DOI:10.3969/j.issn.1003-5060.2023.01.021

# 四元域上一类厄米特互补对偶常循环码

孙世林, 刘 丽
(合肥工业大学 数学学院,安徽 合肥 230601)

**摘 要**:有限域上线性互补对偶码(linear codes with complementary duals,LCD)具有良好的结构和性质,并在双用户加法器信道中得到广泛的应用。文章构造四元厄米特LCD常循环码,分析它们的参数,并确定其维数,给出它们最小距离的下界。

**关键词**:线性互补对偶码;常循环码;生成多项式
**中图分类号**:TN911.22 **文献标志码**:A **文章编号**:1003-5060(2023)01-0136-05

# A class of quaternary Hermitian LCD constacyclic codes

SUN Shilin, LIU Li
(School of Mathematics, Hefei University of Technology, Hefei 230601, China)

**Abstract**: Linear codes with complementary duals (LCD) over finite fields have good structure and properties, and are widely used in two-user adder channels. In this paper, the quaternary Hermitian LCD constacyclic codes are constructed and their parameters are analyzed. The dimensions of these codes are settled and the lower bounds on their minimum distances are presented.

**Key words**: linear codes with complementary duals (LCD); constacyclic codes; generator polynomial

## 0 引 言

常循环码是一类重要的线性码,在纠错码理论中占有重要的地位[1-2]。常循环码可以通过移位寄存器进行有效编码,是工程应用中优先选择的对象。

线性码$C$若满足$C\cap C^{\perp}=\{0\}$则称$C$为线性互补对偶码(linear codes with complementary duals,LCD)。文献[3]首次引入有限域上LCD码,证明了LCD码是渐近好码;文献[4]证明了二元LCD码可以用于密码边道攻击,这引起了学者们对构造LCD码的极大兴趣;文献[5]构造了有限域上几类LCD循环码并分析了它们的参数;文献[6]分析了可逆BCH码的参数;文献[7]分析了有限域上可逆负循环BCH码的几类参数。

但是很少有学者研究厄米特LCD码。文献[8]研究了基于欧几里得和厄米特LCD码的准循环LCD码的性质,证明了这些码是渐近好码;文献[9]利用生成矩阵给出了厄米特LCD码的一个充要条件。

最近,文献[10]利用维数比较小的线性码、自正交码和广义的RS码构造出几类新的欧几里得和厄米特LCD MDS码;文献[11]构造出几类厄米特LCD循环码并分析了它们的参数。

本文目的是构造四元厄米特LCD常循环码,并分析它们的参数,确定这些码的维数,给出它们最小距离的下界。本文提出的厄米特线性互补对偶码不是常循环BCH码。

## 1 预备知识

设$G_F(4)$为四元有限域,$n$为一个正奇数,$G_F(4)$上参数为$[n,k,d]$的四元线性码$C$是

**收稿日期**:2021-06-21;**修回日期**:2021-09-06
**基金项目**:国家自然科学基金资助项目(61972126);中央高校基本科研业务费专项资金资助项目(PA2019GDZC0097)
**作者简介**:孙世林(1995—),女,安徽亳州人,合肥工业大学硕士生;
刘 丽(1965—),女,安徽合肥人,博士,合肥工业大学教授,硕士生导师,通信作者,E-mail:liuli-1128@163.com.

$G_F(4)^n$的线性子空间，其维数为 $k$ 且最小汉明距离为 $d$。对任意的 $x\in G_F(4)$，$x$ 的共轭定义为 $\bar{x}=x^2$。$G_F(4)$上长为 $n$ 的线性码 $C$ 的厄米特对偶码定义为：

$$C^{\perp_H}=\{(b_0,b_1,\cdots,b_{n-1})\in G_F(4)^n:$$
$$\sum_{i=0}^{n-1}b_i\bar{c}_i=0,\forall(c_0,c_1,\cdots,c_{n-1})\in C\}。$$

**定义 1**[9-11]　设 $C$ 为 $G_F(4)$上一个长为 $n$ 的线性码，且 $C^{\perp_H}$ 为 $C$ 的厄米特对偶码，若 $C\oplus C^{\perp_H}=G_F(4)^n$ 或 $C\cap C^{\perp_H}=\{0\}$，则称码 $C$ 为厄米特 LCD 码。

设 $\omega$ 为 $G_F(4)$的本原元素，若 $(c_0,c_1,\cdots,c_{n-1})\in C$，$(\omega c_{n-1},c_0,c_1,\cdots,c_{n-2})\in C$，则称码 $C$ 为 $G_F(4)$上长为 $n$ 的 $\omega$-循环码。若将 $(c_0,c_1,\cdots,c_{n-1})\in G_F(4)^n$ 表示成多项式 $c_0+c_1x+c_2x^2+\cdots+c_{n-1}x^{n-1}\in G_F(4)[x]/(x^n-\omega)$，则 $G_F(4)$上长为 $n$ 的 $\omega$-常循环码对应于 $G_F(4)[x]/(x^n-\omega)$的一个理想，线性码 $C$ 为 $G_F(4)$上长为 $n$ 的 $\omega$-常循环码。注意，$G_F(4)[x]/(x^n-\omega)$的每个理想都是主理想，故存在次数最小的首一多项式 $g(x)$使得 $C=\langle g(x)\rangle$且 $g(x)|(x^n-\omega)$。称 $g(x)$为码 $C$ 的生成多项式，称 $h(x)=(x^n-\omega)/g(x)$为码 $C$ 的校验多项式。假设 $n$ 为正奇数，设 $\alpha$ 为 $G_F(4^m)^*$ 的生成元，令 $\beta=\alpha^{\frac{4^m-1}{3n}}$，则 $\beta$ 为 $3n$ 次本原单位根，其中 $m$ 为 4 模 $3n$ 的乘法阶，即 $m=\mathrm{ord}_{3n}(4)$。

**引理 1**[2,12]　假定 $\gcd(3,n)=1$，设 $C=\langle g(x)\rangle$为 $G_F(4)$上长为 $n$ 的 $\omega$-常循环码。若 $g(x)$的根为 $\{\beta^{1+3i}|0\leqslant i\leqslant\delta-2\}$，则 $C$ 的最小距离 $d\geqslant\delta$。

设 $m_i(x)$表示 $G_F(4)$上 $\beta^i$ 的极小多项式。用 $i \bmod 3n$ 表示在集合 $\{0,1,2,\cdots,3n-1\}$中与 $i \bmod 3n$同余的唯一整数。记

$$m_i(x)=m_{i \bmod 3n}(x),$$

对于整数 $\delta\geqslant 2$，定义：

$$g_{(n,\delta,1)}(x)=\mathrm{lcm}(m_1(x),m_4(x),\cdots,m_{1+3(\delta-2)}(x)) \quad (1)$$

其中，lcm 表示多项式的最小公倍数。设 $C(n,\delta,1)$表示生成多项式为 $g_{(n,\delta,1)}(x)$且长为 $n$ 的 $\omega$-常循环码，由引理 1，码 $C(n,\delta,1)$的最小距离至少为 $\delta$。

设 $Z_{3n}=\{0,1,2,\cdots,3n-1\}$。$\forall s\in Z_{3n}$，4 模 $3n$ 含 $s$ 的分圆陪集定义为：

$$C_s=\{s,4s,4^2s,\cdots,4^{d_s-1}s\}\bmod 3n\subseteq Z_{3n},$$

其中，$d_s$ 为满足 $s4^{d_s}\equiv s \bmod 3n$ 的最小正整数，且 $C_s$ 中有 $d_s$ 个元素。

设 $T=\{1+3i|0\leqslant i\leqslant n-1\}\subseteq 3n$，$C_s$ 中最小整数称为 $C_s$ 的陪集首。对于 $\forall s\in Z_{3n}$，显然有 $T\cap C_s=C_s$ 或 $\{0\}$。

设 $\Gamma_{(n,4)}$为 $T\cap C_s=C_s$ 所有陪集首的集合。$\forall s,t\in\Gamma_{(n,4)}$，$s\neq t$，有 $C_s\cap C_t=\{0\}$且

$$\bigcup_{s\in\Gamma_{(n,4)}}C_s=T \quad (2)$$

$\beta^s$ 在 $G_F(4)$上的极小多项式 $m_s(x)$可表示为：

$$m_s(x)=\prod_{i\in C_s}(x-\beta^i)\in G_F(4)[x],$$

且 $m_s(x)$在 $G_F(4)$上不可约。由(2)式可知 $x^n-\omega=\prod\limits_{s\in\Gamma_{(n,4)}}m_s(x)$为 $x^n-\omega$ 在 $G_F(4)$上不可约因子标准分解。

设 $f(x)=f_tx^t+f_{t-1}x^{t-1}+\cdots+f_1x+f_0$ 为 $G_F(4)$上的多项式，$f_t\neq 0$ 且 $f_0\neq 0$。$f(x)$的互反多项式 $f^*(x)$定义为 $f^*(x)=f_0^{-1}x^tf(x^{-1})$。

**定义 2**　$\bar{f}(x)=f_t^2x^t+f_{t-1}^2x^{t-1}+\cdots+f_1^2x+f_0^2$。

容易验证 2 个运算“$*$”和“—”是可交换的，即 $(\bar{f}^*)(x)=(\bar{f})^*(x)$。

**引理 2**[8]　设 $C$ 为 $G_F(4)$上长为 $n$ 且生成多项式为 $g(x)$的 $\omega$-常循环码，则 $C$ 为厄米特 LCD 码当且仅当 $g(x)=\bar{g}^*(x)$。

**证明**　$C$ 是厄米特 LCD 码等价于 $C=\langle g(x)\rangle$并且 $C^{\perp_H}=\langle h(x)\rangle$，其中，$h(x)=(x^n-\omega)/g(x)$。可以得到 $g(x)=\bar{g}^*(x)$且 $h(x)=\bar{h}^*(x)$。

## 2　四元厄米特 LCD 常循环码的结构

因为多项式 $x^n-\omega$ 在共轭互反下是不变的，所以对于 $x^n-\omega\in G_F(4)[x]$的任一首一不可约因子 $f(x)$，$\bar{f}^*(x)$也是 $x^n-\omega$ 的首一不可约因子。设 $x^n-\omega$ 可以分解为：

$$x^n-\omega=e_1(x)e_2(x)\cdots e_u(x)f_1(x)\bar{f}_1^*(x)\times f_2(x)\bar{f}_2^*(x)\cdots f_v(x)\bar{f}_v^*(x) \quad (3)$$

其中，$e_i(x)$、$f_j(x)$为 $G_F(4)$上首一不可约多项式，且 $e_i(x)=\bar{e}_i^*(x)$，$i=1,2,\cdots,u$。

**定理 1**　设 $C$ 为 $G_F(4)$上长为 $n$ 的 $\omega$-常循环码，且生成多项式为：

$$g(x)=e_1(x)^{a_1}e_2(x)^{a_2}\cdots e_u(x)^{a_u}f_1(x)^{b_1}\times\bar{f}_1^*(x)^{c_1}f_2(x)^{b_2}\bar{f}_2^*(x)^{c_2}\cdots f_v(x)^{b_v}\bar{f}_v^*(x)^{c_v},$$

其中，$a_i,b_j,c_j\in\{0,1\}$，则 $C$ 为四元厄米特 LCD 码当且仅当 $b_j=c_j$，$j=1,2,\cdots,v$。因此，长为 $n$

的四元厄米特LCD常循环码总数为$2^{u+v}$。

**证明** 由引理1和引理2可得。

定理1指出长为$n$的四元厄米特LCD常循环码的个数由(3)式决定,指明四元厄米特LCD常循环码定义集的结构特点,它应具有以下类型:

$$S=\{s\in T:g(\beta^S)=0\},$$

其中,$g(x)=\prod_i e_i(x)\prod_j f_j(x)\overline{f}_j^*(x)$。

类似于文献[11]中定理4,可以得到下面定理。

**定理**2 设$C$是$G_F(4)$上长为$n$的$\omega$-常循环码,其生成多项式为$g(x)$,则$C$为厄米特LCD码,当且仅当下面条件之一成立。

(1) 对于$C$的定义集$S$,$S=-2S$,其中,$-2S=\{-2s:s\in S\}$。

(2) 对于每个$g(x)$的根$\beta$,$\beta^{-2}$也是$g(x)$的一个根。

**定理**3 长为$n$的四元$\omega$-常循环码都是厄米特LCD码充要条件为$-1$是$2 \bmod 3n$的奇幂。

**证明** 一方面,设$-1\equiv 2^{2t+1}(\bmod 3n)$,$t\geqslant 0$。因为对于每个$a\in T$有$-a\equiv a\cdot 2^{2t+1}(\bmod 3n)$且$-2a\equiv a\cdot 2^{2t+2}\equiv a\cdot 4^{t+1}(\bmod 3n)$,所以$-2a\in C_a$,即$f_j(x)$不在(3)式中出现。由定理1可知,在$G_F(4)$上每个长为$n$的$\omega$-常循环码是厄米特LCD码。

另一方面,设$\beta$为$3n$次本原单位根,$m_1(x)$表示$G_F(4)$上$\beta$的极小多项式。设$C$为$G_F(4)$上长为$n$且生成多项式为$m_1(x)$的$\omega$-常循环码,若$C$是厄米特LCD码,则$-2\in C_1$且$-2\equiv 4^t(\bmod 3n)$,其中,$1\leqslant t\leqslant m-1$,$3n$是奇数,因此,$-1\equiv 2^{2t-1}(\bmod 3n)$。

## 3 长为$(4^m-1)/3$的四元厄米特LCD码

**引理** 3[7,13] 设$n$为一个正奇数,且$4^{\lfloor m/2\rfloor}/3<n<(4^m-1)/3$,$m=\mathrm{ord}_{3n}(4)$,对$\forall s\in\Gamma_{(n,4)}$,当$1\leqslant s\leqslant 3n\cdot 4^{\lfloor m/2\rfloor}/(4^m-1)$,则$C_s=T\cap C_s=\{s\cdot 4^i \bmod 3n:0\leqslant i\leqslant m-1\}$含有$m$个元素。而且,若$s\not\equiv 0(\bmod 4)$,则$s$是$C_s$的一个陪集首。

由定理3,设$n=(2^{2t+1}+1)/3$,易证$m=2t+1$。由引理3,1是4模$2^{2t+1}+1$的分圆陪集的陪集首。

下面通过常循环BCH码构造长为$n=(4^m-1)/3$的四元厄米特LCD码且分析其参数。设

$$g(x)=\mathrm{lcm}(g(n,\delta,1),m_{3n-2[1+3(\delta-2)]}(x),$$
$$m_{3n-2[1+3(\delta-3)]}(x),\cdots,m_{3n-8}(x),m_{3n-2}(x)) \quad (4)$$

其中

$$g(n,\delta,1)=\mathrm{lcm}(m_1(x),m_4(x),\cdots,$$
$$m_{1+3(\delta-3)}(x),m_{1+3(\delta-2)}(x))。$$

**引理** 4[11] 设$m\geqslant 2$为一整数且$\overline{m}=\lceil m/2\rceil$。当$1\leqslant i\leqslant 4^{\overline{m}}$且$4\nmid i$时,若任一$i$在此范围内,则$i$是分圆陪集$C_i$的陪集首且$|C_i|=m$。

下面的引理是关于4模$3n$的分圆陪集的性质。

**引理** 5[11] 设$n=(4^m-1)/3$,$i$表示4模$3n$的分圆陪集$C_i$的陪集首,则有:

(1) $|C_{n-2i}|=|C_i|$。

(2) $C_{n-2i}=C_{n-2j}$当且仅当$C_i=C_j$。

(3) $C_{n-8i}=C_{n-2i}$。

设$C$为$G_F(4)$上长为$n$且生成多项式为$g(x)$的$\omega$-常循环码,$C$的定义集可以表示成:

$$S=\bigcup_{\substack{0\leqslant a\leqslant\delta-2\\ 1+3a\not\equiv 0 \bmod 4}}(C_{1+3a}\cup C_{3n-2(1+3a)})。$$

记

$$J^+(\delta)=\bigcup_{\substack{0\leqslant a\leqslant\delta-2\\ 1+3a\not\equiv 0 \bmod 4}}C_{1+3a},$$
$$J^-(\delta)=\bigcup_{\substack{0\leqslant a\leqslant\delta-2\\ 1+3a\not\equiv 0 \bmod 4}}C_{3n-2(1+3a)}。$$

显然

$$-2(1+3a)\equiv 3n-2(1+3a)\bmod 3n,$$
$$-2[3n-2(1+3a)]\equiv 4(1+3a)\bmod 3n。$$

因此,$S=-2S$。由定理2,$C$是$G_F(4)$上厄米特LCD码。

**定理**4 设$m\geqslant 2$,$\overline{m}=\lceil m/2\rceil$,且$2\leqslant\delta\leqslant(4^{\overline{m}}-1)/3+2$,可以得到如下结论:

(1) $|J^+(\delta)|=|J^-(\delta)|=\lceil(3\delta-5)/4\rceil m$。

(2) 当$m$为奇数时,有

$$|J^+(\delta)\cap J^-(\delta)|=$$
$$\begin{cases}0, & 2\leqslant\delta\leqslant\lfloor 2^m-3)/3\rfloor+2;\\ m, & \lfloor(2^m-3)/3\rfloor+3\leqslant\delta\leqslant(2^{m+1}-1)/3+2。\end{cases}$$

(3) 当$m$为偶数时,有

$$|J^+(\delta)\cap J^-(\delta)|=0。$$

**证明** 由引理5,$C_{3n-2(1+3a)}\neq C_{3n-2(1+3b)}$当且仅当$C_{1+3a}\neq C_{1+3b}$。由引理4,对于每个整数$1+3a$,当$1\leqslant 1+3a\leqslant 4^m$且$4\nmid 1+3a$,则$1+3a$是$C_{1+3a}$的陪集首。于是有:

$$|J^+(\delta)|=\lceil(3\delta-5)/4\rceil m,$$

同理,有

$$|J^-(\delta)|=\lceil(3\delta-5)/4\rceil m。$$

当$m$为奇数时,$\overline{m}=(m+1)/2$。假设

$$a\in J^+(\delta)\cap J^-(\delta),$$

则存在$i$、$j$,$0\leqslant i,j\leqslant\delta-2$,使得:

$$a\in C_{1+3i}=C_{3n-2(1+3j)},$$

故有:

$$1+3i\equiv -2(1+3j)4^l \bmod(4^m-1),$$

即

$$1+3i+(1+3j)2^{2l+1}\equiv 0 \bmod(4^m-1) \quad (5)$$

设 $1+3i$,$1+3j$ 的 2−adic 展开分别为:

$$1+3i=i_m2^m+i_{m-1}2^{m-1}+\cdots+i_12+i_0,$$

$$1+3j=j_m2^m+j_{m-1}2^{m-1}+\cdots+j_12+j_0,$$

$$0\leqslant i_k,j_k\leqslant 1,0\leqslant k\leqslant m,(i_0,i_1)\neq(0,0),$$

$$(j_0,j_1)\neq(0,0)。$$

**情况** 1　当 $1\leqslant l\leqslant(m-3)/2$ 时,$0<1+3i+(1+3j)2^{2l+1}<4^m-1$,则

$$1+3i+(1+3j)2^{2l+1}\equiv 0 \bmod(4^m-1)$$

不成立。

**情况** 2　当 $l=(m-1)/2$ 时,可证明 $1+3i+(1+3j)2^{2l+1}\equiv\Delta \bmod(4^m-1)$,其中

$$\Delta=j_{m-1}2^{2m-1}+\cdots+j_12^{m+1}+(j_0+i_m)2^m+i_{m-1}2^{m-1}+\cdots+i_12+(i_0+j_m)。$$

注意 $0<\Delta<6n$,由(5)式得 $\Delta=3n$。因此,$j_{m-1}=\cdots=j_1=j_0+i_m=i_{m-1}=\cdots=i_1=i_0+j_m=1$,则 $i_m=u$,$j_m=v$,$i_0=1-v$,$j_0=1-u$,其中,$u,v=0,1$。因此,$1+3i=(u+1)2^m-v-1$,$1+3j=(v+1)2^m-u-1$。

**情况** 3　当 $(m+1)/2\leqslant l\leqslant m-1$ 时,有

$$m+2\leqslant 2l+1\leqslant 2m-1。$$

令 $2l+1=m+\varepsilon$,$2\leqslant\varepsilon\leqslant m-1$,则 $1+3i+(1+3j)2^{2l+1}\equiv\Delta \bmod(4^m-1)$,其中

$$\Delta=j_{m-\varepsilon-1}2^{2m-1}+\cdots+j_12^{m+\varepsilon+1}+j_02^{m+\varepsilon}+i_m2^m+\cdots+i_{\varepsilon+1}2^{\varepsilon+1}+(i_\varepsilon+j_m)2^\varepsilon+\cdots+(i_1+j_{m-\varepsilon+1})2+(i_0+j_{m-\varepsilon})。$$

$\Delta$ 的 2-adic 展开中 $2^{m+1}$ 的系数为 0。因此,$0<\Delta<3n$。这种情况下(5)式是不成立的。

情况 2 中,$i=i_w$ 且 $j=j_w$。集合 $L$ 为:

$$L=\left\{(u,v):i_w\leqslant\delta-2,j_w\leqslant\delta-2,\ 1+3i_w=(u+1)2^m-v-1,\ 1+3j_w=(v+1)2^m-u-1\right\}。$$

注意情况 1～情况 3 包含全部使 $C_{1+3i}=C_{3n-2(1+3j)}$ 的可能数对 $(1+3i,1+3j)$,$0\leqslant i,j\leqslant\delta-2$,其中,$2\leqslant\delta\leqslant(2^{m+1}-1)/3+2$。于是有:

$$J^+(\delta)\cap J^-(\delta)=\bigcup_{(u,v)\in L}C_{1+3i_w} \quad (6)$$

由引理 4,$1+3i_w$ 为陪集首,由引理 5,$C_{3n-2(1+3a)}\neq C_{3n-2(1+3b)}$ 当且仅当 $C_{1+3a}\neq C_{1+3b}$。因此(6)式中并没有交集,则有:

$$|J^+(\delta)\cap J^-(\delta)|=|L|m。$$

因为 $u,v=0,1$,所以 $1+3i_w$、$1+3j_w$ 都分别可能等于 $2^m-1$、$2^m-2$、$2^{m+1}-1$、$2^{m+1}-2$ 这 4 种情况。因为 $2^m-2$、$2^{m+1}-1$、$2^{m+1}-2$ 不具有 $1+3i$ 的形式,所以舍去。于是,$1+3i_w=2^m-1$,$1+3j_w=2^m-1$。

当 $1+3i_w<2^m-1$ 时,即 $1+3(\delta-2)<2^m-1$,$|L|=0$。于是有:

$$|L|=\begin{cases}0,\ 2\leqslant\delta\leqslant\lfloor(2^m-3)/3\rfloor+2;\\ 1,\ \lfloor(2^m-3)/3\rfloor+3\leqslant\delta\leqslant(2^{m+1}-1)/3+2。\end{cases}$$

当 $m$ 为偶数时可用同样的方法证明。

**定理** 5　设 $m\geqslant 2$,$\overline{m}=\lceil m/2\rceil$,$2\leqslant\delta\leqslant(4^{\overline{m}}-1)/3+2$,$C$ 是 $G_F(4)$ 上长为 $(4^m-1)/3$ 的 $\omega$-常循环码,其生成多项式如(4)式所示,则 $C$ 是 $G_F(4)$ 上厄米特 LCD 码。

(1) 当 $m$ 为奇数时,$C$ 的参数为 $[(4^m-1)/3,k,d]$,其中,$d\geqslant\delta+\lfloor 1+3(\delta-2)/6\rfloor$。

$$k=\begin{cases}(4^m-1)/3-2\lceil 3\delta-5/4\rceil m,\\ \quad 2\leqslant\delta\leqslant\lfloor(2^m-3)/3\rfloor+2;\\ (4^m-1)/3-2\lceil(3\delta-5)/4\rceil m+m,\\ \quad\lfloor(2^m-3)/3\rfloor+3\leqslant\delta\leqslant(2^{m+1}+5)/3。\end{cases}$$

(2) 当 $m$ 为偶数时,$C$ 的参数为 $[(4^m-1)/3,k,d]$,其中:$d\geqslant\delta+\lfloor[1+3(\delta-2)]/6\rfloor$;$k=(4^m-1)/3-2\lceil(3\delta-5)/4\rceil m$。

**证明**　由定义 1,$C$ 的生成多项式 $g(x)$ 的次数等于 $|J^+(\delta)|+|J^-(\delta)|-|J^+(\delta)\cap J^-(\delta)|$,维数 $k=(4^m-1)/3-\deg(g(x))$,则由定理 4 可得。

若 $2|i$,则 $C_{3n-2i}=C_{3n-i/2}$,则集合 $\{3n-\lfloor 1+3(\delta-2)/2\rfloor,\cdots,3n-2,3n+1,3n+4,\cdots,3n+1+3(\delta-2)\}$ 是 $C$ 的定义集。最小距离由引理 1 可得。

**例** 1　设 $m=3$,$\delta=5$,$C$ 是 $G_F(4)$ 上长为 21 的 $\omega$-常循环码,其生成多项式为:

$$g(x)=m_1(x)m_7(x)m_{10}(x)m_{61}(x)m_{43}(x)=x^{15}+x^{14}+\omega x^{13}+x^{12}+x^{11}+x^9+\omega x^8+\omega x^7+\omega^2x^6+\omega^2x^4+\omega^2x^3+\omega x^2+\omega^2x+\omega^2,$$

则 $C$ 是 $G_F(4)$ 上参数为 $[21,6,12]$ 的厄米特 LCD 码。

**例** 2　设 $m=3$,$\delta=2$,$C$ 是 $G_F(4)$ 上长为 21 的 $\omega$-常循环码,其生成多项式为:

$$g(x)=m_1(x)m_{61}(x)=x^6+\omega^2x^5+x^4+\omega^2x^2+x+\omega^2,$$

则 $C$ 是 $G_F(4)$ 上参数为[21,15,5]的厄米特LCD码。

**例3** 设 $m=4,\delta=4$,$C$ 是 $G_F(4)$ 上长为85的$\omega$-常循环码,其生成多项式为:

$$g(x)=m_1(x)m_7(x)m_{253}(x)m_{241}(x)=x^{16}+x^{15}+\omega x^{14}+x^{12}+\omega x^{11}+\omega x^9+\omega^2 x^8+x^7+x^5+\omega x^4+x^2+\omega x+\omega,$$

则 $C$ 是 $G_F(4)$ 上参数为[85,69,5]的厄米特LCD码。

## 4 结 论

本文构造了四元厄米特互补对偶常循环码,并分析它们的参数。确定长度为 $n=(4^m-1)/3$ 的厄米特LCD常循环码的维数,给出了它们最小距离的下界。本文仅分析了长度为 $n=(4^m-1)/3$ 的四元厄米特互补对偶常循环码的参数,其他长度也有待进一步探讨。

## [参 考 文 献]


[1] 刘春颖. 几类特殊的常循环码[D]. 武汉:华中师范大学,2012.

[2] AYDIN N, SIAP I, RAY-CHAUDHURI D K. The structure of 1-generator quasi-twisted codes and new linear codes[J]. Designs, Codes and Cryptography, 2001, 24(3): 313-326.

[3] MASSEY J L. Linear codes with complementary duals[J]. Discrete Mathematics, 1992, 106(107): 337-342.

[4] CARLET C, GUILLEY S. Complementary dual codes for counter-measures to side-channel attacks[C]//The 4th International Castle Meeting Coding Theory and Applications, CIM Series in Mathematical Sciences. [S. l.: s. n.], 2014: 97-105.

[5] LI C J, DING C S, LI S X. LCD cyclic codes over finite fields[J]. IEEE Transactions on Information Theory, 2017, 63(7): 4344-4356.

[6] LI S X, LI C J, DING C S, et al. Two families of LCD BCH codes[J]. IEEE Transactions on Information Theory, 2017, 63(9): 5699-5717.

[7] ZHU S X, PANG B B, SUN Z H. The reversible negacyclic codes over finite fields[J]. Journal of Systems Science and Complexity, 2018, 31(4): 1065-1077.

[8] GÜNERI C, ÖZKAYA B, SOLÉ P. Quasi-cyclic complementary dual codes[J]. Finite Fields and Their Applications, 2016, 42: 67-80.

[9] BOONNIYOMA K, JITMAN S. Complementary dual subfield linear codes over finite fields[J]. Thai Journal of Mathematics, 2016(Special Issue ICMSA2015): 133-152.

[10] CARLET C, MESNAGER S, TANG C, et al. Euclidean and Hermitian LCD MDS codes[J]. Designs Codes and Cryptography, 2018, 86(11): 2605-2618.

[11] LI C J. Hermitian LCD codes from cyclic codes[J]. Designs Codes and Cryptography, 2018, 86(10): 2261-2278.

[12] MACWILLIAMS F J, SLOANE N J A. The theory of error-correcting codes[M]. Amsterdam: Publishing Company, 1977.

[13] ALY S A, KLAPPENECKER A, SARVEPALLI P K. On quantum and classical BCH codes[J]. IEEE Transactions on Information Theory, 2007, 53(3): 1183-1188.


(责任编辑 张 锴)

(上接第41页)


[10] ABEL G G, WEIJER J, BENGIO Y. Image-to-image translation for cross-domain disentanglement[J]. Advances in Neural Information Processing Systems, 2018, 31: 1287-1298.

[11] GOODFELLOW I, JEAN P A, MIRZA M, et al. Generative adversarial nets[J]. Advances in Neural Information Processing Systems, 2014, 27: 2672-2680.

[12] ABERMAN K, LI P, LISCHINSKI D, et al. Skeleton-aware networks for deep motion retargeting[J]. ACM Transactions on Graphics, 2020, 39(4): 62: 1-14.

[13] KINGMA D P, BA J. Adam: a method for stochastic optimization [EB/OL]. [2022-12-14]. https://arxiv.org/pdf/1412.6980.pdf.

[14] TAK S Y, GO H S. Example guided inverse kinematics[J]. Journal of The Korea Computer Graphics Society, 1999, 5(1): 11-17.


(责任编辑 李 凯)