有限非链环上的自对偶常循环码及其应用

高 健,王永康
(山东理工大学数学与统计学院,山东淄博 255000)

摘 要: 纠错码是提高信息传输效率与可靠性的重要手段.构造性能良好的线性码类是纠错码研究中的一个基本问题.本文主要讨论了有限非链环 $F_q[v]/(v^m-v)$ 上自对偶常循环码的代数结构,包括 Euclidean 自对偶常循环码、Hermitian 自对偶常循环码以及 Hermitian 自对偶常循环码的极大距离可分(MDS)码.本文给出了环 $F_q[v]/(v^m-v)$ 上常循环码是 Euclidean 自对偶码的充分条件,以及是 Hermitian 自对偶码的充要条件,并利用 Gray 映射构造了有限域 F_q 上一些参数较好的自对偶码.特别地,本文得到了有限域 F_{192} 上一个新的参数为[16,8,6]的 Hermitian 自对偶码.

关键词: 纠错码;自对偶常循环码;Gray 映射;新的 Hermitian 自对偶码
中图分类号: TN911.22 **文献标识码:** A **文章编号:** 0372-2112 (2020)02-0296-07
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2020.02.011

Self-Dual Constacyclic Codes over Finite Non-Chain Rings and Their Applications

GAO Jian, WANG Yong-kang
(*School of Mathematics and Statistics, Shandong University of Technology, Zibo, Shandong* 255000, *China*)

Abstract: Error-correcting codes are important for the improvement of efficiency and security in information transmission. Constructing codes with good parameters is a fundamental problem in error-correcting codes. In this paper, we mainly study self-dual constacyclic codes over the finite nonchain ring $F_q[v]/(v^m-v)$, including Euclidean self-dual constacyclic codes, Hermitian self-dual constacyclic codes and maximal distance separable (MDS) codes of Hermitian self-dual constacyclic codes. We give a necessary condition for constacyclic codes to be Euclidean self-dual and give a necessary and sufficient condition for constacyclic codes to be Hermitian self-dual over the ring $F_q[v]/(v^m-v)$. Further, some good self-dual codes are constructed by the Gray map. Especially, a Hermitian self-dual code over F_{192} with parameters [16,8,6] is constructed.

Key words: error-correcting codes; self-dual constacyclic codes; gray map; new Hermitian self-dual codes

1 引言

随着现代通讯技术的发展,信息安全技术对整个人类社会起着越来越重要的作用.信息安全中的一个重要部分是信息传输的高效性和可靠性.纠错码理论是提高信息传输效率以及可靠性的重要手段,而构造性能良好的线性码类是纠错码理论研究中的一个基本问题.近几年,随着有限域上的编码理论的发展与完善,编码学者开始考虑环上的编码理论.

有限非链环是一类特殊的有限交换环,因其与有限域有着密切的联系,近几年该环上的编码理论受到了国内外编码学者的广泛关注与研究.在文献[1]中,Zhu 等研究了环 F_2+vF_2 上循环码的代数结构,并通过 F_2+vF_2 到有限域 F_2 上的 Gray 映射构造了一些参数较好的二元线性码;随后,Zhu 等又研究了 F_q+vF_q 上某一类常循环码的代数结构,利用 F_q+vF_q 到 F_q 的 Gray 映射构造了有限域 F_q 上一些参数较好的线性码[2].2013 年,Shi 等研究了环 $F_2+vF_2+v^2F_2$ 上的循环码结构和该环上线性码的重量计数[3].有限非链环 $F_q[v]/(v^m-v)$ 是有限非链环 F_2+vF_2、F_q+vF_q 以及 $F_2+vF_2+v^2F_2$ 的推广,更具有一般性.2016 年,作者等研究了一般有限非链环 $F_p[v]/(v^m-v)$ 上循环码的代数结构,给出了一类具有保持自对偶性的 Gray 映射,并由此构

收稿日期:2018-07-21;修回日期:2019-03-28;责任编辑:覃怀银
基金项目:国家自然科学基金(No.11701336, No.11626144, No.11671235)

造了有限域上一些参数较好的自对偶码[4]. 丁健等介绍了环 $F_2+uF_2+u^2F_2$ 上的常循环码的一些结果[5]. 朱士信等研究了环 Z_{2^s} 上一类常循环码的挠码,并给出了常循环码的一些应用[6].

自对偶码是一类重要的线性码,与很多数学问题紧密相关,如不变量理论、格理论、组合设计等. 基于此,构造参数较好的自对偶码成为纠错码理论研究中的一个热点问题. 目前,已有很多文献和方法致力于研究和构造有限域或有限环上参数较好的自对偶码. Betsumiya 和 Harada 构造了 $F_2\times F_2$ 上基于 Hamming 重量的自对偶码[7];Kima 和 Lee 构造了大域上的一些 Euclidean 与 Hermitian 自对偶 MDS 码[8];在文献[9]中,Qian 和 Ma 研究了有限链环上的自对偶码;施敏加等研究了环 $F_2+uF_2+\cdots+u^{m-1}F_2$ 上的常循环自对偶码[10]. 2015 年,Yang 和 Cai 研究了有限域上的 Hermitian 自对偶常循环码的存在性[11];近期,Liu 等研究了有限非链环 $F_{q^2}+vF_{q^2}$ 上的 Hermitian 自对偶常循环码的代数结构[12].

在本文中,主要研究一般有限非链环 $F_q[v]/(v^m-v)$ 上自对偶常循环码的代数结构,包括 Euclidean 自对偶常循环码、Hermitian 自对偶常循环码以及 Hermitian 自对偶码常循环 MDS 码,给出了环 $F_q[v]/(v^m-v)$ 上的常循环码是 Euclidean 自对偶码的充分条件,是 Hermitian 自对偶码的充要条件,并利用 Gray 映射构造了有限域 F_q 上一些参数较好的自对偶码.

2　环 $F_q[v]/(v^m-v)$ 上的常循环码

设 $R=F_q[v]/(v^m-v)=\{a_0+a_1v+\cdots+a_{m-1}v^{m-1}\mid a_i\in F_q,i=0,1,\cdots,m-1\}$,其中 q 是素数的方幂,$v^m=v$ 且正整数 $m-1$ 整除 $q-1$. 因此,$v^m-v=(v-k_0)(v-k_1)\cdots(v-k_{m-1})$,其中 $k_0,k_1,\cdots,k_{m-1}\in F_q,k_0=0$. 环 R 是一个有限交换非链环,它的每个理想都是主理想生成的. 这些理想中有 m 个是极大理想,分别是$\langle v-k_0\rangle$,$\langle v-k_1\rangle,\cdots,\langle v-k_{m-1}\rangle$.

设 $f_i=v-k_i$ 以及 $\hat{f}_i=(v^m-v)/f_i$,则 f_i 和 $\hat{f}_i$ 在 F_q 上是互素的,即存在 $F_q[v]$ 中的多项式 m_i 和 t_i 使得 $m_if_i+t_i\hat{f}_i=1$. 设 $e_i=t_i\hat{f}_i+\langle v^m-v\rangle$,则 $e_i^2=e_i$,$\sum_{i=0}^{m-1}e_i=1$,以及对于任意的 $i\neq t$ 有 $e_ie_t=0$,即 e_i 是幂等元,$i=0,1,\cdots,m-1$. 故环 R 中任意的元素 r 可以唯一的表示为 $r=e_0r_0+e_1r_1+\cdots+e_{m-1}r_{m-1},r_i\in F_q,i=0,1,\cdots,m-1$. 为书写方便,将 R 中的元素 $a_0+a_1v+\cdots+a_{m-1}v^{m-1}$ 看成 F_q 上一个关于 v 的多项式,用 $a(v)$ 表示.

设 R^n 为环 R 上的秩为 n 的自由模,码 C 是 R^n 的一个非空子集合. 如果 C 是 R^n 的一个 R-子模,则称 C 是 R 上码长为 n 的线性码. 在本文中,均假设码 C 是环 R 上码长为 n 的线性码. 对 $\boldsymbol{c}=(c_0,c_1,\cdots,c_{n-1})\in C$,称 $\boldsymbol{c}$ 为 C 的一个码字. 码字 $\boldsymbol{c}$ 的 Hamming 重量 $wt(\boldsymbol{c})$ 定义为 $\boldsymbol{c}$ 中非零分量的个数. 码 C 的极小 Hamming 距离定义为 $d(C)=\min\{\mathrm{wt}(\boldsymbol{c})\mid 0\neq\boldsymbol{c}\in C\}$. 环 R 上一个参数为$(n,M=|R|^k,d)$的线性码,如果满足 $d=n-k+1$,则称这个码为极大距离可分码(MDS 码),其中 d 是码 C 的极小 Hamming 距离.

对任意的 $a(v)=a_0+a_1v+\cdots+a_{m-1}v^{m-1}=e_0a(k_0)+e_1a(k_1)+\cdots+e_{m-1}a(k_{m-1})\in R$,用 F_q 上长度为 m 的向量 $\boldsymbol{a}$ 来表示,即 $\boldsymbol{a}=(a(k_0),a(k_1),\cdots,a(k_{m-1}))$. 设 $\mathrm{GL}_m(F_q)$ 为有限域 F_q 上所有 m 阶可逆矩阵构成的集合. 定义一个 R 到 F_q^m 映射 φ 如下

$$\varphi:R\to F_q^m,$$
$$\boldsymbol{a}=(a(k_0),a(k_1),\cdots,a(k_{m-1}))\mapsto(a(k_0),a(k_1),\cdots,a(k_{m-1}))\boldsymbol{M}.$$

显然,φ 是一个 F_q-模同构. 为书写方便,将$(a(k_0),a(k_1),\cdots,a(k_{m-1}))\boldsymbol{M}$ 简记为 $\boldsymbol{aM}$. 类似地,将映射 φ 扩展到 R^n 到 F_q^{mn} 如下

$$\Phi:R^n\to F_q^{mn},$$
$$(\boldsymbol{a}_0,\boldsymbol{a}_1,\cdots,\boldsymbol{a}_{n-1})\mapsto(\boldsymbol{a}_0\boldsymbol{M},\boldsymbol{a}_1\boldsymbol{M},\cdots,\boldsymbol{a}_{n-1}\boldsymbol{M}).$$

这个从 R^n 到 F_q^{mn} 的 F_q-模同构映射 Φ 称为 Gray 映射.

对任意的元素 $\boldsymbol{a}=(a(k_0),a(k_1),\cdots,a(k_{m-1}))\in R$,向量 $\boldsymbol{aM}$ 的 Hamming 重量定义为元素 $\boldsymbol{a}$ 的 Gray 重量,即 $\mathrm{wt}_G(\boldsymbol{a})=\mathrm{wt}(\boldsymbol{aM})$. R^n 中任意一个向量的 Gray 重量定义为它的每个分量的 Gray 重量之和. 对任意两个不同的码字 $\boldsymbol{c}_1,\boldsymbol{c}_2\in C$,它们之间的 Gray 距离定义为 $d_G(\boldsymbol{c}_1,\boldsymbol{c}_2)=\mathrm{wt}_G(\boldsymbol{c}_1-\boldsymbol{c}_2)$. 码 C 的极小 Gray 距离定义为 C 中任意两个码字之间 Gray 距离的最小值. 显然,当 C 是线性码时,$d_G(C)=\min\{d_G(\boldsymbol{c})\mid\boldsymbol{c}\in C\}$. Gray 映射 Φ 具有从 C 到$\Phi(C)$的保重和保距性质,即若 C 是 R 上极小 Gray 距离为 d 的线性码,则$\Phi(C)$是有限域 F_q 上极小 Hamming 距离为 d 的线性码.

下面,讨论环 R 上常循环的一些结构性质.

对任意的 $i=0,1,\cdots,m-1$,定义集合

$$C_i=\{\boldsymbol{x}_i\in F_q^n\mid\exists\,\boldsymbol{x}_0,\cdots,\boldsymbol{x}_{i-1},\boldsymbol{x}_{i+1},\cdots,\boldsymbol{x}_{m-1}\in F_q^n,$$
$$e_0\boldsymbol{x}_0+e_1\boldsymbol{x}_1+\cdots+e_{m-1}\boldsymbol{x}_{m-1}\in C\},$$

则 C_i 是有限域 F_q 上码长为 n 的线性码,并且线性码 C 可以唯一的表示为

$$C=e_0C_0\oplus e_1C_1\oplus\cdots\oplus e_{m-1}C_{m-1}.$$

设 $\boldsymbol{G}$ 为 C 的一个生成矩阵,则 C 作为 R^n 的 F_q-线性子空间,矩阵 $\boldsymbol{G}$ 可以表示为

$$\boldsymbol{G}=\begin{pmatrix}e_0\boldsymbol{G}_0\\e_1\boldsymbol{G}_1\\\vdots\\e_{m-1}\boldsymbol{G}_{m-1}\end{pmatrix},$$

其中 $\boldsymbol{G}_0,\boldsymbol{G}_1,\cdots,\boldsymbol{G}_{m-1}$ 分别是线性码 $C_0,C_1,\cdots,C_{m-1}$ 在有限域 F_q 上的生成矩阵. 另外,根据文献[4]的内容有,如果 $C=e_0C_0\oplus e_1C_1\oplus\cdots\oplus e_{m-1}C_{m-1}$ 是环 R 上码长为 n,码字个数为 $q^{\sum_{i=0}^{m-1}k_i}$,极小 Gray 距离为 d 的线性码,则 C 的 Gray 映射象 $\Phi(C)$ 是有限域 F_q 上的一个码长为 mn,维数为 $\sum_{i=0}^{m-1}k_i$,极小 Hamming 距离为 d 的线性码,即 $\Phi(C)$ 是 F_q 上的一个 $\left[mn,\sum_{i=0}^{m-1}k_i,d\right]$ 线性码,其中 k_i 是线性码 C_i 的维数.

对任意一个码字 $(c_0,c_1,\cdots,c_{n-1})\in C$,设 $\lambda\in R$ 是一个单位,如果 $(\lambda c_{n-1},c_0,\cdots,c_{n-2})\in C$,则称 C 是 R 上码长为 n 的 λ-常循环码. 设 $R[X]$ 为 R 上以 X 为变量的多项式环,定义映射 Φ_n 如下

$$\Phi_n:R^n\to R_n=R[X]/(X^n-\lambda),$$
$$(c_0,c_1,\cdots,c_{n-1})\mapsto c_0+c_1X+\cdots+c_{n-1}X^{n-1}.$$

显然,Φ_n 是一个 R-模同构,从而 R 上码长为 n 的 λ-常循环码可以看作商环 R_n 的一个理想.

引理 1 设 $\lambda=a(v)$ 是 R 中的一个元素,则 λ 是 R 中的单位当且仅当 $a(k_i)\neq 0(\mathrm{mod}q)$,其中 $i=0,1,\cdots,m-1$.

证明 由中国剩余定理得,λ 是 R 中的一个单位⇔$a(k_i)$ 是 F_q 上的单位⇔$a(k_i)\neq 0(\mathrm{mod}q)$,其中 $i=0,1,\cdots,m-1$.

注 1 在下文中,均假定 $\lambda=a(v)$ 是环 R 中的单位.

引理 2 线性码 $C=e_0C_0\oplus e_1C_1\oplus\cdots\oplus e_{m-1}C_{m-1}$ 是 R 上的 λ-常循环码当且仅当对任意的 $i=0,1,\cdots,m-1$,C_i 是有限域 F_q 上的 $a(k_i)$-常循环码.

证明 设 $(c_{i,0},c_{i,1},\cdots,c_{i,n-1})\in C_i$ 且 $c_j=\sum_{i=0}^{m-1}e_ic_{ij}$,其中 $j=0,1,\cdots,n-1$,则向量 $(c_0,c_1,\cdots,c_{n-1})\in C$. 由于 C 是 λ-常循环码,则 $(\lambda c_{n-1},c_0,\cdots,c_{n-2})\in C$. 注意到

$$(\lambda c_{n-1},c_0,\cdots,c_{n-2})=\sum_{i=0}^{m-1}e_i(a(k_i)c_{i,n-1},c_{i,0},\cdots,c_{i,n-2}).$$

由 R 上线性码的分解表示唯一性,有 $(a(k_i)c_{i,n-1},c_{i,0},\cdots,c_{i,n-2})\in C_i$,即 C_i 是 F_q 上的 $a(k_i)$-常循环码.

反之,假设对任意的 $i=0,1,\cdots,m-1$ 线性码 C_i 为 F_q 上的 $a(k_i)$-常循环码. 取 $(c_0,c_1,\cdots,c_{n-1})\in C$,其中 $c_j=\sum_{i=0}^{m-1}e_ic_{ij}$,$j=0,1,\cdots,n-1$,则向量 $(c_{i,0},c_{i,1},\cdots,c_{i,n-1})\in C_i$. 注意到

$$\begin{aligned}&(\lambda c_{n-1},c_0,\cdots,c_{n-2})\\&=\sum_{i=0}^{m-1}e_i(a(k_i)c_{i,n-1},c_{i,0},\cdots,c_{i,n-2})\\&\in e_0C_0\oplus e_1C_1\oplus\cdots\oplus e_{m-1}C_{m-1}\\&=C.\end{aligned}$$

故线性码 C 是 R 上的 λ-常循环码.

下面,将 λ-常循环码 C 与商环 R_n 的理想等同. 由引理 2,有以下结果.

定理 1 设线性码 $C=e_0C_0\oplus e_1C_1\oplus\cdots\oplus e_{m-1}C_{m-1}$ 是 R 上码长为 n 的 λ-常循环码,则存在 $R[X]$ 中的多项式 $g(X)\mid(X^n-\lambda)$ 使得 $C=\langle g(X)\rangle$,其中 $g(X)=\sum_{i=0}^{m-1}e_ig_i(X)$ 且 $g_i(X)$ 是 $a(k_i)$-常循环码 C_i 的生成多项式.

证明 设 D 是 R 上码长为 n 的 λ-常循环码且 $D=<\sum_{i=0}^{m-1}e_ig_i(X)>$. 显然,$D\subseteq C$. 另外,由于 $e_iC_i=e_iD$,有 $C\subseteq D$. 故 $C=<\sum_{i=0}^{m-1}e_ig_i(X)>$. 由有限域上的常循环码理论知,对任意的 $i=0,1,\cdots,m-1$,多项式 $g_i(X)$ 整除 $X^n-a(k_i)$. 因此存在 F_q 上的多项式 $h_i(X)$ 使得 $X^n-a(k_i)=g_i(X)h_i(X)$. 故有

$$\begin{aligned}\sum_{i=0}^{m-1}(e_ig_i(X))\sum_{i=0}^{m-1}e_ih_i(X)&=X^n-\sum_{i=0}^{m-1}e_ia(k_i)\\&=X^n-\lambda,\end{aligned}$$

即 $\sum_{i=0}^{m-1}e_ig_i(X)$ 是 $X^n-\lambda$ 的因式.

3 环 $F_q[v]/(v^m-v)$ 上的 Euclidean 自对偶常循环码

设 $\boldsymbol{x}=(x_0,x_1,\cdots,x_{n-1}),\boldsymbol{y}=(y_0,y_1,\cdots,y_{n-1})\in R^n$,定义 Euclidean 内积为

$$\boldsymbol{x}\cdot\boldsymbol{y}=\boldsymbol{x}\boldsymbol{y}^{\mathrm{T}}=\sum_{i=0}^{n-1}x_iy_i.$$

线性码 C 的 Euclidean 对偶码 $C^{\perp}$ 定义为 $C^{\perp}=\{\boldsymbol{x}\in R^n\mid\boldsymbol{x}\cdot\boldsymbol{c}=0,\forall\boldsymbol{c}\in C\}$. 如果 $C\subseteq C^{\perp}$,则称 C 是 Euclidean 自正交的;如果 $C=C^{\perp}$,则称 C 是 Euclidean 自对偶的.

自对偶码是一类重要的线性码类,有着重要的应用. 下面,将讨论环 R 上的 Euclidean 自对偶常循环码,并由此构造有限域上一些参数较好的自对偶码.

引理 3[4] 设 $C=e_0C_0\oplus e_1C_1\oplus\cdots\oplus e_{m-1}C_{m-1}$ 是 R 上码长为 n 的线性码,则

$$C^{\perp}=e_0C_0^{\perp}\oplus e_1C_1^{\perp}\oplus\cdots\oplus e_{m-1}C_{m-1}^{\perp}.$$

另外,C 是 R 上的 Euclidean 自对偶码当且仅当 $C_0,C_1,\cdots,C_{m-1}$ 均是 F_q 上码长为 n 的 Euclidean 自对偶码.

定理 2 设线性码 $C=e_0C_0\oplus e_1C_1\oplus\cdots\oplus e_{m-1}C_{m-1}$ 是 R 上码长为 n 的 λ-常循环码,则它的 Euclidean 对偶码 $C^{\perp}$ 是 R 上码长为 n 的 λ^{-1}-常循环码,其中 $\lambda^{-1}=\sum_{i=0}^{m-1}e_ia(k_i)-1$.

证明 由引理 2,C_i 是有限域 F_q 上的 $a(k_i)$-常循

环码. 因此,$C_i^{\perp}$ 是有限域 F_q 上的 $a(k_i)^{-1}$-常循环码. 由引理 3 得,$C^{\perp}$ 是 R 上码长为 n 的 λ^{-1}-常循环码,其中 $\lambda^{-1}=\sum_{i=0}^{m-1} e_i a(k_i)-1$.

下面,给出 R 上码长为 n 的 λ-常循环码 C 是 Euclidean 自对偶码的充分条件.

定理 3　设线性码 $C=e_0C_0\oplus e_1C_1\oplus\cdots\oplus e_{m-1}C_{m-1}$ 是 R 上码长为 n 的 λ-常循环码,若它是 Euclidean 自对偶码,则必有 $\lambda=\lambda^{-1}$.

证明　根据 Euclidean 自对偶码的定义以及定理 2,结论显然成立.

环 R 上的 Euclidean 自对偶常循环码可以用来构造有限域上参数较好的 Euclidean 自对偶码. 首先,需要如下的引理.

引理 4[4]　设线性码 C 是环 R 上码长为 n 的 Euclidean 自对偶码. 令 $\boldsymbol{M}\in \mathrm{GL}_m(F_q)$ 且 $\boldsymbol{M}\boldsymbol{M}^{\perp}=\mu\boldsymbol{I}_m$,其中 $\mu\in F_q^*=F_q\backslash\{0\}$ 以及 $\boldsymbol{I}_m$ 为 F_q 上的 m 阶单位矩阵,则线性码 $\Phi(C)$ 是 F_q 上码长为 mn 的 Euclidean 自对偶码.

由引理 4、环 R 上的 Euclidean 常循环自对偶码以及环 R 到有限域 F_q 上的 Gray 映射,可以构造 F_q 上一些参数较好的 Euclidean 自对偶码.

例 1　设 $R=F_{11}[v]/(v^3-v)$,其中 $v^3=v$. 另外,设 $C=(1-v^2)C_0+6(v^2+v)C_1+6(v^2-v)C_2$ 是环 R 上码长为 4 的 10-常循环码,则由引理 2 知,$C_i, i=0,1,2$,均是 F_{11} 上码长为 4 的负循环码. 设 C_i 的生成矩阵分别为

$$\boldsymbol{G}_0=\begin{pmatrix}10&3&1&0\\0&10&3&1\end{pmatrix},\boldsymbol{G}_1=\begin{pmatrix}10&3&1&0\\0&10&3&1\end{pmatrix},$$

$$\boldsymbol{G}_2=\begin{pmatrix}10&8&1&0\\0&10&8&1\end{pmatrix},$$

则 $\boldsymbol{G}=\begin{pmatrix}e_0\boldsymbol{G}_0\\e_1\boldsymbol{G}_1\\e_2\boldsymbol{G}_2\end{pmatrix}$ 是 C 作为 R^4 的一个 F_{11}-线性子空间的生成矩阵且 C 是一个 Euclidean 自对偶 10-常循环码. 取 $\boldsymbol{M}=\begin{pmatrix}9&2&1\\10&9&2\\2&1&2\end{pmatrix}\in \mathrm{GL}_3(F_{11})$,则 $\boldsymbol{M}\boldsymbol{M}^{\mathrm{T}}=\begin{pmatrix}9&0&0\\0&9&0\\0&0&9\end{pmatrix}$. 令 Φ 为可逆矩阵 $\boldsymbol{M}$ 定义的 Gray 映射,则 $\Phi(C)$ 为有限域 F_{11} 上参数为[12,6,5]的 Euclidean 自对偶码.

例 2　设 $R=F_{13}[v]/(v^3-v)$,其中 $v^3=v$. 另外,设 $C=(1-v^2)C_0+7(v^2+v)C_1+7(v^2-v)C_2$ 是环 R 上码长为 6 的 12-常循环码,则由引理 2 知,$C_i, i=0,1,2$,均是 F_{13} 上码长为 6 的负循环码. 设 C_i 的生成矩阵分别为

$$\boldsymbol{G}_0=\begin{pmatrix}6&9&5&1&0&0\\0&6&9&5&1&0\\0&0&6&9&5&1\end{pmatrix},\boldsymbol{G}_1=\begin{pmatrix}6&9&5&1&0&0\\0&6&9&5&1&0\\0&0&6&9&5&1\end{pmatrix},$$

$$\boldsymbol{G}_2=\begin{pmatrix}11&3&8&1&0&0\\0&11&3&8&1&0\\0&0&11&3&8&1\end{pmatrix},$$

则 $\boldsymbol{G}=\begin{pmatrix}e_0\boldsymbol{G}_0\\e_1\boldsymbol{G}_1\\e_2\boldsymbol{G}_2\end{pmatrix}$ 是 C 作为 R^6 的一个 F_{13}-线性子空间的生成矩阵且 C 是一个 Euclidean 自对偶 12-常循环码. 取 $\boldsymbol{M}=\begin{pmatrix}11&2&1\\12&11&2\\2&1&2\end{pmatrix}\in \mathrm{GL}_3(F_{13})$,则 $\boldsymbol{M}\boldsymbol{M}^{\mathrm{T}}=\begin{pmatrix}9&0&0\\0&9&0\\0&0&9\end{pmatrix}$. 令 Φ 为可逆矩阵 $\boldsymbol{M}$ 定义的 Gray 映射,则 $\Phi(C)$ 为有限域 F_{13} 上参数为[18,9,7]的 Euclidean 自对偶码.

4　环 $F_{p^2}[v]/(v^m-v)$ 上的 Hermitian 自对偶常循环码

在本节中,令 $q=p^2$,即 $R=F_{p^2}[v]/(v^m-v)$. 设 $\boldsymbol{a}=(a_0,a_1,\cdots,a_{n-1}),\boldsymbol{b}=(b_0,b_1,\cdots,b_{n-1})\in R^n$,定义它们的 Hermitain 内积为

$$\langle\boldsymbol{a},\boldsymbol{b}\rangle=\sum_{i=0}^{n-1} a_i b_i^p.$$

线性码 C 的 Hermitian 对偶码 $C^{\perp_H}$ 定义为 $C^{\perp_H}=\left\{\boldsymbol{a}\in R^n \,\middle|\, \langle\boldsymbol{a},\boldsymbol{c}\rangle=\sum_{i=0}^{n-1} a_i c_i^p=0,\ \forall\,\boldsymbol{c}\in C\right\}$. 如果 $C\subseteq C^{\perp_H}$ 则称 C 是 Hermitian 自正交的;如果 $C=C^{\perp_H}$,则称 C1 是 Hermitian 自对偶的. 对任意的 $\boldsymbol{c}=(c_0,c_1,\cdots,c_{n-1})\in C$,定义 $\boldsymbol{c}^p=(c_0^p,c_1^p,\cdots,c_{n-1}^p)$. 同样地,对 $\boldsymbol{M}=(m_{ij})_{0\leqslant i,j\leqslant n-1}\in \mathrm{GL}_m(F_{p^2})$,定义 $\boldsymbol{M}^p=(m_{ij}^p)_{0\leqslant i,j\leqslant n-1}$.

首先,回顾有限域 F_{q^2} 上 Hermitian 自对偶常循环码的一些结果[11].

设 $\alpha\in F_{q^2}^*, r=\mathrm{ord}_{q^2}(\alpha)$,$C$ 是 F_{q^2} 上的 α-常循环码,则 $r\mid(q^2-1)$. 如果 C 是一 Hermitian 自对偶码,则有 $r\mid(q+1)$. 定义 $O_{r,n}(1)=\{ir+1\mid 0\leqslant i\leqslant n-1\}\pmod{rn}\subseteq Z_{r,n}$. 如果 $T\subset O_{r,n}(1)$ 是一些 q^2-分圆陪集的并,则用 C_T 表示 F_{q^2} 上定义集为 T 的 α-常循环码.

引理 5[11]　设 $T\subset O_{r,n}(1)$ 是 α-常循环码 C_T 的定义集,$\overline{T}=-q[O_{r,n}(1)\backslash T]$ 是 α^{-q}-常循环码 $C_T^{\perp_H}$ 的定义集,则 C_T 是 Hermitian 自对偶常循环码当且仅当 $\overline{T}=T$.

下面介绍环 R 上的 Hermitian 自对偶常循环码.

定理 4　设 $C=e_0C_0\oplus e_1C_1\oplus\cdots\oplus e_{m-1}C_{m-1}$ 是 R 上码长为 n 的 λ-常循环码,则

(1) C 的 Hermitian 对偶码为

$$C^{\perp_H}=e_0C_0^{\perp_H}\oplus e_1C_1^{\perp_H}\oplus\cdots\oplus e_{m-1}C^{\perp_H m-1}.$$

另外,对任意 $i=0,1,\cdots,m-1$,有 $C_i^{\perp_H}$ 是 F_{p^2} 上码长为 n 的 $a(k_i)^{-p}$-常循环码且 $C^{\perp_H}$ 是 R 上码长为 n 的 λ^{-p}-常循环码,其中 $\lambda^{-p}=\sum_{i=0}^{m-1} e_i a(k_i)^{-p}$.

(2) C 是 R 上码长为 n 的 Hermitian 自对偶码当且仅当 $C_0,C_1,\cdots,C_{m-1}$ 均是 F_{p^2} 上码长为 n 的 Hermitian 自

对偶码.

证明

(1)首先,证明

$$C^{\perp_H}=e_0C_0^{\perp_H}\oplus e_1C_1^{\perp_H}\oplus\cdots\oplus e_{m-1}C^{\perp_H m-1}.$$

定义集合

$$D_i^{\perp_H}=\{\boldsymbol{x}_i\in F_p^n\mid\exists\boldsymbol{x}_0,\cdots,\boldsymbol{x}_{i-1},\boldsymbol{x}_{i+1},\cdots,\boldsymbol{x}_{m-1}\in F_p^n,$$
$$e_0\boldsymbol{x}_0+e_1\boldsymbol{x}_1+\cdots+e_{m-1}\boldsymbol{x}_{m-1}\in C^{\perp_H}\},$$

则有 $C^{\perp_H}=e_0D_0^{\perp_H}\oplus e_1D_1^{\perp_H}\oplus\cdots\oplus e_{m-1}D_{m-1}^{\perp_H}$. 显然,对任意的 $i=0,1,\cdots,m-1$,有 $D_i^{\perp_H}\subseteq C_i^{\perp_H}$. 设 $\boldsymbol{c}_i\in C_i^{\perp_H}$,则对任意的 $\boldsymbol{x}_i\in C_i$ 存在 $\boldsymbol{x}_0,\boldsymbol{x}_1,\cdots,\boldsymbol{x}_{i-1},\boldsymbol{x}_{i+1},\cdots,\boldsymbol{x}_{m-1}\in F_p^n$ 使得 $\langle\boldsymbol{c}_i,(e_0\boldsymbol{x}_0+e_1\boldsymbol{x}_1+\cdots+e_{m-1}\boldsymbol{x}_{m-1})\rangle=0$. 令 $\boldsymbol{c}=e_0\boldsymbol{x}_0+e_1\boldsymbol{x}_1+\cdots+e_{m-1}\boldsymbol{x}_{m-1}\in C$,则 $\langle e_i\boldsymbol{c}_i,\boldsymbol{c}\rangle=0$. 因此 $e_i\boldsymbol{c}_i\in C^{\perp_H}$. 由环 R 上线性码分解表示的唯一性,有 $\boldsymbol{c}_i\in D_i^{\perp_H}$ 即 $C_i^{\perp_H}\subseteq D_i^{\perp_H}$.

其次,证明 $C_i^{\perp_H}$ 是 F_{p^2} 上码长为 n 的 $a(k_i)^{-p}$-常循环码. 因为 $C=e_0C_0\oplus e_1C_1\oplus\cdots\oplus e_{m-1}C_{m-1}$ 是 R 上码长为 n 的 λ-常循环码,根据引理2,有 C_i 是 F_{p^2} 上的 $a(k_i)$-常循环码. 从而 $C_i^{\perp_H}$ 是 F_{p^2} 上码长为 n 的 $a(k_i)^{-p}$-常循环码,$i=0,1,\cdots,m-1$.

最后,证明 $C^{\perp_H}$ 是一个 λ^{-p}-常循环码. 通过前面的证明过程,得到 C 的 Hermitian 对偶码 $C^{\perp_H}$ 是 R 上码长为 n 的 $\sum_{i=0}^{m-1}e_ia(k_i)^{-p}$-常循环码,令 $\lambda^{-p}=\sum_{i=0}^{m-1}e_ia(k_i)^{-p}$,结论得证.

(2)显然,对任意的 $i=0,1,\cdots,m-1$,如果 C_i 是 Hermitian 自对偶的,则 C 也是 Hermitian 自对偶的. 另外,如果 C 是 Hermitian 自对偶的,则 C_i 是 Hermitian 自正交的,即 $C_i\subseteq C_i^{\perp_H}$. 事实上 $C_i=C_i^{\perp_H}$. 否则,存在 $\boldsymbol{x}_i\in C_i^{\perp_H}\backslash C_i$ 以及 $x_0\in C_0,\cdots,\boldsymbol{x}_{i-1}\in C_{i-1},\boldsymbol{x}_{i+1}\in C_{i+1},\cdots,\boldsymbol{x}_{m-1}\in C_{m-1}$ 使得

$$\langle e_0\boldsymbol{x}_0+\cdots+e_{m-1}\boldsymbol{x}_{m-1},e_0\boldsymbol{x}_0+\cdots+e_{m-1}\boldsymbol{x}_{m-1}\rangle\neq0.$$

这与 C 是 Hermitian 自对偶的矛盾. 因此 C_i 是有限域 F_{p^2} 上的 Hermitian 自对偶码.

接下来,给出 R 上码长为 n 的常循环码 C_T 是 Hermitian 自对偶常循环码的充要条件.

定理5 设 $T_i\subset O_{r,n}(1)$ 是 $a(k_i)$-常循环码 C_{T_i} 的定义集,$\overline{T}_i=-p[O_{r,n}(1)\backslash T_i]$ 是 $a(k_i)^{-p}$-常循环码 $C_{T_i}^{\perp_H}$ 的定义集,则 $C_T=e_0C_{T_0}\oplus e_1C_{T_1}\oplus\cdots\oplus e_{m-1}C_{T_{m-1}}$ 是 Hermitian 自对偶 λ-常循环码当且仅当 $\overline{T}_i=T_i,i=0,1,\cdots,m-1$.

证明 由定理4和引理5,$C_T=e_0C_{T_0}\oplus e_1C_{T_1}\oplus\cdots\oplus e_{m-1}C_{T_{m-1}}$ 是 R 上码长为 n 的 Hermitian 自对偶码 λ-常循环码$\Leftrightarrow C_{T_0},C_{T_1},\cdots,C_{T_{m-1}}$ 均是 F_{p^2} 上码长为 n 的 Hermitian 自对偶码$\Leftrightarrow\overline{T}_i=T_i,i=0,1,\cdots,m-1$.

例3 设 $p^2=13^2,n=4,r=2$. 考虑 F_{13^2} 上码长为4的 ω^{81}-常循环码,其中 ω 是 F_{13^2} 中的一个本原元. 显然 $r\mid(p+1),O_{2,4}(1)=\{1,3,5,7\}$. 设 $T_i=\{3,5\}$,则 $\overline{T}_i=-13[O_{2,4}(1)\backslash T]=\{3,5\}\pmod8$,其中 $i=0,1,2,3$. 由定理4和定理5,

$$C_T=(1-v^3)C_{T_0}+\frac{(v^3+v^2+v)}{3}C_{T_1}+\frac{(v^3+3v^2+9v)}{3}C_{T_2}+\frac{(v^3+9v^2+3v)}{3}C_{T_3}$$

是一个码长为4的 Hermitian 自对偶 ω^{84}-常循环码.

类似于引理4,环 R 上的 Hermitian 自对偶常循环码也可以用来构造有限域上参数较好的 Hermitian 自对偶码. 首先,给出如下的一个引理.

引理6 设线性码 C 是环 R 上码长为 n 的 Hermitian 自对偶码. 令 $\boldsymbol{M}\in\mathrm{GL}_m(F_{p^2})$ 且 $\boldsymbol{M}(\boldsymbol{M}^p)^{\mathrm{T}}=\mu\boldsymbol{I}_m$,其中 $\mu\in F_{p^2}^*$ 以及 $\boldsymbol{I}_m$ 为 F_{p^2} 上的 m 阶单位矩阵,则线性码 $\Phi(C)$ 是 F_{p^2} 上码长为 mn 的 Hermitian 自对偶码.

证明 对线性码 $\Phi(C)$ 中任意的两个码字 $\boldsymbol{c}=(c_0,c_1,\cdots,c_{mn-1})$ 以及 $\boldsymbol{d}=(d_0,d_1,\cdots,d_{mn-1})$,存在线性码 C 中的两个码字 $\boldsymbol{x}=(x_0,x_1,\cdots,x_{n-1})$ 以及 $\boldsymbol{y}=(y_0,y_1,\cdots,y_{n-1})$ 使得 $\boldsymbol{c}=(x_0\boldsymbol{M},x_1\boldsymbol{M},\cdots,x_{n-1}\boldsymbol{M})$,$\boldsymbol{d}=(y_0\boldsymbol{M},y_1\boldsymbol{M},\cdots,y_{n-1}\boldsymbol{M})$. 因此,$\langle\boldsymbol{c},\boldsymbol{d}\rangle=\sum_{j=0}^{n-1}x_j\boldsymbol{M}(\boldsymbol{M}^p)^{\mathrm{T}}y_j^p$. 由于 $\boldsymbol{M}(\boldsymbol{M}^p)^{\mathrm{T}}=\mu\boldsymbol{I}_m$,因此 $\langle\boldsymbol{c},\boldsymbol{d}\rangle=\mu\sum_{j=0}^{n-1}x_jy_j^p$. 又因为 C 是 Hermitian 自对偶的,故 $\langle\boldsymbol{x},\boldsymbol{y}\rangle=\sum_{j=0}^{n-1}x_jy_j^p=0$. 从而 $\langle\boldsymbol{c},\boldsymbol{d}\rangle=0$,即 $\Phi(C)$ 是 F_{p^2} 上码长为 mn 的 Hermitian 自正交码. 又因为 Φ 是 R^n 上的 F_{p^2}-模同构,因此 $|C|=|\Phi(C)|=(p^{2m})^{n/2}=p^{mn}$. 故 $\Phi(C)$ 是 Hermitian 自对偶的.

例4 设 $R=F_{11^2}[v]/(v^2-v)$,其中 $v^2=v$. 另外,设 $C_T=(1-v)C_{T_0}+vC_{T_1}$ 是码长为4的 Hermitian 自对偶 ω^{60}-常循环码,其中 ω 是 F_{11^2} 中的一个本原元,C_{T_i} 分别是以 $T_i=\{1,3\}$ 为定义集的常循环码. C_{T_i} 的生成多项式均是 $g_i(x)=(x-\omega^{15})(x-\omega^{45})=x^2+8x+10,i=0,1$. 取 $\boldsymbol{M}=\begin{pmatrix}1&1\\-1&1\end{pmatrix}\in\mathrm{GL}_2(F_{11^2})$,则 $\boldsymbol{M}(\boldsymbol{M}^p)^{\mathrm{T}}=\begin{pmatrix}2&0\\0&2\end{pmatrix}$. 令 Φ 为可逆矩阵 M 定义的 Gray 映射,则 $\Phi(C)$ 为有限域 F_{11^2} 上参数为[8,4,3]的 Hermitian 自对偶码. 而文献[11]只是证明了有限域 F_{11^2} 上参数为[8,4,≥3]的 Hermitian 自对偶码的存在性.

例5 设 $R=F_{19^2}[v]/(v^4-v)$,其中 $v^4=v$. 另外,设

$$C_T=(1-v^3)C_{T_0}+\frac{(v^3+v^2+v)}{3}C_{T_1}+\frac{(v^3+7v^2+11v)}{3}C_{T_2}+\frac{(v^3+11v^2+7v)}{3}C_{T_3}$$

是码长为 4 的 Hermitian 自对偶 ω^{180}-常循环码,其中 ω 是 F_{19^2}中的一个本原元. 对于 $i=0,1,2$,C_{T_i}分别是以 $T_i=\{1,3\}$ 为定义集的常循环码,C_{T_i}的生成多项式均是 $g_i(x)=(x-\omega^{45})(x-\omega^{135})=x^2+13x+18$.

取 $$\boldsymbol{M}=\begin{pmatrix}1&1&1&1\\1&1&-1&-1\\1&-1&1&-1\\1&-1&-1&1\end{pmatrix}\in \mathrm{GL}_4(F_{19^2}),$$

则 $$\boldsymbol{M}(\boldsymbol{M}^p)^{\mathrm{T}}=\begin{pmatrix}4&0&0&0\\0&4&0&0\\0&0&4&0\\0&0&0&4\end{pmatrix}.$$

令 $\boldsymbol{\Phi}$ 为可逆矩阵 $\boldsymbol{M}$ 定义的 Gray 映射,则 $\boldsymbol{\Phi}(C)$为有限域 F_{19^2}上参数为[16,8,6]的 Hermitian 自对偶码. 而文献[11]只是证明了有限域 F_{19^2}上存在参数为[16,8,≥3]的 Hermitian 自对偶码. 因此,通过对比文献[11]中的结果,本算例构造的 F_{19^2}上参数为[16,8,6]的 Hermitian 自对偶码是一个新码.

5　环 $F_{p^2}[v]/(v^m-v)$上的 Hermitian 自对偶常循环 MDS 码

设 $R=F_{p^2}[v]/(v^m-v)$,则$\langle v-k_0\rangle,\langle v-k_1\rangle,\cdots,\langle v-k_{m-1}\rangle$是环 R 的极大理想. 如果 $z\in R$ 是一个零因子,则 z 一定在某一个极大理想中. 如果 $d(C)$是 $C=e_0C_0\oplus e_1C_1\oplus\cdots\oplus e_{m-1}C_{m-1}$的极小 Hamming 距离并且存在 $\boldsymbol{x}\in C$,有 $\mathrm{wt}(\boldsymbol{x})=d(C)$,其中 $\mathrm{wt}(\boldsymbol{x})$表示 $\boldsymbol{x}$ 的 Hamming 重量,则 $\boldsymbol{x}$ 的形式要么是 $\boldsymbol{x}$ 的所有分量都在某一个极大理想中,要么是 $\boldsymbol{x}$ 的所有非零分量都是单位,并且集合 $\{d(C_0),d(C_1),\cdots,d(C_{m-1})\}$中存在与 $d(C)$相等的极小 Hamming 距离.

下面给出一个构造环 R 上 Hermitian 自对偶常循环 MDS 码的方法. 在给出这个结果之前,需要如下的几个引理.

引理 7[11]　设 $\alpha\in F_{q^2}^*$的阶是 r 且满足 $rs=q+1$,其中,s 是某个正整数. 设 n 是一个偶数满足 $n\mid q-1$. 定义 $T=O_{r,n}(1)\setminus\left\{ir+1\ \middle|\ -[\frac{s-1}{2}]\leqslant i\leqslant[\frac{n-1-s}{2}]\right\}(\mathrm{mod}\ rn)$则当 s 是奇数时,有 C_T 是一个参数为$[n,\frac{n}{2},\frac{n}{2}+1]$的 Hermitian 自对偶 α-常循环 MDS 码,其中 C_T 表示定义集为 T 的常循环码.

引理 8　码 $C=e_0C_0\oplus e_1C_1\oplus\cdots\oplus e_{m-1}C_{m-1}$是一个 MDS 码当且仅当$\{C_i\}$的维数$\{k_i\}$均相等,$d(C)$等于$\{d(C_i)\}$中的某一个 $d(C_i)$且相应的 C_i 是一个 MDS 码,其中 $i=0,1,\cdots,m-1$.

证明　一方面,由线性码理论知$|C|=|C_0||C_1|\cdots|C_{m-1}|=p^{2(k_0+k_1+\cdots+k_{m-1})}$. 因为 C 是一个 MDS 码,所以 $d(C)=n-\log_{p^{2m}}|C|=n-\frac{1}{m}(k_0+k_1+\cdots+k_{m-1})+1$. 又因为对每个 $i=0,1,\cdots,m-1$ 有 $d(C)\leqslant d(C_i)\leqslant n-k_i+1$,所以 $n-\frac{1}{m}(k_0+k_1+\cdots+k_{m-1})+1\leqslant n-k_i+1$,即$\frac{1}{m}(k_0+k_1+\cdots+k_{m-1})\geqslant k_i$. 这说明维数 $k_0,k_1,\cdots,k_{m-1}$的平均数都大于等于它们本身,故 $k_0=k_1=\cdots=k_{m-1}=\frac{1}{m}(k_0+k_1+\cdots+k_{m-1})$. 因此,$d(C_i)\leqslant n-\frac{1}{m}(k_0+k_1+\cdots+k_{m-1})+1=d(C)$,即 $d(C_i)=d(C)=n-\frac{1}{m}(k_0+k_1+\cdots+k_{m-1})+1$,即 C_i 均是 MDS 码.

另一方面,由于 C_i 是一个 MDS 码,所以 $d(C)=d(C_i)=n-k_i+1=n-\frac{1}{m}(k_0+k_1+\cdots+k_{m-1})+1$. 故 C 是一个 MDS 码.

定理 6　设 $a(v)$中系数 $a_j\in F_{p^2}^*$使得 $r_j=\mathrm{ord}_{p^2}(a(k_j))$且存在正奇数 s_j 使得 $r_js_j=p+1$. 设 n 是一个偶数满足 $n\mid(p-1)$. 定义 $T_j=O_{rj,n}(1)\setminus\left\{ir_j+1\ \middle|\ -[\frac{s_j-1}{2}]\leqslant i\leqslant[\frac{n-1-s_j}{2}]\right\}(\mathrm{mod}r_jn)$. 令 C_{T_j}是一个以 T_j为定义集的 $a(k_j)$-常循环码,$j=0,1,\cdots,m-1$,则 $C=e_0C_{T_0}\oplus e_1C_{T_1}\oplus\cdots\oplus e_{m-1}C_{T_{m-1}}$是一个 Hermitian 自对偶 λ-常循环 MDS 码,其参数为$(n,|C|=p^{mn},\frac{n}{2}+1)$.

证明　由引理 7,C_{T_j}是参数为$[n,\frac{n}{2},\frac{n}{2}+1]$的 Hermitian 自对偶 $a(k_j)$-常循环 MDS 码. 再由引理 8,结论显然成立.

例 6　设 $R=F_{17^2}+vF_{17^2}$,$\lambda=\omega^{144}+v(\omega^{48}-\omega^{144})$,其中 $v^2=v$,ω 是 F_{17^2}中的一个本原元,则由引理 7,$r_0=\mathrm{ord}_{17^2}(\omega^{144})=2$,$r_1=\mathrm{ord}_{17^2}(\omega^{48})=6$. 存在 $s_0=9$,$s_1=3$,使得 $r_0s_0=r_1s_1=18$. 令 $n=8$,则 C_{T_0}是以 $T_0=\{1,3,5,7\}$为定义集的[8,4,5]Hermitian 自对偶 ω^{144}-常循环码,C_{T_1}是以 $T_1=\{19,25,31,37\}$为定义集的[8,4,5]Hermitian 自对偶 ω^{48}-常循环码. 由定理 6,$C_T=(1-v)C_{T_0}+vC_{T_1}$是 R 上一个参数为$(8,(17^4)^4,5)$的 Hermitian 自对偶 λ-常循环 MDS 码.

6　结论

本文中,主要研究了有限非链环 $F_q[v]/(v^m-v)$上常循环码的代数结构. 特别地,研究了这个环上的 Euclidean 自对偶常循环码、Hermitian 自对偶常循环码以

及 Hermitian 自对偶码常循环 MDS 码,给出了环 $F_q[v]/(v^m-v)$ 上的常循环码是 Euclidean 自对偶码的充分条件,是 Hermitian 自对偶码的充要条件,并利用 Gray 映射构造了有限域 F_q 上一些参数较好的自对偶码. 本文结果表明,环 $F_q[v]/(v^m-v)$ 上的自对偶常循环码不仅具有良好的代数结构,而且能够有效的构造有限域上参数较好的自对偶码.

参考文献

[1] ZHU S,WANG Y,SHI M. Some results on cyclic codes over F_2+vF_2[J]. IEEE Trans Inform Theory,2010,56(4):1680 – 1684.

[2] ZHU S,WANG L. A class of constacyclic codes over F_p+vF_p and their Gray images[J]. Discrete Math,2011,311(23 – 24):2677 – 2682.

[3] SHI M,SOLE P,WU B. Cyclic codes and the weight enumerator of linear codes over $F_2+vF_2+v^2F_2$[J]. Appl Comput Math,2013,12(2):247 – 255.

[4] 高健,王现方,施敏加,符方伟. 环 $F_p[v]/(v^m-v)$ 上线性码的 Gray 映射及其应用[J]. 中国科学:数学,2016,46:1329 – 336.
GAO J,WANG X,SHI M,FU F. -W. Grap maps on linear codes over $F_p[v]/(v^m-v)$ and their applications[J]. Sci Sin Math,2016,46:1329 – 336. (in Chinese)

[5] 丁健,李红菊,左学武,梁静. 环 $F_2+uF_2+u^2F_2$ 上的常循环码[J]. 电子学报,2015,43(1):145 – 150.
DING J,LI H,ZUO X,LIANG J. Theconstacyclic codes over $F_2+uF_2+u^2F_2$[J]. Acta Electronica Sinica,2015,43(1):145 – 150. (in Chinese)

[6] 朱士信,孙中华,开晓山. 环 Z_{2m} 上一类常循环码的挠码及其应用[J]. 电子学报,2016,44(8):1826 – 1830.
ZHU S,SUN Z,KAI X. Torsion codes of a class of constacyclic codes over Z_{2m} and their applications[J]. Acta Electronica Sinica,2016,44(8):1826 – 1830. (in Chinese)

[7] BETSUMIYA K,HARADA M. Optimal self-dual codes over $F_2\times F_2$ with respect to the Hamming weight[J]. IEEE Trans Inform Theory,2004,50(2):356 – 358.

[8] KIMA J,LEE Y. Euclidean and Hermitian self-dual MDS codes over large finite fields[J]. Journal of Combinatorial Theory,Series A,2004,105(1):79 – 95.

[9] QIAN J,MA W. Self-dual codes over finite chain rings[J]. IEEE Singapore International Conference on Communication Systems,2008,250 – 252.

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

[11] YANG Y,CAI W. On self-dual constacyclic codes over finite fields[J]. Des Codes Crypptogr,2015,74(2):355 – 364.

[12] LIU Y,SHI M,SEPASDAR Z,SOLE P. Construction of Hermitain self-dual constacyclic codes over $F_{q^2}+vF_{q^2}$[J]. Appl Comput Math,2016,15(3):359 – 369.

作者简介

高 健 男,1987 年生于山东德州. 博士、硕士生导师,研究方向为编码理论及其应用.
E-mail:dezhougaojian@163.com

王永康 男,1993 年生于山东潍坊. 硕士研究生,研究方向为编码理论及其应用.
E-mail:zcyongkang@163.com