环 $F_{p^m}+uF_{p^m}$ 上长为 p^k 的循环码计数

朱士信　　丁　健
(合肥工业大学数学学院　合肥　230009)

摘　要：环 $R=F_{p^m}+uF_{p^m}$ 上长为 p^k 的循环码可看作 $R[x]/<x^{p^k}-1>$ 上的理想。该文通过对 $R[x]/<x^{p^k}-1>$ 上理想的研究，得到了环 $F_{p^m}+uF_{p^m}$ 上长为 p^k 的循环码的唯一表示方法和计数，并给出了该环上长为 p^k 的循环自对偶码的结构和计数。

关键词：循环码；自对偶码；零化子
中图分类号：TN911.22　　**文献标识码**：A　　**文章编号**：1009-5896(2010)09-2101-05
DOI: 10.3724/SP.J.1146.2009.01325

Mass Formulas for Cyclic Codes of Length p^k over the Ring $F_{p^m}+uF_{p^m}$

Zhu Shi-xin　　Ding Jian
(*School of Mathematics, Hefei Univercity of Technology, Hefei* 230009, *China*)

Abstract: Cyclic codes over the ring $R=F_{p^m}+uF_{p^m}$ can be seen as the ideals of $R[x]/<x^{p^k}-1>$. Based on the studing of ideals of $R[x]/<x^{p^k}-1>$, a unique method of representing cyclic codes of length p^k and their mass formulas over the ring $F_{p^m}+uF_{p^m}$ are provided. For the cyclic self-dual codes of length p^k over the ring $F_{p^m}+uF_{p^m}$, their structures and mass formulas are given.

Key words: Cyclic codes; Self-dual codes; Annihilator

1　引言

循环码的结构研究是纠错码研究的核心问题之一，对环 $F_q+uF_q+\cdots+u^{k-1}F_q$ 上的纠错码的研究是近年来纠错码研究的热点(q 为素数 p 的方幂)。文献[1]利用环 F_q+uF_q 上的线性码进行了格的构造；文献[2]等利用环 F_q+uF_q 上的码通过线性码的Gray映射找到了一大批 F_q 上的最优码；文献[3]给出了环 F_q+uF_q 上关于厄米特内积的线性码的自对偶码计数公式；文献[4]研究了 $F_q+uF_q+\cdots+u^{k-1}F_q$ 上单根循环码及其对偶码的结构。大量文章研究了含幺有限交换环上的单根循环码及其对偶码的结构，而重根循环码的研究相比较还很不完善。文献[5]给出了环 F_2+uF_2 的扩环上长为 2^e 的循环码计数；环 F_q+uF_q 上任意长度的循环码的结构在文献[6]中得到阐述。本文将研究环 $F_{p^m}+uF_{p^m}$ 上长为 p^k 的循环码的结构和计数，并给出了该环上长 p^k 的循环自对偶码的充要条件。

2　基本概念

令 $R=F_{p^m}+uF_{p^m}$，其中 p 为素数，$u^2=0$，σ 是从 R^{p^k} 到 R^{p^k} 满足 $\sigma(r_0,r_1,\cdots,r_{p^k-1})=(r_{p^k-1},r_0,r_1,\cdots,r_{p^k-2})$ 的映射，若 $\sigma(C)=C$ 则称 C 是 R 上长为 p^k 的循环码。本文把 $r_0+r_1x+\cdots+r_{p^k-1}x^{p^k-1}$ 称为码字 $(r_0,r_1,\cdots,r_{p^k-1})$ 的多项式表示，令 $S=R[x]/(x^{p^k}-1)$，则 C 是 R 上长为 p^k 的循环码的充分必要条件为 C 是 S 上的理想。

定义 1[7]　令 C 是 S 上的理想，称 $Ann(C)=\{f(x)\in S\mid f(x)g(x)=0,\forall g(x)\in C\}$ 为 C 的零化子。

定义 2[7]　若 $f(x)=\sum_{j=0}^{p^k-1}f_jx^j$，$g(x)=\sum_{j=0}^{p^k-1}g_jx^j\in S$，定义 $f(x)$ 与 $g(x)$ 的点积为 $f(x)\cdot g(x)=\sum_{j=0}^{p^k-1}f_jg_j$。若 C 是 S 上的任意理想，定义 C 的对偶理想为 $C^{\perp}=\{f(x)\in S\mid f(x)\cdot g(x)=0,\forall g(x)\in C\}$。若 $C=C^{\perp}$，称 C 是自对偶的。

令“-”：$R\mapsto R$，$\sum_{j=0}^{p^k-1}r_jx^j\mapsto\sum_{j=0}^{p^k-1}r_jx^{-j}$ 为从 R 到 R 的共轭映射，易得

$$\overline{Ann(C)}\subseteq C^{\perp}\tag{1}$$

3　S 中的理想计数

文献[6]研究了环 F_q+uF_q 上任意长度的循环码的结构，有如下引理：

引理 1[6]　设 C 是 S 上的任意理想，其中 q 为素数 p 的方幂，则存在唯一的满足 $a(x)\mid g(x)\mid(x^{p^k}-1)$，$\deg a(x)>\deg p(x)$ 的 $F_q[x]$ 中的一组多项式 $a(x)$，

2009-10-12 收到，2010-04-28 改回
国家自然科学基金(60673074)资助课题
通信作者：丁健　dingjian_happy@163.com

$g(x)$， $p(x)$，使得 $C=<g(x)+up(x),ua(x)>$，且 $a(x)|p(x)\dfrac{(x^{p^k}-1)}{g(x)}$。

由上面的引理得到本文的一个重要定理。

定理 1 设 C 是 S 上的任意一个理想，则存在唯一的一对整数 $0\le T_1\le T_0\le p^k$ 及 $h(x)\in F_{p^m}[x]$ 使得 $C=<(x-1)^{T_0}+uh(x),u(x-1)^{T_1}>$ 且 $(x-1)^{T_1}\mid h(x)(x-1)^{p^k-T_0}$，其中

$$h(x)=\begin{cases}0, & T_1=0\\ \sum_{j=0}^{T_1-1}h_j(x-1)^j,\ h_j\in F_{p^m}, & T_1\ge 1\end{cases}$$

证明 设 C 是 S 上的任意一个理想，由引理1可知存在 $\boldsymbol{F}_{p^m}[x]$ 中唯一的多项式 $g(x)$, $a(x)$, $p(x)$ 使得 $C=<g(x)+up(x),ua(x)>$，其中 $a(x)\mid g(x)\mid(x^{p^k}-1)$,显然当 $a(x)=1$ 时 $p(x)=0$，当 $\deg(a(x))\ge 1$ 时 $\deg(p(x))<\deg(a(x))$。在 S 中 $0=x^{p^k}-1$，我们约定当 $a(x)=0$ 时 $\deg(a(x))=p^k$。又由于在 $\boldsymbol{F}_{p^m}[x]$ 中 $x^{p^k}-1=(x-1)^{p^k}$，所以存在唯一的整数 T_0，T_1 且 $0\le T_1\le T_0\le p^k$ 使得 $g(x)=(x-1)^{T_0}$，$a(x)=(x-1)^{T_1}$。当 $a(x)=1$ 即 $T_1=0$ 时 $h(x)=p(x)=0$；当 $\deg(a(x))\ge 1$ 即 $T_1\ge 1$ 时，把 $p(x)$ 中的 x 用 $(x-1)+1$ 替换化简可得唯一的 $h(x)=\sum_{j=0}^{T_1-1}h_j(x-1)^j$, $h_j\in F_{p^m}$。由引理1中 $a(x)\mid p(x)\dfrac{(x^{p^k}-1)}{g(x)}$ 可以得到 $(x-1)^{T_1}\mid h(x)(x-1)^{p^k-T_0}$。 证毕

注： 在定理1中，当 $T_0=p^k$，$T_1\ne 0$ 时，由 $(x-1)^{T_1}\mid h(x)(x-1)^{p^k-T_0}$ 且 $\deg(h(x))<T_1$ 可知 $h(x)=0$，所以当 $T_0=p^k$ 时 $h(x)=0$。

在定理1中我们给出了 S 中的理想 C 的唯一表示，为了与其它表示相区分，记为

$$C=<<(x-1)^{T_0}+uh(x),u(x-1)^{T_1}>>$$

定理 2 令 $C=<<(x-1)^{T_0}+uh(x),u(x-1)^{T_1}>>$，则

(1) $|C|=(p^m)^{2p^k-T_0-T_1}$；

(2) $Ann(C)=<<(x-1)^{p^k-T_1}-u(x-1)^{p^k-T_0-T_1}h(x),u(x-1)^{p^k-T_0}>>$。

证明 (1) $\forall c\in C$ 都存在 $Y(x)$，$Z(x)\in R[x]$ 使得 $c=Y(x)[(x-1)^{T_0}+uh(x)]+Z(x)u(x-1)^{T_1}$ 理想 $<u(x-1)^{T_1}>$ 有 $(p^m)^{p^k-T_1}$ 个互异元素且 $0\in<u(x-1)^{T_1}>$。

可令 $Y(x)=f(x)+ut(x)\in R[x]$，其中

$$\sum_{j=0}^{p^k-1}f_j(x-1)^j,\ t(x)=\sum_{j=0}^{p^k-1}t_j(x-1)^j$$

$t_j,f_j\in F_{p^m}$, $j=0,1,\cdots,p^k-1$，因为 $T_0\ge T_1$，所以

$$ut(x)[(x-1)^{T_0}+uh(x)]=t(x)(x-1)^{T_0-T_1}\cdot[u(x-1)^{T_1}]\in<u(x-1)^{T_1}>$$

若 $T_1\ge 1$，$T_0=p^k$，由定理1的注知 $f(x)[(x-1)^{T_0}+uh(x)]=0$。

若 $T_1\ge 1$，$T_0<p^k$，则

$$\begin{aligned}&f(x)[(x-1)^{T_0}+uh(x)]\\ &=\sum_{j=0}^{p^k-T_0-1}f_j(x-1)^{j+T_0}+u\sum_{j=0}^{p^k-T_0-1}f_j(x-1)^jh(x)\\ &\quad+u\sum_{j=p^k-T_0}^{p^k-1}f_j(x-1)^jh(x)\\ &=\sum_{j=0}^{p^k-T_0-1}f_j(x-1)^{j+T_0}+u\sum_{j=0}^{p^k-T_0-1}f_j(x-1)^jh(x)\\ &\quad+u(x-1)^{p^k-T_0}h(x)\sum_{j=0}^{T_0-1}f_{j+p^k-T_0}(x-1)^j\end{aligned}$$

又因为 $(x-1)^{T_1}\mid h(x)(x-1)^{p^k-T_0}$ 即有

$$u(x-1)^{p^k-T_0}h(x)\sum_{j=0}^{T_0-1}f_{j+p^k-T_0}(x-1)^j\in<u(x-1)^{T_1}>$$

所以 $<(x-1)^{T_0}+uh(x)>$ 中有 $(p^m)^{p^k-T_0}-1$ 个元素与 $<u(x-1)^{T_1}>$ 元素互异且 $0\in<(x-1)^{T_0}+uh(x)>$，所以

$$|C|=(p^m)^{p^k-T_1}\cdot(p^m)^{p^k-T_0}=(p^m)^{2p^k-T_0-T_1}\tag{2}$$

若 $T_1=0$，则 $h(x)=0$，与 $T_1\ge 1$ 时讨论类似，易得

$$|C|=(p^m)^{2p^k-T_0-T_1}\tag{3}$$

由式(2)，式(3)可知 $|C|=(p^m)^{2p^k-T_0-T_1}$。

(2) 由 $Ann(C)$ 及理想的定义易得 $Ann(C)$ 是 S 中的理想，又因为

$(x-1)^{T_1}\mid h(x)(x-1)^{p^k-T_0}$ 即

$(x-1)^{p^k-T_0-T_1}h(x)\in F_{p^m}[x]$

$[(x-1)^{p^k-T_1}-u(x-1)^{p^k-T_0-T_1}h(x)][(x-1)^{T_0}+uh(x)]=0$

$[(x-1)^{p^k-T_1}-u(x-1)^{p^k-T_0-T_1}h(x)][u(x-1)^{T_1}]=0$

$[u(x-1)^{p^k-T_0}][(x-1)^{T_0}+uh(x)]=0$

$[u(x-1)^{p^k-T_0}][u(x-1)^{T_1}]=0$

所以 $D=<(x-1)^{p^k-T_1}-u(x-1)^{p^k-T_0-T_1}h(x)\ u(x-1)^{p^k-T_0}>\subseteq Ann(C)$

而 $p^k-T_1\ge p^k-T_0$，$(x-1)^{p^k-T_0}\mid(x-1)^{p^k-T_0-T_1}h(x)\cdot(x-1)^{p^k-(p^k-T_1)}$，当 $p^k-T_0=0$, 即 $T_0=p^k$ 时，由定理1的注可知 $(x-1)^{p^k-T_0-T_1}h(x)=0$，当 $p^k-T_0\ge 1$ 时，若 $T_1=0$，$\deg[(x-1)^{p^k-T_0-T_1}h(x)]=0<p^k-T_0$；若 $T_1\ge 1$，$\deg[(x-1)^{p^k-T_0-T_1}h(x)]<p^k-T_0$。满足定理1的条件，所以

$$D=<<(x-1)^{p^k-T_1}-u(x-1)^{p^k-T_0-T_1}h(x),\ u(x-1)^{p^k-T_0}>>\subseteq Ann(C)\tag{4}$$

由式(1)，定理 2 的(1)及文献[8]的定理5.3的证明可知

$$(p^m)^{T_0+T_1} =\mid D \mid\leq\mid Ann(C) \mid=\mid \overline{Ann(C)} \mid\leq\mid C^{\perp} \mid$$

$$=\frac{(p^m)^{2p^k}}{\mid C \mid}=(p^m)^{T_0+T_1} \tag{5}$$

即$\mid D \mid=\mid Ann(C) \mid$，由式(4)可知

$Ann(C)=<<(x-1)^{p^k-T_1}-u(x-1)^{p^k-T_0-T_1}h(x),u(x-1)^{p^k-T_0}>>$ 。　　证毕

注： 由式(5)知$\mid \overline{Ann(C)} \mid=\mid C^{\perp} \mid$，又由式(1)可得$\overline{Ann(C)}=C^{\perp}$。

记τ为S里的所有理想，则我们有下面的定理。

定理 3 令C是S上的理想，$\boldsymbol{A}=\{C\in\tau\mid T_0+T_1\leq p^k\}$，$\boldsymbol{A}'=\{C\in\tau\mid T_0+T_1\geq p^k\}$，定义映射$\Phi:\boldsymbol{A}\mapsto\boldsymbol{A}'$，$C\mapsto Ann(C)$，那么$\Phi$是一一映射。

证明 $\forall C\in\tau$，由定理1知存在唯一的T_0，T_1及$h(x)$使得

$$C=<<(x-1)^{T_0}+uh(x),\ u(x-1)^{T_1}>>$$

由定理 2 的(2)理想C存在唯一的零化子

$$Ann(C)=<<(x-1)^{p^k-T_1}-u(x-1)^{p^k-T_0-T_1}h(x),$$

$$u(x-1)^{p^k-T_0}>>$$

若$C_1,C_2\in\tau$且$C_1\neq C_2$，显然$Ann(C_1)\neq Ann(C_2)$。而当$T_0+T_1\leq p^k$时，$p^k-T_1+p^k-T_0\geq p^k$即Φ是单射；当$T_0+T_1\geq p^k$时，$p^k-T_1+p^k-T_0\leq p^k$即Φ是满射，所以Φ是一一映射。　　证毕

由定理3可知只需求出$\boldsymbol{A}$中的理想数目就可以求出S上的所有理想数目。

定理 4 $C=<<(x-1)^{T_0}+uh(x),u(x-1)^{T_1}>>$是$\boldsymbol{A}$中的理想充分必要条件为

$$0\leq T_1\leq T_0\leq p^k,\ T_0+T_1\leq p^k且$$

$$h(x)=\begin{cases}0, & T_1=0\\ \sum_{j=0}^{T_1-1}h_j(x-1)^j,\ h_j\in F_{p^m}, & T_1\geq 1\end{cases}$$

证明 由定理1，定义1及$\boldsymbol{A}$的定义可知必要性是显然成立的。要证明充分性，只需证明$(x-1)^{T_1}\mid h(x)(x-1)^{p^k-T_0}$。事实上，当$T_1=0$时显然成立；当$T_1\geq 1$时，因为$T_0+T_1\leq p^k$即$(x-1)^{T_1}\mid(x-1)^{p^k-T_0}$，所以对于任意的$h_j\in F_{p^m}$，$j=0,1,\cdots,T_1-1$，都有$(x-1)^{T_1}\mid h(x)(x-1)^{p^k-T_0}$成立。　　证毕

由定理4我们可得下面的推论。

推论 1 若$T_0+T_1=d$，$d\leq p^k$，则S上所有的互异理想数目$N_d=\dfrac{p^{m(n+1)}-1}{p^m-1}$，其中$n=\lfloor d/2\rfloor$，即$d/2$的整数部分。

证明 若$T_1=0$，此时只有唯一的理想$<<(x-1)^d,u>>$；若$T_1\geq 1$，有$(p^m)^{T_1}$个不同的$h(x)=\sum_{j=0}^{T_1-1}h_j(x-1)^j,h_j\in F_{p^m}$，而$0\leq T_1\leq T_0$，$T_0+T_1=d$，所以$T_1\leq\lfloor d/2\rfloor=n$，所以

$$N_d=1+p^m+\cdots+(p^m)^n=\frac{p^{m(n+1)}-1}{p^m-1}$$　　证毕

由定理3及推论1可得S上的所有互异理想数目。

推论 2 S上的所有互异理想的数目

$$\mid\tau\mid=2\left[\sum_{i=0}^{p^k-1}N_d\right]+N_{p^k}$$

4 S 中的对偶理想及自对偶理想

定理 5 令C是S上的理想，则$Ann(Ann(C))=C$。

证明 令C是S上的理想 由零化子的定义可知$C\subseteq Ann(Ann(C))$，而由式(5)可知

$$\mid Ann(Ann(C))\mid=\frac{p^{2p^k}}{\mid Ann(C)\mid}=p^{2p^k}\frac{\mid C\mid}{p^{2p^k}}=\mid C\mid$$

所以$Ann(Ann(C))=C$。　　证毕

由定理2的注知$\overline{Ann(C)}=C^{\perp}$，而由定理5及定理3可知只需求出$\boldsymbol{A}$中的所有理想的对偶就可以得到$S$上的所有理想的对偶。令$p$为素数，$\delta(p)=\begin{cases}0,p=2\\1,p\neq 2\end{cases}$，那么有下面的定理。

定理 6 令C是$\boldsymbol{A}$中的理想且$C=<<(x-1)^{T_0}+uh(x),u(x-1)^{T_1}>>$，则

$$C^{\perp}=<<(x-1)^{p^k-T_1}-ul(x),u(x-1)^{p^k-T_0}>>$$

其中

$$h(x)=\begin{cases}0, & T_1=0\\ \sum_{j=0}^{T_1-1}h_j(x-1)^j,\ h_j\in F_{p^m}, & T_1\geq 1\end{cases}$$

$$l(x)=\begin{cases}0, & T_1=0\\ (x-1)^{p^k-T_0-T_1}\sum_{r=0}^{T_1-1}\left[\sum_{j=0}^{r}(-1)^{(T_0+j)\delta(p)}h_j\binom{T_0-j}{r-j}\right]\\ \quad\cdot(x-1)^r, & T_1\geq 1\end{cases}$$

证明 由定理 2 的(2)知

$$Ann(C)=<<(x-1)^{p^k-T_1}-u(x-1)^{p^k-T_0-T_1}h(x),$$

$$u(x-1)^{p^k-T_0}>>$$

当 $T_1\geq 1$ 时，由定理1可设 $h(x)=\sum_{j=0}^{T_1-1}h_j(x-1)^j$，$h_j\in F_{p^m}$，显然 $C^{\perp}=\overline{Ann(C)}$ 包含元素 $u(x-1)^{p^k-T_0}\cdot(x-1)^{p^k-T_1}-u(x-1)^{p^k-T_0-T_1}\sum_{j=0}^{T_1-1}(-1)^{(T_0+j)\delta(p)}h_j(x-1)^j x^{T_0-j}$，所以

$$B=<(x-1)^{p^k-T_1}-u(x-1)^{p^k-T_0-T_1}\cdot\sum_{j=0}^{T_1-1}(-1)^{(T_0+j)\delta(p)}h_j(x-1)^j x^{T_0-j},u(x-1)^{p^k-T_0}>\subseteq C^{\perp} \tag{6}$$

将 B 中的 x 用 $(x-1)+1$ 替换，同时去除 $u(x-1)^j$，$j\geq p^k-T_0$ 可得

$$B=<(x-1)^{p^k-T_1}-ul(x),u(x-1)^{p^k-T_0}>$$

其中

$$l(x)=(x-1)^{p^k-T_0-T_1}\cdot\sum_{r=0}^{T_1-1}\left[\sum_{j=0}^{r}(-1)^{(T_0+j)\delta(p)}h_j\binom{T_0-j}{r-j}\right](x-1)^r$$

与定理 2 的(2)中证明类似可证得 B 满足定理1的条件即

$$B=<<(x-1)^{p^k-T_1}-ul(x),u(x-1)^{p^k-T_0}>>$$

由定理 2 的(1)得 $|B|=(p^m)^{T_0+T_1}=|C^{\perp}|$，所以此时，

$$C^{\perp}=<<(x-1)^{p^k-T_1}-ul(x),\ u(x-1)^{p^k-T_0}>>$$

其中

$$l(x)=(x-1)^{p^k-T_0-T_1}\cdot\sum_{r=0}^{T_1-1}\left[\sum_{j=0}^{r}(-1)^{(T_0+j)\delta(p)}h_j\binom{T_0-j}{r-j}\right](x-1)^r$$

当 $T_1=0$ 类似可证得 $C^{\perp}=<<(x-1)^{p^k-T_1},u(x-1)^{p^k-T_0}>>$，此时 $l(x)=0$。 证毕

下面分析一下 S 上的自对偶理想。令 $C=<<(x-1)^{T_0}+uh(x),u(x-1)^{T_1}>>$ 是 S 上的自对偶理想，由定理 2 的(1)及 $|C|=|C^{\perp}|=p^{2p^k}/|C|$ 可得 $T_0+T_1=p^k$，所以由定理 6 可设 $C^{\perp}=<<(x-1)^{T_0}-ul(x),u(x-1)^{T_1}>>$，所以 $C=C^{\perp}\Leftrightarrow T_0+T_1=p^k$，且 $h(x)=-l(x)$。

当 $T_1=0$ 时 $h(x)=0=-l(x)$；

当 $T_1\geq 1$ 时，由 $h(x)=-l(x)$ 可得

$$h_r=-\sum_{j=0}^{r}(-1)^{(T_0+j)\delta(p)}h_j\binom{T_0-j}{r-j},\ r=0,\cdots,T_1-1$$

令 $T_1\times T_1$ 矩阵

$$\boldsymbol{M}(\boldsymbol{T}_0,\boldsymbol{T}_1)=\begin{pmatrix}\mathbf{1}+(-\mathbf{1})^{T_0\delta(p)} & \mathbf{0} & \cdots & \mathbf{0}\\ (-\mathbf{1})^{T_0\delta(p)}\binom{\boldsymbol{T}_0}{\mathbf{1}} & \mathbf{1}+(-\mathbf{1})^{(T_0+1)\delta(p)} & \cdots & \mathbf{0}\\ \vdots & \vdots & \ddots & \mathbf{0}\\ (-\mathbf{1})^{T_0\delta(p)}\binom{\boldsymbol{T}_0}{\boldsymbol{T}_1-\mathbf{1}} & (-\mathbf{1})^{(T_0+1)\delta(p)}\binom{\boldsymbol{T}_0-\mathbf{1}}{\boldsymbol{T}_1-\mathbf{2}} & \cdots & \mathbf{1}+(-\mathbf{1})^{(T_0+T_1-1)\delta(p)}\end{pmatrix}$$

所以当 $\boldsymbol{T}_1\geq 1$ 时，$C=C^{\perp}\Leftrightarrow\boldsymbol{T}_0+\boldsymbol{T}_1=p^k$ 且 $\boldsymbol{M}(\boldsymbol{T}_0,\boldsymbol{T}_1)(h_0,h_1,\cdots,h_{T_1-1})^{\mathrm{T}}=0$。

而方程 $\boldsymbol{M}(\boldsymbol{T}_0,\boldsymbol{T}_1)(h_0,h_1,\cdots,h_{T_1-1})^{\mathrm{T}}=0$ 在 F_{p^m} 上肯定有解，由定理 3 可知其在 F_{p^m} 不同解的个数就是自对偶理想的个数，所以有下面的定理。

定理 7 令 ω 是矩阵 $\boldsymbol{M}(\boldsymbol{T}_0,\boldsymbol{T}_1)$ 在 F_{p^m} 上的零化度，那么 τ 上 $\boldsymbol{T}_1\geq 1$ 的自对偶理想个数 $N_{(P^k,T_1)}=(p^m)^{\omega}$。

推论 3 令 $p=3$，下面列出了 $k=1$ 和 $k=2$ 时 S 上的所有自对偶理想：

(1)($k=1$)

$<<0,u>><<(x-1)^2,u(x-1)>>$

(2)($k=2$)

$<<0,u>>$，$<<(x-1)^8,u(x-1)>>$

$<<(x-1)^7-u[h_0+2h_0(x-1)],u(x-1)^2>>$

$<<(x-1)^6-u[h_1(x-1)+h_1(x-1)^2],u(x-1)^3>>$

$<<(x-1)^5-u[h_0+h_0(x-1)+h_2(x-1)^2+2h_0(x-1)^3],u(x-1)^4>>$

其中 $h_j\in F_{p^m}$。此时 τ 上自对偶码的个数为

$$N=\begin{cases}2, & k=1\\ 2+2(3^m)+(3^m)^2, & k=2\end{cases}$$

5 结束语

本文给出了 $S=R[x]/(x^{p^k}-1)$ 上的理想的唯一表达式，从而得到了 S 上的理想计数，并在此基础上给出了对偶理想的唯一表达式。当 p 及 k 较小时运用本文的方法可以列出其所有的长为 p^k 的自对偶理想，但是当 p 或 k 较大时列出其所有的长为 p^k 的自对偶理想较繁琐，需进一步改进。

参 考 文 献

[1] Bachoc C. Application of coding theory to the construction of modular lattices [J]. *Journal of Combinational Theory Series*

A, 1997, 78(1): 92–119.

[2] Gulliver T A and Harada M. Codes over F_3+uF_3 and improvements to the bounds on ternary linear codes [J]. *Designs, Codes and Cryptography*, 2001, 22(1): 89–96.

[3] Gaborit P. Mass formula for self-dual codes over Z_4 and F_q+uF_q rings [J]. *IEEE Transactions on Information Theory*, 1996, 42(4): 1222–1228.

[4] Qian J F, Zhang L N, and Zhu S X. Cyclic codes over $F_q+uF_q+\cdots+u^{k-1}F_q$ [J]. *IEICE Transactions on Fundamentals*, 2005, 88(3): 795–797.

[5] Dinh H Q. Constacyclic codes of length over 2^s galois extension rings of F_2+uF_2 [J]. *IEEE Transactions on Information Theory*, 2009, 55(4): 1730–1740.

[6] 李平，朱士信. 环 F_q+uF_q 上任意长度的循环码[J]. 中国科技大学学报，2008, 38(12): 1392–1396.

Li Ping and Zhu S X. Cyclic codes of arbitrary lengths over the ring F_q+uF_q [J]. *Journal of University of Science and Technology of China*, 2008, 38(12): 1392–1396.

[7] Kiah H M, Leung K H, and Ling S. Cyclic codes over $GR(p^2,m)$ of length p^k [J]. *Finite Fields and their Applications*, 2008, 14(3): 834–846.

[8] Dougherty S T and Ling S. Cyclic codes over Z_4 of even length[J]. *Designs, codes and cryptography*, 2006, 39(2): 127–153.

朱士信：　男，1962 年生，教授，博士生导师，研究方向为代数编码、信息安全、非线性移位寄存器序列.

丁　健：　男，1982 年生，硕士生，研究方向为代数编码.