五元域上 LCD 码的构造

宋　倩，李瑞虎，付　强，杨瑞磻
(空军工程大学基础部，西安，710051)

摘要　基于最优线性码与射影几何理论，针对不同码长最优码的距离特性，研究了低维五元最优 LCD 码的构造。首先利用删截等方法构造了较小码长的三维和四维最优线性码以及最优 LCD 码；其次，借助部分已知矩阵和删截等方法构造了较大码长的三维和四维最优线性码以及最优 LCD 码；最后，利用已知最优 LCD 码和特殊码长最优自正交码构造了任意大码长的最优 LCD 码，完全解决了三维和四维最优 LCD 码的构造问题。这些 LCD 码的构造方法对于五元高维最优 LCD 码以及一般域上最优 LCD 码的研究具有重要的理论指导意义。

关键词　五元最优码；生成矩阵；LCD 码；自正交码；射影几何
DOI　10.3969/j.issn.1009-3516.2018.05.018
中图分类号　O157.4　　**文献标志码**　A　　**文章编号**　1009-3516(2018)05-0104-05

On the Construction of LCD Codes over F_5

SONG Qian, LI Ruihu, FU Qiang, YANG Ruipan
(Department of Basic Science, Air Force Engineering University, Xi'an 710051, China)

Abstract: Focuses on the construction of low-dimensional optimal LCD codes over F_5 on the basis of the theory of optimal codes, projective geometry in view of the characteristic of the distance of optimal codes. First, via some known and puncturing, the paper constructs a short-distance optimal and optimal LCD codes of dimension 3 and 4. Then the theory of projective geometry is used to construct those codes with long-distance. Moreover, with the combination of the known optimal LCD codes and optimal self-orthogonal codes, the paper can construct any long-distance optimal LCD codes. With these methods, all the optimal LCD codes of dimension 3 and 4 can be solved. The theories and methods of constructing LCD codes have a certain of important guiding significance for the study of high-dimensional optimal LCD codes over F_5 and those over general field.

Key words: optimal 5-ary codes; generator matrix; LCD codes; self-orthogonal codes; projective geometry

根据实际应用的需求，设计不同特性的最优码，一直是编码研究和使用中最关键的问题[1]。线性补对偶码(Linear Codes with Complementary Dual)，简称 LCD 码。近年来，人们发现 LCD 码能够防御侧信道攻击。这是特殊线性码除数据存储和通信系统之外的另一项新用途。近几年 LCD 码成为研究的热点，而构造最优 LCD 码则是研究的重点和难点。

收稿日期：2018-03-05
基金项目：国家自然科学基金(11471011)
作者简介：宋　倩(1993—)，女，江苏无锡人，硕士生，主要从事代数编码与密码研究。E-mail:352029356@qq.com

引用格式：*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(自然科学版)，2018，19(5)：104-108．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.*

LCD 码，最先称为可逆码，由 Massey 于 1964 年首次提出[2]。1992 年，Massey[3] 给出了线性 LCD 码的严格定义：即当码 C 满足 $C\cap C^{\perp}=\{0\}$ 时，称 C 为线性补对偶码。同时，通过对 LCD 码进一步研究，他解决了 2 个问题：一是证明了渐近最优 LCD 码的存在性；二是 LCD 码可为双用户双边加法器信道提供最优线性编码方法。2014 年，Carlet 等学者发现 LCD 码能够防御边带信道攻击，在密码学中具有重要应用价值[4]。此后，人们对 LCD 码的构造和应用进行深入、广泛的研究[5-15]。比如，极大纠缠辅助量子码能够由最优 LCD 码导出[5-8]；一些类似于线性码的最优 LCD 码基础理论与构造方法也逐步确立[6-15]。(本文探讨了 LCD 码的构造并完全解决了 3 维和 4 维最优 LCD 码的构造问题)。

1　预备知识

设 $F_5=\{0,1,2,3,4\}$ 为五元域，F_5^n 为 F_5 上 n 维向量空间，若 C 为 F_5^n 的 k 维子空间，则称 C 为码长为 n 的 k 维五元线性码，C 中每一个向量称为 C 的一个码字。若 C 中所有非零码字的最小 Hamming 重量为 d，则称 d 为 C 的距离，记做 $C=[n,knd]_5$。如果不存在 $[n,k,d+1]_5$ 码，则称 C 为最优线性码。

关于任意 q-元最优线性码有如下著名的上界——Griesmer 界：若存在 $[n,k,d]_q$ 码，则有：

$$n\geqslant g(k,d)=\sum_{i=0}^{k-1}\left\lceil\frac{d}{q^i}\right\rceil$$

使等式成立的码叫 Griesmer 码，Griesmer 码一定是最优码，但是最优线性码未必都能达到 Griesmer 界，为此，我们称最优线性码饱和 Griesmer 界。

对于任意线性码 $[n,k,d]_q$，记其为 C，令 $C^{\perp}=\{x\mid x\cdot c=0,c\in C\}$，称 $C^{\perp}$ 为 C 的对偶码。当 $C\subseteq C^{\perp}$，称 C 为自正交码。

以 C 的任意一组仅为行向量的矩阵 $\boldsymbol{G}$ 叫做 C 的生成矩阵，而 $C^{\perp}$ 的生成矩阵叫做 C 的校验矩阵. 熟知，C 为自正交码当且仅当 $\boldsymbol{G}\boldsymbol{G}^{\mathrm{T}}=0$。

定理 1.1[3]　设 C 是一个线性码。$\boldsymbol{G}$ 是 C 的生成矩阵，$\boldsymbol{H}$ 是其校验阵，则以下 3 个条件等价：

1) C 是 LCD 码；

2) $\boldsymbol{H}\boldsymbol{H}^{\mathrm{T}}$ 是可逆的；

3) $\boldsymbol{G}\boldsymbol{G}^{\mathrm{T}}$ 是可逆的。

为简化下文叙述，作如下规定：

1) 下文讨论的均为五元线性码，$[n,k,d]_5$ 简记为 $[n,k,d]$。为区别起见，用 $\boldsymbol{L}_{k,n}$ 代表 $[n,k,d]$ 最优 LCD 码的生成阵，而用 $\boldsymbol{G}_{k,n}$ 代表一般 $[n,k,d]$ 最优码的生成阵。

令 Z^+ 表示正整数集合，用 $N(a,b)$ 表示连续取值的正整数集合 $\{a,a+1,a+2,\cdots,b\}$ $(a,b\in Z^+)$。用 $\boldsymbol{1}_n=(1,\cdots,1)_{1\times n}$ 和 $\boldsymbol{0}_n=(0,\cdots,0)_{1\times n}$ 分别表示全 1 与全 0 向量。

2) 将一个矩阵看作列向量的集合，若 $\boldsymbol{A}$ 为一个矩阵，$\boldsymbol{\alpha}$ 为 $\boldsymbol{A}$ 中一个列向量，则可将其记作 $\boldsymbol{\alpha}\in\boldsymbol{A}$，$(\boldsymbol{A}\backslash\alpha)$ 表示在 $\boldsymbol{A}$ 中删除 α 后剩余列向量构成的矩阵。

$(\boldsymbol{A}\mid\boldsymbol{B})$ 表示矩阵 $\boldsymbol{A}$ 和矩阵 $\boldsymbol{B}$ 并置而得到的新矩阵，用 $m\boldsymbol{A}$ 表示 m 个矩阵 $\boldsymbol{A}$ 并置而成的新矩阵 $(m\in Z^+)$。

假设 $\boldsymbol{B}$ 为 $\boldsymbol{A}$ 的子集，$(\boldsymbol{A}\backslash\boldsymbol{B})$ 表示在矩阵 $\boldsymbol{A}$ 中删除矩阵 $\boldsymbol{B}$ 后剩余列向量构成的矩阵。

3) 若 $\boldsymbol{A}$ 为 $m\times n$ 矩阵，则 $\overline{\boldsymbol{A}}=\begin{pmatrix}\boldsymbol{0}_n\\ \boldsymbol{A}\end{pmatrix}$ 和 $\overline{\overline{\boldsymbol{A}}}=\begin{pmatrix}\boldsymbol{0}_{2\times n}\\ \boldsymbol{A}\end{pmatrix}$ 分别为 $(m+1)\times n$ 和 $(m+2)\times n$ 矩阵。记：

$$\boldsymbol{\alpha}=(0,0,1)^{\mathrm{T}},\boldsymbol{\beta}=(0,0,0,1)^{\mathrm{T}},$$

$$\boldsymbol{\gamma}=(0,1)^{\mathrm{T}},\boldsymbol{A}_{2,5}=\begin{pmatrix}11111\\01234\end{pmatrix}。$$

利用以上的几个矩阵和向量我们可构造如下自正交码的矩阵：

$$\boldsymbol{A}_{3,25}=\begin{bmatrix}\boldsymbol{A}_2 & \boldsymbol{A}_2 & \boldsymbol{A}_2 & \boldsymbol{A}_2 & \boldsymbol{A}_2\\ \boldsymbol{0}_5 & \boldsymbol{1}_5 & \boldsymbol{2}_5 & \boldsymbol{3}_5 & \boldsymbol{4}_5\end{bmatrix},$$

$$\boldsymbol{A}_{3,50}=(\boldsymbol{A}_{3,25}\mid\boldsymbol{A}_{3,24}),\ \boldsymbol{A}_{3,30}=(\boldsymbol{A}_{3,25}\mid\overline{\boldsymbol{A}}_{2,5}),$$

$$\boldsymbol{A}_{3,62}=(\boldsymbol{A}_{3,30}\mid\boldsymbol{A}_{3,30}\mid\boldsymbol{\alpha},2\boldsymbol{\alpha}),$$

$$\boldsymbol{A}_{4,125}=\begin{bmatrix}\boldsymbol{A}_{3,25} & \boldsymbol{A}_{3,25} & \boldsymbol{A}_{3,25} & \boldsymbol{A}_{3,25} & \boldsymbol{A}_{3,25}\\ \boldsymbol{0}_{25} & \boldsymbol{1}_{25} & 2\cdot\boldsymbol{1}_{25} & 3\cdot\boldsymbol{1}_{25} & 4\cdot\boldsymbol{1}_{25}\end{bmatrix},$$

$$\boldsymbol{A}_{4,150}=(\boldsymbol{A}_{4,125}\mid\overline{\boldsymbol{A}}_{3,25}),\boldsymbol{A}_{4,155}=(\boldsymbol{A}_{4,150}\mid\overline{\overline{\boldsymbol{A}}}_{2,5}),$$

$$\boldsymbol{A}_{4,315}=(\boldsymbol{A}_{4,155}\mid\boldsymbol{A}_{4,155}\mid\boldsymbol{\beta},2\boldsymbol{\beta})。$$

它们所生成码的参数分别为 [25,3,20]，[30,3,24]，[62,3,50]，[125,4,100]，[150,4,120]，[155,4,124] 及 [312,4,250]。

令 $\boldsymbol{S}_2(\boldsymbol{A}_{2,5}\mid\gamma)$ 为 2 维 Simplex 码的生成矩阵，利用 $\boldsymbol{S}_2$ 可递归构造出 k 维 Simplex 码的生成矩阵

$$\boldsymbol{S}_k=\begin{bmatrix}\boldsymbol{S}_{k-1} & \boldsymbol{0}_{k-1}^{\mathrm{T}} & \boldsymbol{S}_{k-1} & \boldsymbol{S}_{k-1} & \boldsymbol{S}_{k-1} & \boldsymbol{S}_{k-1}\\ \boldsymbol{0}_{n_{k-1}} & \boldsymbol{1} & \boldsymbol{1}_{n_{k-1}} & \boldsymbol{2}\cdot\boldsymbol{1}_{n_{k-1}} & \boldsymbol{3}\cdot\boldsymbol{1}_{n_{k-1}} & \boldsymbol{4}\cdot\boldsymbol{1}_{n_{k-1}}\end{bmatrix}$$

五元最优码的研究至今已有 20 余年，但进展缓慢[16-23]。关于五元三维最优码的存在性问题，现已得到解决[24]；五元四维最优码的存在性问题，接近完全解决；而五元更高维最优码的存在性问题，还远未能确定[16-20]。但在以前对五元最优码的研究中，人们并未涉及 LCD 的概念，如何构造具有 LCD 性质的 $[n,k,d]$ 最优码，目前仍无具体通用的方法，而

现有文献中给出的最优 LCD 码并不多,为此需进行深入研究。我们在 2017 年用最优线性码、置换理论和单项变换等方法研究了较小码长最优 LCD 码的构造问题,主要结果如下:

命题 1.1　1) 若 $3\leqslant n\leqslant 62$,则可构造 $[n,3,d]$ 最优 LCD 码,其生成阵 $\boldsymbol{L}_{3,n}$ 如文献[25]所述。

2) 若 $4\leqslant n\leqslant 156$,则可构造 $[n,4,d]$ 最优 LCD 码,其生成阵 $\boldsymbol{L}_{4,n}$ 如文献[25]所述。

下文将在本节的基础上,进一步给出三维和四维最优 LCD 码的构造。

2　三维最优 LCD 码的构造

为完全解决三维最优 LCD 码的构造问题,我们先构造几个特定码长的三维最优 LCD 码,然后按照码长 $63\leqslant n\leqslant 93$ 以及 $n\geqslant 94$ 分情况讨论。文献[26]中已给出 $k=3$,$3\leqslant n\leqslant 62$ 的最优生成阵。

2.1　码长 n 满足 $63\leqslant n\leqslant 93$ 时三维最优 LCD 码

1) $n=63,64$ 时,分别构造 $\boldsymbol{L}_{3,63}=(\boldsymbol{L}_{3,38}\mid\boldsymbol{A}_{3,25})$,$\boldsymbol{L}_{3,64}=(\boldsymbol{L}_{3,39}\mid\boldsymbol{A}_{3,25})$;

2) $n=62+i$,$3\leqslant i\leqslant 6$,$9\leqslant i\leqslant 11$,$15\leqslant i\leqslant 17$ 以及 $21\leqslant i\leqslant 31$ 时,构造 $\boldsymbol{L}_{3,n}=(\boldsymbol{L}_{3,i}\mid\boldsymbol{A}_{3,62})$。

3) $n=69$ 时,$\boldsymbol{L}_{3,69}=(\boldsymbol{L}_{3,39}\mid\boldsymbol{A}_{3,30})$;$n=70$ 时,$\boldsymbol{L}_{3,70}=(\boldsymbol{L}_{3,40}\mid\boldsymbol{A}_{3,30})$;

4) $n=74,75,79,80,81$ 时,$\boldsymbol{L}_{3n}=(\boldsymbol{L}_{3,n-50}\mid\boldsymbol{A}_{3,50})$。

由文献[23]、[25]以及第 1 节中最优自正交码的构造,不难验证 $63\leqslant n\leqslant 93$ 时,所构造的 $\boldsymbol{L}_{3,81}$ 生成相应码长的三维最优 LCD 码。

2.2　码长 n 满足 $n\geqslant 94$ 时的三维最优 LCD 码

$n=31t+j_1$,$0\leqslant j_1\leqslant 30$,则 $t\geqslant 3$。

1) 若 $t=2m+1$ 为奇数,当 $n=62m+(31+j)$ 时,$\boldsymbol{L}_{3,n}=(\boldsymbol{L}_{3,31+j}\mid\boldsymbol{A}_{3,62})$。

2) 若 $t=2m$ 为偶数,则 $n=31\times 2m+j=62(m-1)+(62+j)$ 且 $62\leqslant 62+j\leqslant 93$,构造 $\boldsymbol{L}_{3,n}=(\boldsymbol{L}_{3,31+j}\mid(m-1)\boldsymbol{A}_{3,61})$。由文献[23]和 Griesmer 界可知上述 $\boldsymbol{L}_{3,n}$ 生成最优线性码,而命题 1.1 和 2.1 小节则可保证 $\boldsymbol{L}_{3,n}$ 生成最优 LCD 码。于是定理 2.1 得证。

定理 2.1　若码长 $n\geqslant 3$,存在参数为 $[n,3,d]$ 的三维最优 LCD 码。

3　四维最优 LCD 码的构造

为完全解决四维最优 LCD 码的构造问题,我们利用有限几何理论先构造几个特定码长的四维最优 LCD 码,然后再按照码长 $157\leqslant n\leqslant 624$ 以及 $n\geqslant 625$ 分情况讨论四维最优 LCD 码。

3.1　特定码长 n 的四维最优 LCD 码

设 $\boldsymbol{S}_4$ 为 4 维 Simplex 码的生成阵,我们选取 $\boldsymbol{S}_4$ 中任意 3 个互不相关的向量组成向量组,构造 6 个向量组 $\boldsymbol{F}_1,\boldsymbol{F}_2,\cdots,\boldsymbol{F}_5,\boldsymbol{F}_5$ 是非平凡相交向量组,经筛选得到如下:

$$\boldsymbol{F}_1=\begin{pmatrix}130\\433\\123\\302\end{pmatrix},\boldsymbol{F}_2=\begin{pmatrix}111\\423\\040\\112\end{pmatrix},\boldsymbol{F}_3=\begin{pmatrix}110\\431\\240\\442\end{pmatrix},$$

$$\boldsymbol{F}_4=\begin{pmatrix}111\\241\\400\\432\end{pmatrix},\boldsymbol{F}_5=\begin{pmatrix}111\\042\\234\\214\end{pmatrix},\boldsymbol{F}_6=\begin{pmatrix}111\\042\\234\\214\end{pmatrix}$$

设 $\boldsymbol{F}_i$ 生成的子空间 $\boldsymbol{V}_i$,$\boldsymbol{V}_i$ 中首一向量组成向量组 $\boldsymbol{E}_i$,则可得到 $\boldsymbol{E}_1,\boldsymbol{E}_2,\boldsymbol{E}_3,\boldsymbol{E}_4,\boldsymbol{E}_5$ 和 $\boldsymbol{E}_6$。令 $\boldsymbol{S}_{156}\backslash(\boldsymbol{E}_1\cup\boldsymbol{E}_3)=\boldsymbol{E}_{4,100}$,然后在 $\boldsymbol{E}_{4,100}$ 中选取 2 个互不相关的向量 $\boldsymbol{u}_1,\boldsymbol{u}_1$,记其生成的子空间为 $\boldsymbol{W}_1$,选取 $\boldsymbol{W}_1$ 中首一向量,得到向量组:

$$(\boldsymbol{u}_1,\boldsymbol{u}_2)=\begin{pmatrix}11\\43\\20\\11\end{pmatrix},\boldsymbol{B}_6=\begin{pmatrix}110111\\341012\\022413\\110111\end{pmatrix}$$

在 $\boldsymbol{E}_5$ 中分别选取与 $\boldsymbol{E}_2$ 和 $\boldsymbol{E}_4$ 重复的列,这些列组成的向量组分别记为 $\boldsymbol{H}_6$ 和 $\boldsymbol{I}_6$。

$$\boldsymbol{A}_1=\begin{pmatrix}1111111111111000011101111011111\\4320310414142110102310123101234\\2142031014031101232434203404321\\2302413430413404312020241140123\end{pmatrix}$$

$$\boldsymbol{A}_2\begin{pmatrix}1111010111011111111010111110111\\3210141200141043214031123041123\\0432100310441432142112024313203\\2104114420241321020243420130333\end{pmatrix}$$

于是,我们可以进一步构造:

$$\boldsymbol{B}_{62}=(\boldsymbol{A}_1\mid\boldsymbol{A}_2),\boldsymbol{B}_{68}=(\boldsymbol{B}_{62}\mid\boldsymbol{H}_6),$$

$$\boldsymbol{B}_{74}=(\boldsymbol{B}_{68}\mid\boldsymbol{I}_6),$$

$$\boldsymbol{B}_{124}=3\boldsymbol{S}_{156}\backslash(\boldsymbol{E}_1\mid\boldsymbol{E}_3\mid\boldsymbol{E}_5\mid\boldsymbol{E}_6)$$

基于以上步骤所得到的结果,我们可以构造 $\boldsymbol{L}_{4,168}=(\boldsymbol{L}_{4,167}\mid(0001)^{\mathrm{T}})$,$\boldsymbol{L}_{4,169}=(\boldsymbol{L}_{4,170}\backslash(1000)^{\mathrm{T}})$,$\boldsymbol{L}_{4,170}=(\boldsymbol{L}_{4,176}\backslash\boldsymbol{B}_6)$,$\boldsymbol{L}_{4,312}=(\boldsymbol{L}_{4,156}\mid\boldsymbol{L}_{4,244}=(\boldsymbol{L}_{312}\backslash\boldsymbol{B}_{68}))$,$\boldsymbol{L}_{4,182}=(\boldsymbol{G}_{4,26}\mid\boldsymbol{L}_{4,145})$;这些矩阵都能生成相应码长的四维最优 LCD 码。

3.2　码长 n 满足 $157\leqslant n\leqslant 624$ 时的四维最优 LCD 码

在 3.1 节的基础上,下面分 6 种类型具体给出最优 LCD 码的生成矩阵,用递归的方法简要给出构

造结果。

1）若 $n\in[159,161]$，构造 $\boldsymbol{L}_{4,n}=(\boldsymbol{L}_{4,n-155}\mid\boldsymbol{A}_{4,155})$。若 n 属于$[171,177]$，$[221,227]$或者$[316,331]$，构造 $\boldsymbol{L}_{4,n}=(\boldsymbol{L}_{4,n-15}\mid\boldsymbol{A}_{4,150})$。

2）若 $n=220$ 或属于下面任意一个区间$[162,165]$，$[183,189]$，$[190,202]$，$[203,219]$，$[245,283]$，$[312,315]$，$[345,377]$，$[407,432]$，$[496,500]$，$[515,531]$；构造 $\boldsymbol{L}_{4,n}=(\boldsymbol{L}_{4,n-125}\mid\boldsymbol{A}_{4,125})$。

3）若 $n\in[166,167]$，$[178,181]$，$[284,311]$；构造 $\boldsymbol{L}_{4,n}=(\boldsymbol{L}_{4,n-155}\mid\boldsymbol{A}_{4,155})$。

4）若 $n\in[378,406]$，构造 $\boldsymbol{L}_{4,n}=(\boldsymbol{L}_{4,n-250}\mid\boldsymbol{A}_{4,250})$。

5）若 $n\in[433,468]$，$[469,495]$，$[501,514]$，$[532,624]$；构造 $\boldsymbol{L}_{4,n}=(\boldsymbol{L}_{4,n-312}\mid\boldsymbol{A}_{4,312})$。

6）ε 表示从给定矩阵 $\boldsymbol{L}$ 中删去 $\boldsymbol{K}$ 矩阵的前 ξ 列。若 $n\in[239,242]$，$\boldsymbol{L}_{4,n}=\varepsilon(\boldsymbol{L}_{4,244},\boldsymbol{K}_{244-n},\xi)$，$\xi=244-n$。

利用文献[20]和 Griesmer 界可逐条验证上述 $\boldsymbol{L}_{4,n}$生成最优线性码，而命题 1.2 和 3.1 节则可保证 $\boldsymbol{L}_{4,n}$生成最优 LCD 码。

3.3　码长 n 满足 $n\geqslant 625$ 时的四维最优 LCD 码

若 $625\leqslant n\leqslant 780$，令 $n_1=n-312$，则 $313\leqslant n_1\leqslant 468$，构造 $\boldsymbol{L}_{4,n}=(\boldsymbol{L}_{4,n-312}\mid\boldsymbol{A}_{4,312})$。

当 n 满足 $n\geqslant 781$ 时，令 $n=156\times t+n_2$，$0\leqslant n_2\leqslant 155$，则 $t\geqslant 5$。

1）若 $t=2m+1\geqslant 5$，$n=156t+n_1=312(m-1)+(456+n_1)$，构造 $\boldsymbol{L}_{4,n}=(\boldsymbol{L}_{4,456+n_2}\mid(m-1)\boldsymbol{A}_{4,312})$。

2）$t=2m\geqslant 6$，$n=312(m-1)+(312+n_2)$，构造 $\boldsymbol{L}_{4,n}=(\boldsymbol{L}_{4,312+n_2}\mid(m-1)\boldsymbol{A}_{4,312})$。

利用 3.1 节和 3.2 节，依据 Griesmer 界可逐条验证上述 $\boldsymbol{L}_{4,n}$生成最优 LCD 码。

总结前文，即证得以下定理成立：

定理 3.1　若码长 $n\geqslant 4$，存在参数为$[n,4,d]$的四维最优 LCD 码。

4　结语

本文利用五元域上的最优线性码、射影几何等理论为基础，具体构造出三维、四维最优 LCD 码的生成矩阵，彻底解决了五元三维、四维最优 LCD 码的构造问题。文中所得的 LCD 码除码长为 183～189，203～219 的 4 维码达不到 Griesmer 界，其余 LCD 码都是饱和 Griesmer 界的。经判断，当 $k=3$，$n\geqslant 62$ 时，所构造的三维 LCD 码都达到界[27]；当 $k=4$，$n\geqslant 624$ 时，所构造的三维 LCD 码都达到界。

参考文献(References)：

[1] HUFFMAN W，PLESS V. Fundamentals of Error-Correcting Codes[M]. Cambridge：Cambridge University Press，2003.

[2] MASSEY J. Reversible Codes[J]. Information and Control，1964，7(3)：369-380.

[3] MASSEY J. 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 [J]. Coding Theory and Applications，2015，10(1)：131-150.

[5] QIAN J，ZHANG L. Entanglement-Assisted Quantum Codes from Arbitrary Binary Linear Codes[J]. Designs Codes and Cryptography，2015，77(1)：193-202.

[6] LU L D，LI R H，GUO L B，et al. Maximal Entanglement Entanglement-Assisted Quantum Codes Constructed from Linear Codes[J]. Quantum Information Processing，2015，14(1)：165-182.

[7] GUENDA K，JITMAN S，GULLIVER T. Constructions of Good Entanglement-Assisted Quantum Error Correcting Codes [J]. Designs Codes and Cryptography，2018，86 (1)：121-136.

[8] LU L D，LI R H，GUO L B. Entanglement-Assisted Quantum Codes from Quaternary Codes of Dimension Five[J]. International Journal of Quantum Information，2017，15(3)：1750017.

[9] HOU X，OGGIER F. On LCD Codes and Lattices [C]// IEEE International Symposium on Information Theory. Barcelona，Spain，2016：1501-1505.

[10] LINA E，NOCON E. On the Construction of Some LCD Codes over Finite Fields[J]. Manila Journal of Science，2016，9：67-82.

[11] BOONNIYOMA K，JITMAN S. Complementary Dual Subfield Linear Codes over Finite Fields[EB/OL]. (2016-5-22)[2017-12-03]. http：// arxiv. org/ abs/ 1605. 06827v1.

[12] ZHU S，PANG B，SUN Z. The Reversible Negacyclic Codes over Finite Fields [EB/OL]. (2016-10-26) [2017-12-03]. http：//arxiv. org/abs/1610. 08206v1.

[13] JIN L. Construction of MDS Codes with Conplementary Duals [J]. IEEE Transactions on Information Theory，2017，63 (5)：2843-2847.

[14] LIU X，FAN Y，LIU H. Galois LCD Codes over Finite Fields [J]. Finite Fields and Their Applications，2018，49：227-242.

[15] CARLET C，MMSNAGER S，TANG C，et al. Linear Codes over F_q Which are Equivalent to LCD Codes for $q>3$[J]. IEEE Transactions on Information Theory，2018，64 (4)：3010-3017.

[16] FUKUI M，MARUTA T. Optimal Linear Codes over

GF(5) [J]. Rims Kokyuroku, 1995: 910.

[17] BOUKLIEV I, DASKALOV R, KAPRALOV. Optimal Quaternary Linear Codes of Dimension Five[J]. IEEE Press, 1996, 42(4): 1228-1235.

[18] KAGEYAMA Y, MARUTA T. New 5-dimensional Linear Codes over F_5 [C]// The 7th International Workshop on Optimal Codes and Related Topics. 2013, Albena, Bulgaria, 107-112.

[19] CHOEN E, KATO T, KIM S. On the Minimum Length of Some Linear Codes of Dimension 5 [J]. Designs Codes and Cryptography, 2005, 37 (3): 421-434.

[20] BOUYUKLIEV I, KAGEYAMA Y, MARUTA T. On the Minimum Length of Linear Codes over F_5[J]. Discrete Mathematics, 2015, 338(6): 938-953.

[21] KAGEYAMA Y, MARUTA T. On the Construction of Griesmer Codes of Dimension 5 [J]. Designs Codes and Cryptography, 2013, 75(2): 1-4.

[22] MARUTA T. On the Nonexistence of q-ary Linear Codes of Dimension Five [J]. Designs Codes and Cryptography, 2001, 22(2): 165-177.

[23] DODUNEKOV S M. Optimal Linear Codes [C]// Mathematics & Mathematical Education. 1986: 57-68.

[24] MARUTA T, SHINOHARA M, KIKUI A. On Optimal Linear Codes over F_5[J]. Discrete Mathematics, 2009, 309(6): 1255-1272.

[25] SONG Q, LI R H, FU Q, et al. On the Construction of LCD Codes over F_5 [C]// ITM Web of Conferences. Suzhou, China, 2017: 04006.

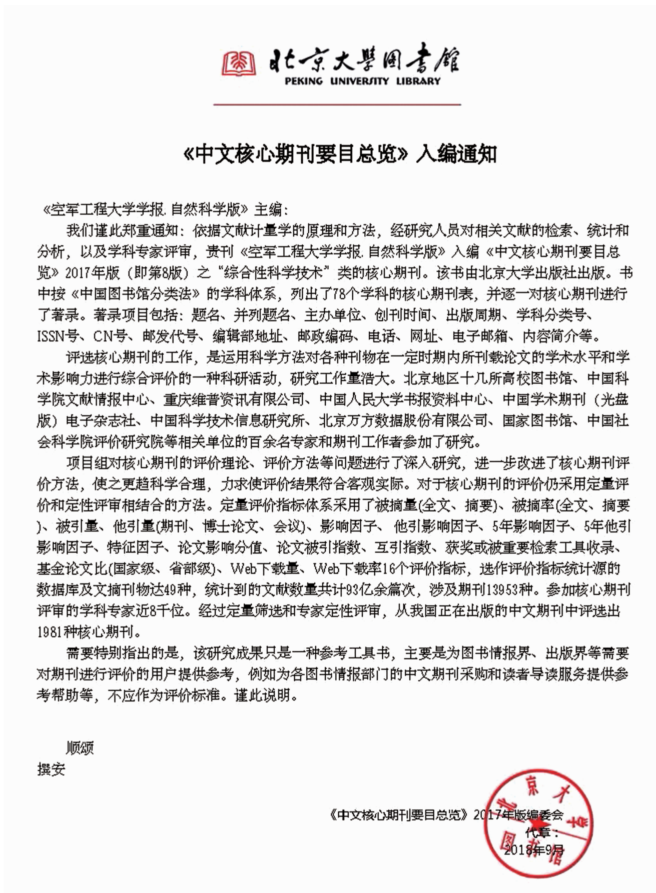
[26] BOUKLIEV I, KAPRALOV S, MARUTA T, et al. Optimal Linear Codes of Dimension 4 over F_5 [J]. IEEE Transactions on Information Theory, 1997, 43 (1): 308-313.

（编辑：徐楠楠）

《空军工程大学学报(自然科学版)》连续 14 年入选中文核心期刊

2018 年 9 月 6 日,接中文核心期刊要目总览编委会入编通知,《空军工程大学学报》(自然科学版)入编《中文核心期刊要目总览》2017 年版(即第 8 版)中“综合性科学技术”类核心期刊。

《中文核心期刊要目总览》采用了采用了被摘量(全文、摘要)、被摘率(全文、摘要)、被引量、他引量(期刊、博士论文、会议)、影响因子、他引影响因子、5 年影响因子、5 年他引影响因子、特征因子、论文影响分值、论文被引指数、互引指数、获奖或被重要检索系统收录、基金论文比(国家级、省部级)、Web 下载量、Web 下载率等 16 个评价指标,选作评价指标统计源的数据库及文摘刊物达 49 种。统计文献量 93 亿余篇次,涉及期刊 13 953 种。参加核心期刊评审的学科专家有近 8 000 位。经过定量评价和定性评审,从我国正在出版的中文期刊中评选出 1 981种核心期刊。



空军工程大学学报继 2004 年首次入选中文核心期刊以来,连续 14 年保持了核心期刊地位,特别是在军队调整改革全面落地、重整重塑不断推进期间,能够始终确保核刊地位实属不易。

能够再次入选中文核心期刊,得益于校内外广大科研工作者的踊跃投稿,得益于审稿专家们的严格把关,本刊学术质量不断提升离不开各位作者及审稿专家们长期的支持与贡献。在此,编辑部表示深深的感谢! 希望今后继续支持我们的工作!