一种三元线性互补对偶码与自正交码的构造方法

李 平 张嘉媛* 孙中华
(合肥工业大学数学学院 合肥 230601)

摘 要：有限域上线性互补对偶(LCD)码有良好的相关特性和正交特性，并能够防御信道攻击。自正交码是编码理论中一类非常重要的码，可以用于构造量子纠错码。该文研究了有限域F_3上的LCD码。通过选取4种合适的定义集，利用有限域F_3上线性码是LCD码或自正交码的判定条件，构造了4类3元LCD码和一些自正交码，并研究了这4类线性码的对偶码，得到了一些3元最优线性码。

关键词：线性码；3元线性互补对偶码；自正交码；定义集
中图分类号：TN911.22 **文献标识码**：A **文章编号**：1009-5896(2022)11-4018-07
DOI: 10.11999/JEIT210979

A Construction Method of Ternary Linear Complementary Dual Codes and Self-orthogonal Codes

LI Ping ZHANG Jiayuan SUN Zhonghua
(*School of Mathematics*, *Hefei University of Technology*, *Hefei* 230601, *China*)

Abstract: Due to good correlation and orthogonal properties, Linear Complementary Dual (LCD) codes over the finite fields can be used to defend against channel attacks. As a very important class of codes in coding theory, self-orthogonal codes can be used to construct quantum error-correcting codes. In this paper, LCD codes over the finite field F_3 are studied. By selecting appropriate defining sets and using the conditions for linear codes over the finite field F_3 to be LCD codes or self-orthogonal codes, four kinds of ternary LCD codes and some self-orthogonal codes are constructed. And the dual codes of these four kinds of liner codes are also studied and some ternary optimal linear codes are obtained.

Key words: Linear codes; Ternary Linear Complementary Dual (LCD) codes; Self-orthogonal codes; Defining sets

1 引言

自正交码包含自对偶码，它是一类非常重要的码。文献[1]利用经典的2元自正交线性码构造了量子码，自此自正交码的构造成为编码理论研究的一个热点[2–6]。文献[4]研究了3元域上对偶距离为3的自正交码的构造，并得到了参数好的量子码。文献[5]研究了4元域上自正交码的构造方法，得到了一些最优的3维自正交码。

线性互补对偶(Linear Complementary Dual, LCD)码作为一类特殊的线性码，在编码理论中有着丰富的应用前景。文献[7]证明有限域上LCD码能够防御信道攻击。文献[8]最先提出线性互补对偶(LCD)码，同时证明存在渐进好的LCD码。文献[9]证明LCD码能达到渐进(gilbert-varshamov)界，从而激发学者研究LCD码的兴趣[9–16]。文献[10]总结有限域上LCD码的一些主要研究成果及其进展，并提出了一些未解决的重要问题。

文献[11]证明$q>3$元LCD码和q元线性码等价。因此，LCD码的研究重点聚焦于研究2元LCD码和3元LCD码。文献[12]解决了5元域上3维和4维最优LCD码的构造问题。文献[13]利用合适的定义集构造了2元LCD码和2元自正交码。文献[14]推广到q元域，其中q是素数。文献[15]通过合适的定义集构造了4元厄米特LCD码和厄米特自正交码。受这3篇文献启发，本文研究了合适的定义集下的3元LCD码和3元自正交码的构造。利用有限域上线性码是LCD码或自正交码的判定条件，构造了4类3元LCD码和一些自正交码。

收稿日期：2021-09-15；改回日期：2021-11-21；网络出版：2021-11-26
*通信作者： 张嘉媛 zjy981202@163.com
基金项目：国家自然科学基金(61972126, 61572168, 62002098)
Foundation Items: The National Natural Science Foundation of China (61972126, 61572168, 62002098)

2　基础知识

设q是素数的幂，F_q是q元域，F_q^n是F_q上n维向量空间。对F_q^n中的任意向量$\boldsymbol{x}=(x_0,x_1,\cdots,x_{n-1})$和$\boldsymbol{y}=(y_0,y_1,\cdots,y_{n-1})$，定义$\boldsymbol{x}$和$\boldsymbol{y}$的欧几里得内积为

$$\boldsymbol{x}\cdot\boldsymbol{y}=x_0\cdot y_0+x_1\cdot y_1+\cdots+x_{n-1}\cdot y_{n-1} \tag{1}$$

设C是一个q元$[n,k]$线性码，则$C^{\perp}$是一个q元$[n,n-k]$线性码。若$C\subseteq C^{\perp}$，则称C为自正交码。若$C\cap C^{\perp}=\{0\}$，则称C为LCD码。

设集合$D=\{\boldsymbol{g}_1,\boldsymbol{g}_2,\cdots,\boldsymbol{g}_n\}\subseteq F_q^m$。由集合$D$构造

$$C_D=\{(\boldsymbol{a}\cdot\boldsymbol{g}_1,\boldsymbol{a}\cdot\boldsymbol{g}_2,\cdots,\boldsymbol{a}\cdot\boldsymbol{g}_n):\boldsymbol{a}\in F_q^m\} \tag{2}$$

易证，C_D是一个码长为n的q元线性码，并称D是码C_D的定义集。设$\boldsymbol{G}$是由向量$\boldsymbol{g}_1^{\mathrm{T}},\boldsymbol{g}_2^{\mathrm{T}},\cdots,\boldsymbol{g}_n^{\mathrm{T}}$形成的$m\times n$矩阵

$$\boldsymbol{G}=[\boldsymbol{g}_1^{\mathrm{T}}\,\boldsymbol{g}_2^{\mathrm{T}}\cdots\boldsymbol{g}_n^{\mathrm{T}}] \tag{3}$$

且$\mathrm{Rank}(\boldsymbol{G})=k$。则$C_D$是一个$[n,k]$线性码。特别地，如果$k=m$，则$\boldsymbol{G}$恰好是$C_D$的生成矩阵。由文献[13]，可得以下结论。

引理1[13]　C_D和$C_D\cap C_D^{\perp}$的维数分别等于$\mathrm{Rank}(\boldsymbol{G})$, $\mathrm{Rank}(\boldsymbol{G})-\mathrm{Rank}(\boldsymbol{G}\boldsymbol{G}^{\mathrm{T}})$。

推论1[13]　C_D是LCD码当且仅当$\mathrm{Rank}(\boldsymbol{G}^{\mathrm{T}})=\mathrm{Rank}(\boldsymbol{G}\boldsymbol{G}^{\mathrm{T}})$。$C_D$是自正交码当且仅当$\boldsymbol{G}\boldsymbol{G}^{T}=0$。

3　主要结果

设m和t是两个任意正整数且$1\le t\le m-1$，设D_t表示${F_3}^m$上重量为t且第1个非0位上的数为1的向量集合。设$D_{\le t}$是${F_3}^m$上重量小于等于t且第1个非0位上的数为1的向量集合。定义

$$\left.\begin{aligned}\overline{D}_t&=D_t\cup\{\boldsymbol{1}_m\}\\ \overline{D}_{\le t}&=D_{\le t}\cup\{\boldsymbol{1}_m\}\end{aligned}\right\} \tag{4}$$

其中，$\boldsymbol{1}_m$是${F_3}^m$上分量全为1的向量。下文通过以上4个集合，构造LCD码和自正交码。

3.1　定义集为D_t的3元线性码

令$D_t=\{\boldsymbol{g}_1,\boldsymbol{g}_2,\cdots,\boldsymbol{g}_{n_t}\}$，其中$n_t=|D_t|$，则$n_t=2^{t-1}\binom{m}{t}$。设$\boldsymbol{G}_t=[\boldsymbol{g}_1^{\mathrm{T}}\,\boldsymbol{g}_2^{\mathrm{T}}\cdots\boldsymbol{g}_{n_t}^{\mathrm{T}}]$且$C_{D_t}$是以$D_t$为定义集的3元码长为$n_t$的线性码。下面研究$C_{D_t}$的参数。首先证明几个重要的引理。

引理2　设$1\le t\le m-1$，则$\mathrm{Rank}(\boldsymbol{G}_t)=m$。

证明　当$t=1$时，$\boldsymbol{G}_t=\boldsymbol{E}_m$，其中$\boldsymbol{E}_m$表示$m$阶单位矩阵，显然$\mathrm{Rank}(\boldsymbol{G}_t)=m$。

当$t\ge 2$时，则$\boldsymbol{G}_t$中一定包含m列线性无关的向量

$$\left.\begin{aligned}&(\underbrace{1,\cdots,1}_{t},0,\cdots,0)^{\mathrm{T}},(1,2,\underbrace{1,\cdots,1}_{t-2},0,\cdots,0)^{\mathrm{T}},\cdots,(\underbrace{1,\cdots,1}_{t-1},2,0,\cdots,0)^{\mathrm{T}}\\ &(0,\underbrace{1,\cdots,1}_{t},0,\cdots,0)^{\mathrm{T}},(0,0,\underbrace{1,\cdots,1}_{t},0,\cdots,0)^{\mathrm{T}},\cdots,(0,\cdots,0,\underbrace{1,\cdots,1}_{t})^{\mathrm{T}}\end{aligned}\right\} \tag{5}$$

因此$\mathrm{Rank}(\boldsymbol{G}_t)=m$。　证毕

引理3　设$1\le t\le m-1$，$\boldsymbol{M}=(m_{ij})_{m\times m}=\boldsymbol{G}_t{\boldsymbol{G}_t}^{\mathrm{T}}$，则

(1) 当$t=1$时，$\boldsymbol{M}=\boldsymbol{E}_m$，其中$\boldsymbol{E}_m$表示$m$阶单位矩阵。

(2) 当$t\ge 2$时，

$$m_{ij}=\begin{cases}2^{t-1}\binom{m-1}{t-1}\,(\mathrm{mod}3), & i=j\\ 0(\mathrm{mod}3), & i\ne j\end{cases}。$$

证明　(1) 当$t=1$时，结论显然正确。

(2) 设c_i表示$\boldsymbol{G}_t$的第i行，则$m_{ij}=\sum_{l=1}^{n_t}c_{il}c_{jl}$。当$i\ne j$时，$(c_{il},c_{jl})$使$c_{il}c_{jl}\ne 0$的可能取值为$(11),(12),(21),(22)$。对$i,j\in\{1,2\}$，令$\lambda_{ij}$表示$(ij)$出现的次数。将$\boldsymbol{G}_t$的每一列以$i,j$为界分成第1行至第$i-1$行，第$i+1$行至第$j-1$行，第$j$行至第$m$行3个部分。根据这3个部分出现非0元的个数，分以下几种情况讨论。

情形1　第1个部分不出现非0元，第2个部分不出现非0元，则第3个部分必须出现$t-2$个非0元，因此情形1在$\boldsymbol{G}_t$中出现的次数共计

$$l_1=2^{t-2}\binom{m-j}{t-2} \tag{6}$$

情形2　第1个部分出现$s\ge 1$个非0元且这部分第1个非0元为1，则第2个部分不出现非0元，则第3个部分必须出现$t-s-2$个非0元。因此情形2在$\boldsymbol{G}_t$中出现的次数共计

$$l_2=\sum_{s=1}^{t-2}2^{s-1}\binom{i-1}{s}2^{t-s-2}\binom{m-j}{t-s-2} \tag{7}$$

情形3　第1个部分不出现非0元，第2个部分出现$k\ge 1$个非0元，则第3个部分必须出现$t-k-2$个非0元。因此情形3在$\boldsymbol{G}_t$中出现的次数共计

$$l_3=\sum_{k=1}^{t-2}2^{k}\binom{j-i-1}{k}2^{t-k-2}\binom{m-j}{t-k-2} \tag{8}$$

情形4　第1个部分出现$s\ge 1$个非0元且这部分第1个非0元为1，第2个部分出现$k\ge 1$个非0元，则第3个部分必须出现$t-s-k-2$个非0元。因此情形5在$\boldsymbol{G}_t$中出现的次数共计

$$l_4=\sum_{s=1}^{t-2}\sum_{k=1}^{t-2}2^{s-1}\binom{i-1}{s}2^k\binom{j-i-1}{k}\cdot 2^{t-s-k-2}\binom{m-j}{t-s-k-2} \tag{9}$$

在$\boldsymbol{G}_t$中(11)出现的情况有情形1、情形2、情形3、情形4。在$\boldsymbol{G}_t$中(12)出现的情况有情形1、情形2、情形3、情形4。在$\boldsymbol{G}_t$中(21)出现的情况有情形2、情形4。在$\boldsymbol{G}_t$中(22)出现的情况有情形2、情形4。则 $\lambda_{11}=l_1+l_2+l_3+l_4$ ， $\lambda_{12}=l_1+l_2+l_3+l_4$ ，$\lambda_{21}=l_2+l_4$, $\lambda_{22}=l_2+l_4$。所以在$\boldsymbol{G}_t$中(11), (12)出现次数相同，且$1\cdot 1+1\cdot 2=3$。在$\boldsymbol{G}_t$中(21), (22)出现次数相同，且$2\cdot 1+2\cdot 2=3$。所以$m_{ij}=0 \pmod 3$, $i\neq j$。当$i=j$时，因为$c_{ij}\in F_3$，而$0\cdot 0=0$, $1\cdot 1=1$, $2\cdot 2=1 \pmod 3$，则m_{ii}等于第i行非0元的数目模3。下面证明$\boldsymbol{G}_t$的每一行非0元数目是相等的。当$i=1$时，非0元素只有1，个数为$2^{t-1}\binom{m-1}{t-1}$。当$j\neq 1$时，(c_1,c_j)有以下几种情况，(00), (01), (02), (10), (11), (12)，则只需要证明(01)(02)和(10)的个数相等即可。对$i,j\in\{0,1,2\}$，令δ_{ij}表示(ij)出现的次数。将$\boldsymbol{G}_t$的每一列以$1,j$为界分成第2行至第$j-1$行，第$j+1$行至第m行2个部分。根据这2个部分出现非0元的个数，分以下几种情形讨论。

情形1 第1个部分不出现非0元，则第2个部分必须出现$t-1$个非0元。因此情形1在$\boldsymbol{G}_t$中出现的次数共计

$$h_1=2^t\binom{m-j}{t-1} \tag{10}$$

情形2 第1个部分出现$s\geq 1$个非0元，则第2部分必须出现$t-s-1$个非0元。因此情形2在$\boldsymbol{G}_t$中出现的次数共计

$$h_2=\sum_{s=1}^{t-1}2^s\binom{j-2}{s}2^{t-s-1}\binom{m-j}{t-s-1} \tag{11}$$

情形3 第1个部分出现$s\geq 1$个非0元且这部分第1个非0元为1，则第2个部分必须出现$t-s-1$个非0元。因此情形3在$\boldsymbol{G}_t$中出现的次数共计

$$h_3=\sum_{s=1}^{t-1}2^{s-1}\binom{j-2}{s}2^{t-s-1}\binom{m-j}{t-s-1} \tag{12}$$

在$\boldsymbol{G}_t$中(10)出现的情况有情形1、情形2。在$\boldsymbol{G}_t$中(01)出现的情况有情形1、情形3。在$\boldsymbol{G}_t$中(02)出现的情况有情形3。则$\delta_{10}=h_1+h_2$, $\delta_{01}=h_1+h_3$, $\delta_{02}=h_3$，又因为$h_2=2h_3$，所以$\delta_{10}=\delta_{01}+\delta_{02}$。所以$c_1$和$c_j$中的非0数目都是相等

$$m_{ii}=2^{t-1}\binom{m-1}{t-1} \pmod 3 \tag{13}$$

综上所述，引理得证。

根据引理3，有如下结论。

引理4 设$m\geq 3$且$2\leq t\leq m-1$，则

$$\mathrm{Rank}(\boldsymbol{G}_t\boldsymbol{G}_t^{\mathrm{T}})=\begin{cases}0, & \binom{m-1}{t-1}\equiv 0 \pmod 3\\ m, & \binom{m-1}{t-1}\not\equiv 0 \pmod 3\end{cases} \tag{14}$$

命题1 设$m\geq 3$且$2\leq t\leq m-1$，则

$$\dim_{F_3}(C_{D_t}\cap C_{D_t}^{\perp})=\begin{cases}\dim_{F_3}(C_{D_t}), & \binom{m-1}{t-1}\equiv 0 \pmod 3\\ 0, & \binom{m-1}{t-1}\not\equiv 0 \pmod 3\end{cases} \tag{15}$$

证明 由引理1，$\dim_{F_3}(C_{D_t}\cap C_{D_t}^{\perp})=\mathrm{Rank}(\boldsymbol{G})-\mathrm{Rank}(\boldsymbol{G}\boldsymbol{G}^{\mathrm{T}})$，由引理2和引理4，结论成立。

根据推论1、引理4、命题1，可得下面定理。

定理1 设$m\geq 3$且$2\leq t\leq m-1$，则C_{D_t}是一个3元$[2^{t-1}\binom{m}{t},m]$线性码。

(1) C_{D_t}是自正交码当且仅当$\binom{m-1}{t-1}\equiv 0 \pmod 3$。

(2) C_{D_t}是LCD码当且仅当$\binom{m-1}{t-1}\not\equiv 0 \pmod 3$。

定理2 设$m\geq 3$且$2\leq t\leq m-1$，则$C_{D_t}^{\perp}$是一个3元$[2^{t-1}\binom{m}{t}, 2^{t-1}\binom{m}{t}-m, 3]$线性码。当$1+2^t\binom{m}{t}>3^{m-1}$时，$C_{D_t}^{\perp}$是最优码。

证明 由定理1，易证$C_{D_t}^{\perp}$是$\left[2^{t-1}\binom{m}{t}, 2^{t-1}\binom{m}{t}-m\right]$线性码。下证$C_{D_t}^{\perp}$的最小距离是3。显然$\boldsymbol{G}_t$是$C_{D_t}^{\perp}$的校验矩阵。首先证明$\boldsymbol{G}_t$的任何两列都是线性无关的。假设$\boldsymbol{G}_t$中存在两列$\boldsymbol{l}_i$和$\boldsymbol{l}_j$线性相关，则存在$\alpha\in F_3$使得$\boldsymbol{l}_j=\alpha\boldsymbol{l}_i$。又由于$\boldsymbol{l}_j$的第1个非0位为1，故$\alpha=1$且$i=j$。因此，$\boldsymbol{G}_t$中任何两列是线性无关的。由此推出，$C_{D_t}^{\perp}$中不存在重量为1和2的码字。另外，容易验证$\boldsymbol{G}_t$中存在3个列向量

$$\begin{aligned}&\boldsymbol{g}_1=(\overbrace{1,\cdots,1}^{t},0,\cdots,0)^{\mathrm{T}}, \boldsymbol{g}_2=(0,\overbrace{1,\cdots,1}^{t-2},2,1,0,\cdots,0)^{\mathrm{T}},\\ &\boldsymbol{g}_3=(\overbrace{1,2,\cdots,2}^{t-2},0,1,0,\cdots,0)^{\mathrm{T}}\end{aligned} \tag{16}$$

且$\boldsymbol{g}_3=\boldsymbol{g}_1+\boldsymbol{g}_2$，故$C_{D_t}^{\perp}$的最小距离为3。

下面讨论码$C_{D_t}^{\perp}$的最优性。由球包界，码长为$n_t=2^{t-1}\binom{m}{t}$最小距离为3的3元线性码的维数

$$k' \le 2^{t-1}\binom{m}{t} - \log_3^{1+2^t\binom{m}{t}} \tag{17}$$

当 $1+2^t\binom{m}{t} > 3^{m-1}$ 时，$k' \le 2^{t-1}\binom{m}{t} - m$。因此，$C_{D_t}^{\perp}$的维数达到最大值。由文献[17]中的定义5.1.1，对于给定的码长和最小距离的线性码，如果其维数达到最大值，则称该码为最优码。因此，$C_{D_t}^{\perp}$是最优码。

例 1　当 $m=3$ 和$t=2$ 时，$n_t=6$ 且 $\boldsymbol{G}_t=\begin{pmatrix}1&1&1&1&0&0\\1&2&0&0&1&1\\0&0&1&2&1&2\end{pmatrix}$。由定理1，码$C_{D_t}$是一个3元[6,3]线性码。经MAGMA计算，$C_{D_t}$的最小距离为3，则码$C_{D_t}$是一个3元[6,3,3]线性码。由定理2，码$C_{D_t}^{\perp}$是一个3元[6,3,3]LCD最优码。

例2　当$m=4$和$t=2$时，$n_t=12$且

$$\boldsymbol{G}_t=\begin{pmatrix}1&1&1&1&1&1&0&0&0&0&0&0\\1&2&0&0&0&0&1&1&1&1&0&0\\0&0&1&2&0&0&1&2&0&0&1&1\\0&0&0&0&1&2&0&0&1&2&1&2\end{pmatrix} \tag{18}$$

由定理1，码C_{D_t}是一个3元[12,4]线性码。经MAGMA计算，C_{D_t}的最小距离为6，则码C_{D_t}是一个3元[12,4,6]线性码。由定理2，码$C_{D_t}^{\perp}$是一个3元[12,8,3]自正交最优码。

3.2 定义集为$\overline{D}_t$的3元线性码

令 $\overline{D}_t = D_t \cup \{\boldsymbol{1}_m\}$，$\overline{\boldsymbol{G}}_t=[\boldsymbol{g}_1\,\boldsymbol{g}_2\cdots\boldsymbol{g}_{nt}\,\boldsymbol{1}_m]$，类似引理2的证明，可得

引理5　设 $m\ge 2$ 且$1\le t\le m-1$，则 Rank $(\overline{\boldsymbol{G}}_t)=m$。

注意到$\overline{\boldsymbol{G}}_t\overline{\boldsymbol{G}}_t^{\mathrm{T}}=\boldsymbol{G}_t\boldsymbol{G}_t^{\mathrm{T}}+\boldsymbol{1}_m^{\mathrm{T}}\boldsymbol{1}_m$。

由引理3，可得

$$\mathrm{Rank}(\overline{\boldsymbol{G}}_t\overline{\boldsymbol{G}}_t^{\mathrm{T}})=\begin{cases}1, & \text{当}\binom{m-1}{t-1}\equiv 0(\mathrm{mod}3);\\ m-1, & \text{当}2^{t-1}\binom{m-1}{t-1}\equiv 1(\mathrm{mod}3)\\ & \text{且}m\equiv 2(\mathrm{mod}3)\\ & \text{或}2^{t-1}\binom{m-1}{t-1}\equiv 2(\mathrm{mod}3)\\ & \text{且}m\equiv 1(\mathrm{mod}3);\\ m, & \text{其他情形}\end{cases} \tag{19}$$

由引理1和引理5，得到

$$\dim_{F_3}(C_{\overline{D_t}}\cap C_{\overline{D_t}}^{\perp})=\begin{cases}\dim_{F_3}(C_{\overline{D_t}})-1, \text{当}\binom{m-1}{t-1}\equiv 0(\mathrm{mod}3);\\ 1, \quad \text{当}2^{t-1}\binom{m-1}{t-1}\equiv 1(\mathrm{mod}3)\\ \quad \text{且}m\equiv 2(\mathrm{mod}3)\\ \quad \text{或}\ 2^{t-1}\binom{m-1}{t-1}\equiv 2(\mathrm{mod}3)\\ \quad \text{且}m\equiv 1(\mathrm{mod}3);\\ 0, \quad \text{其他情形}\end{cases} \tag{20}$$

因此，本文得到以下结论。

定理3　设$m\ge 3$且$2\le t\le m-1$，则码$C_{\overline{D}_t}$是一个3元$[2^{t-1}\binom{m}{t}+1, m]$线性码。

（1）$C_{\overline{D}_t}$是LCD码当且仅当$2^{t-1}\binom{m-1}{t-1}\equiv 2(\mathrm{mod}3)$且$m\not\equiv 1(\mathrm{mod}3)$或$2^{t-1}\binom{m-1}{t-1}\equiv 1(\mathrm{mod}3)$且 $m\not\equiv 2(\mathrm{mod}3)$。

(2) $C_{\overline{D}_t}$不可能是自正交码。

由定理2与定理3，类似可得如下结论。

定理4　设$m\ge 3$且$2\le t\le m-1$，则$C_{\overline{D}_t}^{\perp}$是一个 3 元 $[2^{t-1}\binom{m}{t}+1, 2^{t-1}\binom{m}{t}+1-m, 3]$ 线性码，当$2^t\binom{m}{t}>3^{m-1}-3$ 时，$C_{\overline{D}_t}^{\perp}$ 是最优码。

例3　当$m=5$和$t=3$。由定理3，码$C_{\overline{D}_t}$是一个3元[41,5]线性码。经MAGMA计算，$C_{\overline{D}_t}$的最小距离为24，则码$C_{\overline{D}_t}$是一个3元[41,5,24]线性码。由定理4，$C_{\overline{D}_t}^{\perp}$码是一个3元[41,36,3]最优码。

例4　当$m=5$和$t=4$。由定理3，码$C_{\overline{D_t}}$是一个3元[41,5]线性码。经MAGMA计算，$C_{\overline{D}_t}$的最小距离为24，则码$C_{\overline{D}_t}$是一个3元[41,5,24]线性码。由定理4，$C_{\overline{D}_t}^{\perp}$码是一个3元[41,36,3]LCD最优码。

3.3 定义集为$D_{\le t}$的3元线性码

令$D_{\le t}=\bigcup_{i=1}^{t}D_t\subseteq F_3^m$，则$\boldsymbol{G}_{\le t}=[\boldsymbol{G}_1|\boldsymbol{G}_2|\cdots\boldsymbol{G}_t]$，其中$\boldsymbol{G}_i$是由$D_i$形成的$m\times\left[2^{i-1}\binom{m}{i}\right]$矩阵。

由引理2，$\mathrm{Rank}(\boldsymbol{G}_{\le t})=m$。设

$$P(a,b)=2^0\binom{a}{0}+2^1\binom{a}{1}+\cdots+2^b\binom{a}{b} \tag{21}$$

由引理3

$$\begin{aligned}\boldsymbol{G}_{\le t}\boldsymbol{G}_{\le t}^{\mathrm{T}} &= [\boldsymbol{G}_1|\boldsymbol{G}_2|\cdots|\boldsymbol{G}_t][\boldsymbol{G}_1|\boldsymbol{G}_2|\cdots|\boldsymbol{G}_t]^{\mathrm{T}}\\ &= \sum_{i=1}^{t}\boldsymbol{G}_i\boldsymbol{G}_i^{\mathrm{T}}\\ &= (m_{ij})_{m\times m}\end{aligned} \tag{22}$$

其中，m_{ii}=$P(m-1,\ t-1)$, $m_{ij}=0$, $i\ne j$。因此

$$\mathrm{Rank}(\boldsymbol{G}_{\le t}\boldsymbol{G}_{\le t}^{\mathrm{T}}) = \begin{cases}0,\ P(m-1,t-1)\equiv 0(\mathrm{mod}3)\\ m, P(m-1,t-1)\not\equiv 0(\mathrm{mod}3)\end{cases} \tag{23}$$

由引理1

$$\dim_{F_3}(C_{D_{\le t}}C_{D_{\le t}}^{\mathrm{T}}) = \begin{cases}m,\ P(m-1,t-1)\equiv 0(\mathrm{mod}3)\\ 0,\ P(m-1,t-1)\not\equiv 0(\mathrm{mod}3)\end{cases} \tag{24}$$

因此，如下结论成立。

定理5 设$m\ge 3$且$2\le t\le m-1$，则$C_{D_{\le t}}$是一个3元$\left[\sum\limits_{i=1}^{t}2^{i-1}\binom{m}{i}, m\right]$线性码。

（1）$C_{D_{\le t}}$是自正交码当且仅当$P(m-1,\ t-1)\equiv 0(\mathrm{mod}3)$。

（2）$C_{D_{\le t}}$是LCD码当且仅当$P(m-1,t-1)\not\equiv 0(\mathrm{mod}3)$。

与定理2和定理4，类似可得如下结论。

定理6 设$m\ge 3$且$2\le t\le m-1$，则$C_{D_{\le t}}^{\perp}$是一个3元$\left[\sum\limits_{i=1}^{t}2^{i-1}\binom{m}{i}, \sum\limits_{i=1}^{t}2^{i-1}\binom{m}{i}-m, 3\right]$线性码，当$\sum\limits_{i=1}^{t}2^{i}\binom{m}{i} > 3^{m-1}-1$时，$C_{D_{\le t}}^{\perp}$是最优码。

例5 若$m=4$和$t=2$，则

$$\boldsymbol{G}_{\le t} = \begin{pmatrix}1&0&0&0&1&1&1&1&1&1&0&0&0&0&0&0\\ 0&1&0&0&1&2&0&0&0&0&1&1&1&1&0&0\\ 0&0&1&0&0&0&1&2&0&0&1&2&0&0&1&1\\ 0&0&0&1&0&0&0&0&1&2&0&0&1&2&1&2\end{pmatrix} \tag{25}$$

由定理5，码$C_{D_{\le t}}$是一个3元$[16,4]$线性码。经MAGMA计算，$C_{D_{\le t}}$的最小距离为7，则码$C_{D_{\le t}}$是一个3元$[16,4,7]$线性码。由定理6，码$C_{D_{\le t}}^{\perp}$是一个3元$[16,12,3]$LCD最优码。

3.4 定义集为$D_{\le t}\cup\{\boldsymbol{1}_m\}$的3元线性码

令$\overline{D}_{\le t}=D_{\le t}\cup\{\boldsymbol{1}_m\}$,$\overline{\boldsymbol{G}}_{\le t}=[\boldsymbol{G}_{\le t}\,|\boldsymbol{1}_m]$，与第2节类似，可得

$$\overline{\boldsymbol{G}}_{\le t}\overline{\boldsymbol{G}}_{\le t}{}^{\mathrm{T}} = [\boldsymbol{G}_1|\boldsymbol{G}_2|\cdots|\boldsymbol{G}_t|\boldsymbol{1}_m][\boldsymbol{G}_1|\boldsymbol{G}_2|\cdots|\boldsymbol{G}_t|\boldsymbol{1}_m]^{\mathrm{T}} = \sum_{i=1}^{t}\boldsymbol{G}_i\boldsymbol{G}_i^{\mathrm{T}} + \boldsymbol{1}_m\boldsymbol{1}_m^{\mathrm{T}} \tag{26}$$

即m_{ii}= $P(m-1,t-1)+1$。$m_{ij}=1$, $i\ne j$。

由引理3

$$\mathrm{Rank}(\overline{\boldsymbol{G}}_{\le t}\overline{\boldsymbol{G}}_{\le t}^{\mathrm{T}}) = \begin{cases}1, & \text{当}P(m-1,t-1)\equiv 0(\mathrm{mod}3);\\ m-1, & \text{当}P(m-1,t-1)\equiv 1(\mathrm{mod}3)\\ & \text{且}m\equiv 2(\mathrm{mod}3)\\ & \text{或}P(m-1,t-1)\equiv 2(\mathrm{mod}3)\\ & \text{且}m\equiv 1(\mathrm{mod}3);\\ m, & \text{其他情形}\end{cases} \tag{27}$$

$$\dim_{F_3}(C_{\overline{D}_{\le t}}\cap C_{\overline{D}_{\le t}}^{\perp}) = \begin{cases}\dim_{F_3}(C_{\overline{D}_{\le t}})-1, & \text{当}P(m-1,t-1)\equiv 0(\mathrm{mod}3);\\ 1, & \text{当}P(m-1,t-1)\equiv 1(\mathrm{mod}3)\\ & \text{且 }m\equiv 2(\mathrm{mod}3)\\ & \text{或 }P(m-1,t-1)\equiv 2(\mathrm{mod}3)\\ & \text{且}m\equiv 1(\mathrm{mod}3);\\ 0, & \text{其他}\end{cases} \tag{28}$$

因此，可以得到以下结论：

定理7 设$m\ge 3$且$2\le t\le m-1$，$C_{\overline{D}_{\le t}}$是一个3元$\left[1+\sum\limits_{i=1}^{t}2^{i-1}\binom{m}{i}, m\right]$线性码。

(1) $C_{\overline{D}_{\le t}}$是LCD码当且仅当$P(m-1,t-1)\equiv 1(\mathrm{mod}3)$且$m\not\equiv 2(\mathrm{mod}3)$或$P(m-1,t-1)\equiv 2(\mathrm{mod}3)$且$m\not\equiv 1(\mathrm{mod}3)$。

(2) $C_{\overline{D}_{\le t}}$不可能是自正交码。

与定理2和定理5类似，可得如下结论。

定理8 设$m\ge 3$且$2\le t\le m-1$，则$C_{\overline{D}_{\le t}}^{\perp}$是一个3元$\left[1+\sum\limits_{i=1}^{t}2^{i-1}\binom{m}{i}, 1+\sum\limits_{i=1}^{t}2^{i-1}\binom{m}{i}-m, 3\right]$

线性码。当$\sum_{i=1}^{t}2^i\binom{m}{i}>3^{m-1}-3$时，$C_{\overline{D}_{\le t}}^{\perp}$是最优码。

例6　当$m=4$和$t=3$。由定理7，码$C_{\overline{D}_{\le t}}$是一个3元[32,4]线性码。经MAGMA计算，$C_{\overline{D}_{\le t}}$的最小距离为20，则码$C_{\overline{D}_{\le t}}$是一个3元[33,4,20]线性码。由定理8，码$C_{\overline{D}_{\le t}}^{\perp}$是一个3元[33,29,3]LCD最优码。

4　比较

文献[14]4类合适的定义集构造了4类3元LCD码和自正交码，它们的参数分别为$\left[2^t\binom{m}{t},2^t\binom{m}{t}-m,2\right]$，其中$1\le t\le m$；$\left[2^t\binom{m}{t}+2^m,2^t\binom{m}{t}+2^m-m,2\right]$，其中$1\le t\le m-1$；

$$\left[\sum_{i=1}^{t}2^i\binom{m}{i},\sum_{i=1}^{t}2^i\binom{m}{i}-m,2\right] \tag{29}$$

其中，$1\le t\le m$和$\left[\sum_{i=1}^{t}2^i\binom{m}{i}+2^m,\sum_{i=1}^{t}2^i\binom{m}{i}+2^m-m,2\right]$，其中$1\le t\le m$。

当$m\equiv 4(\mathrm{mod}5)$时，在定理2中，令$t=i$。在文献[14]的定理3.6中，令$t=i+1$且i和m满足$i=\dfrac{4m-1}{5}$，有$2^{\frac{4m-1}{5}-1}\binom{m}{\frac{4m-1}{5}}=2^{\frac{4(m+1)}{5}}\binom{m}{\frac{4(m+1)}{5}}$，此时本文构造的码距离更大。

当$\binom{m}{i}=\dfrac{2^m-1}{2^{i-1}-2^{m-i}}$时，在定理4中，令$t=i$。在文献[14]的定理3.8中，令$t=m-i$。有$2^{i-1}\binom{m}{i}+1=2^{m-i}\binom{m}{m-i}$，此时本文构造的码距离更大。

当$\sum_{i=1}^{b}2^i\binom{m}{i}=\sum_{i=b+1}^{a}2^i\binom{m}{i}$时，在定理6中，令$t=a$。在文献[14]的定理3.10中，令$t=b$，其中$a>b$。有$\sum_{i=1}^{a}2^{i-1}\binom{m}{i}=\sum_{i=1}^{b}2^i\binom{m}{i}$，此时本文构造的码距离更大。

当$\sum_{i=b+1}^{a}2^i\binom{m}{i}-\sum_{i=1}^{b}2^i\binom{m}{i}=2^{m+1}-2$时，在定理8中，令$t=a$。在文献[14]的定理3.12中，令$t=b$，其中$a>b$。有

$$1+\sum_{i=1}^{a}2^{i-1}\binom{m}{i}=\sum_{i=1}^{b}2^i\binom{m}{i}+2^m \tag{30}$$

此时本文构造的码距离更大。

文献[4]构造了3元$[n,n-k,3]$自正交码，其中$n=4+9i$或$n=9j$，$N_{k-1}\le n\le N_k$，$N_k=\dfrac{3^k-1}{3-1}$，$k\ge 3$。

当$2^{t-1}\binom{m}{t}\not\equiv 0,4(\mathrm{mod}9)$或$2^{t-1}\binom{m}{t}\not\equiv 3,8(\mathrm{mod}9)$时，定理2和定理4构造出和文献[3]不同参数的码。

当$\sum_{i=1}^{t}2^{i-1}\binom{m}{i}\not\equiv 0,4(\mathrm{mod}9)$或$\sum_{i=1}^{t}2^{i-1}\binom{m}{i}\not\equiv 3,8(\mathrm{mod}9)$时，定理6和定理8构造出和文献[3]不同参数的码。

5　结束语

本文研究了3元LCD码和自正交码的构造。根据有限域F_q上线性码是LCD码和自正交码的充要条件，通过选择了4类合适的定义集构造出3元LCD码和自正交码，接着研究了这4类线性码的对偶码，得到一些3元最优码。下一步研究的问题是通过选择合适的定义集构造一般域上的自正交码。

参 考 文 献

[1] COHEN G, ENCHEVA S, and LITSYN S. On binary constructions of quantum codes[J]. *IEEE Transactions on Information Theory*, 1999, 45(7): 2495–2498. doi: 10.1109/18.796389.

[2] SHI Minjia, ÖZBUDAK F, XU Li, *et al*. LCD codes from tridiagonal Toeplitz matrices[J]. *Finite Fields and Their Applications*, 2021, 75: 101892. doi: 10.1016/J.FFA.2021.101892.

[3] 陈刚, 李瑞虎. 三元域上对偶距离为3的自正交码构造[J]. 计算机工程与应用, 2011, 47(16): 38–39. doi: 10.3778/j.issn.1002-8331.2011.16.012.

CHEN Gang and LI Ruihu. Construction of self-orthogonal codes with dual distance three on ternary filed[J]. *Computer Engineering and Applications*, 2011, 47(16): 38–39. doi: 10.3778/j.issn.1002-8331.2011.16.012.

[4] CHEN Gang and LI Ruihu. Ternary self-orthogonal codes of dual distance three and ternary quantum codes of distance three[J]. *Designs, Codes and Cryptography*, 2013, 69(1): 53–63. doi: 10.1007/s10623-012-9620-7.

[5] 李益群, 刘三阳, 王雷. F_4上的3维最优自正交码[J]. 西北大学学报:自然科学版, 2006, 36(6): 871–874.

LI Yiqun, LIU Sanyang, and WANG Lei. Optimal quaternary self-orthogonal codes of dimension three[J].

Journal of Northwest University:Natural Science Edition, 2006, 36(6): 871–874.

[6] SOK L, SHI Minjia, and SOLÉ P. Constructions of optimal LCD codes over large finite fields[J]. *Finite Fields and Their Applications*, 2018, 50: 138–153. doi: 10.1016/j.ffa.2017.11.007.

[7] CARLET C and GUILLEY S. Complementary dual codes for counter-measures to side-channel attacks[M]. PINTO R, MALONEK P R, and VETTORI P. Coding Theory and Applications. Cham: Springer, 2015: 97–105. doi: 10.1007/978-3-319-17296-5_9.

[8] YANG Xiang and MASSEY J L. The condition for a cyclic code to have a complementary dual[J]. *Discrete Mathematics*, 1994, 126(1/3): 391–393. doi: 10.1016/0012-365x(94)90283-6.

[9] SENDRIER N. Linear codes with complementary duals meet the Gilbert–Varshamov bound[J]. *Discrete Mathematics*, 2004, 285(1/3): 345–347. doi: 10.1016/j.disc.2004.05.005.

[10] 唐春明, 吴虹佳, 亓延峰. 有限域上的LCD码和LCP码[J]. 西华师范大学学报:自然科学版, 2020, 41(1): 1–10. doi: 10.16246/j.issn.1673-5072.2020.01.001.

TANG Chunming, WU Hongjia, and QI Yanfeng. LCD codes and LCP codes over finite fields[J]. *Journal of China West Normal University:Natural Sciences*, 2020, 41(1): 1–10. doi: 10.16246/j.issn.1673-5072.2020.01.001.

[11] CARLET C, MESNAGER S, TANG Chunming, *et al*. Linear codes over $\mathbb{F}_q$ are equivalent to LCD codes for $q>3$[J]. *IEEE Transactions on Information Theory*, 2018, 64(4): 3010–3017. doi: 10.1109/TIT.2018.2789347.

[12] 宋倩, 李瑞虎, 付强, 等. 五元域上LCD码的构造[J]. 空军工程大学学报, 2018, 19(5): 104–108. doi: 10.3969/j.issn.1009-3516.2018.05.018.

SONG Qian, LI Ruihu, FU Qiang, *et al*. On the construction of LCD codes over F_5[J]. *Journal of Air Force Engineering University:Natural Science Edition*, 2018, 19(5): 104–108. doi: 10.3969/j.issn.1009-3516.2018.05.018.

[13] ZHOU Zhengchun, LI Xia, TANG Chunming, *et al*. Binary LCD codes and self-orthogonal codes from a generic construction[J]. *IEEE Transactions on Information Theory*, 2019, 65(1): 16–27. doi: 10.1109/TIT.2018.2823704.

[14] LI Xia, CHENG Feng, TANG Chunming, *et al*. Some classes of LCD codes and self-orthogonal codes over finite fields[J]. *Advances in Mathematics of Communications*, 2019, 13(2): 267–280. doi: 10.3934/amc.2019018.

[15] 钱毅, 李平, 唐永生. 一种四元厄米特LCD码与厄米特自正交码的构造方法[J]. 电子学报, 2020, 48(3): 577–581. doi: 10.3969/j.issn.0372-2112.2020.03.022.

QIAN Yi, LI Ping, and TANG Yongsheng. A construction method of quaternary hermitian LCD codes and hermitian self-orthogonal codes[J]. *Acta Electronica Sinica*, 2020, 48(3): 577–581. doi: 10.3969/j.issn.0372-2112.2020.03.022.

[16] PANG Binbin, ZHU Shixin, and KAI Xiaoshan. Some new bounds on LCD codes over finite fields[J]. *Cryptography and Communications*, 2020, 12(4): 743–755. doi: 10.1007/s12095-019-00417-y.

[17] HUFFMAN W C and PLESS V. Fundamentals of Error-Correcting Codes[M]. Cambridge: Cambridge University Press, 2010: 48–52.

李 平：男，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.

张嘉媛：女，硕士生，研究方向为代数编码.

孙中华：男，副教授，硕士生导师，研究方向为代数编码.

责任编辑：余 蓉