authors such as Massey *et al.* [19], Falkner *et al.* [10]. However, repeated-root codes over finite fields were investigated in the most generality in the 1990's by Castagnoli *et al.* [5], and van Lint [30], 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 (see, for example, [21]).

The class of finite rings of the form $\frac{\mathbb{F}_{p^m}[u]}{\langle u^2\rangle} = \mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ has been used widely as alphabets of certain constacyclic codes. For example, the structure of $\frac{\mathbb{F}_2[u]}{\langle u^2\rangle}$ is interesting, because this ring lies between $\mathbb{F}_4$ and $\mathbb{Z}_4$ in the sense that it is additively analogous to $\mathbb{F}_4$, and multiplicatively analogous to $\mathbb{Z}_4$. Codes over $\frac{\mathbb{F}_2[u]}{\langle u^2\rangle}$ have been extensively studied by many researchers, whose work includes cyclic and self-dual codes, decoding of cyclic codes, Type II codes, duadic codes, repeated-root constacyclic codes.

The rest of this paper is organized as follows. After presenting some preliminary concepts about constacyclic codes over finite commutative rings in Section 2, we classify and investigate the units of the ring $\mathcal{R}_4 = \frac{\mathbb{F}_{2^m}[u]}{\langle u^4\rangle} = \mathbb{F}_{2^m} + u\mathbb{F}_{2^m} + u^2\mathbb{F}_{2^m} + u^3\mathbb{F}_{2^m}$ in Section 3. $\mathcal{R}_4$ is a chain ring with residue field $\mathbb{F}_{2^m}$ that contains precisely $(2^m-1)2^{3m}$ units, namely, $\alpha_0 + u\alpha_1 + u^2\alpha_2 + u^3\alpha_3$, where $\alpha_0, \alpha_1, \alpha_2, \alpha_3 \in \mathbb{F}_{2^m}$, $\alpha_0 \neq 0$. We partition these units into 4 distinct types, and we show that for any unit α of Type k, a unit α^* of Type k^* can be constructed, where $1 \leq k \leq 3$.

2. CONSTACYCLIC CODES OVER FINITE COMMUTATIVE RINGS

Let R be a finite commutative ring. An ideal I of R is called *principal* if it is generated by one element. The following equivalent conditions are well-known for the class of finite commutative chain rings (cf. [8, Proposition 2.1]).

Proposition 2.1. *For a finite commutative ring R the following conditions are equivalent:*

(*i*) *R is a local ring and the maximal ideal M of R is principal,*

(*ii*) *R is a local principal ideal ring,*

(*iii*) *R is a chain ring.*

Let z be a fixed generator of the maximal ideal M of a finite commutative chain ring R. Then z is nilpotent and we denote its nilpotency index by ϖ. The ideals of R form a chain:

$$R = \langle z^0\rangle \supsetneq \langle z^1\rangle \supsetneq \cdots \supsetneq \langle z^{\varpi-1}\rangle \supsetneq \langle z^{\varpi}\rangle = \langle 0\rangle .$$

The following is a well-known fact about finite commutative chain rings (cf. [20]).

Proposition 2.2. *Let R be a finite commutative chain ring, with maximal ideal $M = \langle z\rangle$, and let ϖ be the nilpotency of z. Then*

(*a*) *For some prime p and positive integers k, l ($k \geq l$), $|R| = p^k, |\overline{R}[= p^l$, and the characteristic of R and $\overline{R}$ are powers of p,*

(*b*) *For $i = 0, 1, \ldots, \varpi$, $|\langle z^i\rangle| = |\overline{R}|^{\varpi-i}$. In particular, $|R| = |\overline{R}|^{\varpi}$, i.e., $k = l\varpi$.*

Given n-tuples $x = (x_0, x_1, \ldots, x_{n-1}), y = (y_0, y_1, \ldots, y_{n-1}) \in R^n$, their inner product or dot product is defined in the usual way:

$$x \cdot y = x_0 y_0 + x_1 y_1 + \cdots + x_{n-1} y_{n-1},$$

evaluated in R. x, y are called *orthogonal* if $x \cdot y = 0$. For a linear code C over R, its *dual code* $C^{\perp}$ is the set of n-tuples over R that are orthogonal to all codewords of C, i.e.,

$$C^{\perp} = \{x \mid x \cdot y = 0, \forall y \in C\}.$$

A code C is called *self-orthogonal* if $C \subseteq C^{\perp}$, and it is called *self-dual* if $C = C^{\perp}$. The following result is well known (cf. [8, 14, 23]).

Proposition 2.3. *Let R be a finite chain ring of size p^{α}. The number of codewords in any linear code C of length n over R is p^k, for some integer k, $0 \leq k \leq \alpha n$. Moreover, the dual code $C^{\perp}$ has $p^{\alpha n-k}$ codewords, so that $|C| \cdot |C^{\perp}| = |R|^n$.*

Given an n-tuple $(x_0, x_1, \ldots, x_{n-1}) \in R^n$, the *cyclic shift* τ and *negashift* ν on R^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 α is a unit of the ring R, then the *α-constacyclic* (α-twisted) *shift* τ_{α} on R^n is the shift

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

and a code C is said to be *α-constacyclic* if $\tau_{\alpha}(C) = C$, i.e., if C is closed under the α-constacyclic shift τ_{α}.

Each codeword $c = (c_0, c_1, \ldots, c_{n-1})$ is customarily identified with its polynomial representation $c(x) = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}$, and the code C is in turn identified with the set of all polynomial representations of its codewords. Then in the ring $\frac{R[x]}{\langle x^n - \alpha \rangle}$, $xc(x)$ corresponds to a α-constacyclic shift of $c(x)$. From that, the following fact is well-known and straightforward (cf. [18]) :

Proposition 2.4. *A linear code C of length n is α-constacyclic over R if and only if C is an ideal of $\frac{R[x]}{\langle x^n - \alpha \rangle}$ (Hence, this quotient ring is referred to as the ambient ring of the code C).*

The dual of a cyclic code is a cyclic code, and the dual of a negacyclic code is a negacyclic code. In general, we have the following implication of the dual of a α-constacyclic code.

Proposition 2.5. *The dual of a α-constacyclic code is a α^{-1}-constacyclic code.*

The following result is also well known (cf. [7]).

Proposition 2.6. *Let R be a finite commutative ring, α be a unit of R and*

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

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

For a nonempty subset S of the ring R, the annihilator of S, denoted by $ann(S)$, is the set

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

Then $ann(S)$ 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^*. For example, if

$$f(x) = a_0 + a_1x + \cdots + a_{k-1}x^{k-1} + a_kx^k,$$

then

$$f^*(x) = x^k(a_0 + a_1x^{-1} + \cdots + a_{k-1}x^{-(k-1)} + a_kx^{-k}) = a_k + a_{k-1}x + \cdots + a_1x^{k-1} + a_0x^k.$$

Note that $(f^*)^* = f$ if and only if the constant term of f is nonzero, if and only if $\deg(f) = \deg(f^*)$.

3. THE RING $\mathcal{R}_4 = \frac{\mathbb{F}_{2^m}[u]}{\langle u^4\rangle}$ AND ITS UNITS

The ring $\mathcal{R}_4 = \frac{\mathbb{F}_{2^m}[u]}{\langle u^4\rangle}$ is a local ring with maximal ideal $u\mathcal{R}_4 = \langle u\rangle_{\mathcal{R}_4}$. Applying Proposition 2.1, $\mathcal{R}_4$ is a chain ring. Then $\mathcal{R}_4$ can be viewed as $\mathcal{R}_4 = \mathbb{F}_{2^m} + u\mathbb{F}_{2^m} + u^2\mathbb{F}_{2^m} + u^3\mathbb{F}_{2^m}$. It is closed under 2^m-ary polynomial addition and multiplication modulo u^4. The set $\mathcal{R}_4 \setminus \langle u\rangle_{\mathcal{R}_4}$ is the set of all units of $\mathcal{R}_4$, it consists of elements of the form

$$\alpha_0 + u\alpha_1 + u^2\mathbb{F}_{2^m} + u^3\alpha_3,$$

where $\alpha_0, \alpha_1, \alpha_2, \alpha_3 \in \mathbb{F}_{2^m}$, $\alpha_0 \neq 0$. More precisely, we have the following result:

Proposition 3.1. *Let $\mathcal{R}_4 = \frac{\mathbb{F}_{2^m}[u]}{\langle u^4\rangle} = \mathbb{F}_{2^m} + u\mathbb{F}_{2^m} + u^2\mathbb{F}_{2^m} + u^3\mathbb{F}_{2^m}$. Then*

(i) $\mathcal{R}_4$ is a chain ring with maximal ideal $\langle u\rangle_{\mathcal{R}_4}$.

(ii) The ideals of $\mathcal{R}_4$ are $\langle u^i\rangle_{\mathcal{R}_4} = u^i\mathcal{R}_4$, each ideal $\langle u^i\rangle_{\mathcal{R}_4}$ contains $2^{m(4-i)}$ elements, $0 \leq i \leq 4$.

(iii) $\mathcal{R}_4$ *has* $(2^m-1)2^{3m}$ *units, they are of the form*

$$\alpha_0 + u\alpha_1 + u^2\alpha_2 + u^3\alpha_3,$$

where $\alpha_0, \alpha_1, \alpha_2, \alpha_3 \in \mathbb{F}_{2^m}$, $\alpha_0 \neq 0$.

For a nonzero code C, let i_C denote the smallest integer such that there is a nonzero component of a codeword of C belonging to $\langle u^{i_C}\rangle_{\mathcal{R}_4} \setminus \langle u^{i_C+1}\rangle_{\mathcal{R}_4}$. Clearly, $0 \le i_C \le 3$, and $C \subseteq \langle u^{i_C}\rangle^n_{\mathcal{R}_4} \subseteq \mathcal{R}_4^n$.

It is known that, over a finite field F, a code C of length n is α- and β-constacyclic, for two different units $\alpha, \beta \in F$, if and only if $C = \{0\}$ or $C = F^n$. Over a finite ring R, there are many codes satisfying this property. For example, let I be an ideal of R. then I^n is a α-constacyclic code of length n over R for any unit α of R. In the following, we give some more results for constacyclic codes over the chain ring $\mathcal{R}_4$.

Proposition 3.2. *Let* α *be a unit of* $\mathcal{R}_4$. *If a code* C *of length* n *is* α*-constacyclic over* $\mathcal{R}_4$ *then* C *is also* Γ*-constacyclic for any unit* Γ *such that* $\Gamma - \alpha \in \langle u^j\rangle_{\mathcal{R}_4}$, *for every* $j \ge 4 - i_C$.

Proof. Since $\Gamma - \alpha \in \langle u^j\rangle_{\mathcal{R}_4} \subseteq \langle u^{4-i_C}\rangle_{\mathcal{R}_4}$, there is an element $\zeta \in \mathcal{R}_4$ such that $\Gamma = \alpha + u^{4-i_C}\zeta$. Consider an arbitrary codeword $\mathbb{C}$ of C, by definition of i_C, it has the form $\mathbb{C} = (u^{i_C}c_0, u^{i_C}c_1, \dots, u^{i_C}c_{n-1})$. Clearly,

$$\Gamma u^{i_C}c_{n-1} = (\alpha + u^{4-i_C})u^{i_C}c_{n-1} = \alpha u^{i_C}c_{n-1}.$$

Thus, C is also a Γ-constacyclic code. □

Proposition 3.3. *Let* C *be a code of length* n *over* $\mathcal{R}_4$, *and* α, α' *be units of* $\mathcal{R}_4$ *such that* $\alpha - \alpha' \in \langle u^j\rangle_{\mathcal{R}_4} \setminus \langle u^{j+1}\rangle_{\mathcal{R}_4}$, $0 \le j \le 4 - i_C$. *If* C *is both* α*- and* α'*-constacyclic over* $\mathcal{R}_4$ *then* $\langle u^{j+i_C}\rangle^n_{\mathcal{R}_4} \subseteq C$. *In particular, if* $\alpha - \alpha'$ *is a unit, then* $C = \langle u^{i_C}\rangle^n_{\mathcal{R}_4}$.

Proof. Since $\alpha - \alpha' \in \langle u^j\rangle_{\mathcal{R}_4} \setminus \langle u^{j+1}\rangle_{\mathcal{R}_4}$, there is a unit $\zeta \in \mathcal{R}_4$ such that $\alpha - \alpha' = u^j\zeta$. Without loss of generality, we can assume that $(c_0, \dots, c_{n-1}) \in C$ where $c_{n-1} = u^{i_C}v$, for a unit $v \in \mathcal{R}_4$. It follows that both $(\alpha c_{n-1}, c_0, \dots, c_{n-1})$ and $(\alpha' c_{n-1}, c_0, \dots, c_{n-1})$ belong to C, and hence, their difference is in C. Clearly,

$$\begin{aligned}(\alpha c_{n-1}, c_0, \dots, c_{n-1}) - (\alpha' c_{n-1}, c_0, \dots, c_{n-1}) &= ((\alpha - \alpha')c_{n-1}, 0, \dots, 0) \\ &= u^{j+i_C}\zeta v(1, 0, \dots, 0),\end{aligned}$$

so $u^{j+i_C}(1, 0, \dots, 0) \in C$. That means $u^{j+i_C}(1, 0, \dots, 0)$ and all its cyclic shifts are in C, and hence, $\langle u^{j+i_C}\rangle^n_{\mathcal{R}_4} \subseteq C$. In the case that $\alpha - \alpha'$ is a unit, then $j = 0$. Therefore, $\langle u^{i_C}\rangle^n_{\mathcal{R}_4} \subseteq C \subseteq \langle u^{i_C}\rangle^n_{\mathcal{R}_4}$, i.e., $C = \langle u^{i_C}\rangle^n_{\mathcal{R}_4}$. □

We now give a partition for the units of $\mathcal{R}_4$ into 4 distinct types. For an integer $k \in \{1, 2, 3\}$, we call a unit $\alpha = \alpha_0 + u\alpha_1 + u^2\alpha_2 + u^3\alpha_3$ of $\mathcal{R}_4$ to be of Type k, if k is the smallest index such that $\alpha_k \neq 0$. If, in addition, $\alpha_0 = 1$, then $1 + u\alpha_1 + u^2\alpha_2 + u^3\alpha_3$ is said to be of Type k^*. If $\alpha_i = 0$ for all $1 \leq i \leq 3$, i.e., the unit is of the form $\alpha = \alpha_0 \in \mathbb{F}_{2^m}$, we say that α is of Type 0 (or Type 0^* if $\alpha_0 = 1$). Clearly, $\mathcal{R}_4$ has $2^m - 1$ units of Type 0, and $(2^m - 1)^2 2^{m(3-k)}$ units of Type k, which give $2^m - 1$ Type 0 constacyclic codes and $(2^m - 1)^2 2^{m(3-k)}$ Type k constacyclic codes.

For $1 \leq k \leq 3$, let α be a unit of Type k of $\mathcal{R}_4$, i.e.,

$$\alpha = \alpha_0 + u^k\alpha_k + u^2\alpha_2 + u^3\alpha_3,$$

where $\alpha_0, \alpha_k, \alpha_2, \alpha_3 \in \mathbb{F}_{2^m}$, $\alpha_0 \neq 0$, $\alpha_k \neq 0$. Let $\alpha = 1 + u^k\alpha_k + \cdots + u^3\alpha_3$, where, for $k \leq i \leq 3$, $\alpha_i - \alpha_i\alpha_0^{-1} \in \mathbb{F}_{2^m}$. Then α is a unit of Type k^*, and $\alpha = \alpha_0\alpha$. Clearly, in the case of α is a unit of Type 0 and α is of Type 0^*, we also have $\alpha = \alpha_0\alpha$. The following theorem shows that $\langle u^2 \rangle_{\mathcal{R}_4}^n$ is the unique self-dual α-constacyclic code of length n over $\mathcal{R}_4$.

Theorem 3.4. *Let $\alpha = \alpha_0 + u\alpha_1 + u^2\alpha_2 + u^3\alpha_3$ be a unit of $\mathcal{R}_4$ such that $\alpha_0^2 \neq 1$. Then $\langle u^2 \rangle_{\mathcal{R}_4}^n$ is the unique self-dual α-constacyclic code of length n over $\mathcal{R}_4$.*

Proof. Since $\alpha_0^2 \neq 1$, $\alpha_0 \neq \alpha_0^{-1}$, $\alpha - \alpha^{-1}$ is a unit of $\mathcal{R}_4$. Let C be a self-dual α-constacyclic code of length n. Then by Proposition 2.5, C is both α- and α^{-1}-constacylic codes. Thus, Proposition 3.3 implies that $C = \langle u^{i_C} \rangle_{\mathcal{R}_4}^n$. In light of Proposition 2.7, $C^\perp = \langle u^{a-i_C} \rangle_{\mathcal{R}_4}^n$, and hence, $a = 2i_C$, as required. □

References

[1] T. Blackford, *Cyclic codes over $\mathbb{Z}_4$ of oddly even length*, International Workshop on Coding and Cryptography (WCC 2001) (Paris), Appl. Discr. Math. **128** (2003), 27-46.

[2] E.R. Berlekamp, Algebraic Coding Theory, revised 1984 edition, Aegean Park Press, 1984.

[3] S.D. Berman, *Semisimple cyclic and Abelian codes. II*, Kibernetika (Kiev) **3**, 1967, 21-30 (Russian); translated as Cybernetics **3** (1967), 17-23.

[4] A.R. Calderbank and N.J. A. Sloane, *Modular and p-adic codes*, Des. Codes Cryptogr **6** (1995), 21-35.

[5] 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.

[6] I. Constaninescu, *Lineare Codes über Restklassenringen ganzer Zahlen und ihre Automorphismen bezüglich einer verallgemeinerten Hamming-Metrik*, Ph.D. dissertation, Technische Universität, München, Germany, 1995.

[7] H.Q. Dinh, *Constacyclic codes of length p^s over $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m}$*, J. Algebra **324** (2010), 940-950.

[8] H.Q. Dinh and S.R. López-Permouth, *Cyclic and negacyclic codes over finite chain rings*, IEEE Trans. Inform. Theory **50** (2004), 1728-1744.

[9] S. Dougherty, P. Gaborit, M. Harada, and P. Sole, *Type II codes over* $\mathbb{F}_2 + u\mathbb{F}_2$, IEEE Trans. Inform. Theory 45 (1999), 32-45.

[10] 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.

[11] M. Greferath and S E Schmidt, *Gray Isometries for Finite Chain Rings and a Nonlinear Ternary* $(36, 3^{12}, 15)$ *Code*, IEEE Trans. Inform. Theory **45** (1999), 2522-2524.

[12] W. Heise, T. Honold, and A.A. Nechaev, *Weighted modules and representations of codes*, Proceedings of the ACCT 6, Pskov, Russia (1998), 123-129.

[13] T. Honold and I. Landjev, *Linear representable codes over chain rings*, Proceedings of the ACCT 6, Pskov, Russia (1998), 135-141.

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

[15] S. Ling and P. Solé, *Duadic codes over* $\mathbb{F}_2+u\mathbb{F}_2$, Appl. Algebra Engrg. Comm. Comput. **12** (2001), 365-379.

[16] F.J. MacWilliams, *Error-correcting codes for multiple-level transmissions*, Bell System Tech. J. **40** (1961), 281-308.

[17] F.J. MacWilliams, *Combinatorial problems of elementary abelian groups*, PhD. Dissertaion, Harvard University, Cambridge, MA, 1962.

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

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

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

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

[22] G. Norton and A. Sălăgean-Mandache, *On the structure of linear cyclic codes over finite chain rings*, Appl. Algebra Engrg. Comm. Comput. **10** (2000), 489-506.

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

[24] E. Prange, *Cyclic Error-Correcting Codes in Two Symbols*, (September 1957), TN-57-103.

[25] E. Prange, *Cyclic Error-Correcting Codes in Two Symbols*, (September 1957), TN-57-103.

[26] E. Prange, *Some cyclic error-correcting codes with simple decoding algorithms*, (April 1958), TN-58-156.

[27] E. Prange, *The use of coset equivalence in the analysis and decoding of group codes*, (1959), TN-59-164.

[28] E. Prange, *An algorithm for factoring $x^n - 1$ over a finite field*, (October 1959), TN-59-175.

[29] A. Sălăgean, *Repeated-root cyclic and negacyclic codes over finite chain rings*, Discrete Appl. Math. **154** (2006), 413-419.

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

TÓM TẮT
PHẦN TỬ KHẢ NGHỊCH CỦA VÀNH $\frac{\mathbb{F}_{2^m}[u]}{\langle u^4\rangle}$ VÀ MỘT ỨNG DỤNG

Nguyễn Thị Thu Hường,
Đỗ Thanh Phúc*, Nguyễn Quỳnh Hoa, Hoàng Thanh Hải, Trần Thị Mai Linh

Đại học Kinh Tế và QTKD

Phần tử khả nghich của vành $\mathcal{R}_4$ được chia thành 4 loại phân biêt. Phần tử khả nghich của vành $\mathcal{R}_4$ được xem xét một cách chi tiết. Như một ứng dụng mã tự đối ngẫu của mã α-constacyclic có độ dài 2^s trên $\mathcal{R}_4$. Chúng tôi có thể chứng minh rằng nó là duy nhất.

Key words and phrases: *mã constacyclic, mã, mã đối ngẫu, vành chuỗi*

Ngày nhận bài: 08/02/2017; Ngày phản biện: 30/3/2017; Ngày duyệt đăng: 31/5/2017

[0]*Tel: 0949374386; Email: thanhphuc@tueba.edu.vn