Vol. 36 (2016)
No. 5

数 学 杂 志
J. of Math. (PRC)

A NOTE ON CYCLIC CODES OVER $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m} + u^2\mathbb{F}_{p^m}$

LIU Xiu-sheng

(*School of Mathematics and Physics, Hubei Polytechnic University, Huangshi 435003, China*)

Abstract: In this paper, we study cyclic codes of length p^s over the ring $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}+u^2\mathbb{F}_{p^m}$. By establishing the homomorphism from ring $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}+u^2\mathbb{F}_{p^m}$ to ring $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}$, we give the new classify method for cyclic codes of length p^s over the ring $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}+u^2\mathbb{F}_{p^m}$. Using the method of the classify, we obtain the number of codewords in each of cyclic codes of length p^s over ring $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}+u^2\mathbb{F}_{p^m}$.

Keywords: local ring; cyclic codes; repeated-root codes; the number of codewords

2010 MR Subject Classification: 94B05; 94B15

Document code: A **Article ID:** 0255-7797(2016)05-0981-06

1 Introduction

Let $\mathbb{F}_{p^m}$ be a finite field with p^m elements, where p is a prime and m is an integer number. Let R be the commutative ring $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}+u^2\mathbb{F}_{p^m}=\{a+bu+cu^2|a,b,c\in\mathbb{F}_{p^m}\}$ with $u^3=0$. The ring R is a chain ring, which has a unique maximal ideal $\langle u\rangle=\{au|a\in\mathbb{F}_{p^m}\}$ (see [3]). A code of length n over R is a nonempty subset of R^n, and a code is linear over R if it is an R-submodule of R^n. Let C be a code of length n over R and $P(C)$ be its polynomial representation, i.e.,

$$P(C)=\{\sum_{i=0}^{n-1}c_ix^i|(c_0,c_1,\cdots,c_{n-1})\in C\}.$$

The notions of cyclic shift and cyclic codes are standard for codes over R. Briefly, for the ring R, a cyclic shift on R^n is a permutation T such that

$$T(c_0,c_1,\cdots,c_{n-1})=(c_{n-1},c_0,\cdots,c_{n-2}).$$

A linear code over ring R of length n is cyclic if it is invariant under cyclic shift. It is known that a linear code over ring R is cyclic if and only if $P(C)$ is an ideal of $\frac{R[x]}{\langle x^n-1\rangle}$ (see [5]).

The following two theorems can be found in [1].

Theorem 1.1

* **Received date:** 2015-11-16 **Accepted date:** 2016-03-04

Foundation item: Supported by Scientific Research Foundation of Hubei Provincial Education Department of China (D20144401; B2015096) and the National Science Foundation of Hubei Polytechnic University of China (12xjz14A).

Biography: Liu Xiusheng (1960–), male, born at Daye, Hubei, professor, major in groups and algebraic coding, multiple linear algebra.

Type 1 $\langle 0\rangle, \langle 1\rangle$.

Type 2 $I=\langle u(x-1)^i\rangle$, where $0\le i\le p^s-1$.

Type 3 $I=\langle (x-1)^i+u\sum\limits_{j=0}^{i-1}c_{1j}(x-1)^j\rangle$, where $1\le i\le p^s-1, c_{1j}\in\mathbb{F}_{p^m}$; or equivalently, $I=\langle (x-1)^i+u(x-1)^t h(x)\rangle$, where $1\le i\le p^s-1, 0\le t<i$, and either $h(x)$ is 0 or $h(x)$ is a unit where it can be represented as $h(x)=\sum\limits_j h_j(x-1)^j$ with $h_j\in\mathbb{F}_{p^m}$, and $h_0\neq 0$.

Type 4 $I=\langle (x-1)^i+u\sum\limits_{j=0}^{w-1}c_{1j}(x-1)^j, u(x-1)^w\rangle$, where $1\le i\le p^s-1, c_{1j}\in\mathbb{F}_{p^m}, w<l$ and $w<T$, where T is the smallest integer such that $u(x-1)^T\in\langle (x-1)^i+u\sum\limits_{j=0}^{i-1}c_{1j}(x-1)^j\rangle$; or equivalently, $\langle (x-1)^i+u(x-1)^t h(x), u(x-1)^w\rangle$, with $h(x)$ as in Type 3, and $\deg(h)\le w-t-1$.

Theorem 1.2 Let C be a cyclic code of length p^s over $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}$, as classified in Theorem 1.1. Then the number of codewords n_C of C is determined as follows.

If $C=\langle 0\rangle$, then $n_C=1$.

If $C=\langle 1\rangle$, then $n_C=p^{2mp^s}$.

If $C=\langle u(x-1)^i\rangle$, where $0\le i\le p^s-1$, then $n_C=p^{m(p^s-i)}$.

If $C=\langle (x-1)^i\rangle$, where $1\le i\le p^s-1$, then $n_C=p^{2m(p^s-i)}$.

If $C=\langle (x-1)^i+u(x-1)^t h(x)\rangle$, where $1\le i\le p^s-1,\ 0\le t<i$, and $h(x)$ is a unit, then

$$n_C=\begin{cases} p^{2m(p^s-i)}, & \text{if } 1\le i\le p^{s-1}+\dfrac{t}{2},\\ p^{m(p^s-t)}, & \text{if } p^{s-1}+\dfrac{t}{2}<i\le p^{s-1}-1.\end{cases}$$

If $C=\langle (x-1)^i+u(x-1)^t h(x), u(x-1)^\kappa\rangle$, where $1\le i\le p^s-1,\ 0\le t<i$, either $h(x)$ is 0 or $h(x)$ is a unit, and

$$\kappa<T=\begin{cases} i, & \text{if } h(x)=0\ ,\\ \min\{i,p^s-i+t\}, & \text{if } h(x)\neq 0,\end{cases}$$

then $n_C=p^{m(2p^s-i-\kappa)}$.

Recently, Liu and Xu [3] studied constacyclic codes of length p^s over R. In particular, they classified all cyclic codes of length p^s over R. But they did not give the number of codewords in each of cyclic codes of length p^s over R. In this note, we study repeated-root cyclic codes over R by using the different method from [2], and obtain the number of codewords in each of cyclic codes of length p^s over R.

2 Cyclic Codes of Length p^s over R

Cyclic codes of length p^s over R are ideals of the residue ring $R_1=\frac{R[x]}{\langle x^{p^s}-1\rangle}$. It is easy to prove the ring R_1 is a local ring with the maximal ideal $\langle u, x-1\rangle$, but it is not a chain ring.

We can list all cyclic codes of length p^s over R_1 as follows.

Theorem 2.1 Cyclic codes of length p^s over R are

Type 1 $\langle 0\rangle, \langle 1\rangle$.

Type 2 $I=\langle u^2(x-1)^k\rangle$, where $0\le k\le p^s-1$.

Type 3 $I=\langle u(x-1)^l+u^2\sum\limits_{j=0}^{l}c_{2j}(x-1)^j\rangle$, where $0\le l\le p^s-1, c_{2j}\in\mathbb{F}_{p^m}$; or equivalently, $I=\langle u(x-1)^l+u^2(x-1)^t h(x)\rangle$, where $0\le l\le p^s-1, 0\le t<l$, and either $h(x)$ is 0 or $h(x)$ is a unit where it can be represented as $h(x)=\sum_j h_j(x-1)^j$ with $h_j\in\mathbb{F}_{p^m}$, and $h_0\ne 0$.

Type 4 $I=\langle u(x-1)^l+u^2\sum\limits_{j=0}^{w}c_{2j}(x-1)^j, u^2(x-1)^w\rangle$, where $1\le l\le p^s-1, c_{2j}\in\mathbb{F}_{p^m}, w<l$ and w is the smallest integer such that $u^2(x-1)^w\in\langle u(x-1)^l+u^2\sum\limits_{j=0}^{l-1}c_{2j}(x-1)^j\rangle$; or equivalently, $I=\langle u(x-1)^l+u^2(x-1)^t h(x), u(x-1)^w\rangle$, with $h(x)$ as in Type 3, and $\deg(h)\le w-t-1$.

Type 5 $I=\langle (x-1)^i+u(x-1)^t h_1(x)+u^2(x-1)^z h_2(x)\rangle$, where $1\le i\le p^s-1, 0\le t<i, 0\le z<i$ and $h_1(x), h_2(x)$ are similar to $h(x)$ in Type 3.

Type 6 $I=\langle (x-1)^i+u(x-1)^t h_1(x)+u^2(x-1)^z h_2(x), u^2(x-1)^\eta\rangle$, where $1\le i\le p^s-1, 0\le t<i, 0\le z<i$, $h_1(x), h_2(x)$ are similar to $h(x)$ in Type 3, $\eta<i$, and η is the smallest integer such that $u^2(x-1)^\eta\in\langle (x-1)^i+u(x-1)^t h_1(x)+u^2(x-1)^z h_2(x)\rangle$.

Type 7 $I=\langle (x-1)^i+u(x-1)^t h_1(x)+u^2(x-1)^z h_2(x), u(x-1)^q+u^2\sum\limits_{j=0}^{q}e_{2j}(x-1)^j\rangle$, where $1\le i\le p^s-1$, $0\le t\le i$, $0\le z\le i$, $q<T\le i$, T is the smallest integer such that $u(x-1)^T\in\langle (x-1)^i+u(x-1)^t h_1(x)\rangle$, and $h_1(x), h_2(x)$ are similar to $h(x)$ in Type 3.

Type 8 $I=\langle (x-1)^i+u(x-1)^t h_1(x)+u^2(x-1)^z h_2(x), u(x-1)^q+u^2\sum\limits_{j=0}^{\sigma}e_{2j}(x-1)^j, u^2(x-1)^\sigma\rangle$, where $1\le i\le p^s-1, \sigma<q\le i$, $0\le t\le i$, $0\le z\le i$, $q<T\le i$, T is the smallest integer such that $u(x-1)^T\in\langle (x-1)^i+u(x-1)^t h_1(x)\rangle$, and σ is the smallest integer such that $u^2(x-1)^\sigma\in\langle u(x-1)^q+u^2\sum\limits_{j=0}^{q-1}e_{2j}(x-1)^j\rangle$, and $h_1(x), h_2(x)$ are similar to $h(x)$ in Type 3.

Proof Ideals of Type 1 are the trivial ideals. Consider an arbitrary nontrivial ideal of R_1.

Start with the homomorphism $\varphi:\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}+u^2\mathbb{F}_{p^m}\to\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}$ with $\varphi(a+ub+u^2c)=a+ub$. This homomorphism then can be extended to a homomorphism of rings of polynomials

$$\varphi:\ R_1=\frac{(\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}+u^2\mathbb{F}_{p^m})[x]}{\langle x^p-1\rangle}\to\overline{R_1}=\frac{(\mathbb{F}_{p^m}+u\mathbb{F}_{p^m})[x]}{\langle x^p-1\rangle}$$

by letting $\varphi(c_0+c_1x+\cdots+c_{p^s-1}x^{p^s-1})=\varphi(c_0)+\varphi(c_1)x+\cdots+\varphi(c_{p^s-1})x^{p^s-1}$. Note that $\mathrm{Ker}\varphi=u^2\frac{\mathbb{F}_{p^m}[x]}{\langle x^{p^s}-1\rangle}$.

Now, let us assume that I is a nontrivial ideal of R_1. Then $\varphi(I)$ is an ideal of $\overline{R_1}$. But ideals of $\overline{R_1}$ are characterized. So we can make use of these results.

On the other hand, $\mathrm{Ker}\varphi$ is also an ideal of $u^2\frac{\mathbb{F}_{p^m}[x]}{\langle x^{p^s}-1\rangle}$. We can consider it to be u^2 times a ideal of $\frac{\mathbb{F}_{p^m}[x]}{\langle x^{p^s}-1\rangle}$. This means that we can again use the results in the aforementioned papers. By using the characterization in [2], we have

$$\mathrm{Ker}\varphi = 0 \ \text{ or } \ \mathrm{Ker}\varphi = \langle u^2(x-1)^k \rangle, \ \ 0 \le k \le p^s.$$

For $\varphi(I)$, by using the characterization in [1], we shall discuss $\varphi(I)$ by carrying out the following cases.

Case 1 $\varphi(I) = 0$. Then $I = \langle u^2(x-1)^k \rangle$, where $0 \le k \le p^s - 1$.

Case 2 $\varphi(I) \neq 0$. We now have seven subcases.

Case 2a $\varphi(I) = \langle u(x-1)^l \rangle$, where $0 \le l \le p^s - 1$.

If $\mathrm{Ker}\varphi = 0$, then $I = \langle u(x-1)^l + u^2 \sum\limits_{j=0}^{l} c_{2j}(x-1)^j \rangle$, where $0 \le l \le p^s - 1$, $c_{2j} \in \mathbb{F}_{p^m}$, or equivalently, $I = \langle u(x-1)^l + u^2(x-1)^t h(x) \rangle$, where $0 \le l \le p^s - 1, 0 \le t < l$, and either $h(x)$ is 0 or $h(x)$ is a unit where it can be represented as $h(x) = \sum_j h_j(x-1)^j$ with $h_j \in \mathbb{F}_{p^m}$, and $h_0 \neq 0$.

If $\mathrm{Ker}\varphi \neq 0$, then $\mathrm{Ker}\varphi = \langle u^2(x-1)^w \rangle$, where $0 \le w \le p^s - 1$. Hence

$$I = \langle u(x-1)^l + u^2 \sum_{j=0}^{w} c_{2j}(x-1)^j, u^2(x-1)^w \rangle,$$

where $1 \le l \le p^s - 1$, $c_{2j} \in \mathbb{F}_{p^m}$, $w < l$ and w is the smallest integer such that $u^2(x-1)^w \in \langle u(x-1)^l + u^2 \sum\limits_{j=0}^{l-1} c_{2j}(x-1)^j \rangle$, or equivalently, $\langle u(x-1)^l + u^2(x-1)^t h(x), u(x-1)^w \rangle$, with $h(x)$ as in Type 3, and $\deg(h) \le w - t - 1$.

Case 2b $\varphi(I) = \langle (x-1)^i + u \sum\limits_{j=0}^{i-1} c_{2j}(x-1)^j \rangle = \langle (x-1)^i + u(x-1)^t h_1(x) \rangle$, where $1 \le i \le p^s - 1$, $c_{2j} \in \mathbb{F}_{p^m}$, and $h_1(x)$ as in Type 3.

If $\mathrm{Ker}\varphi = 0$, then $I = \langle (x-1)^i + u \sum\limits_{j=0}^{i-1} c_{1j}(x-1)^j + u^2 \sum\limits_{j=0}^{i-1} c_{2j}(x-1)^j \rangle = \langle (x-1)^i + u(x-1)^t h_1(x) + u^2(x-1)^z h_2(x) \rangle$, where $1 \le i \le p^s - 1$, $c_{1j}, c_{2j} \in \mathbb{F}_{p^m}$, $0 \le t < i, 0 \le z < i$, and $h_1(x), h_2(x)$ are similar to $h(x)$ in Type 3.

If $\mathrm{Ker}\varphi \neq 0$, then

$$I = \langle (x-1)^i + u \sum_{j=0}^{i-1} c_{1j}(x-1)^j + u^2 \sum_{j=0}^{\eta} c_{2j}(x-1)^j, u^2(x-1)^\eta \rangle$$

or

$$I = \langle (x-1)^i + u(x-1)^t h_1(x) + u^2(x-1)^z h_2(x), u^2(x-1)^\eta \rangle,$$

where $1 \le i \le p^s - 1$,$c_{1j}, c_{2j} \in \mathbb{F}_{p^m}$, $\eta < i$, η is the smallest integer such that $u^2(x-1)^\eta \in \langle (x-1)^i + u(x-1)^t h_1(x) + u^2(x-1)^z h_2(x) \rangle$, and $h_1(x), h_2(x)$ are similar to $h(x)$ in Type 3.

Case 2c $\varphi(I) = \langle (x-1)^i + u(x-1)^t h_1(x), u(x-1)^q \rangle$, where $1 \le i \le p^s - 1$, $0 \le t \le i$, $q < T$, and T is the smallest integer such that $u(x-1)^T \in \langle (x-1)^i + u(x-1)^t h_1(x) \rangle$, $h_1(x)$ is similar to $h(x)$ in Type 3.

If $\mathrm{Ker}\varphi=0$, then $I=\langle (x-1)^i+u(x-1)^th_1(x)+u^2(x-1)^zh_2(x), u(x-1)^q+u^2\sum\limits_{j=0}^{q-1}e_{2j}(x-1)^j\rangle$, where $1\le i\le p^s-1$, $0\le t\le i$, $0\le z\le i$, $q<T\le i$, T is the smallest integer such that $u(x-1)^T\in\langle (x-1)^i+u(x-1)^th_1(x)\rangle$, and $h_1(x),h_2(x)$ are similar to $h(x)$ in Type 3 .

If $\mathrm{Ker}\varphi\neq 0$, then $I=\langle (x-1)^i+u(x-1)^th_1(x)+u^2(x-1)^zh_2(x), u(x-1)^q+u^2\sum\limits_{j=0}^{\sigma}e_{2j}(x-1)^j, u^2(x-1)^\sigma\rangle$, where $1\le i\le p^s-1$, $0\le t\le i$, $0\le z\le i$, $\sigma<q\le i$, $q<T\le i$, T is the smallest integer such that $u(x-1)^T\in\langle (x-1)^i+u(x-1)^th_1(x)\rangle$, and σ is the smallest integer such that $u^2(x-1)^\sigma\in\langle u(x-1)^q+u^2\sum\limits_{j=0}^{q}e_{2j}(x-1)^j\rangle$, and $h_1(x),h_2(x)$ are similar to $h(x)$ in Type 3.

By Theorem 6.2 in [2], each cyclic code of length p^s over $\mathbb{F}_{p^m}$ is an ideal of the form $\langle (x-1)^i\rangle$ of the chain ring $\frac{\mathbb{F}_{p^m}[x]}{\langle x^{p^s}-1\rangle}$, where $0\le i\le p^s$, and this code $\langle (x-1)^i\rangle$ contains $p^{m(p^s-i)}$ codewords. In light of Theorem 1.2, we can now determine the sizes of all cyclic codes of length p^s over R by multiplying the sizes of $\varphi(C)$ and $\mathrm{Ker}\varphi$ in each case.

Theorem 2.2 Let C be a cyclic code of length p^s over R, as classified in Theorem 2.1. Then the number of codewords n_C of C is determined as follows.

If $C=\langle 0\rangle$, then $n_C=1$.

If $C=\langle 1\rangle$, then $n_C=p^{3mp^s}$.

If $C=\langle u^2(x-1)^k\rangle$, where $0\le k\le p^s-1$, then $n_C=p^{m(p^s-k)}$.

If $C=\langle u(x-1)^l+u^2\sum\limits_{j=0}^{l}c_{2j}(x-1)^j\rangle$, where $0\le l\le p^s-1, c_{2j}\in\mathbb{F}_{p^m}$, then $n_C=p^{m(p^s-l)}$.

If $C=\langle u(x-1)^l+u^2\sum\limits_{j=0}^{w}c_{2j}(x-1)^j, u^2(x-1)^w\rangle$, where $0\le l\le p^s-1, c_{2j}\in\mathbb{F}_{p^m}, w<l$ and w the smallest integer such that $u^2(x-1)^w\in\langle u(x-1)^l+u^2\sum\limits_{j=0}^{l-1}c_{2j}(x-1)^j\rangle$, then $n_C=p^{2mp^s-m(l+w)}$.

If $C=\langle (x-1)^i\rangle$, where $1\le i\le p^s-1$, then $n_C=p^{2m(p^s-i)}$.

If $C=\langle (x-1)^i+u(x-1)^th_1(x)+u^2(x-1)^zh_2(x)\rangle$, where $1\le i\le p^s-1, 0\le t<i, 0\le z<i$ and $h_1(x)$ is a unit, then

$$n_C=\begin{cases} p^{2m(p^s-i)}, & \text{if } 1\le i\le p^{s-1}+\dfrac{t}{2},\\ p^{m(p^s-t)}, & \text{if } p^{s-1}+\dfrac{t}{2}<i\le p^{s-1}-1.\end{cases}$$

If $C=\langle (x-1)^i+u(x-1)^th_1(x)+u^2(x-1)^zh_2(x), u^2(x-1)^\eta\rangle$, where $1\le i\le p^s-1, 0\le t<i, 0\le z<i$, $h_1(x)$ is a unit, $\eta<i$, η is the smallest integer such that $u^2(x-1)^\eta\in\langle (x-1)^i+u(x-1)^th_1(x)+u^2(x-1)^zh_2(x)\rangle$, and $h_1(x)$ is a unit, then

$$n_C=\begin{cases} p^{3mp^s-2mi-m\eta}, & \text{if } 1\le i\le p^{s-1}+\dfrac{t}{2},\\ p^{2mp^s-m(t+\eta)}, & \text{if } p^{s-1}+\dfrac{t}{2}<i\le p^{s-1}-1.\end{cases}$$

If $C=\langle (x-1)^i+u(x-1)^th_1(x)+u^2(x-1)^zh_2(x), u(x-1)^q+u^2\sum\limits_{j=0}^{q}e_{2j}(x-1)^j\rangle$, where $1\leq i\leq p^s-1, q<T\leq i$, T is the smallest integer such that $u(x-1)^T\in\langle (x-1)^i+u(x-1)^th_1(x)\rangle$, either $h_1(x), h_2(x)$ are 0 or $h_1(x), h_2(x)$ are units, and

$$q<T=\begin{cases} i, & \text{if } h_1(x)=0,\\ \min\{i, p^s-i+t\}, & \text{if } h_1(x)\neq 0,\end{cases}$$

then $n_C=p^{m(2p^s-i-q)}$.

If $C=\langle (x-1)^i+u(x-1)^th_1(x)+u^2(x-1)^zh_2(x), u(x-1)^q+u^2\sum\limits_{j=0}^{\sigma}e_{2j}(x-1)^j, u^2(x-1)^\sigma\rangle$, where $1\leq i\leq p^s-1, \sigma<q\leq i$, $q<T\leq i$, T is the smallest integer such that $u(x-1)^T\in\langle (x-1)^i+u(x-1)^th_1(x)\rangle$, and σ is the smallest integer such that $u^2(x-1)^\sigma\in\langle u(x-1)^q+u^2\sum\limits_{j=0}^{q}e_{2j}(x-1)^j\rangle$, either $h_1(x), h_2(x)$ are 0 or $h_1(x), h_2(x)$ are units, and

$$q<T=\begin{cases} i, & \text{if } h_1(x)=0,\\ \min\{i, p^s-i+t\}, & \text{if } h_1(x)\neq 0,\end{cases}$$

then $n_C=p^{3mp^s-m(i+q+\sigma)}$.

References

[1] Dinh H Q. Constacyclic codes of length p^s over $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}$[J]. J. Alg., 2010, 324: 940–950.

[2] Dinh H Q. On the linear ordering of some classes of negacyclic and cyclic codes and their distance distributions[J]. Finite Field Appl., 2008, 14: 22–40.

[3] Liu X S, Xu X. Some classes of repeated-root constacyclic codes over $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}+u^2\mathbb{F}_{p^m}$[J]. J. Korean Math. Soc., 2014, 51(4): 853–866.

[5] Hammous A, Kumar P V, Calderbark A R, Sloame J A, Solé P. The $\mathbb{Z}_4$-linearity of Kordock, Preparata, Goethals, and releted codes[J]. IEEE Trans. Inform. The., 1994, 40: 301–319.

[5] Huffman W C, Pless V. Fundamentals of error-correcting codes[M]. Cambridge: Cambridge Univ. Press, 2003.

关于环 $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}+u^2\mathbb{F}_{p^m}$ 上循环码的注记

刘修生

(湖北理工学院数理学院, 湖北 黄石 435003)

摘 要: 本文研究了环 $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}+u^2\mathbb{F}_{p^m}$ 上长度为 p^s 的循环码分类. 通过建立环 $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}+u^2\mathbb{F}_{p^m}$ 到环 $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}$ 的同态, 给出了环 $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}+u^2\mathbb{F}_{p^m}$ 上长度为 p^s 的循环码的新分类方法. 应用这种方法, 得到了环 $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}+u^2\mathbb{F}_{p^m}$ 长度为 p^s 的循环码的码词数.

关 键 词: 局部环; 循环码; 重根循环码; 码词数

MR(2010)**主题分类号:** 94B05; 94B15 **中图分类号:** O157.4