有限域上最优码的一种新的构造方法

丁 健,李红菊
(安徽新华学院公课部,安徽合肥 230088)

摘 要: 基于域 F_{p^m} 上一类特殊的矩阵,定义了环 $R_{(p^m,k)}=F_{p^m}[u]/\langle u^k\rangle$ 到 $F_{p^m}^j$ 的一个新的 Gray 映射,其中 $u^k=0$、p 为素数、j 为正整数且 $p^{j-1}+1\leqslant k\leqslant p^j$.得到了环 $R_{(p^m,k)}$ 上码长为任意长度 N 的$(1+u)$常循环码的 Gray 象是 F_{p^m} 上长为 p^jN 的保距线性循环码,并给出了 Gray 象的生成多项式,构造了 F_3,F_5 和 F_7 上的一些最优线性循环码.

关键词: 线性码;循环码;常循环码;Gray 映射;最优码
中图分类号: TN911.22 **文献标识码:** A **文章编号:** 0372-2112 (2015)08-1662-06
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2015.08.029

A New Method on the Construction of Optimal Codes over Finite Field

DING Jian, LI Hong-ju
(*Department of Common Course, Anhui Xinhua University, Hefei, Anhui* 230088, *China*)

Abstract: Let $R_{(p^m,k)}$ denote the polynomial residue ring $F_{p^m}[u]/\langle u^k\rangle$, where $p^{j-1}+1\leqslant k\leqslant p^j$ and $u^k=0$ for some positive prime number p and positive integer j. Based on a kind of matrix over F_{p^m}, a new Gray map from $R_{(p^m,k)}$ to $F_{p^m}^j$ is defined. It is proved that the Gray image of a linear $(1+u)$ constacyclic code of an arbitrary length N over $R_{(p^m,k)}$ is a distance invariant linear cyclic code of length p^jN over F_{p^m}. Moreover, the generator polynomial of the Gray image of such a constacyclic code is determined, and some optimal linear cyclic codes over F_3, F_5 and F_7 are constructed via the Gray map.

Key words: linear code; cyclic code; constacyclic code; Gray map; optimal code

1 引言

二十世纪九十年代,Hammons[1]等人发现了二元 Kerdock 码和 Preparata 码等一些高效的二元非线性码可以看作是环 Z_4 上线性码在 Gray 映射下的二元象,由此从根本上解决了二元非线性 Preparata 码和 Kerdock 码关于重量计数器具有形式对偶性这一困扰人们近 30 年的问题.自此,Gray 映射的构造成为有限环上纠错码理论研究的热点[2~15].Qian[2]等人得到了有限环 F_2+uF_2 上单根$(1+u)$常循环码在 Gray 映射下的象是距离不变的二元线性循环码;Amarra[3]等人确定了环 $F_{p^k}+uF_{p^k}$ 上的单根$(1-u)$常循环码在所定义的 Gray 映射下的象是 F_{p^k} 上的准循环码;Abular[4]等人得到了环 F_2+uF_2 上任意长度的$(1+u)$常循环码在其定义下的 Gray 象是二元线性循环码,且给出了相应 Gray 象的生成多项式;Sobhani[5]等人得到环 $F_q[u]/\langle u^{t+1}\rangle$ 上$(1+u^t)$常循环码在所定义的 Gray 映射下的象是 F_q 上的准循环码;Kai[6]等人得到了环 F_p+uF_p 上任意长度的$(1+\lambda u)$常循环码的 Gray 象是 F_p 上距离不变的线性码;Qian[7]等人得到了环 $F_2+uF_2+u^2F_2$ 上单根$(1+u+u^2)$常循环码的 Gray 象是距离不变的二元线性循环码;王立启[8]给出了环 $F_2[u]/\langle u^4\rangle$ 上的单根$(1+u+u^2+u^3)$常循环码的 Gray 象的结构和生成多项式.近来,Ding[13,14]等人确定了环 $F_{2^m}[u]/\langle u^k\rangle$ 上$(1+u)$和$(1+u+\cdots+u^{k-1})$常循环码的 Gray 象的结构和生成多项式.本文将文献[13]的结论推广至 $F_{p^m}[u]/\langle u^k\rangle$ 上任意长度的$(1+u)$常循环码(其中 $p^{j-1}+1\leqslant k\leqslant p^j$,$j$ 为正整数),确定了该常循环码的 Gray 象的结构及 Gray 象的生成多项式,构造了 F_3、F_5 和 F_7 上的一些最优线性循环码.

2 预备知识

令 $R_{(p^m,k)}=F_{p^m}[u]/\langle u^k\rangle$,其中 $u^k=0$、p 为素数、j 为正整数且 $p^{j-1}+1\leqslant k\leqslant p^j$.在 $F_{p^m}[x]$ 中,令 $x^n-1=f_1(x)f_2(x)\cdots f_s(x)$,其中 $\gcd(n,p)=1$ 且 $f_1(x)$、$f_2(x)$、$\cdots$、$f_s(x)$ 为 $F_{p^m}[x]$ 上两两互素的首一不可约多项式,以下简记

收稿日期:收稿日期:2014-12-17;修回日期:2015-04-27;责任编辑:蓝红杰
基金项目:安徽省教育厅自然科学项目(No.KJ2013B107);安徽新华学院校级科研项目、质量工程项目(No.2014Zr009, No.2013tskcx06, No.2013jgkcx09, No.2014xgg09)

为 f_1、f_2、…、f_j,则该分解是唯一的且在 $R_{(p^m,k)}[x]$ 中该分解仍然成立.令 C 是 $R_{(p^m,k)}$ 上长为 $N=p^e n$ 的码(其中 e 为非负整数),α 是 $R_{(p^m,k)}$ 上的一个单位,$R^N_{(p^m,k)}$ 上的 α 常循环移位 τ_α 定义为 $\tau_\alpha(c_0,c_1,\cdots,c_{N-1})=(\alpha c_{N-1},c_0,c_1,\cdots,c_{N-2})$. 若 $\tau_\alpha(C)=C$,则称 C 是 $R_{(p^m,k)}$ 上的 α 常循环码.令 $\boldsymbol{c}=(c_0,c_1,\cdots,c_{N-1})$ 的多项式表示为 $c(x)=c_0+c_1x+\cdots+c_{N-1}x^{N-1}$,则 $xc(x)$ 即为 $R_{(p^m,k)}[x]/\langle x^N-\alpha\rangle$ 上 $c(x)$ 的 α 常循环移位,此时 $R_{(p^m,k)}$ 上长为 N 的 α 常循环码即为 $R_{(p^m,k)}[x]/\langle x^N-\alpha\rangle$ 的一个理想.以下皆假设 p 为素数、j 为正整数且 $p^{j-1}+1\leqslant k\leqslant p^j$.

3　F_{p^m} 上的一类矩阵 $\boldsymbol{A}_{p^j}$

令 $C_r^s=\dfrac{r!}{s!\ (r-s)!}$,其中 $1\leqslant r\leqslant p-1$ 且 $0\leqslant s\leqslant r$,此时定义如下矩阵.

定义 1　当 $j=1$ 时,

$$\boldsymbol{A}_p=\begin{pmatrix} C_{p-1}^{p-1} & 0 & \cdots & 0 & 0\\ C_{p-1}^{p-2} & C_{p-2}^{p-2} & \cdots & 0 & 0\\ \vdots & \vdots & \cdots & \vdots & \vdots\\ C_{p-1}^{1} & C_{p-2}^{1} & \cdots & C_1^1 & 0\\ C_{p-1}^{0} & C_{p-2}^{0} & \cdots & C_1^0 & 1 \end{pmatrix};$$

当 $j\geqslant 2$ 时,

$$\boldsymbol{A}_{p^j}=\begin{pmatrix} C_{p-1}^{p-1}\boldsymbol{A}_{p^{j-1}} & 0 & \cdots & 0 & 0\\ C_{p-1}^{p-2}\boldsymbol{A}_{p^{j-1}} & C_{p-2}^{p-2}\boldsymbol{A}_{p^{j-1}} & \cdots & 0 & 0\\ \vdots & \vdots & \cdots & \vdots & \vdots\\ C_{p-1}^{1}\boldsymbol{A}_{p^{j-1}} & C_{p-2}^{1}\boldsymbol{A}_{p^{j-1}} & \cdots & C_1^1\boldsymbol{A}_{p^{j-1}} & 0\\ C_{p-1}^{0}\boldsymbol{A}_{p^{j-1}} & C_{p-2}^{0}\boldsymbol{A}_{p^{j-1}} & \cdots & C_1^0\boldsymbol{A}_{p^{j-1}} & \boldsymbol{A}_{p^{j-1}} \end{pmatrix}.$$

从矩阵 $\boldsymbol{A}_{p^j}$ 的定义可知 $\boldsymbol{A}_{p^j}$ 是一个 $p^j\times p^j$ 的方阵.若令 $\boldsymbol{A}_{p^j}[R(i)]$ 和 $\boldsymbol{A}_{p^j}(i)$ 分别表示 $\boldsymbol{A}_{p^j}$ 的第 i 行和第 i 列,则 $\boldsymbol{A}_{p^j}[R(1)]=(1,\underbrace{0,\cdots,0}_{(p^j-1)\text{ zeros}})$,$\boldsymbol{A}_{p^j}(p^j)=(\underbrace{0,\cdots,0}_{(p^j-1)\text{ zeros}},1)^{\mathrm{T}}$.

引理 1　$\boldsymbol{A}_{p^j}$ 是 F_{p^m} 上的可逆矩阵.

证明　从矩阵 $\boldsymbol{A}_{p^j}$ 的定义可知,$\boldsymbol{A}_{p^j}$ 是主对角线上元素全为 1 的下三角矩阵,故 $\boldsymbol{A}_{p^j}$ 在 F_{p^m} 上可逆.

引理 2　令 $\boldsymbol{B}_{p^j}=\begin{pmatrix} 0 & 0 & \cdots & 0\\ \vdots & \vdots & \vdots & \vdots\\ 0 & 0 & \cdots & 0\\ 1 & 0 & \cdots & 0 \end{pmatrix}$ 是 $p^j\times p^j$ 方阵,则在 F_{p^m} 上 $\boldsymbol{B}_{p^j}\boldsymbol{A}_{p^j}=(\boldsymbol{A}_{p^j}(p^j),\underbrace{0,\cdots,0}_{(p^j-1)\text{ zeros}})$.

证明　因为 $\boldsymbol{A}_{p^j}[R(1)]=(1,\underbrace{0,\cdots,0}_{(p^j-1)\text{ zeros}})$ 且 $\boldsymbol{A}_{p^j}(p^j)=(\underbrace{0,\cdots,0}_{(p^j-1)\text{ zeros}},1)^{\mathrm{T}}$,所以 $\boldsymbol{B}_{p^j}\boldsymbol{A}_{p^j}=\boldsymbol{B}_{p^j}=(\boldsymbol{A}_{p^j}(p^j),\underbrace{0,\cdots,0}_{(p^j-1)\text{ zeros}})$.

定理 1　设

$$\boldsymbol{H}_{p^j}=\begin{pmatrix} 1 & 1 & \cdots & 0 & 0\\ 0 & 1 & \cdots & 0 & 0\\ \vdots & \vdots & \vdots & \vdots & \vdots\\ 0 & 0 & \cdots & 1 & 1\\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix}\text{和}$$

$$\boldsymbol{D}_{p^j}=\begin{pmatrix} 0 & 1 & 0 & \cdots & 0\\ 0 & 0 & 1 & \cdots & 0\\ \vdots & \vdots & \vdots & \vdots & \vdots\\ 0 & 0 & 0 & \cdots & 1\\ 1 & 0 & 0 & \cdots & 0 \end{pmatrix}$$

为 $p^j\times p^j$ 的方阵,则在 F_{p^m} 上 $\boldsymbol{H}_{p^j}\boldsymbol{A}_{p^j}=\boldsymbol{A}_{p^j}\boldsymbol{D}_{p^j}$.

证明　利用数学归纳法证明.当 $j=1$ 时 $\boldsymbol{H}_P\boldsymbol{A}_P(1)=(\underbrace{0,\cdots,0}_{(p-1)\text{ zeros}},1)^{\mathrm{T}}=\boldsymbol{A}_P(p)$.

若 $2\leqslant i\leqslant p$,则在 F_{p^m} 上有

$$\begin{aligned}&\boldsymbol{H}_P\boldsymbol{A}_P(i)\\ &=\boldsymbol{H}_P(\underbrace{0,\cdots,0}_{(i-1)\text{ zeros}},C_{p-i}^{p-i},C_{p-i}^{p-i-1},\cdots,C_{p-i}^{1},C_{p-i}^{0})^{\mathrm{T}}\\ &=(\underbrace{0,\cdots,0}_{(i-2)\text{ zeros}},C_{p-i}^{p-i},C_{p-i}^{p-i}+C_{p-i}^{p-i-1},\cdots,C_{p-i}^{1}+C_{p-i}^{0},C_{p-i}^{0})^{\mathrm{T}}\\ &=(\underbrace{0,\cdots,0}_{(i-2)\text{ zeros}},C_{p-i+1}^{p-i+1},C_{p-i+1}^{p-i},\cdots,C_{p-i+1}^{1},C_{p-i+1}^{0})^{\mathrm{T}}\\ &=\boldsymbol{A}_P(i-1).\end{aligned}$$

所以 $\boldsymbol{H}_P\boldsymbol{A}_P=(\boldsymbol{A}_P(p),\boldsymbol{A}_P(1),\boldsymbol{A}_P(2),\cdots,\boldsymbol{A}_P(p-1))=\boldsymbol{A}_P\boldsymbol{D}_p$,即当 $j=1$ 时结论成立.

假设当 $j=j_1\geqslant 1$ 时结论成立,则在 F_{p^m} 上有 $\boldsymbol{H}_{p^{j_1}}\boldsymbol{A}_{p^{j_1}}=\boldsymbol{A}_{p^{j_1}}\boldsymbol{D}_{p^{j_1}}$ 即 $\boldsymbol{H}_{p^{j_1}}\boldsymbol{A}_{p^{j_1}}=(\boldsymbol{A}_{p^{j_1}}(p^{j_1}),\boldsymbol{A}_{p^{j_1}}(1),\boldsymbol{A}_{p^{j_1}}(2),\cdots,\boldsymbol{A}_{p^{j_1}}(p^{j_1}-1))$,所以

$$\boldsymbol{H}_{p^{j_1+1}}\boldsymbol{A}_{p^{j_1+1}}=\begin{pmatrix} \boldsymbol{H}_{p^{j_1}} & \boldsymbol{B}_{p^{j_1}} & \cdots & 0 & 0\\ 0 & \boldsymbol{H}_{p^{j_1}} & \cdots & 0 & 0\\ \vdots & \vdots & \vdots & \vdots & \vdots\\ 0 & 0 & \cdots & \boldsymbol{H}_{p^{j_1}} & \boldsymbol{B}_{p^{j_1}}\\ 0 & 0 & \vdots & 0 & \boldsymbol{H}_{p^{j_1}} \end{pmatrix}\cdot\begin{pmatrix} C_{p-1}^{p-1}\boldsymbol{A}_{p^{j_1}} & 0 & \cdots & 0 & 0\\ C_{p-1}^{p-2}\boldsymbol{A}_{p^{j_1}} & C_{p-2}^{p-2}\boldsymbol{A}_{p^{j_1}} & \cdots & 0 & 0\\ \vdots & \vdots & \cdots & \vdots & \vdots\\ C_{p-1}^{1}\boldsymbol{A}_{p^{j_1}} & C_{p-2}^{1}\boldsymbol{A}_{p^{j_1}} & \cdots & C_1^1\boldsymbol{A}_{p^{j_1}} & 0\\ C_{p-1}^{0}\boldsymbol{A}_{p^{j_1}} & C_{p-2}^{0}\boldsymbol{A}_{p^{j_1}} & \cdots & C_1^0\boldsymbol{A}_{p^{j_1}} & \boldsymbol{A}_{p^{j_1}} \end{pmatrix}.$$

由引理 2 可知

$$\boldsymbol{H}_{p^{j_1+1}}\begin{pmatrix} C_{p-1}^{p-1}\boldsymbol{A}_{p^{j_1}}\\ C_{p-1}^{p-2}\boldsymbol{A}_{p^{j_1}}\\ \vdots\\ C_{p-1}^{1}\boldsymbol{A}_{p^{j_1}}\\ C_{p-1}^{0}\boldsymbol{A}_{p^{j_1}} \end{pmatrix}=\begin{pmatrix} C_{p-1}^{p-1}\boldsymbol{H}_{p^{j_1}}\boldsymbol{A}_{p^{j_1}}+C_{p-1}^{p-2}\boldsymbol{B}_{p^{j_1}}\boldsymbol{A}_{p^{j_1}}\\ C_{p-1}^{p-2}\boldsymbol{H}_{p^{j_1}}\boldsymbol{A}_{p^{j_1}}+C_{p-1}^{p-3}\boldsymbol{B}_{p^{j_1}}\boldsymbol{A}_{p^{j_1}}\\ \vdots\\ C_{p-1}^{1}\boldsymbol{H}_{p^{j_1}}\boldsymbol{A}_{p^{j_1}}+C_{p-1}^{0}\boldsymbol{B}_{p^{j_1}}\boldsymbol{A}_{p^{j_1}}\\ C_{p-1}^{0}\boldsymbol{H}_{p^{j_1}}\boldsymbol{A}_{p^{j_1}} \end{pmatrix}$$

$$=\begin{pmatrix} 0 & C_{p-1}^{p-1}\boldsymbol{A}_{p^{j_1}}(1) & \cdots & C_{p-1}^{p-1}\boldsymbol{A}_{p^{j_1}}(p^{j_1}-1) \\ 0 & C_{p-1}^{p-2}\boldsymbol{A}_{p^{j_1}}(1) & \cdots & C_{p-1}^{p-2}\boldsymbol{A}_{p^{j_1}}(p^{j_1}-1) \\ \vdots & \vdots & \vdots & \vdots \\ 0 & C_{p-1}^{1}\boldsymbol{A}_{p^{j_1}}(1) & \cdots & C_{p-1}^{1}\boldsymbol{A}_{p^{j_1}}(p^{j_1}-1) \\ \boldsymbol{A}_{p^{j_1}}(p^{j_1}) & C_{p-1}^{0}\boldsymbol{A}_{p^{j_1}}(1) & \cdots & C_{p-1}^{0}\boldsymbol{A}_{p^{j_1}}(p^{j_1}-1) \end{pmatrix}$$

$=(\boldsymbol{A}_{p^{j_1+1}}(p^{j_1+1}),\boldsymbol{A}_{p^{j_1+1}}(1),\boldsymbol{A}_{p^{j_1+1}}(2),\cdots,\boldsymbol{A}_{p^{j_1+1}}(p^{j_1}-1))$.

若 $2\leqslant i\leqslant p$,则

$\boldsymbol{H}_{p^{j_1+1}}(0,\cdots,0,\ C_{p-i}^{p-i}\boldsymbol{A}_{p^{j_1}},\ C_{p-i}^{p-i-1}\boldsymbol{A}_{p^{j_1}},\ \cdots,\ C_{p-i}^{1}\boldsymbol{A}_{p^{j_1}},\ C_{p-i}^{0}\boldsymbol{A}_{p^{j_1}})^{\mathrm{T}}$

$=(0,\cdots,0,C_{p-i}^{p-i}\boldsymbol{B}_{p^{j_1}}\boldsymbol{A}_{p^{j_1}},C_{p-i}^{p-i}\boldsymbol{H}_{p^{j_1}}\boldsymbol{A}_{p^{j_1}}+C_{p-i}^{p-i-1}\boldsymbol{B}_{p^{j_1}}\boldsymbol{A}_{p^{j_1}},\cdots,$

$C_{p-i}^{1}\boldsymbol{H}_{p^{j_1}}\boldsymbol{A}_{p^{j_1}}+C_{p-i}^{0}\boldsymbol{B}_{p^{j_1}}\boldsymbol{A}_{p^{j_1}},\ C_{p-i}^{0}\boldsymbol{H}_{p^{j_1}}\boldsymbol{A}_{p^{j_1}})^{\mathrm{T}}=$

$$\begin{pmatrix} 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 \\ C_{p-i+1}^{p-i+1}\boldsymbol{A}_{p^{j_1}}(p^{j_1}) & 0 & \cdots & 0 \\ C_{p-i+1}^{p-i}\boldsymbol{A}_{p^{j_1}}(p^{j_1}) & C_{p-i}^{p-i}\boldsymbol{A}_{p^{j_1}}(1) & \cdots & C_{p-i}^{p-i}\boldsymbol{A}_{p^{j_1}}(p^{j_1}-1) \\ \vdots & \vdots & \vdots & \vdots \\ C_{p-i+1}^{1}\boldsymbol{A}_{p^{j_1}}(p^{j_1}) & C_{p-i}^{1}\boldsymbol{A}_{p^{j_1}}(1) & \cdots & C_{p-i}^{1}\boldsymbol{A}_{p^{j_1}}(p^{j_1}-1) \\ C_{p-i+1}^{0}\boldsymbol{A}_{p^{j_1}}(p^{j_1}) & C_{p-i}^{0}\boldsymbol{A}_{p^{j_1}}(1) & \cdots & C_{p-i}^{0}\boldsymbol{A}_{p^{j_1}}(p^{j_1}-1) \end{pmatrix}$$

$=(\boldsymbol{A}_{p^{j_1+1}}((i-1)p^{j_1}),\boldsymbol{A}_{p^{j_1+1}}((i-1)p^{j_1}+1),\boldsymbol{A}_{p^{j_1+1}}((i-1)$ $p^{j_1}+2),\cdots,\boldsymbol{A}_{p^{j_1+1}}(ip^{j_1}-1))$.

所以 $\boldsymbol{H}_{p^{j_1+1}}\boldsymbol{A}_{p^{j_1+1}}=\boldsymbol{A}_{p^{j_1+1}}\boldsymbol{D}_{p^{j_1+1}}$即当 $j=j_1+1$ 时结论成立,综上所述定理 1 成立.

4 环 $R_{(p^m,k)}$上一个新的 Gray 映射

对于任意 $a,b\in R_{(p^m,k)}$,必存在唯一的 $r_i(a)$, $r_i(b)\in F_{p^m}$使得 $a=\sum_{i=0}^{k-1}u^i r_i(a)$, $b=\sum_{i=0}^{k-1}u^i r_i(b)$. 显然对于任意的 $0\leqslant i\leqslant k-1$ 有 $r_i(a+b)=r_i(a)+r_i(b)$.

定义 2 对于任意的 $a\in R_{(p^m,k)}$,定义 Gray 映射 $\Phi_{(p^m,k)}:R_{(p^m,k)}\to F_{p^m}^{p^j}$为

$$\Phi_{(p^m,k)}(a)=(\underbrace{0,\cdots,0}_{(p^j-k)\text{ zeros}},r_0(a),r_1(a),\cdots,r_{k-1}(a))\boldsymbol{A}_{p^j}.$$

由 $\Phi_{(p^m,k)}$的定义可知该映射是线性的,这是因为

$\Phi_{(p^m,k)}(a+b)$

$=(\underbrace{0,\cdots,0}_{(p^j-k)\text{ zeros}},r_0(a+b),r_1(a+b),\cdots,r_{k-1}(a+b))\boldsymbol{A}_{p^j}$

$=[(\underbrace{0,\cdots,0}_{(p^j-k)\text{ zeros}},r_0(a),r_1(a),\cdots,r_{k-1}(a))+$

$(\underbrace{0,\cdots,0}_{(p^j-k)\text{ zeros}},r_0(b),r_1(b),\cdots,r_{k-1}(b))]\boldsymbol{A}_{p^j}$

$=\Phi_{(p^m,k)}(a)+\Phi_{(p^m,k)}(b)$.

此外,由 $\boldsymbol{A}_{p^j}$是 F_{p^m}上的可逆矩阵知 $\Phi_{(p^m,k)}$是从 $R_{(p^m,k)}$到 $F_{p^m}^{p^j}$上的 Gray 象的双射. 任取 $c=(c_0,c_1,\cdots,c_{N-1})\in R_{(p^m,k)}^N$,则其多项式表示为 $\boldsymbol{c}(x)=(c_0+c_1x+\cdots+c_{N-1}x^{N-1}$. 对于 $0\leqslant i\leqslant k-1$,定义 $P_i[c(x)]=\sum_{l=0}^{N-1}r_i(c_l)x^l$,此时 $c(x)=\sum_{i=0}^{k-1}u^iP_i[c(x)]$. 现将定义 2 拓展到 $R_{(p^m,k)}[x]$上.

定义 3 令 $\boldsymbol{c}=(c_0,c_1,\cdots,c_{N-1})\in R_{(p^m,k)}^N$,其多项式表示为 $c(x)=c_0+c_1x+\cdots+c_{N-1}x^{N-1}\in R_{(p^m,k)}[x]$,定义多项式 Gray 映射 $\Phi_{(p^m,k)}:R_{(p^m,k)}[x]\to F_{p^m}[x]$为

$$\Phi_{(p^m,k)}[c(x)]=(\underbrace{0,\cdots,0}_{(p^j-k)\text{ zeros}},P_0[c(x)],P_1[c(x)],$$

$$\cdots,P_{k-1}[c(x)]\boldsymbol{A}_{p^j}(1,x^N,\cdots,x^{(p^j-1)N})^{\mathrm{T}}$$

显然该映射是线性的且是从 $R_{(p^m,k)}[x]$上码字的多项式表示到 $F_{p^m}[x]$上的 Gray 象的双射.

定义 4 用 W_L 表示 $R_{(p^m,k)}$中元素的 Lee 重量,W_H 表示 $F_{p^m}^{p^j}$上元素的 Hamming 重量. 对于任意的 $a\in R_{(p^m,k)}$,定义 $\mathrm{W}_L(a)=\mathrm{W}_H[\Phi_{(p^m,k)}(a)]$. $R_{(p^m,k)}^N$中码字的 Lee 重量定义为其码元的 Lee 重量之和,两个码字 $\boldsymbol{c}$, $\boldsymbol{c}'$的 Lee 距离为$(\boldsymbol{c}-\boldsymbol{c}')$的 Lee 重量. 相应的,多项式情形下的码字的 Lee 重量即为系数的 Lee 重量之和.

由 Gray 映射及 Lee 距离的定义,可得如下定理.

定理 2 Gray 映射 $\Phi_{(p^m,k)}$是保线性和保距离(从 $R_{(p^m,k)}[x]$上码字的 Lee 距离到 $F_{p^m}[x]$上 Gray 象的 Hamming 距离)的双射.

5 环 $R_{(p^m,k)}$常循环码的 Gray 象

定理 3 若 C 是环 $R_{(p^m,k)}$上码长为 N 的$(1+u)$常循环码,则 $\Phi_{(p^m,k)}(C)$为 F_{p^m}上长为 p^jN 的线性循环码.

证明 只需证明对于码 C 中的任一码字 $c(x)$有 $\Phi_{(p^m,k)}[xc(x)]=x\Phi_{(p^m,k)}[c(x)]$. 事实上,在 $R_{(p^m,k)}[x]/\langle x^N-(1+u)\rangle$中 $x^N=1+u$,所以 $x^{p^jN}=1$. 任取 $c(x)=c_0+c_1x+c_2x^2+\cdots+c_{N-1}x^{N-1}\in C$,则 $xc(x)=(1+u)c_{N-1}+c_0x+c_1x^2+\cdots+c_{N-2}x^{N-1}=\sum_{i=0}^{k-1}u^iP_i[xc(x)]$,其中当 $i=0$ 时 $P_0[xc(x)]=r_0(c_{N-1})+xP_0[c(x)]-x^Nr_0(c_{N-1})$;

当 $1\leqslant i\leqslant k-1$ 时,

$$P_i[xc(x)]=r_i[(1+u)c_{N-1}]+\sum_{l=0}^{N-2}r_i(c_l)x^{l+1}$$

$=[r_{i-1}(c_{N-1})+r_i(c_{N-1})]+xP_i[c(x)]-x^Nr_i(c_{N-1})$.

所以 $\Phi_{(p^m,k)}[xc(x)]=(\underbrace{0,\cdots,0}_{(p^j-k)\text{ zeros}},P_0[xc(x)],$

$P_1[xc(x)],\cdots,P_{k-1}[xc(x)])\boldsymbol{A}_{p^j}(1,x^N,\cdots,x^{(p^j-1)N})^{\mathrm{T}}$

$=(\underbrace{0,\cdots,0}_{(p^j-k)\text{ zeros}},r_0(c_{N-1}),\ \sum_{i=0}^{1}r_i(c_{N-1}),\cdots,\ \sum_{i=k-2}^{k-1}r_i(c_{N-1}))$

$\cdot\boldsymbol{A}_{p^j}(1,x^N,\cdots,x^{(p^j-1)N})^{\mathrm{T}}$

$$-(\underbrace{0,\cdots,0}_{(p^j-k)\text{ zeros}},x^N r_0(c_{N-1}),x^N r_1(c_{N-1}),\cdots,x^N r_{k-1}(c_{N-1}))$$
$$\cdot\boldsymbol{A}_{p^j}(1,x^N,\cdots,x^{(p^j-1)N})^{\mathrm{T}}$$
$$+(\underbrace{0,\cdots,0}_{(p^j-k)\text{ zeros}},xP_0[c(x)],xP_1[c(x)],\cdots,xP_{k-1}[c(x)])$$
$$\cdot\boldsymbol{A}_{p^j}(1,x^N,\cdots,x^{(p^j-1)N})^{\mathrm{T}}$$
$$=(\underbrace{0,\cdots,0}_{(p^j-k)\text{ zeros}},r_0(c_{N-1}),r_1(c_{N-1}),\cdots,r_{k-1}(c_{N-1}))$$
$$\cdot(\boldsymbol{H}_{p^j}\boldsymbol{A}_{p^j}-\boldsymbol{A}_{p^j}\boldsymbol{D}_{p^j})(1,x^N,\cdots,x^{(p^j-1)N})^{\mathrm{T}}$$
$$+x\Phi_{(p^m,k)}[c(x)].$$

由定理 1 可知,$\Phi_{(p^m,k)}[xc(x)]=x\Phi_{(p^m,k)}[c(x)]$.

引理 3　在 $F_{p^m}[x]$中,

$$\boldsymbol{A}_P(1,x^N,\cdots,x^{(p-1)N})^{\mathrm{T}}=(1,x^N-1,\cdots,(x^N-1)^{p-1})^{\mathrm{T}}.$$

证明　在 $F_{p^m}[x]$中,

$$\boldsymbol{A}_P[R(1)](1,x^N,\cdots,x^{(p-1)N})^{\mathrm{T}}=1.$$

若 $1\leqslant i\leqslant p-1$,则

$$(x^N-1)\boldsymbol{A}_P[R(i)](1,x^N,\cdots,x^{(p-1)N})^{\mathrm{T}}$$
$$=(x^N-1)(C_{p-1}^{p-i},C_{p-2}^{p-i},\cdots,C_{p-i}^{p-i},\underbrace{0,\cdots,0}_{(p-i)\text{ zeros}})$$
$$\cdot(1,x^N,\cdots,x^{(p-1)N})^{\mathrm{T}}$$
$$=(C_{p-1}^{p-i},C_{p-2}^{p-i},\cdots,C_{p-i}^{p-i},\underbrace{0,\cdots,0}_{(p-i)\text{ zeros}})(x^N,x^{2N},\cdots,x^{pN})^{\mathrm{T}}$$
$$-(C_{p-1}^{p-i},C_{p-2}^{p-i},\cdots,C_{p-i}^{p-i},\underbrace{0,\cdots,0}_{(p-i)\text{ zeros}})(1,x^N,\cdots,x^{(p-1)N})^{\mathrm{T}}$$
$$=(0,C_{p-1}^{p-i},C_{p-2}^{p-i},\cdots,C_{p-i}^{p-i},\underbrace{0,\cdots,0}_{(p-i-1)\text{ zeros}})$$
$$\cdot(x^{pN},x^N,\cdots,x^{(p-1)N})^{\mathrm{T}}$$
$$-(C_{p-1}^{p-i},C_{p-2}^{p-i},\cdots,C_{p-i}^{p-i},\underbrace{0,\cdots,0}_{(p-i)\text{ zeros}})(1,x^N,\cdots,x^{(p-1)N})^{\mathrm{T}}$$
$$=(-C_{p-1}^{p-i},C_{p-1}^{p-i}-C_{p-2}^{p-i},\cdots,C_{p-i+1}^{p-i}-C_{p-i}^{p-i},C_{p-i}^{p-i},\underbrace{0,\cdots,0}_{(p-i-1)\text{ zeros}})$$
$$\cdot(1,x^N,\cdots,x^{(p-1)N})^{\mathrm{T}}$$
$$=(C_{p-1}^{p-i-1},C_{p-2}^{p-i-1},\cdots,C_{p-i}^{p-i-1},C_{p-i-1}^{p-i-1},\underbrace{0,\cdots,0}_{(p-i-1)\text{ zeros}})\cdot(1,x^N,\cdots,x^{(p-1)N})^{\mathrm{T}}$$
$$=\boldsymbol{A}_P[R(i+1)](1,x^N,\cdots,x^{(p-1)N})^{\mathrm{T}},$$

所以引理 3 成立.

引理 4　在 $F_{p^m}[x]$中,

$$\boldsymbol{A}_{p^j}(1,x^N,\cdots,x^{(p^j-1)N})^{\mathrm{T}}=(1,x^N-1,\cdots,(x^N-1)^{p^j-1})^{\mathrm{T}}.$$

证明　利用数学归纳法证明.由引理 3 可知,当 $j=1$ 时结论成立;

假设当 $j=j_1\geqslant 1$ 时结论成立,则在 $F_{p^m}[x]$中

$$\boldsymbol{A}_{p^{j_1}}(1,x^N,\cdots,x^{(p^{j_1}-1)N})^{\mathrm{T}}=(1,x^N-1,\cdots,(x^N-1)^{p^{j_1}-1})^{\mathrm{T}},$$

此时 $C_{p-1}^{p-1}\boldsymbol{A}_{p^{j_1}}(1,x^N,\cdots,x^{(p^{j_1}-1)N})^{\mathrm{T}}$

$$=(1,x^N-1,\cdots,(x^N-1)^{(p^{j_1}-1)})^{\mathrm{T}}.$$

当 $1\leqslant i\leqslant p-1$ 时有

$$(x^N-1)^{p^{j_1}}(C_{p-1}^{p-i}\boldsymbol{A}_{p^{j_1}},C_{p-2}^{p-i}\boldsymbol{A}_{p^{j_1}},\cdots,C_{p-i}^{p-i}\boldsymbol{A}_{p^{j_1}},$$
$$\underbrace{0,\cdots,0}_{(p^{j_1+1}-ip^{j_1})\text{ zeros}})(1,x^N,\cdots,x^{(p^{j_1+1}-1)N})^{\mathrm{T}}$$
$$=(x^{p^{j_1}N}-1)(C_{p-1}^{p-i}\boldsymbol{A}_{p^{j_1}},C_{p-2}^{p-i}\boldsymbol{A}_{p^{j_1}},\cdots,C_{p-i}^{p-i}\boldsymbol{A}_{p^{j_1}},$$
$$\underbrace{0,\cdots,0}_{(p^{j_1+1}-ip^{j_1})\text{ zeros}})(1,x^N,\cdots,x^{(p^{j_1+1}-1)N})^{\mathrm{T}}$$
$$=(C_{p-1}^{p-i}\boldsymbol{A}_{p^{j_1}},C_{p-2}^{p-i}\boldsymbol{A}_{p^{j_1}},\cdots,C_{p-i}^{p-i}\boldsymbol{A}_{p^{j_1}},\underbrace{0,\cdots,0}_{(p^{j_1+1}-ip^{j_1})\text{ zeros}})$$
$$\cdot(x^{p^{j_1}N},x^{(p^{j_1+1})N},\cdots,x^{(p^{j_1+1}+p^{j_1}-1)N})^{\mathrm{T}}$$
$$-(C_{p-1}^{p-i}\boldsymbol{A}_{p^{j_1}},C_{p-2}^{p-i}\boldsymbol{A}_{p^{j_1}},\cdots,C_{p-i}^{p-i}\boldsymbol{A}_{p^{j_1}},\underbrace{0,\cdots,0}_{(p^{j_1+1}-ip^{j_1})\text{ zeros}})$$
$$\cdot(1,x^N,\cdots,x^{(p^{j_1+1}-1)N})^{\mathrm{T}}$$
$$=(\underbrace{0,\cdots,0}_{p^{j_1}\text{zeros}},C_{p-1}^{p-i}\boldsymbol{A}_{p^{j_1}},C_{p-2}^{p-i}\boldsymbol{A}_{p^{j_1}},\cdots,C_{p-i}^{p-i}\boldsymbol{A}_{p^{j_1}},$$
$$\underbrace{0,\cdots,0}_{[p^{j_1+1}-(i+1)p^{j_1}]\text{ zeros}})(1,x^N,\cdots,x^{(p^{j_1+1}-1)N})^{\mathrm{T}}$$
$$-(C_{p-1}^{p-i}\boldsymbol{A}_{p^{j_1}},C_{p-2}^{p-i}\boldsymbol{A}_{p^{j_1}},\cdots,C_{p-i}^{p-i}\boldsymbol{A}_{p^{j_1}},$$
$$\underbrace{0,\cdots,0}_{(p^{j_1+1}-ip^{j_1})\text{ zeros}})(1,x^N,\cdots,x^{(p^{j_1+1}-1)N})^{\mathrm{T}}$$
$$=(-C_{p-1}^{p-i}\boldsymbol{A}_{p^{j_1}},(C_{p-1}^{p-i}-C_{p-2}^{p-i})\boldsymbol{A}_{p^{j_1}},\cdots,(C_{p-i+1}^{p-i}-C_{p-i}^{p-i})\boldsymbol{A}_{p^{j_1}},$$
$$C_{p-i}^{p-i}\boldsymbol{A}_{p^{j_1}},\underbrace{0,\cdots,0}_{[p^{j_1+1}-(i+1)p^{j_1}]\text{ zeros}})(1,x^N,\cdots,x^{(p^{j_1+1}-1)N})^{\mathrm{T}}$$
$$=(C_{p-1}^{p-i-1}\boldsymbol{A}_{p^{j_1}},C_{p-2}^{p-i-1}\boldsymbol{A}_{p^{j_1}},\cdots,C_{p-i}^{p-i-1}\boldsymbol{A}_{p^{j_1}},C_{p-i-1}^{p-i-1}\boldsymbol{A}_{p^{j_1}},$$
$$\underbrace{0,\cdots,0}_{[p^{j_1+1}-(i+1)p^{j_1}]\text{ zeros}})(1,x^N,\cdots,x^{(p^{j_1+1}-1)N})^{\mathrm{T}}.$$

所以当 $j=j_1+1$ 时结论成立,综上所述引理 4 成立.

在 $F_{p^m}[x]$中,令 $x^n-1=f_1f_2\cdots f_s$,其中 $\gcd(n,p)=1$ 且 $f_1,f_2,\cdots,f_s$ 是 $F_{p^m}[x]$上两两互素的首一不可约多项式,则由文献[15]中的定理 4 和引理 3 易得如下引理.

引理 5　设 C 是环 $R_{(p^m,k)}$上长为 $N=p^en$ 的$(1+u)$常循环码,则 $C=\langle f_1^{k_1}f_2^{k_2}\cdots f_s^{k_s}\rangle$,其中 $0\leqslant k_i\leqslant p^ek$, $i=1,2,\cdots,s$.若令 $\omega=\sum_{i=1}^{s}k_i\deg(f_i)$,则 $|C|=p^{m(kN-\omega)}$.

定理 4　设 $C=\langle f_1^{k_1}f_2^{k_2}\cdots f_s^{k_s}\rangle$是环 $R_{(p^m,k)}$上长为 $N=p^en$ 的$(1+u)$常循环码,其中 $0\leqslant k_i\leqslant p^ek$, $i=1,2,\cdots,s$,则其 Gray 象 $\Phi_{(p^m,k)}(C)$是 F_{p^m}上长为 p^jN 的线性循环码,且有

$$\Phi_{(p^m,k)}(C)=\langle(x^N-1)^{p^j-k}f_1^{k_1}f_2^{k_2}\cdots f_s^{k_s}\rangle.$$

证明　由定理 3 可知 $\Phi_{(p^m,k)}(C)$是 F_{p^m}上长为 p^jN 的线性循环码,所以只需证明 $\Phi_{(p^m,k)}(C)=\langle(x^N-1)^{p^j-k}f_1^{k_1}f_2^{k_2}\cdots f_s^{k_s}\rangle$.事实上,取 $c(x)=f_1^{k_1}f_2^{k_2}\cdots f_s^{k_s}\in C$,则

$$c(x)=\sum_{i=0}^{k-1}u^iP_i[c(x)]=\sum_{i=0}^{k-1}(x^N-1)^iP_i[c(x)].$$

由引理 4 可得

$$\Phi_{(p^m,k)}[c(x)]=(\underbrace{0,\cdots,0}_{(p^j-k)\text{ zeros}},P_0[c(x)],P_1[c(x)],$$

$$\cdots, P_{k-1}[c(x)])\boldsymbol{A}_{p^j}(1, x^N, \cdots, x^{(p^j-1)N})^{\mathrm{T}}$$
$$= (\underbrace{0, \cdots, 0}_{(p^j-k)\text{ zeros}}, P_0[c(x)], P_1[c(x)], \cdots, P_{k-1}[c(x)])$$
$$\cdot (1, x^N-1, \cdots, (x^N-1)^{p^j-1})^{\mathrm{T}}$$
$$= (x^N-1)^{p^j-k}\sum_{i=0}^{k-1}(x^N-1)^i P_i[c(x)]$$
$$= (x^N-1)^{p^j-k} f_1^{k_1} f_2^{k_2}\cdots f_s^{k_s} \in \Phi_{(p^m,k)}(C).$$

所以$\langle (x^N-1)^{p^j-k} f_1^{k_1} f_2^{k_2}\cdots f_s^{k_s}\rangle \subseteq \Phi_{(p^m,k)}(C)$. 由引理 5,比较码字的个数可知 $\Phi_{(p^m,k)}(C) = \langle (x^N-1)^{p^j-k} f_1^{k_1} f_2^{k_2}\cdots f_s^{k_s}\rangle$.

6 例题

例 1 在定义 3 和定理 4 中令 $p=k=3$,得到了文献[6]和[13]无法构造的一些最优码. 令 $f_1 = x+2, f_2 = x^3+2x+2, f_3 = x^3+x^2+2, f_4 = x^4+x^2+x+2, f_5 = x^3+2x^2+2x+2$,则在 $F_3[x]$中有 $x^{13}-1 = \prod_{i=1}^{5} f_i$. 表 1 列出了由 $F_3[u]/\langle u^3\rangle$上长为 $N=13$ 的$(1+u)$常循环码构造的 F_3 上的一些最优线性循环码.

表 1

码长	生成多项式	Gray 象
13	$f_1^2 f_2$	[39,34,3]
13	$f_1^2 f_3$	[39,34,3]
13	$f_1^2 f_4$	[39,34,3]
13	$f_1^2 f_5$	[39,34,3]
13	$f_1^3 f_4 f_5^2$	[39,27,6]
13	$f_1^3 f_4^2 f_5$	[39,27,6]
13	$f_1^3 f_3 f_5^2$	[39,27,6]
13	$f_1^3 f_3^2 f_5$	[39,27,6]
13	$f_1^3 f_3 f_4^2$	[39,27,6]
13	$f_1^3 f_3^2 f_4$	[39,27,6]
13	$f_1^3 f_2 f_5^2$	[39,27,6]
13	$f_1^3 f_2^2 f_5$	[39,27,6]
13	$f_1^3 f_2 f_4^2$	[39,27,6]
13	$f_1^3 f_2^2 f_4$	[39,27,6]
13	$f_1^3 f_2 f_3^2$	[39,27,6]
13	$f_1^3 f_2^2 f_3$	[39,27,6]

例 2 令 $g_1 = x+1, g_2 = x+2, g_3 = x+3, g_4 = x+4$,则在 $F_5[x]$上 $x^4-1 = g_1 g_2 g_3 g_4$. 表 2 列出了由 $F_5[u]/\langle u^5\rangle$上长为 $N=4$ 的$(1+u)$常循环码构造的 F_5 上的一些最优线性循环码.

表 2

码长	生成多项式	Gray 象
4	$g_1 g_2^2$	[20,17,3]
4	$g_1^2 g_2$	[20,17,3]
4	$g_1 g_3^2$	[20,17,3]
4	$g_1^2 g_3$	[20,17,3]
4	$g_2 g_4^2$	[20,17,3]
4	$g_2^2 g_4$	[20,17,3]
4	$g_3 g_4^2$	[20,17,3]
4	$g_3^2 g_4$	[20,17,3]
4	$g_2 g_3 g_4^3$	[20,15,4]
4	$g_2 g_3^3 g_4$	[20,15,4]
4	$g_2^3 g_3 g_4$	[20,15,4]
4	$g_1 g_3 g_4^3$	[20,15,4]
4	$g_1 g_3^3 g_4$	[20,15,4]
4	$g_1^3 g_3 g_4$	[20,15,4]
4	$g_1 g_2 g_4^3$	[20,15,4]
4	$g_1^3 g_2 g_4$	[20,15,4]
4	$g_1 g_2 g_3^3$	[20,15,4]
4	$g_1 g_2^3 g_3$	[20,15,4]
4	$g_1^3 g_2 g_3$	[20,15,4]

例 3 令 $h_1 = x+1, h_2 = x+2, h_3 = x+3, h_4 = x+4, h_5 = x+5, h_6 = x+6$,则在 $F_7[x]$上有 $x^6-1 = \prod_{i=1}^{6} h_i$. 表 3 列出了由 $F_7[u]/\langle u^7\rangle$上长为 $N=6$ 的$(1+u)$常循环码构造的 F_7 上的一些最优线性循环码.

表 3

码长	生成多项式	Gray 象
6	$h_1^2 h_2$	[42,39,3]
6	$h_1 h_5^2$	[42,39,3]
6	$h_1^2 h_5$	[42,39,3]
6	$h_2 h_3^2$	[42,39,3]
6	$h_2 h_6^2$	[42,39,3]
6	$h_2^2 h_6$	[42,39,3]
6	$h_4 h_5^2$	[42,39,3]
6	$h_1^3 h_2 h_3$	[42,37,4]
6	$h_1 h_2^3 h_3$	[42,37,4]
6	$h_2^3 h_3 h_6$	[42,37,4]
6	$h_2 h_4 h_6^3$	[42,37,4]
6	$h_4^3 h_5 h_6$	[42,37,4]
6	$h_4 h_5^3 h_6$	[42,37,4]
6	$h_4 h_5 h_6^3$	[42,37,4]
6	$h_2^2 h_3 h_4 h_5 h_6^5$	[42,32,6]
6	$h_2 h_3 h_4 h_5^2 h_6^5$	[42,32,6]
6	$h_1 h_3 h_4^2 h_5 h_6^5$	[42,32,6]
6	$h_1^2 h_3 h_4 h_5^5 h_6$	[42,32,6]
6	$h_1^2 h_3^5 h_4 h_5 h_6$	[42,32,6]
6	$h_1 h_2^2 h_3 h_5 h_6^5$	[42,32,6]
6	$h_1^2 h_2 h_3 h_5^5 h_6$	[42,32,6]
6	$h_1^5 h_2 h_3^2 h_5 h_6$	[42,32,6]
6	$h_1 h_2 h_3 h_4^2 h_6^5$	[42,32,6]
6	$h_1 h_2^2 h_3 h_4 h_6^5$	[42,32,6]
6	$h_1^2 h_2 h_3^5 h_4 h_5$	[42,32,6]
6	$h_1^5 h_2 h_3^2 h_4 h_5$	[42,32,6]

7 结束语

本文将文献[13]的结论推广至 $R_{(p^m,k)} = F_{p^m}[u]/\langle u^k\rangle$,其中 p 为素数、$u^k = 0$、$p^{j-1}+1 \leqslant k \leqslant p^j$ 且 j 为正整

数,构造了环 $R_{(p^m,k)}$ 到 $F_p^{p^m}$ 的一个新的 Gray 映射,并以此得到了 F_3、F_5 和 F_7 上的一些最优线性循环码.

参考文献

[1] A R Hammons, P V Kumar, A R Calderbank, N J A Sloane, P Solé. The Z_4-linearity of Kerdock, Preparata, Goethals, and related codes[J]. IEEE Transactions on Information Theory, 1994, 40(2): 301 – 319.

[2] J F Qian, L N Zhang, S X Zhu. $(1+u)$ Constacyclic and cyclic codes over $F_2 + uF_2$[J]. Applied Mathematics Letters, 2006, 19(8): 820 – 823.

[3] M C V Amarra, F R Nemenzo. On $(1-u)$ cyclic codes over $F_{p^k} + uF_{p^k}$[J]. Applied Mathematics Letters 21, 2008, 11: 1129 – 1133.

[4] T Abular, I Siap. Constacyclic codes over $F_2 + uF_2$[J]. Journal of the Franklin Institute, 2009, 345: 520 – 529.

[5] R Sobhani, E Esmaeili. Some constacyclic and cyclic codes over $F_q[u]/\langle u^{t+1}\rangle$[J]. IEICE Transactions on Foundamentals of Electronics, Communications and Computer Sciences, 2010, 93(4): 808 – 813.

[6] X S Kai, S X Zhu, P Li. $(1+\lambda u)$ Constacyclic codes over $F_p[u]/\langle u^k\rangle$[J]. Journal of the Franklin Institute, 2010, 347: 751 – 762.

[7] J F Qian. Cyclic codes over finite rings[A]. Wireless Communications, Networking and Mobile Computing (WiCOM), 7th International Conference[C]. Wahan: IEEE Transations on Information Theory, 2011. 1 – 4.

[8] 王立启,朱士信.环 $F_2[u]/\langle u^4\rangle$ 上的一类常循环码及其 Gray 象[J].电子与信息学报,2013,35(2):499 – 503.
L Q Wang, S X Zhu. A class of constacyclic codes over $F_2[u]/\langle u^4\rangle$ and its Gray image[J]. Journal of Electronics and Information Technology, 2013, 35(2): 499 – 503. (in Chinese)

[9] 施敏加,杨善林,朱士信.环 $F_2 + uF_2$ 上长为 2^e 的循环码的距离[J].电子学报,2011,39(1):29 – 34.
Shi Min-jia, Yang Shan-lin, Zhu Shi-xin. On minimum distances of cyclic codes of length 2^e over $F_2 + uF_2$[J]. Acta Electronica Sinica, 2011, 39(1): 29 – 34. (in Chinese)

[10] 施敏加.环 $F_2 + uF_2 + \cdots + u^{m-1}F_2$ 常循环自对偶码[J].电子学报,2013,41(6):1088-1092.
Shi Min-jia. Constacyclic self-dual codes over ring $F_2 + uF_2 + \cdots + u^{m-1}F_2$[J]. Acta Electronica Sinica, 2013, 41(6): 1088 – 1092. (in Chinese)

[11] 施敏加,刘艳.环 $F_p + vF_p + v^2F_p$ 上线性码的各种重量的 MacWilliams 恒等式[J].电子学报,2014,42(7):1387 – 1391.
Shi Min-jia, Liu Yan. Several weight enumerators of linear codes and their Macwilliams identities over ring $F_p + vF_p + v^2F_p$[J]. Acta Electronica Sinica, 2014, 42(7): 1387 – 1391. (in Chinese)

[12] Minjia Shi. Optimal p-ary codes from constacyclic codes over $F_p + vF_p$[J]. Chinese Journal of Electronics, 2014, 23(4): 773 – 777.

[13] J Ding, H J Li. The Gray images of $(1+u)$ constacyclic codes over $F_{2^m}[u]/\langle u^k\rangle$[J]. Journal of Applied Mathematics and Computing, 2014, DOI 10.1007/s12190-014-0847-5.

[14] J Ding, H J Li. The Gray image of a class of constacyclic codes over polynomial residue rings[J]. Journal of the Franklin Institute, 2014, 351: 5467 – 5479.

[15] 李岩,朱士信.环 $F_{p^m} + uF_{p^m} + \cdots + u^{k-1}F_{p^m}$ 上的一类常循环码[J].合肥工业大学学报(自然科学版),2013,35(3):408 – 411.
Y Li, S X Zhu. A class of constacyclic codes over the ring $F_{p^m} + uF_{p^m} + \cdots + u^{k-1}F_{p^m}$[J]. Journal of Hefei University of Technology, 2013, 35(3): 408 – 411. (in Chinese)

作者简介

丁　健　男,1982 年生于安徽合肥.安徽新华学院讲师.研究方向为代数编码与密码.
E-mail: dingjian_happy@163.com

李红菊　女,1982 年生于安徽宿州.安徽新华学院讲师.研究方向为代数编码与密码.