二元广义反码与最优 LCD 码

李瑞虎，付　强，宋　昊，刘　杨
（空军工程大学基础部，西安，710051）

摘要　基于二元线性码的定义向量理论，引入广义反码及其定义向量概念，确立广义反码、它的参数与二元最优线性码之间的联系。利用广义反码的性质和参数研究对应二元最优线性码的线性补对偶（LCD）性质，证明 11 类二元最优线性码不是 LCD 码。该方法突破现有方法的局限性，为研究高维二元 LCD 的参数确定与构造问题提供了可借鉴的新理论和新方法。

关键词　广义反码；线性补对偶码；定义向量；最优码
DOI　10.3969/j.issn.2097-1915.2024.01.018
中图分类号　O157.4　　**文献标志码**　A　　**文章编号**　2097-1915(2024)01-0123-05

Binary Generalized Anti-Code and Optimal LCD Code

LI Ruihu, FU Qiang, SONG Hao, LIU Yang
(Department of Basic Sciences, Air Force Engineering University, Xi'an 710051, China)

Abstract　Based on the defining vector of binary linear code, new concept of generalized anti-code of a given code is introduced into this paper, and the defining vector of a generalized anti-code is described by the given code. The parameters of a generalized anti-code are utilized for determining corresponding binary optimal code. It is proved that 11 classes of binary optimal codes are not LCD codes. And such method breaks through the limitations of the current methods, and provides a new theory and a new method for study of LCD parameters determination and structure.

Key words　generalized anti-code; LCD code; defining vector; optimal code

二元反码是由 Farrell [1] 首先提出的，反码在小码长最优码构造和局部修复码研究方面得到广泛应用[2-3]。近年来，人们证明线性补对偶（linear complementary dual，LCD）码能够用于经典与量子信息保护、防止侧信道攻击[3-5]，从而掀起研究 LCD 码的热潮[5-15]。研究一般码长的 LCD 码时，用组合构造、计算机辅助搜索和解方程等方法确定出一些小码长（$n\leqslant 40$）最优 LCD 码以及维数 $k\leqslant 4$ 的 LCD 码，但是却难以确定码长超过 40 的最优 LCD 码以及维数更大的最优 LCD 码[6-14]。为突破现有方法的局限性，借鉴文献[17～19]中线性码的定义向量（defining vector）理论，本文引入广义反码及其定义向量、定义向量的重复度概念，确立广义反码、其参数与定义向量之间的联系。利用广义反码描述任意码长线性码的参数，将确定任意码长线性码的参数问题转化为确定小码长广义反码问题。

设 $N_m=2^m-1$，关于二元最优$[sN_m+N_m-a,m]$的 LCD 性，可得到如下结果：

1）$m=3$，且 $a=2$ 时，存在二元最优$[sN_m+N_m$

收稿日期：2023-05-25
基金项目：国家自然科学基金（U21A20428）；陕西省自然科学基础研究计划（2022JQ046）
作者简介：李瑞虎（1966－），男，安徽亳州人，教授，博士生导师，研究方向为代数编码、量子编码。E-mail：liruihu@aliyun.com
通信作者：付　强（1989－），男，陕西西安人，副教授，博士，研究方向为分布式存储编码、量子编码。E-mail：qiang-fu@aliynn.com

引用格式：*李瑞虎，付强，宋昊，等. 二元广义反码与最优 LCD 码[J]. 空军工程大学学报，2024，25(1)：123-127. LI Ruihu, FU Qiang, SONG Hao, et al. Binary Generalized Anti-Code and Optimal LCD Code[J]. Journal of Air Force Engineering University, 2024, 25(1): 123-127.*

$-a,m]$码为 LCD 码[8-10]。

2)$m=4,5,6$ 且 $a=5,9$ 时，存在二元最优 $[sN_m+N_m-a,m]$码为 LCD 码[10-13]。

本文将利用线性码的定义向量和广义反码理论，研究二元最优$[sN_m+N_m-a,m]$的根维数以及 LCD 性，设法证明 $1\leqslant a\leqslant 11$，m 适当大时，二元最优$[sN_m+N_m-a,m]$线性码不是 LCD 码。

1 基本理论

本文中 F_2 为二元域，线性码 C 指二元线性码，C 的 Euclid 对偶表示为 $C^{\perp}$，定义为：

$$C^{\perp}=\{\boldsymbol{x}\in F_2^n \mid \boldsymbol{x}\cdot\boldsymbol{y}=\boldsymbol{x}\boldsymbol{y}^{\mathrm{T}}=\boldsymbol{0},\forall\,\boldsymbol{y}\in C\}.$$

若 $C\subseteq C^{\perp}$，C 叫做自正交（self-orthogonal，SO）码。$Hull(C)=C\cap C^{\perp}$ 叫做 C 的根码[3,15]，又称为 C 的包壳，$Hull(C)$的维数记为 $h(C)$。

若 $Hull(C)=\{0\}$（或 $h(C)=0$），C 叫做线性补对偶码[3]。

若$[n,k,d]$码存在，定义：

$h([n,k,d])=\min\{h(C)\mid C=[n,k,d]\}$。

如果存在置换将码 C 变成 C'，C 和 C' 称为等价码，$C\cong C'$。若 G_1 与 G_2 生成等价码，则记为 $G_1\cong G_2$。等价码性能一样，故可以不区分等价码与置换等价的生成矩阵，将它们视作同一对象进行。

约定：由二维 Simplex 码的生成矩阵 $\boldsymbol{S}_2$ 结合递归构造方法，可构造 k－维 Simplex 的生成矩阵：

$$\boldsymbol{S}_2=\begin{pmatrix}101\\011\end{pmatrix},\boldsymbol{S}_3=\begin{pmatrix}\boldsymbol{S}_2 & \boldsymbol{0}_2 & \boldsymbol{S}_2\\ \boldsymbol{0}_3^T & 1 & \boldsymbol{1}_3^T\end{pmatrix},\cdots,$$

$$\boldsymbol{S}_k=\begin{pmatrix}\boldsymbol{S}_{k-1} & \boldsymbol{0}_{k-1} & \boldsymbol{S}_{k-1}\\ \boldsymbol{0}_{2^k-1}^T & 1 & \boldsymbol{1}_{2^k-1}^T\end{pmatrix}。$$

记 $\boldsymbol{\alpha}_i$ 为 $i(1\leqslant i\leqslant N=2^k-1)$ 的二进制 k－维向量表示，即 $\boldsymbol{\alpha}_1=(1,0,\cdots,0)^{\mathrm{T}}$，$\cdots$，$\boldsymbol{\alpha}_N=(1,1,\cdots,1)^{\mathrm{T}}$，则 $\boldsymbol{S}_k=(\alpha_1,\cdots,\alpha_N)$。

记 $\boldsymbol{S}_k$ 的后 2^k-2^m 列$(1\leqslant m\leqslant k-1)$构成的矩阵为 $\boldsymbol{M}_{k,m}$，$\boldsymbol{M}_{k,m}$ 生成 $\mathscr{M}_{k,m}=[2^k-2^m,k,2^{k-1}-2^{m-1}]$ MacDonald 码[21]。

若 $\boldsymbol{G}$ 是 $C=[n,k]$ 的生成矩阵，$\boldsymbol{G}$ 中有 l_i，$\boldsymbol{\alpha}_i(1\leqslant i\leqslant N)$，称 $\boldsymbol{L}=(l_1,\cdots,l_N)$为 $\boldsymbol{G}$ 的定义向量，并记 $\boldsymbol{G}$ 为 $\boldsymbol{G}=(l_1\alpha_1,\cdots,l_N\alpha_N)$。

设 $l_{j_l}(1\leqslant l\leqslant t)$为 $\boldsymbol{L}=(l_1,l_2,\cdots,l_N)$的不同坐标且 $l_{j_1}<l_{j_2}<\cdots<l_{j_t}$，若有 m_l 个坐标为 l_{j_l}，则称 $\boldsymbol{L}$ 具有类型$]](l_{j_l})_{m_l}\mid\cdots\mid(l_{j_t})_{m_t}]]$，并记为 $l_{\max}=l_{j_t}$ 和 $l_{\min}=l_{j_1}$。

例如 $L_1=(s+1,s-1,s,s,s+1,s-1,s+1)$ 具有类型$]](s-1)_2\mid(s)_2\mid(s+1)_3]]$，$L_2=(3,1,1,3,1,3,1)$ 具有类型$]](1)_4\mid(3)_3]]$。

设 $\boldsymbol{P}_k$ 为 $\boldsymbol{S}_k$ 中全体非零向量为行的$(2^k-1)\times(2^k-1)$矩阵，$\boldsymbol{J}_k$ 为$(2^k-1)\times(2^k-1)$全一矩阵，$\boldsymbol{Q}_k=\boldsymbol{J}_k-\boldsymbol{P}_k$。线性码 $C=[n,k]$的距离和性质可由定义向量 $\boldsymbol{L}=(l_1,\cdots,l_N)$得到。若 $C=[n,k]$具有生成矩阵 $\boldsymbol{G}=(l_1\alpha_1,\cdots,l_N\alpha_N)$和定义向量 $\boldsymbol{L}=(l_1,\cdots,l_N)$，$\boldsymbol{W}^{\mathrm{T}}=\boldsymbol{P}_k\boldsymbol{L}^{\mathrm{T}}$，则 $\boldsymbol{W}=(w_1,w_2,\cdots,w_N)$对应 C 中 2^k-1 个非零向量的重量，$d=\min_{1\leqslant i\leqslant 2^k-1}\{w_i\}$为 $\boldsymbol{C}$ 最小距离[16-17]。记 $\boldsymbol{W}=(w_1,w_2,\cdots,w_N)=d\ \boldsymbol{1}_{2^k-1}+\boldsymbol{\Lambda}$，其中 $\boldsymbol{\Lambda}=(\lambda_1,\lambda_2,\cdots,\lambda_N)$且 $\lambda_i=w_i-d\geqslant 0$ 则至少有一个 $\lambda_i=0$. 设 $\sigma=\lambda_1+\lambda_2+\cdots+\lambda_N$，则 $\sigma=2^{k-1}n-d(2^k-1)$。

可由 $\boldsymbol{W}^{\mathrm{T}}=\boldsymbol{P}_k\boldsymbol{L}^{\mathrm{T}}$ 得到 $\boldsymbol{L}=(l_1,\cdots,l_N)$，由如下方程解出：

$$\boldsymbol{L}^T=\boldsymbol{P}_k^{-1}\boldsymbol{W}^{\mathrm{T}}=\frac{1}{2^{k-1}}[(d+\sigma)\boldsymbol{1}_{2^k-1}^{\mathrm{T}}-2Q_k\boldsymbol{\Lambda}^{\mathrm{T}}]$$

定义 1.1 设 $C=[n,k,d]$的生成矩阵和定义向量分别为 $\boldsymbol{G}$ 与 $\boldsymbol{L}=(l_1,\cdots,l_N)$，若 $l_{\min}<l_{\max}=s$，记 $l_i^c=s-l_i(1\leqslant i\leqslant N)$。称 $\boldsymbol{G}^a=(l_1^c\alpha_1,\cdots,l_N^c\alpha_N)$为 $\boldsymbol{G}$ 的反矩阵，$\boldsymbol{L}^c=(l_1^c,\cdots,l_N^c)$为 $\boldsymbol{G}^a$ 的定义向量，$\boldsymbol{G}^a$ 中行的 2^k 种线性组合构成的向量全体 $\boldsymbol{C}^a$ 称为 $\boldsymbol{C}$ 的广义反码，$l_{\max}^c=t$ 叫 $\boldsymbol{C}^a$ 的重数，$l_{\max}^c=1$ 时 $\boldsymbol{C}^a$ 称为 $\boldsymbol{C}$ 的反码。当 $m=l_1^c+\cdots+l_N^c$ 且 $\boldsymbol{C}^a$ 中向量的最大重量为 δ 时，记 $\boldsymbol{C}^a=(m,2^k,\{\delta\})$。

引理 1.1 设 $\boldsymbol{C}=[n,k,d]$的生成矩阵和定义向量分别为 $\boldsymbol{G}$ 与 $\boldsymbol{L}$，有：

1)若 $l_{\min}<l_{\max}=s$，$C^a=(m,2^k,\{\delta\})$，则 $d=s2^{k-1}-\delta$；

2) 若 $k\geqslant 3$，则 $\boldsymbol{G}\boldsymbol{G}^{\mathrm{T}}=\boldsymbol{G}^a(\boldsymbol{G}^a)^{\mathrm{T}}$；

3)C 为 LCD 码当且仅当 $\boldsymbol{G}^a(\boldsymbol{G}^a)^{\mathrm{T}}$ 可逆。

证明 1)从 $s\boldsymbol{S}_k$ 中删除 $\boldsymbol{G}$ 的列得到 $\boldsymbol{G}^a$，$s\boldsymbol{S}_k$ 生成等重码$[s(2^k-1),k,s2^{k-1}]$，而 $\boldsymbol{G}^a$ 中行的 2^k 种线性组合向量的最大重量为 δ，故 $d=s2^{k-1}-\delta$。

2)当 $k\geqslant 3$，$\boldsymbol{S}_k\boldsymbol{S}_k^{\mathrm{T}}=0$，由(1)可得：

$$\boldsymbol{G}\boldsymbol{G}^{\mathrm{T}}=\boldsymbol{G}^a(\boldsymbol{G}^a)^{\mathrm{T}}$$

3)C 为 LCD 码当且仅当 $\boldsymbol{G}\boldsymbol{G}^{\mathrm{T}}$ 可逆，由(2)可得 C 为 LCD 码当且仅当 $\boldsymbol{G}^a(\boldsymbol{G}^a)^{\mathrm{T}}$ 可逆。

下文要用到 C 的约化码和扩展码的 $h(C)$[15]。

定义 1.2 设 $\boldsymbol{G}$ 和 $\boldsymbol{G}_1$ 分别为 $C=[n,k,d]$以及 $C_1=[n-m,k-1,\geqslant d]$的生成矩阵。若 $\boldsymbol{G}=\begin{pmatrix}\boldsymbol{1}_m & u\\ \boldsymbol{0}_m & G_1\end{pmatrix}$，称 C_1 为 C 的约化码。

引理 1.2[15] 若 C_1 为 C 的约化码，$h(C_1)=h\geqslant 2$，则 $h(C)\geqslant h-1\geqslant 1$，$C$ 不是 LCD 码。

引理 1.3[15] 设 d 为奇数，C^e 为 $C=[n,k,d]$的扩展码，若 $h(C^e)=h\geqslant 2$，则 $h(C)\geqslant h-1\geqslant 1$，$C$ 不是 LCD 码。

本文的主要结论如下：

定理 1.1 设 $s\geqslant 0$，$N_k=2^k-1$，$1\leqslant a\leqslant 11$. 若

(k,a)满足条件：①$k\geqslant 4, a=1,3,4,7,8$；②$k\geqslant 5, a=2,6,10$；③$k\geqslant 7, a=5,9,11$。则相应条件下二元$[sN_k+N_k-a,k]$最优码不是 LCD 码。

2　定理 1.1 的证明

本节证明引理 1.1，分 3 步进行：①$a=1,3,4,7,8$；② $a=2,6,10,11$；③$a=5,9$。

引理 2.1　若 $s\geqslant 0, k\geqslant 4$，$N_k=2^k-1$ 且 $a=1,3,4,7,8$，则 $[N_k s+N_k-a,k]$ 最优码不是 LCD 码。

证明　设 $a=1,3,7$，则相应有 $a=2^r-1$，其中 r 分别对应 1,2,3。$1\leqslant r\leqslant k-1$ 时[18]，有：

$$C=[sN+2^k-2^r,k,s2^{k-1}+2^{k-1}-2^{r-1}]$$

唯一，$C=\mathscr{M}_s(k,r)=[sN+2^k-2^r,k,s2^{k-1}+2^{k-1}-2^{r-1}]$是 s 个 Simplex 码与 MacDonald 码的并置；故 r 对应为 1,2,3 时 C 的根维数 $h(C)$ 分别为 $k-1,k-2,k$。从而 C 不是 LCD 码。

当 $a=4,8$ 时，二元最优$[N_k s+N_k-a,k]$的距离分别为 $2^{k-1}s+2^{k-1}-3$ 和 $2^{k-1}s+2^{k-1}-5$，这时它们的扩展码分别对应 $a=3,7$ 的最优码。

由扩展码的根维数可推出 $a=4,8$，最优码 $[N_k s+N_k-a,k]$的根维数分别为 $k-2\geqslant 2$ 以及 k，故二元最优$[N_k s+N_k-a,k]$是根维数不小于 1 的码，不是 LCD 码。

引理 2.2　若 $k\geqslant 5$，则二元最优$[N_k s+N_k-2,k,2^{k-1}s+2^{k-1}-2]$码不是 LCD 码。

证明　若 $k\geqslant 5$，记 $N_k=N$，则 $C=[n,k,d]=[N_k s+N_k-2,k,2^{k-1}s+2^{k-1}-2]$为二元最优码。

对此码有 $\sigma=2^{k-1}n-d(2^k-1)=2^{k-1}+d$，且 L 满足 $s-1\leqslant l_i\leqslant s+2, 1\leqslant i\leqslant N$。

1)若 $l_{\max}=s+2$，则 C 有约化码：$[N_k s+N_k-4,k-1,2^{k-1}s+2^{k-1}-2]=[(2s+1)N_{k-1}+N_{k-1}-3,k-1,(2s+1)2^{k-2}s+2^{k-2}-2]$

此约化码的 $h\geqslant(k-1)-2=k-3$。故 $h(C)\geqslant k-4$。

2)若 $l_{\max}=s+1$ 且 $l_{\min}=s$，则有广义反码$(2,2^k,\{2\})$，此广义反码$(2,2^k,\{2\})$的秩为 2，因此 $h(C)\geqslant k-2$。

3)若 $l_{\max}=s+1$ 且 $l_{\min}=s-1$，则 C 的定义向量 $\boldsymbol{L}$ 以及 $\boldsymbol{L}^c$ 分别具有以下形式：

$$\boldsymbol{L}:]](s-1)_1\mid(s)_0\mid(s+1)_{N-1}]],$$
$$L_1^c:]](2)_1\mid(1)_0\mid(0)_{N-1}]].$$

从而此时 C 为自正交码，$h(C)\geqslant k$。

总结以上讨论结果，可得到：

$h([N_k s+N_k-2,k,2^{k-1}s+2^{k-1}-2])\geqslant k-4$，引理成立。

引理 2.3　若 $k\geqslant 5$，则二元最优$[N_k s+N_k-6,k]$码不是 LCD 码。

证明　记 $C=[n,k,d]=[N_k s+N_k-6,k,2^{k-1}s+2^{k-1}-4]$为二元最优码，对此码有 $\sigma=2^{k-1}n-d(2^k-1)=2^{k-1}+d$，且 L 满足 $s-1\leqslant l_i\leqslant s+2$，$1\leqslant i\leqslant N$。

1)若 $l_{\max}=s+2$，则 C 有约化码：

$$[N_k s+N_k-8,k-1,2^{k-1}s+2^{k-1}-4]=[(2s+1)N_{k-1}+N_{k-1}-7,k-1,(2s+1)2^{k-2}s+2^{k-2}-4]$$

其为自正交码，因此 $h(C)\geqslant k-2$。

2)若 $l_{\max}=s+1$ 且 $l_{\min}=s$，则有广义反码$(6,2^k,\{4\})$，此广义反码$(6,2^k,\{4\})$的秩至多为 4，故 $h(C)\geqslant k-4$。

3)若 $l_{\max}=s+1$ 且 $l_{\min}=s-1$，则 C 的定义向量 $\boldsymbol{L}$ 以及 $\boldsymbol{L}^c$ 分别具有形式：

①$L_1:]](s-1)_1\mid(s)_4\mid(s+1)_{N-5}]]$，
$L_1^c:]](2)_1\mid(1)_4\mid(0)_{N-5}]]$；

②$L_2:]](s-1)_2\mid(s)_2\mid(s+1)_{N-4}]]$，
$L_2^c:]](2)_2\mid(1)_2\mid(0)_{N-4}]]$；

③$L_3:]](s-1)_3\mid(s+1)_{N-3}]]$；
$L_3^c:]](2)_3\mid(0)_{N-3}]]]](2)_3\mid(0)_{N-3}]]$.

以上 3 种定义向量 $\boldsymbol{L}$ 分别对应码的 $h(C)$ 值为 $h\geqslant k-4$，$h\geqslant k-2$ 以及 $h=k$。

总结以上各种情况，可得到 $h([N_k s+N_k-6,k,2^{k-1}s+2^{k-1}-4])\geqslant k-4$，故引理成立。

引理 2.4　若 $k\geqslant 7$，则二元最优$[N_k s+N_k-5,k]$码不是 LCD 码。

证明　记 $C=[n,k,d]=[N_k s+N_k-5,k,2^{k-1}s+2^{k-1}-4]$为二元最优码，$\sigma=2^{k-1}n-d(2^k-1)=2\times 2^{k-1}+d$，且 $s-2\leqslant l_i\leqslant s+3, 1\leqslant i\leqslant N$。

1)若 $l_{\max}=s+3$，则 C 有约化码$[N_k s+N_k-8,k-1,2^{k-1}s+2^{k-1}-4]=[(2s+1)N_{k-1}+N_{k-1}-7,k-1,(2s+1)2^{k-2}s+2^{k-2}-4]$为自正交码。因此 $h(C)\geqslant k-2$。

2)若 $l_{\max}=s+2$，则 C 有约化码$[N_k s+N_k-7,k-1,2^{k-1}s+2^{k-1}-4]=[(2s+1)N_{k-1}+N_{k-1}-6,k-1,(2s+1)2^{k-2}s+2^{k-2}-4]$，此约化码的 h 值为 $h\geqslant k-1-4=k-5$. 因此 $h(C)\geqslant k-6$。

3)若 $l_{\max}=s+1$ 且 $l_{\min}=s$，则有广义反码$(5,2^k,\{4\})$，此广义反码$(5,2^k,\{4\})$的秩至多为 4，故 $h(C)\geqslant k-4$。

4)若 $l_{\max}=s+1$ 且 $l_{\min}=s-1$，则 C 的定义向量 $\boldsymbol{L}$ 以及 $\boldsymbol{L}^c$ 分别具有以下形式：

①$L_1:]](s-1)_1\mid(s)_3\mid(s+1)_{N-4}]]$，
$L_1^c:]](2)_1\mid(1)_3\mid(0)_{N-5}]]$；

②$L_2:]](s-1)_2\mid(s)_1\mid(s+1)_{N-3}]]$，
$L_2^c:]](2)_2\mid(1)_1\mid(0)_{N-4}]]$；

以上 2 种定义向量 $\boldsymbol{L}$ 分别对应码的 $h(C)$ 值为 $h\geqslant k-3, h\geqslant k-1$。

5)若 $l_{\max}=s+1$ 且 $l_{\min}=s-2$,则 C 的定义向量 $\boldsymbol{L}$ 以及 $\boldsymbol{L}^c$ 分别具有形式:

①L_1:]](s−2)$_1$ | (s−1)$_0$ | (s)$_2$ | (s+1)$_{N-3}$]], L_1^c:]](3)$_1$ | (1)$_2$ | (0)$_{N-3}$]];

②L_2:]](s−2)$_1$ | (s−1)$_1$ | (s)$_0$ | (s+1)$_{N-2}$]], L_2^c:]](3)$_1$ | (2)$_1$ | (0)$_{N-2}$]];

以上 2 种定义向量 $\boldsymbol{L}$ 分别对应码的 $h(C)$ 值为 $h\geqslant k-3, h\geqslant k-1$。

总结以上各种情况,可得到 $h([N_k s+N_k-5, k, 2^{k-1}s+2^{k-1}-4])\geqslant k-6$,故引理成立。

引理 2.5 若 $k\geqslant 5$,则二元最优 $[N_k s+N_k-10, k]$ 码不是 LCD 码。

证明 记 $[n,k,d]=[N_k s+N_k-10, k, 2^{k-1}s+2^{k-1}-6]$,则 $C=[n,k,d]$ 为二元最优码,并有 $\sigma=2^{k-1}n-d(2^k-1)=2^{k-1}+d$,且 L 满足 $s-1\leqslant l_i\leqslant s+2, 1\leqslant i\leqslant N$。

首先,我们可断言 $l_{\max}=s+2$ 不会出现,否则 C 有约化码 $[N_k s+N_k-12, k-1, 2^{k-1}s+2^{k-1}-6]=[(2s+1)N_{k-1}+N_{k-1}-11, k-1, (2s+1)2^{k-2}+2^{k-2}-6]$ 违背 Griesmer 界,矛盾。从而可得 $l_{\max}=s+1$。

1)若 $l_{\max}=s+1, l_{\min}=s$,则 C 对应的反码为 $(10, 2^k, \{6\})$,此广义反码生成矩阵 $\boldsymbol{G}^a$ 的秩至多为 6,下面证明 $\boldsymbol{G}^a$ 的秩至多为 5。否则,可设 $\boldsymbol{G}^a\cong(I_6 \mid u_1, u_2, u_3, u_4)$,$u_i(1\leqslant i\leqslant 4)$ 是互不相同的向量且重量都大于 2。若 u_i 中有一个具有奇重量,则反码具有码字 的重量 $\delta\geqslant 7$,矛盾。若 u_i 都具有偶重量,则由 $\lceil 4\times 2/6\rceil=2$ 可知 (u_1, u_2, u_3, u_4) 具有一行的重量不小于 2,于是 $\boldsymbol{G}^a$ 中存在 5 行的线性组合得到的码字重量 $\delta\geqslant 7$,矛盾。故可得出 $\boldsymbol{G}^a$ 的秩至多为 5。

根据文献[20],秩不超过 5 的 $(10, 2^k, \{6\})$ 反码仅有 2 个,分别满足 $\mathrm{rank}(\boldsymbol{G}^a(\boldsymbol{G}^a)^{\mathrm{T}})=4$,2 故此种情况下 $h(C)\geqslant k-4$。

2)若 $l_{\max}=s+1, l_{\min}=s-1$,则 C 的定义向量 $\boldsymbol{L}$ 以及 $\boldsymbol{L}^c$ 分别具有形式:

①L_1:]](s−1)$_1$ | (s)$_8$ | (s+1)$_{N-9}$]], L_1^c:]](2)$_1$ | (1)$_8$ | (0)$_{N-9}$]];

②L_2:]](s−1)$_2$ | (s)$_6$ | (s+1)$_{N-8}$]], L_2^c:]](2)$_2$ | (1)$_6$ | (0)$_{N-8}$]];

③L_3:]](s−1)$_3$ | (s)$_4$ | (s+1)$_{N-7}$]], L_2^c:]](2)$_3$ | (1)$_4$ | (0)$_{N-7}$]];

④L_4:]](s−1)$_4$ | (s)$_2$ | (s+1)$_{N-6}$]], L_2^c:]](2)$_4$ | (1)$_2$ | (0)$_{N-6}$]];

⑤L_5:]](s−1)$_5$ | (s)$_0$ | (s+1)$_{N-5}$]], L_2^c:]](2)$_5$ | (1)$_0$ | (0)$_{N-5}$]];

若 $\boldsymbol{L}(\boldsymbol{L}^c)$ 具有形式 L_i,$(3\leqslant i\leqslant 5)$,则有 $\mathrm{rank}(\boldsymbol{G}^a(\boldsymbol{G}^a)^{\mathrm{T}})\leqslant 4$。

于是,仅需要确定 1)和 2)这 2 种情况下广义反码对应的 $\mathrm{rank}(\boldsymbol{G}^a(\boldsymbol{G}^a)^{\mathrm{T}})$。首先仿照情形 1 可证明 $\mathrm{rank}(\boldsymbol{G}^a(\boldsymbol{G}^a)^{\mathrm{T}})=6$ 不会出现,若 $\mathrm{rank}(\boldsymbol{G}^a(\boldsymbol{G}^a)^{\mathrm{T}})=5$,则 L_1^c 和 L_2^c 对应的广义反码的 $\boldsymbol{G}^a$ 分别为 $(I_5 \mid u_1, u_2, u_3 \mid 2v_1)$ 和 $(I_5 \mid u_1, \mid 2v_1, 2v_2)$。不难验证此时 $\boldsymbol{G}^a$ 的码字重量 $\delta\geqslant 7$,矛盾。此时 $h(C)\geqslant k-4$。

总结上面 2 种情形,即证明引理成立。

推论 2.6 若 $k\geqslant 6$,则二元最优 $[N_k s+N_k-11, k]$ 码不是 LCD 码。

证明 参数 $[N_k s+N_k-11, k, 2^{k-1}s+2^{k-1}-7]$ 的码是二元最优码,它的扩展码是 $[N_k s+N_k-10, k, 2^{k-1}s+2^{k-1}-6]$ 二元最优码,此扩展码的根维数 $h\geqslant k-4$。

当 $k\geqslant 6$,扩展码的根维数 $h\geqslant k-4\geqslant 2$,故二元最优 $[N_k s+N_k-11, k]$ 码的根维数 $h\geqslant k-5$,不是 LCD 码。

引理 2.7 若 $k\geqslant 7$,则二元最优 $[N_k s+N_k-9, k]$ 码不是 LCD 码。

证明 记 $C=[n,k,d]=[N_k s+N_k-9, k, 2^{k-1}s+2^{k-1}-6]$ 为二元最优码,对此最优码有 $\sigma=2^{k-1}n-d(2^k-1)=2\times 2^{k-1}+d$,且 $s-2\leqslant l_i\leqslant s+3$ $(1\leqslant i\leqslant N)$。

仿照引理 2.4 可证明 $l_{\max}=s+3$ 不会出现,于是 $l_{\max}\leqslant s+2$。

1)$l_{\max}=s+2$,则 C 有约化码 $[N_k s+N_k-11, k-1, 2^{k-1}s+2^{k-1}-6]=[(2s+1)N_{k-1}+N_{k-1}-10, k-1, (2s+1)2^{k-2}s+2^{k-2}-6]$,

此约化码的 h 值为 $h\geqslant=k-5$,因此 $h(C)\geqslant k-6$。

2)若 $l_{\max}=s+1, l_{\min}=s$,则 C 的则有广义反码 $(9, 2^k, \{6\})$,此广义反码 $(9, 2^k, \{6\})$ 的秩至多为 6,故 $h(C)\geqslant k-6$。

3)若 $l_{\max}=s+1, l_{\min}=s-1$,则 C 的定义向量 $\boldsymbol{L}$ 以及 $\boldsymbol{L}^c$ 分别具有形式:

①L_1:]](s−1)$_1$ | (s)$_7$ | (s+1)$_{N-8}$]], L_1^c:]](2)$_1$ | (1)$_7$ | (0)$_{N-8}$]];

②L_2:]](s−1)$_2$ | (s)$_5$ | (s+1)$_{N-7}$]], L_2^c:]](2)$_2$ | (1)$_5$ | (0)$_{N-7}$]];

③L_3:]](s−1)$_3$ | (s)$_3$ | (s+1)$_{N-6}$]], L_2^c:]](2)$_3$ | (1)$_3$ | (0)$_{N-6}$]];

④L_4:]](s−1)$_4$ | (s)$_5$ | (s+1)$_{N-5}$]], L_2^c:]](2)$_4$ | (1)$_1$ | (0)$_{N-5}$]];

若 $\boldsymbol{L}(\boldsymbol{L}^c)$ 具有形式 L_i,$(2\leqslant i\leqslant 4)$,则有 $\mathrm{rank}(\boldsymbol{G}^a(\boldsymbol{G}^a)^{\mathrm{T}})\leqslant 5$。

于是，我们仅需要确定情形 1)下广义反码$(9,2^k,\{6\})$的秩，仿照情形 1)可证明广义反码生成矩阵 $\boldsymbol{G}^a$ 的秩至多为 5。这表明 $l_{\max}=s+1$ 且 $l_{\min}=s-1$ 时 $h(C)\geqslant k-5$。

4)若 $l_{\max}=s+1, l_{\min}=s-2$，则 C 的定义向量 $\boldsymbol{L}$ 以及 $\boldsymbol{L}^c s$ 分别具有形式：

①L_1:]](s−2)$_1$ | (s−1)$_0$ | (s)$_6$ | (s+1)$_{N-7}$]]，L_1^c:]](3)$_1$ | (1)$_6$ | (0)$_{N-7}$]]；

②L_2:]](s−2)$_1$ | (s−1)$_1$ | (s)$_4$ | (s+1)$_{N-6}$]]，L_2^c:]](3)$_1$ | (2)$_1$ | (1)$_4$ | (0)$_{N-6}$]]；

③L_3:]](s−2)$_1$ | (s−1)$_2$ | (s)$_2$ | (s+1)$_{N-5}$]]，L_3^c:]](3)$_1$ | (2)$_2$ | (1)$_2$ | (0)$_{N-5}$]]；

④L_4:]](s−2)$_2$ | (s−1)$_0$ | (s)$_3$ | (s+1)$_{N-5}$]]，L_4^c:]](3)$_2$ | (2)$_0$ | (1)$_3$ | (0)$_{N-5}$]]；

⑤L_5:]](s−2)$_2$ | (s−1)$_1$ | (s)$_1$ | (s+1)$_{N-4}$]]，L_5^c:]](3)$_2$ | (2)$_1$ | (1)$_1$ | (0)$_{N-4}$]]；

⑥L_6:]](s−2)$_1$ | (s−1)$_3$ | (s)$_0$ | (s+1)$_{N-4}$]]，L_6^c:]](3)$_1$ | (2)$_3$ | (1)$_0$ | (0)$_{N-4}$]]；

⑦L_7:]](s−2)$_3$ | (s−1)$_0$ | (s)$_0$ | (s+1)$_{N-3}$]]，L_7^c:]](3)$_3$ | (2)$_0$ | (1)$_0$ | (0)$_{N-3}$]]；

以上 L_i^c 对应广义反码$(9,2^k,\{6\})$，它们的生成矩阵 $\boldsymbol{G}^a$ 均满足 $\mathrm{rank}(\boldsymbol{G}^a(\boldsymbol{G}^a)^{\mathrm{T}})\leqslant 6$，从而此时 $h(C)\geqslant k-6$。

总结以上 4 类情形，即证明引理成立。

3　结语

本文利用广义反码理论与方法研究形如$[sN_k+N_k-a,k]$的二元性质，证明 $1\leqslant a\leqslant 11, k\geqslant 7$ 时，二元最优码不是 LCD 码。这为确定对应码长最优 LCD 码的距离以及研究如何构造最优 LCD 码奠定了基础，为研究高维二元 LCD 提供了可借鉴的新理论和新方法。

参考文献

[1] FARRELL P. Linear Binary Anticodes[J]. Electronic Letter, 1970, 6(13):419-421.

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

[3] LV L, LI R, GUO L, et al. Maximal Entanglement Entanglement-Assisted Quantum Codes Constructed from Linear Codes [J]. Quantum Information Processing, 2015, 14:165-182.

[4] MASSEY J L. Linear Codes with Complementary Duals [J]. Discrete Mathematics, 1992, 106:337-342.

[5] CARLET C, GUILLEY S. Complementary Dual Codes for Countermeasures to Side-Channel Attacks [J]. Springer Cham, 2016 (1). DOI: 10. 1007/798-3-319-17296-5-9.

[6] CARLET C, MESNAGER S, TANG C, et al, PELLIKAAN R. Linear Codes over F_q are Equivalent to LCD Codes for $q>3$[J]. IEEE Trans Information Theory, 2018, 64(4): 3010-3017.

[7] 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.

[8] FU Q, LI R H, FU F, et al. On the Construction of Binary Optimal LCD Codes with Short Length[J]. International Journal of Foundation Computation Science, 2019, 30(6):1237-1245.

[9] HARADA M, SAITO K. Binary Linear Complementary Dual Codes [J]. Cryptography Communication, 2019, 11(4): 677-696.

[10] ARAYA M, HARADA M, SAITO K. Characterization and Classification of Optimal LCD Codes [J]. Designs, Codes and Cryptography, 2021, 89(4):617-340.

[11] ARAYA M, HARADA M. On the Minimum Weights of Binary Linear Complementary Dual Codes[J]. Cryptography Communication, 2020, 12(2):285-300.

[12] ARAYA M, HARADA M, SAITO K. On the Minimum Weights of Binary LCD Codes and Ternary LCD codes[Z]. arXiv: 1908. 08661v3 18. 2020.

[13] BOUYUKLIEVA S. Optimal Binary LCD Codes [J]. Designs, Codes and Cryptography, 2021, 89(11): 2445-2461.

[14] LI S, SHI M. Improved Lower and Upper Bounds for LCD Codes[Z]. arXiv:2206. 04, 2023.

[15] LI R H, LIU Y, FU Q. On Some Problems of LCD Codes[C]//2016 Symposium on Coding Theory and Cryptogram and Their Related Topics. China: [s. n.], 2016.

[16] GRASSL M. Code Tables: Bounds on the Parameters of Various Types of Codes[EB/OL]. (2023-05-07). http://www.codetables.de/.

[17] LI R, XU Z, ZHAO X. On the Classification of Binary Optimal Self-orthogonal Codes [J]. IEEE Transactions on Information Theory, 2008, 54(8):3778-3782.

[18] ZUO F, LI R, LIU Y. Weight Distributation of Binary Optimal Codes and Its Application [C]//International Conference on Opto-Electronics Engineering and Information Science. Xi'an: IEEE, 2011:1-8.

[19] 左飞. 线性码的两个问题研究 [D]. 西安：空军工程大学，2011.

[20] BOUYUKLIEV I. On the Binary Projective Codes with Dimension 6[J]. Dis Application Math, 2006, 154:1693-1708.

[21] MACDONALD J. Design Methods for Maximum Minimum-Distance Error-Correcting Codes [J]. IBM Journal of Res and Development, 1960, 4:43-57.

（编辑：徐敏）