一种四元厄米特 LCD 码与厄米特自正交码的构造方法

钱 毅[1],李 平[1],唐永生[2]
(1. 合肥工业大学数学学院,安徽合肥 230009;2. 合肥师范学院数学与统计学院,安徽合肥 230601)

摘 要: 有限域上线性互补对偶(LCD)码具有良好的结构和性质,并在双用户加法器信道中得到了广泛的应用. 自正交码是编码理论中一类重要的线性码,常被用于构造量子纠错码. 本文根据有限域上线性码是厄米特 LCD 码或厄米特自正交码的判定条件,通过选取合适的定义集,构造出了四类四元厄米特 LCD 码和厄米特自正交码. 同时,本文还研究了这四类线性码的厄米特对偶码,并得到了一些四元最优线性码.

关键词: 线性码; 四元码; 最优码; 厄米特 LCD 码; 厄米特自正交码; 厄米特对偶码
中图分类号: TN911.22 **文献标识码:** A **文章编号:** 0372-2112 (2020)03-0577-05
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2020.03.022

A Construction Method of Quaternary Hermitian LCD Codes and Hermitian Self-Orthogonal Codes

QIAN Yi[1], LI Ping[1], TANG Yong-sheng[2]
(1. *School of Mathematics, Hefei University of Technology, Hefei, Anhui* 230009, *China*;
2. *School of Mathematics and Statistics, Hefei Normal University, Hefei, Anhui* 230601, *China*)

Abstract: Linear complementary dual (LCD) codes over finite fields have good structure and properties, and are widely used in two-user adder channels. Self-orthogonal codes are important linear codes in coding theory and are often used to construct quantum error-correcting codes. In this paper, we consider that linear codes over finite fields are Hermitian LCD codes or Hermitian self-orthogonal codes. By selecting the appropriate set of definitions, four kinds of quaternary Hermitian LCD codes and Hermitian self-orthogonal codes are constructed. At the same time, Hermitian dual codes of these four kinds of linear codes are studied and some quaternary optimal linear codes are obtained.

Key words: linear codes; quaternary codes; optimal codes; Hermitian linear complementary dual (LCD) codes; Hermitian self-orthogonal codes; Hermitian dual codes

1 引言

自正交码是包含自对偶码为子类的一类重要码. 随着量子纠错码的发展,自正交码作为纠错码理论研究的一个热点受到广泛的关注[1~3]. 文献[2]指出量子码构造的关键点是构造参数好的厄米特自正交码,因此厄米特自正交码的构造受到广泛的关注. 文献[4]研究了四元域上的厄米特自正交码,并构造了参数好的量子纠错码.

LCD 码具有丰富的应用前景,Carlet 等人在文献[5]中证明有限域上的 LCD 码可用于应对双通道攻击. LCD 码还具有良好的性质与结构,Massey 在文献[6]中第一次正式提出 LCD 码的概念,并证明存在渐进好的 LCD 码. 随后,Yang 等人给出判断有限域上循环码是 LCD 码的充要条件[7]. Sendrier 证明 LCD 码能达到渐进的 Gilbert-Varshamov 界[8].

Güneri 等人证明厄米特 LCD 码是渐进好码[9]. 这些结果激发学者们研究有限域上 LCD 码的极大兴趣. 最近,Carlet 等人在文献[10]和[11]中给出利用线性码构造 LCD 码的一般方法,并证明 $F_q(q>3)$ 上任意线性

收稿日期:2019-02-25;修回日期:2019-06-20;责任编辑:覃怀银
基金项目:国家自然科学基金(No. 61572186, No. 61972126, No. 61572168);中央高校基本科研业务费专项资金项目(No. PA2019GDZC0097);安徽省自然科学基金面上项目 (No. 1808085MA15);安徽省教育厅高校省级自然科学重点项目(No. KJ2018A0497)

码等价于一个欧几里得 LCD 码,$F_{q2}(q>2)$上任意线性码等价于一个厄米特 LCD 码. 自此之后,LCD 码研究的重点在于构造二元 LCD 码、三元 LCD 码和四元厄米特 LCD 码. Zhou 等人在文献[12]中提出一种构造 F_p 上 LCD 码与自正交码的方法,其中 p 为素数,并具体地构造了四类二元 LCD 码和自正交码. 受文献[12]的启发,本文研究了 F_{p2} 上厄米特 LCD 码和厄米特自正交码. 基于 F_{p2} 上线性码是厄米特 LCD 码和厄米特自正交码的充要条件,构造了四类四元厄米特 LCD 码和厄米特自正交码.

2 基础知识

设 p 是一个素数,F_{p2} 是 p^2 阶有限域. 设 F_{p2}^n 是域 F_{p2} 上 n 维行向量空间. 对任意 $x\in F_{p2}$,x 的共轭定义为 $\bar{x}=x^p$. 设向量 $\boldsymbol{x}=(x_0,x_1,\cdots,x_{n-1})$,$\boldsymbol{x}$ 的共轭定义为 $\bar{\boldsymbol{x}}=(\bar{x}_0,\bar{x}_1,\cdots,\bar{x}_{n-1})$. 下面设 $\boldsymbol{x}=(x_0,x_1,\cdots,x_{n-1})$,$\boldsymbol{y}=(y_0,y_1,\cdots,y_{n-1})\in F_{p2}^n$,它们的内积定义为

$$\boldsymbol{x}\cdot\boldsymbol{y}=x_0y_0+x_1y_1+\cdots+x_{n-1}y_{n-1} \tag{1}$$

它们的厄米特内积定义为 $\boldsymbol{x}\cdot\bar{\boldsymbol{y}}$. 如果 $\boldsymbol{x}\cdot\bar{\boldsymbol{y}}=0$,则称 $\boldsymbol{x}$ 和 $\boldsymbol{y}$ 是厄米特自正交的.

一个 p^2 元$[n,k]$线性码是 F_{p2}^n 的一个 k 维子空间. 设 C 是一个 p^2 元$[n,k]$线性码,则 C 中存在 k 个 F_{p2} 线性无关的向量 $\boldsymbol{c}_i$,$1\leqslant i\leqslant k$. 设

$$\boldsymbol{G}=[\boldsymbol{c}_1^{\mathrm{T}},\boldsymbol{c}_2^{\mathrm{T}},\cdots,\boldsymbol{c}_k^{\mathrm{T}}]^{\mathrm{T}} \tag{2}$$

其中 $\boldsymbol{c}_i^{\mathrm{T}}$ 表示向量 $\boldsymbol{c}_i$ 的转置. 矩阵 $\boldsymbol{G}$ 称为码 C 的生成矩阵,码 C 则称为由矩阵 $\boldsymbol{G}$ 生成的线性码. 码 C 的厄米特对偶码定义为

$$C^{\perp\mathrm{H}}=\{\boldsymbol{y}\in F_{p2}^n\mid\boldsymbol{x}\cdot\bar{\boldsymbol{y}}=0,\forall\boldsymbol{x}\in C\} \tag{3}$$

则 $C^{\perp\mathrm{H}}$ 是一个 p^2 元$[n,n-k]$线性码. 如果 $C\cap C^{\perp\mathrm{H}}=\{\boldsymbol{0}\}$,则称 C 为厄米特 LCD 码. 如果 $C\cap C^{\perp\mathrm{H}}=C$,则称 C 为厄米特自正交码.

设集合 $D=\{\boldsymbol{g}_1,\boldsymbol{g}_2,\cdots,\boldsymbol{g}_n\}\subseteq F_{p2}^k$,由 D 定义一个矩阵 $\boldsymbol{G}=[\boldsymbol{g}_1^{\mathrm{T}},\boldsymbol{g}_2^{\mathrm{T}},\cdots,\boldsymbol{g}_n^{\mathrm{T}}]$,则 $\boldsymbol{G}$ 是 F_{p2} 上一个 $k\times n$ 矩阵. 定义码 $C(D)$ 是由矩阵 $\boldsymbol{G}$ 生成的 p^2 元线性码,即

$$C(D)=\{(\boldsymbol{a}\cdot\boldsymbol{g}_1,\boldsymbol{a}\cdot\boldsymbol{g}_2,\cdots,\boldsymbol{a}\cdot\boldsymbol{g}_n)\mid\boldsymbol{a}\in F_{p2}^k\} \tag{4}$$

称集合 D 为线性码 $C(D)$ 的定义集. 如果矩阵 $\boldsymbol{G}$ 的秩 $\mathrm{Rank}(\boldsymbol{G})=k$,则码 $C(D)$ 是一个 p^2 元$[n,k]$线性码. 矩阵 $\boldsymbol{G}$ 的厄米特共轭定义为

$$\bar{\boldsymbol{G}}=[\bar{\boldsymbol{g}}_1^{\mathrm{T}},\bar{\boldsymbol{g}}_2^{\mathrm{T}},\cdots.\bar{\boldsymbol{g}}_n^{\mathrm{T}}] \tag{5}$$

即对矩阵 $\boldsymbol{G}$ 中的每个元素共轭. 用 $\boldsymbol{G}^\dagger$ 表示矩阵 $\boldsymbol{G}$ 的厄米特共轭的转置. 由文献[11],命题[1]和文献[13],码 $C(D)$ 是厄米特 LCD 码或厄米特自正交码有如下判定条件.

引理 1 码 $C(D)$ 是一个码长 n 的 p^2 元厄米特 LCD 码当且仅当 $\mathrm{Rank}(\boldsymbol{G})=\mathrm{Rank}(\boldsymbol{G}\boldsymbol{G}^\dagger)$. 码 $C(D)$ 是一个码长 n 的 p^2 元厄米特自正交码当且仅当 $\boldsymbol{G}\boldsymbol{G}^\dagger=0$.

3 主要结果

设 $F_4=\{0,1,w,\bar{w}\}$,其中 $\bar{w}=w+1$. 设 k 和 t 是两个正整数且 $1\leqslant t\leqslant k-1$,定义 D_t 是 F_k^4 上非零位数为 t 且第一个非零位上的元素是 1 的全体向量的集合,则 D_t 的阶 $n_t=\binom{k}{t}\cdot 3^{t-1}$,其中 $\binom{k}{t}$ 表示组合数,即从 k 个不同元素中选取 t 个进行组合的个数. 定义集合 $D_{\leqslant t}=\bigcup_{i=1}^{t}D_i$,则 $D_{\leqslant t}$ 的阶可写作 $\sum_{i=1}^{t}\binom{k}{i}\cdot 3^{i-1}$. 设 $\boldsymbol{1}$ 表示 F_4^k 上分量全是 1 的向量,定义 $\bar{D}_t=D_t\cup\{\boldsymbol{1}\}$ 和 $\bar{D}_{\leqslant t}=D_{\leqslant t}\cup\{\boldsymbol{1}\}$. 下文,通过以上四个集合,构造厄米特 LCD 码和厄米特自正交码.

3.1 定义集为 D_t 的四元线性码

设 $D_t=\{\boldsymbol{g}_1,\boldsymbol{g}_2,\cdots,\boldsymbol{g}_{n_t}\}$,$\boldsymbol{G}_t=[\boldsymbol{g}_1^{\mathrm{T}},\boldsymbol{g}_2^{\mathrm{T}},\cdots,\boldsymbol{g}_{n_t}^{\mathrm{T}}]$. 设码 $C(D_t)$ 是由 $\boldsymbol{G}_t$ 生成的四元线性码.

引理 2 设 $k\geqslant 2$. 对任意 $1\leqslant t\leqslant k-1$,$\mathrm{Rank}(\boldsymbol{G}_t)=k$.

证明 当 $t=1$ 时,结论显然成立. 下面我们假设 $t\geqslant 2$.

记矩阵 $\boldsymbol{G}_t$ 的行向量为 $\boldsymbol{i}_1,\boldsymbol{i}_2,\cdots,\boldsymbol{i}_k\in F_4^k$. 假设向量 $\boldsymbol{i}_1,\boldsymbol{i}_2,\cdots,\boldsymbol{i}_k$ 线性相关,则在 F_4 中存在不全为零的 $a_1,a_2,\cdots,a_k$ 使得 $a_1\boldsymbol{i}_1+a_2\boldsymbol{i}_2+\cdots+a_k\boldsymbol{i}_k=\boldsymbol{0}$. 不妨设矩阵 $\boldsymbol{G}_t$ 的前 t 列为

$$(\underbrace{1,\cdots,1}_{t},0,\cdots,0)^{\mathrm{T}},(1,w,\underbrace{1,\cdots,1}_{t-2},0,\cdots,0)^{\mathrm{T}},\cdots,(\underbrace{1,\cdots,1}_{t-1},w,0,\cdots,0)^{\mathrm{T}},$$

则

$$\begin{cases}a_1+a_2+\cdots+a_t=0\\ a_1+wa_2+\cdots+a_t=0\\ \quad\vdots\\ a_1+a_2+\cdots+wa_t=0\end{cases} \tag{6}$$

由式(6)得 $a_1=a_2=\cdots=a_t=0$. 同理可证 $a_{t+1}=a_{t+2}=\cdots=a_k=0$. 综合上述,可得 $a_1=a_2=\cdots=a_k=0$,这与假设矛盾.

引理 3 设 $k\geqslant 2$,$1\leqslant t\leqslant k-1$,以及 $\boldsymbol{M}=\boldsymbol{G}_t\boldsymbol{G}_t^\dagger=(m_{ij})_{k\times k}$.

(1) 当 $t=1$ 时,$\boldsymbol{M}=\boldsymbol{E}$,其中 $\boldsymbol{E}$ 表示 F_4 上 k 阶单位矩阵.

(2) 当 $t\geqslant 2$ 时,对任意的 $1\leqslant i,j\leqslant k$,

$$m_{ij}=\begin{cases}\binom{k-1}{t-1}(\mathrm{mod}2), & i=j\\ 0, & i\neq j\end{cases} \tag{7}$$

证明 (1) 当 $t=1$ 时,结论显然成立.

(2)对任意的 $1\leqslant i,j\leqslant k$,记矩阵 $\boldsymbol{G}_t$ 的第 i 行为 $\boldsymbol{c}_i=(c_{i1},c_{i2},\cdots,c_{in_t})$,则

$$m_{ij}=\boldsymbol{c}_i\cdot\bar{\boldsymbol{c}}_j=c_{i1}c_{j1}^2+c_{i2}c_{j2}^2+\cdots+c_{in_t}c_{jn_t}^2 \tag{8}$$

由矩阵 $\boldsymbol{M}$ 定义得 $m_{ij}=m_{ji}$.

当 $i=j$ 时,因为 $c_{ij}\in F_4$,所以 $c_{ij}^3=1$ 或 0. 由此推出,m_{ij} 等于矩阵 $\boldsymbol{G}_t$ 第 i 行中非零元的数目. 根据 $\boldsymbol{G}_t$ 的定义,矩阵 $\boldsymbol{G}_t$ 每一行中非零元数目是相等. 又因为矩阵 $\boldsymbol{G}_t$ 中非零元的数目为 $t\cdot n_t$,所以

$$m_{ii}=\frac{t\cdot n_t}{k}=\binom{k-1}{t-1}(\bmod 2)$$

当 $1\leqslant i<j\leqslant k$ 时,证明分如下两种情况.

情形 1　$t=2$ 时. $m_{ij}=1\cdot 1^2+1\cdot w^2+1\cdot(w^2)^2=0$.

情形 2　$t>2$ 时. 令 $a=\binom{m-2}{t-2}$. 当 $i=1$ 时,$m_{ij}=3^a\cdot[1\cdot 1^2+1\cdot w^2+1\cdot(w^2)^2]=0$. 当 $i\geqslant 2$ 时,因为向量 $\boldsymbol{c}_i$ 和 $\boldsymbol{c}_j$ 中非零元 $1,w,w^2$ 的数目相等,并且 $1\cdot 1^2+1\cdot w^2+1\cdot(w^2)^2=0$,所以 $m_{ij}=c_{i1}c_{j1}^2+c_{i2}c_{j2}^2+\cdots+c_{in_t}c_{jn_t}^2=0$.

综上,引理得证.

根据引理 3,有如下结论.

引理 4　设 $k\geqslant 3$. 对任意 $2\leqslant t\leqslant k-1$,

$$\mathrm{Rank}(\boldsymbol{G}_t\boldsymbol{G}_t^{\dagger})=\begin{cases}0, & \binom{k-1}{t-1}\equiv 0(\bmod 2)\\ k, & \binom{k-1}{t-1}\equiv 1(\bmod 2)\end{cases}$$

定理 1　设 $k\geqslant 3$. 对任意 $2\leqslant t\leqslant k-1$,码 $C(D_t)$ 是一个四元 $\left[\binom{k}{t}\cdot 3^{t-1},k\right]$ 线性码且

(1) $C(D_t)$ 是厄米特自正交码当且仅当

$$\binom{k-1}{t-1}\equiv 0(\bmod 2)$$

(2) $C(D_t)$ 是厄米特 LCD 码当且仅当

$$\binom{k-1}{t-1}\equiv 1(\bmod 2)$$

证明　由引理 2,矩阵 $\boldsymbol{G}_t$ 是码 $C(D_t)$ 的生成矩阵,所以,$C(D_t)$ 是一个四元 $\left[\binom{k}{t}\cdot 3^{t-1},k\right]$ 线性码. 再结合引理 1 和引理 4,结论成立.

最后,讨论四元线性码 $C(D_t)$ 的厄米特对偶码 $\boldsymbol{C}^{\perp_{\mathrm{H}}}(D_t)$.

定理 2　设 $k\geqslant 3$. 对任意的 $2\leqslant t\leqslant k-1$,码 $C^{\perp_{\mathrm{H}}}(D_t)$ 是一个四元 $\left[\binom{k}{t}\cdot 3^{t-1},\binom{k}{t}\cdot 3^{t-1}-k,3\right]$ 线性码,满足当 $4^{k-1}<1+\binom{k}{t}\cdot 3^t$ 时,$C^{\perp_{\mathrm{H}}}(D_t)$ 是最优码.

证明　根据定理 1 可得码 $C^{\perp_{\mathrm{H}}}(D_t)$ 是域 F_4 上一个 $\left[\binom{k}{t}\cdot 3^{t-1},\binom{k}{t}\cdot 3^{t-1}-k\right]$ 线性码. 下面证明线性码 $C^{\perp_{\mathrm{H}}}(D_t)$ 的最小距离为 3. 显然,矩阵 $\boldsymbol{G}_t$ 是码 $C^{\perp_{\mathrm{H}}}(D_t)$ 的校验矩阵. 所以,码 $C^{\perp_{\mathrm{H}}}(D_t)$ 的最小距离为 3 当且仅当 D_t 中任意两个向量线性无关且存在三个向量是线性相关的. 容易验证 D_t 中任意两个向量是线性无关的. 下面证明 D_t 中存在三个向量是线性相关的. 设

$$\boldsymbol{g}_1=(\underbrace{1,\cdots,1}_{t},0,\cdots,0) \tag{9}$$

$$\boldsymbol{g}_2=(0,1,\underbrace{w,\cdots,w}_{t-1},0,\cdots,0) \tag{10}$$

显然,$\boldsymbol{g}_1,\boldsymbol{g}_2\in D_t$. 令 $\boldsymbol{g}_3=\boldsymbol{g}_1+\boldsymbol{g}_2$,则 $\boldsymbol{g}_3\in D_t$. 所以,码 $C^{\perp_{\mathrm{H}}}(D_t)$ 的最小距离为 3.

下面讨论码 $C^{\perp_H}(D_t)$ 的最优性. 由球包界[14],域 F_4 上码长为 $\binom{k}{t}\cdot 3^{t-1}$ 最小距离为 3 的线性码的维数 $k'\leqslant\binom{k}{t}\cdot 3^{t-1}-\log_4^{1+\binom{k}{t}\cdot 3^t}$. 当 $4^{k-1}<1+\binom{k}{t}\cdot 3^t$ 时,则 $k'\leqslant\binom{k}{t}\cdot 3^{t-1}-k$. 由文献[15]中定义 5.1.1,对于一个给定码长和最小距离的线性码,如果其维数达到最大值,则称这个码为最优码. 因此,码 $C^{\perp_{\mathrm{H}}}(D_t)$ 是最优码.

例 1　当 $k=3$ 和 $t=2$. 码 $C(D_t)$ 是一个四元[9,3,6]厄米特自正交码. 由定理 2,码 $C^{\perp_{\mathrm{H}}}(D_t)$ 是一个四元[9,6,3]最优码.

例 2　当 $k=4$ 和 $t=3$. 线性码 $C(D_t)$ 是一个四元[36,4,25]厄米特 LCD 码. 由于 LCD 码的对偶码还是 LCD 码,结合定理 2 可得线性码 $C^{\perp_{\mathrm{H}}}(D_t)$ 是一个四元[36,32,3]最优厄米特 LCD 码.

3.2　定义集为 $D_{\leqslant t}$ 的四元线性码

设 $D_{\leqslant t}=\bigcup_{i=1}^{t}D_t\subseteq F_4^k$,$\boldsymbol{G}_{\leqslant t}=[\boldsymbol{G}_1\mid\boldsymbol{G}_2\mid\cdots\mid\boldsymbol{G}_t]$. 设码 $C(D_{\leqslant t})$ 是由矩阵 $\boldsymbol{G}_{\leqslant t}$ 生成的码长 $\sum_{i=1}^{t}\binom{k}{i}\cdot 3^{i-1}$ 的四元线性码. 由 $\boldsymbol{G}_{\leqslant t}$ 的定义和引理 2,容易验证 $\mathrm{Rank}(\boldsymbol{G}_{\leqslant t})=k$. 设

$$\boldsymbol{G}_{\leqslant t}\boldsymbol{G}_{\leqslant t}^{\dagger}=\sum_{i=1}^{t}\boldsymbol{G}_i\boldsymbol{G}_i^{\dagger}=(m_{ij})_{k\times k} \tag{11}$$

定义二项系数的部分和 $P(a,b)$ 为 $P(a,b)=\sum_{i=0}^{b}\binom{a}{i}$. 根据引理 3,对任意的 $1\leqslant i,j\leqslant k$,当 $i=j$ 时,$m_{ij}=P(m-1,t-1)$;当 $i\neq j$ 时,$m_{ij}=0$. 所以,

$$\mathrm{Rank}(\boldsymbol{G}_{\leqslant t}\boldsymbol{G}_{\leqslant t}^{\dagger})=\begin{cases}0, & P(k-1,t-1)\equiv 0(\bmod 2)\\ k, & P(k-1,t-1)\equiv 1(\bmod 2)\end{cases}$$

由引理 1,结合矩阵 $\boldsymbol{G}_{\leqslant t}\boldsymbol{G}_{\leqslant t}^{\dagger}$ 的秩,有如下结论.

定理 3　设 $k\geqslant 3$. 对任意 $2\leqslant t\leqslant k-1$,码 $C(D_{\leqslant t})$ 是

一个四元 $\left[\sum_{i=1}^{t}\binom{k}{i}\cdot 3^{i-1},k\right]$ 线性码.

(1)线性码 $C(D_{\leqslant t})$ 是厄米特自正交码当且仅当

$$P(k-1,t-1)\equiv 0 \pmod 2$$

(2)线性码 $C(D_{\leqslant t})$ 是厄米特 LCD 码当且仅当

$$P(k-1,t-1)\equiv 1 \pmod 2$$

下面,介绍二项系数部分和及组合数的性质.

引理 5[12] 设 $k\geqslant 4$,有如下结论:

(1)如果 k 是奇数,则

$$P(k-1,\frac{k-3}{2})\equiv\frac{1}{2}\binom{k-1}{\frac{k-1}{2}}\pmod 2 \tag{12}$$

(2) 如果 k 是偶数,则

$$P(k-1,\frac{k-2}{2})\equiv 0\pmod 2 \tag{13}$$

引理 6[12] 设 a 是一个正整数,$\frac{1}{2}\binom{2a}{a}$ 是奇数当且仅当 a 是 2 的幂.

由定理 3,引理 5 和引理 6,得到如下推论.

推论 1 设 $k\geqslant 4$ 是偶数,则 $C(D_{\leqslant\frac{k}{2}})$ 是厄米特自正交码.

推论 2 设 $k\geqslant 5$ 是奇数.

(1) 线性码 $C(D_{\leqslant\frac{k-1}{2}})$ 是厄米特 LCD 码当且仅当 $k=2^r+1$,r 是正整数.

(2) 线性码 $C(D_{\leqslant\frac{k-1}{2}})$ 是厄米特自正交码当且仅当 $k-1$ 不是 2 的幂.

与定理 2 类似,关于码 $C(D_{\leqslant t})$ 的厄米特对偶码 $C^{\perp H}(D_{\leqslant t})$ 有如下结论.

定理 4 设 $2\leqslant t\leqslant k-1$,码 $C^{\perp H}(D_{\leqslant t})$ 是一个四元 $\left[\sum_{i=1}^{t}\binom{k}{i}\cdot 3^{i-1},\sum_{i=1}^{t}\binom{k}{i}\cdot 3^{i-1}-k,3\right]$ 线性码. 并且,当 $4^{k-1}<1+\sum_{i=1}^{t}\binom{k}{i}\cdot 3^{i}$ 时,$C^{\perp H}(D_{\leqslant t})$ 是最优码.

例 3 当 $k=4$ 和 $t=2$,线性码 $C(D_{\leqslant t})$ 是一个四元 [22,4,10] 厄米特自正交码. 由定理 4,$C^{\perp H}(D_{\leqslant t})$ 是一个四元[22,18,3]最优线性码.

例 4 当 $k=4$ 和 $t=2$,线性码 $C(D_{\leqslant t})$ 是一个四元 [58,4,37] 厄米特 LCD 码. 由定理 4,$C^{\perp H}(D_{\leqslant t})$ 是一个四元[58,54,3]最优厄米特 LCD 码.

3.3 定义集为 $\overline{D}_t$ 的四元线性码

设 $\overline{D}_t=D_t\cup\{\mathbf{1}\}\subseteq F_4^k$ 和 $\overline{\boldsymbol{G}}_t=[\boldsymbol{G}_t|\mathbf{1}^{\mathrm{T}}]$. 设 $C(\overline{D}_t)$ 是由 $\overline{\boldsymbol{G}}_t$ 生成的码长 $\binom{k}{t}\cdot 3^{t-1}+1$ 的四元线性码. 由 $\overline{\boldsymbol{G}}_t$ 的定义和引理 2,得到下面结论.

引理 7 设 $k\geqslant 2$. 对任意 $1\leqslant t\leqslant k-1$,$\mathrm{Rank}(\overline{\boldsymbol{G}}_t)=k$.

注意到 $\overline{\boldsymbol{G}}_t\overline{\boldsymbol{G}}_t^{\dagger}=\boldsymbol{G}_t\boldsymbol{G}_t^{\dagger}+\mathbf{1}^{\mathrm{T}}\cdot\mathbf{1}$. 根据引理 3 有如下结论.

引理 8 设 $k\geqslant 3$. 对任意 $2\leqslant t\leqslant k-1$,

$$\mathrm{Rank}(\overline{\boldsymbol{G}}_t\overline{\boldsymbol{G}}_t^{\dagger})=\begin{cases}1, & \binom{k-1}{t-1}\equiv 0\pmod 2\\ k, & \binom{k-1}{t-1}\equiv k+1\equiv 1\pmod 2\\ k-1, & \binom{k-1}{t-1}\equiv k\equiv 1\pmod 2\end{cases}$$

由引理 1,引理 7 和引理 8,有如下结论.

定理 5 设 $k\geqslant 3$. 对任意 $2\leqslant t\leqslant k-1$,码 $C(\overline{D}_t)$ 是一个四元 $\left[\binom{k}{t}\cdot 3^{t-1}+1,k\right]$ 线性码.

(1)$C(\overline{D}_t)$ 是厄米特 LCD 码当且仅当 $\binom{k-1}{t-1}\equiv k+1\equiv 1\pmod 2$

(2)$C(\overline{D}_t)$ 不可能是厄米特自正交码.

由定理 5,与定理 2 类似可得如下结论.

定理 6 设 $2\leqslant t\leqslant k-1$,则 $C^{\perp H}(\overline{D}_t)$ 是一个四元 $\left[\binom{k}{t}\cdot 3^{t-1}+1,\binom{k}{t}\cdot 3^{t-1}+1-k,3\right]$ 线性码. 并且,当 $4^{k-1}<4+\binom{k}{t}\cdot 3^{t}$ 时,$C^{\perp H}(\overline{D}_t)$ 是最优码.

例 5 当 $k=4$ 和 $t=3$ 时,码 $C(\overline{D}_t)$ 是一个四元 [37,4,25] 厄米特 LCD 码. 由定理 6,码 $C^{\perp H}(\overline{D}_t)$ 是一个四元[37,33,3]最优厄米特 LCD 码.

3.4 定义集为 $\overline{D}_{\leqslant t}$ 的四元线性码

设 $\overline{D}_{\leqslant t}=D_{\leqslant t}\cup\{\mathbf{1}\}\subseteq F_4^k$ 和 $\overline{\boldsymbol{G}}_{\leqslant t}=[\boldsymbol{G}_{\leqslant t}|\mathbf{1}^{\mathrm{T}}]$. 设码 $C(\overline{D}_{\leqslant t})$ 是由 $\overline{\boldsymbol{G}}_{\leqslant t}$ 生成的码长 $\sum_{i=1}^{t}\binom{k}{i}\cdot 3^{i-1}+1$ 的四元线性码. 与 3.2 节类似,关于 $C(\overline{D}_{\leqslant t})$ 及其厄米特对偶码 $C^{\perp H}(\overline{D}_{\leqslant t})$ 有如下结论.

定理 7 设 $2\leqslant t\leqslant k-1$,则码 $C(\overline{D}_{\leqslant t})$ 是一个四元 $\left[\sum_{i=1}^{t}\binom{k}{i}\cdot 3^{i-1}+1,k\right]$ 线性码且

(1)线性码 $C(\overline{D}_{\leqslant t})$ 是厄米特 LCD 码当且仅当

$$P(k-1,t-1)\equiv k+1\equiv 1 \pmod 2$$

(2)$C(\overline{D}_{\leqslant t})$ 不可能是厄米特自正交码.

定理 8 设 $2\leqslant t\leqslant k-1$,则 $C^{\perp H}(\overline{D}_{\leqslant t})$ 是一个四元 $\left[\sum_{i=1}^{t}\binom{k}{i}\cdot 3^{i-1}+1,\sum_{i=1}^{t}\binom{k}{i}\cdot 3^{i-1}+1-k,3\right]$ 线性码,且当 $4^{k-1}<4+\sum_{i=1}^{t}\binom{k}{i}\cdot 3^{i}$ 时,$C^{\perp H}(\overline{D}_{\leqslant t})$ 是最优码.

例 6 当 $k=4$ 和 $t=3$ 时,码 $C(\overline{D}_{\leqslant t})$ 是一个四元

[59,4,38]厄米特 LCD 码. 由定理 8,$C^{\perp_H}(\overline{D}_{\leqslant t})$是一个四元[59,55,3]最优厄米特 LCD 码.

4　结束语

本文研究了四元域上厄米特 LCD 码与厄米特自正交码的构造. 根据线性码是厄米特 LCD 码和厄米特自正交码的充要条件,通过选择特定的定义集构造了四类四元厄米特 LCD 码和厄米特自正交码,进而研究了这四类线性码的厄米特对偶码,并得到了一些四元最优线性码. 本文构造的四类线性码的重量分布和一般域上自正交码的构造是进一步研究的问题.

参考文献

[1] CALDERBANK A R, RAINS E M, SHOR PW, SLOANE N J A. Quantum error correction via codes over GF(4)[J]. IEEE Transactions on Information Theory, 1998, 44(4):1369 – 1387.

[2] ASHIKHMIN A, KNILL E. Nonbinary quantum stabilizer codes[J]. IEEE Transactions on Information Theory, 2001, 47(7):3065 – 3072.

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

[4] KIM J L. New Quantum error-correcting codes from Hermitian self-orthogonal codes over GF(4)[A]. Proceedings of the Sixth International Conference on Finite Fields with Applications[C]. New York: Springer Verlag, 2002: 209 – 213.

[5] CARLET C, GUILLEY S. Complementary dual codes for counter-measures to side-channel attacks[A]. Coding Theory and Applications[C]. Cham: Springer, 2015. 97 – 105.

[6] MASSEY J L. Linear codes with complementary duals[J]. Discrete Mathematics, 1992, 106: 337 – 342.

[7] YANG X, MASSEY J L. The condition for a cyclic code to have a complementary dual[J]. Discrete Mathematics, 1994, 126(1 – 3): 391 – 393.

[8] SENDRIER N. Linear codes with complementary duals meet the Gilbert-Varshamov bound[J]. Discrete Mathematics, 2004, 285(1 – 3): 345 – 347.

[9] GUNERI C, ÖZKAYA B, SOLE P. Quasi-cyclic complementary dual codes[J]. Finite Fields and Their Applications, 2016, 42: 67 – 80.

[10] CARLET C, MESNAGER S, TANG C, Qi Y. Euclidean and Hermitian LCD MDS codes[J]. Designs Codes and Crypto-graphy, 2018, 86(11): 2605 – 2618.

[11] CARLET C, MESNAGER S, TANG C, Qi Y, PELLIKAAN R. Linear codes over F_q are equivalent to LCD codes for q > 3[J]. IEEE Transactions on Information Theory, 2018, 64(4): 3010 – 3017.

[12] ZHOU Z, LI X, TANG C, DING C. Binary LCD codes and self-orthogonal codes from a generic construction[J]. IEEE Transactions on Information Theory, 2019, 65(1): 16 – 27.

[13] JITMAN S, MANKEAN T. Matrix-product constructions for Hermitian self-orthogonal codes[J]. arXiv preprint, 2017, arXiv: 1710.04999.

[14] HUFFMAN W C, PLESS V. Fundamentals of Error-Correcting codes[M]. Cambridge: Cambridge university press, 2010. 48 – 52.

[15] J H Van LINT. Introduction to Coding Theory[M]. Berlin: Springer, 1999. 64 – 65.

作者简介

钱　毅　男,1995 年生,安徽铜陵人,合肥工业大学数学学院硕士研究生,研究方向为代数编码.
E-mail:1304123894@qq.com

李　平　男,1971 年生,安徽无为人,合肥工业大学数学学院副教授,硕士生导师. 研究方向为代数编码及非线性移位寄存器序列.
E-mail:lpmath@126.com

唐永生　男,1981 年生,安徽庐江人,合肥师范学院数学与统计学院副教授. 研究方向为代数编码、量子信息以及线性和非线性移位寄存器序列.
E-mail:ysh_tang@163.com