文章编号：2096-1618(2016)03-0332-05

几类低密度奇偶校验码及其对偶码

谢德荣， 廖群英
(四川师范大学数学与软件科学学院，四川 成都 610066)

摘要：低密度奇偶校验码和极大距离可分码都是性质优良码，也是近年来编码理论研究热点. 极大距离可分码推广至 m-极大距离可分码。文中进一步将 m-极大距离可分码推广至几乎 m-极大距离可分码，并借助低密度奇偶校验码的构造原理及初等方法和技巧，确定几类低密度奇偶校验码的对偶码及相应性质，由此得到一些新的 m-极大距离可分码例子。

关 键 词：应用数学；编码理论；有限几何；m-极大距离可分码；低密度奇偶校验码；几乎 m-极大距离可分码
中图分类号：O157.4 **文献标志码**：A

0 引言

设$\mathbb{F}_q$为 q 元有限域，行满秩矩阵 $\boldsymbol{G}\in\mathbb{F}_q^{k\times n}$是线性码 $C=[n,k,d]_q$ 的一个生成矩阵，若$\mathbb{F}_q$上 $m\times n(m\geq n-k)$矩阵 $\boldsymbol{H}$ 满足：$Rank(H)=n-k$，且对任意 $v\in\mathbb{F}_q^n$，$v\in C$ 当且仅当 $vH^{\top}=0$，则称 $\boldsymbol{H}$ 是 C 的一个校验矩阵，特别的，当 $m=n-k$ 时，则称 $\boldsymbol{H}$ 是 C 的一个一致校验矩阵[1]。早在1962年，Gallager[2]定义了低密度奇偶校验码(简称为 LDPC 码)：线性码 $C=[n,k,d]_q$ 称为 LDPC 码，如果存在正整数 ρ 及 γ，使 C 的校验矩阵 $\boldsymbol{H}_{m\times n}$同时满足下列性质：

(1)每行恰有 ρ 个1；

(2)每列恰有 γ 个1；

(3)任意两列至多在一行同时为1；

(4)ρ 和 γ 相对于校验矩阵 $\boldsymbol{H}$ 的行数和列数很小。

熟知 LDPC 码是一类性质优良码，20世纪90年代，MacKay 等[3-4]证明 LDPC 码具有逼近香农限的优异性能和译码复杂度低等特点，因此 LDPC 码成为近年来研究热点之一。

另一方面，设 C 是 q 元线性码(n,K,d)，如果 $K=q^{n-d+1}$，即 $n=k+d-1$(其中 $K=q^k$)，即参数达到 Singleton 界，则称 C 为极大距离可分码，简称为 MDS 码[5]，从而 MDS 线性码是一类性能最优纠错码，但是很多好码都不有达到 Singleton 界。随之，将 MDS 线性码推广至几乎 MDS 码[6]，NMDS 码[7]及 NNMDS 码[8]。2014年，文献[9]将 MDS 码、NMDS 码及 NNMDS 码的概念统一，定义一般的 m-MDS 线性码，即 q 元码 $C=[n,k,d]$为 m-MDS 线性码，若 $S(C)=S(C^{\perp})=m$，其中 $S(C)=n-k-d+1$，$C^{\perp}$ 为 C 的对偶码，m 为非负整数，显然 MDS 线性码是一类特殊的 m-MDS 线性码，即0-MDS 线性码，对任意给定的非负整数 m，文献[9]证明 m-MDS 线性码的存在性，给出一个判别条件和一些具体例子。同样，有这么多性能良好码都不是 m-MDS 线性码，可能条件更弱，即使是基于有限几何构造的性能优良的 LDPC 线性码，基本都不是 m-MDS 线性码。

基于此，通过引进一类性质更为广泛的线性码几乎 m-MDS 线性码，并利用初等的方法和技巧，对几类 LDPC 码确定其对偶码及相应的性质，由此对文献[9]中定义的 m-MDS 线性码补充一些新例子。

1 预备知识

给出文中所需的编码理论知识及基于有限几何的 LDPC 码的相关结果。

定义1 若图 G 的顶点集 V 可划分成2个非空子集 X 和 Y，即 $V=X\cup Y$ 且 $X\cap Y=\phi$，且每一条边都有一个顶点在 X 中，而另一个顶点在 Y 中，则称这样的图为二部图。

命题1[1,5] 设 q 元线性码 $C=[n,k]$的一致校验矩阵 $\boldsymbol{H}=(u_1,u_2,\cdots,u_n)$，若 $u_1,u_2,\cdots,u_n$ 中任意 $d-1$ 个列向量均$\mathbb{F}_q$-线性无关，且存在 d 个列向量$\mathbb{F}_q$-线性相关，则 C 的最小距离为 d。

命题2[1,5] 设 $\boldsymbol{G}$ 是 q 元线性码 $C=[n,k]$的一个生成矩阵，则

(1)$\boldsymbol{H}\in\mathbb{F}_q^{(n-k)\times n}$是 C 的一致校验阵当且仅当 $\boldsymbol{H}$ 的秩 $\mathrm{Rank}(\boldsymbol{H})=n-k$ 且 $GH^{\top}=0$.

(2)存在与 C 等价的线性码 C'，使 C'的生成矩阵形如 $\boldsymbol{G}'=[I_k\ P]$，其中 I_k 是 k 阶单位方阵，$P\in\mathbb{F}_q^{k\times(n-k)}$。此时，$C'$有一致校验阵型 $H'=[-P^{\top}I_{n-k}]$.

收稿日期：2015-09-21
基金项目：国家自然科学基金资助项目(11401408)；四川省教育厅重点资助项目(14ZA0034)

命题 3[1,5]　设 $C^{\perp}$ 是 q 元线性码 C 的对偶码,G 和 H 分别是 C 的一个生成阵和一致校验阵,则 $(C^{\perp})^{\perp}=C$,且 G 和 H 分别是对偶码 $C^{\perp}$ 的一个一致校验阵和生成阵。

命题 4[11-15]　设 q 为素数的幂,$2\le m\le v$,$C(m,2v,q)$ 是基于辛空间以二部图 $\Gamma(m,2v,q)$ 的邻接矩阵为检验矩阵的 LDPC 码 $[n,k,d]_q$,则

(1) $C(m,2v,q)$ 的码长 $n=\dfrac{\prod\limits_{i=v-m+2}^{v}(q^{2i}-1)}{\prod\limits_{i=1}^{m-1}(q^{i}-1)}$

(2) $C(2,4,q)$ 的维数

$$k=\begin{cases}\dfrac{q^3+q}{2}, & 2\nmid q,\\ q^3+q^2+q-\left(\dfrac{1+\sqrt{17}}{2}\right)^{2t}-\left(\dfrac{1-\sqrt{17}}{2}\right)^{2t}, & q=2^t\end{cases}$$

(3) $C(v,2v,q)$ 的最小距离 $d=2q+2$

命题 5[12,14-15]　设 q 为素数的幂,$2\le m\le v$,$C_*(m,2v,q)$ 是基于辛空间以二部图 $\Gamma_*(m,2v,q)$ 的邻接矩阵为检验矩阵的 LDPC 码 $[n,k,d]_q$ 则

(1) $C_*(2,4,q)$ 的码长 $n=q^3$

(2) 当 q 为奇素数方幂时,$C_*(2,4q)$ 的维数 $k=\dfrac{q^3-2q^2+3q-2}{2}$

(3) $C_*(2,4,q)$ 的最小距离 $d=2q$

命题 6[12,14]　设 q 为素数的幂,$2\le m\le v$,$C_o(m,2v,q)$ 是基于正交空间以二部图 $\Gamma_o(m,2v,q)$ 的邻接矩阵为检验矩阵的 LDPC 码 $[n,k,d]_q$,则 $C_o(m,2v,q)$ 码长 $n=\dfrac{\prod\limits_{i=v-m+2}^{v}(q^{i}-1)(q^{i-1}+1)}{\prod\limits_{i=1}^{m-1}(q^{i}-1)}$,$C_o(v,2v,q)$ 的最小距离 $d=4$。

2　主要结果及证明

首先给出几乎 m-MDS 线性码的定义,其中 m 为给定的非负整数,借助 LDPC 码及其构造原理,给出几类 LDPC 码的对偶码及其相应的性质,由此对文献[9]定义的 m-MDS 线性码的存在性补充一些新例子。

定义 2　q 元线性码 $C=[n,k,d]_q$ 称为几乎 m-MDS 线性码,若 $S(C)=n-k-d+1=m$,其中 m 为非负整数。

注:(1)由上述定义及文献[9]的 Definition 3.1 可知,线性码 C 是 m-MDS 码当且仅当 C 及其对偶码 $C^{\perp}$ 同时为几乎 m-MDS 线性码,从而几乎 m-*MDS* 码是一类性质更为广泛的线性码。

(2) 当 $m=0$ 时,即 $S(C)=0$,易知此时必有 $S(C^{\perp})=0$,从而几乎 0-MDS 码即为 MDS 码。

定理 1　(1)设 q 为素数的幂,则 LDPC 码 $C(2,4,q)$ 为几乎 m-MDS 线性码,其中

$$m=\begin{cases}\dfrac{(q-1)q(q+3)}{2}, & 2\nmid q,\\ \dfrac{\sum\limits_{i=0}^{t}C_{2t}^{2t-2i}17^{i}}{2^{2t-1}}-2^{t+1}, & q=2^t\end{cases}$$

(2) $C(2,4,2)$ 为几乎 5-MDS 线性码,其对偶码 $C^{\perp}$ 为几乎 3-MDS 线性码。

(3)当 $2\nmid q$ 时,$C_*(2,4,q)$ 为几乎 m-MDS 线性码,其中 $m=\dfrac{q^3+2q^2-7q+4}{2}$.

证明　(1)由命题 4 可知,LDPC 码 $C(2,4,q)$ 的最小距离 $d=2q+2$,码长

$$n=\frac{q^4-1}{q-1}=(q+1)(q^2+1).$$

再由命题 4 的(2)可得:

$$m=S(C)=n-k-d+1=(q+1)(q^2+1)-(2q+2)+1-k=q^3+q^2-q-k$$

$$=\begin{cases}q^3+q^2-q-\dfrac{q^3+q}{2}, & 2\nmid q,\\ q^3+q^2-q-\left(q^3+q^2+q-\left(\dfrac{1+\sqrt{17}}{2}\right)^{2t}-\left(\dfrac{1-\sqrt{17}}{2}\right)^{2t}\right), & q=2^t.\end{cases}$$

$$=\begin{cases}\dfrac{(q-1)q(q+3)}{2}, & 2\nmid q,\\ \dfrac{\sum\limits_{i=0}^{t}C_{2t}^{2t-2i}17^{i}}{2^{2t-1}}-2^{t+1}, & q=2^t.\end{cases}$$

这就完成了定理 1 的(1)的证明.

(2) 由(1)可知,当 $q=2$ 时,$n=15$,$m=5$,即 $S(C)=5$,从而 $C(2,4,2)$ 为几乎 5-MDS 线性码. 进而,由文献[8]的 Example 1 可知 $C(2,4,2)$ 的校验矩阵为

$$\boldsymbol{H}(2,4,2)=\begin{pmatrix}
1&0&0&1&0&0&1&0&0&0&0&0&0&0&0\\
0&1&0&0&1&0&0&1&0&0&0&0&0&0&0\\
0&0&1&0&0&1&0&0&1&0&0&0&0&0&0\\
1&0&0&0&1&0&0&0&1&0&0&0&0&0&0\\
0&1&0&0&0&1&1&0&0&0&0&0&0&0&0\\
0&0&1&1&0&0&0&1&0&0&0&0&0&0&0\\
1&0&0&0&0&0&0&0&0&0&1&0&1&0&0\\
0&0&0&1&0&0&0&0&0&0&0&1&0&1&0\\
0&0&0&0&0&0&1&0&0&1&0&0&0&0&1\\
0&1&0&0&0&0&0&0&0&0&0&1&1&0&0\\
0&0&0&0&1&0&0&0&0&1&0&0&0&1&0\\
0&0&0&0&0&0&0&1&0&0&1&0&0&0&1\\
0&0&1&0&0&0&0&0&0&1&0&0&1&0&0\\
0&0&0&0&0&1&0&0&0&0&1&0&0&1&0\\
0&0&0&0&0&0&0&0&1&0&0&1&0&0&1
\end{pmatrix}_{15\times 15}$$

对 $\boldsymbol{H}(2,4,2)$ 进行初等行变换,并移去分量全为零的行即可得 $C(2,4,2)$ 的一致校验矩阵

$$\boldsymbol{A}(2,4,2)=\begin{pmatrix}1&0&0&0&0&0&0&0&0&0&1&0&1&0&0\\0&1&0&0&0&0&0&0&0&0&0&1&1&0&0\\0&0&1&0&0&0&0&0&0&0&1&1&0&1&1\\0&0&0&1&0&0&0&0&0&0&0&1&0&1&0\\0&0&0&0&1&0&0&0&0&0&1&1&1&0&1\\0&0&0&0&0&1&0&0&0&0&1&0&0&1&0\\0&0&0&0&0&0&1&0&0&0&1&1&1&1&0\\0&0&0&0&0&0&0&1&0&0&1&0&0&0&1\\0&0&0&0&0&0&0&0&1&0&1&0&0&0&1\\0&0&0&0&0&0&0&0&0&1&1&1&1&1&1\end{pmatrix}_{10\times15}=(I_{10}P).$$

于是由命题 3 可知 $A(2,4,2)$ 即为对偶码 $C^{\perp}(2,4,2)$ 的生成矩阵,再由命题 2 的(2)可知对偶码 $C^{\perp}(2,4,2)$ 有如下一致校验矩阵:

$$H^{\perp}(2,4,2)=(-P^{\top}I_5)=\begin{pmatrix}1&0&1&0&1&1&1&1&0&1&1&0&0&0&0\\0&1&1&1&1&0&1&0&1&1&0&1&0&0&0\\1&1&0&0&1&0&1&0&0&1&0&0&1&0&0\\0&0&1&1&0&1&1&0&0&1&0&0&0&1&0\\0&0&1&0&1&0&0&1&1&1&0&0&0&0&1\end{pmatrix}_{5\times15}$$

注意到 $\mathrm{Rank}(H^{\perp}(2,4,2))=5$,从而由命题 2 的(1)知 $C^{\perp}(2,4,2)$ 的维数 $k^{\perp}=10$。又 $H^{\perp}(2,4,2)$ 中任意两个列线性无关,且第 1,4,7 列线性相关,故由命题 1 可知 $C^{\perp}(2,4,2)$ 最小距离 $d^{\perp}=3$。因此

$$S(C^{\perp}(2,4,2))=n-k^{\perp}-d^{\perp}+1=15-10-3+1=3$$

即 $C^{\perp}(2,4,2)$ 为几乎 3-MDS 线性码。

这就证明了定理 1 的(2)。

(3)由命题 5 可知,LDPC 码 $C_*(2,4,q)$ 的码长 $n=q^3$,最小距离 $d=2q$,且当 $2\nmid q$ 时,维数 $k=\dfrac{q^3-2q^2+3q-2}{2}$因此

$$m=S(C)=n-k-d+1=q^3-\frac{q^3-2q^2+3q-2}{2}-2q+1=\frac{q^3+2q^2-7q+4}{2}$$

这就完成了定理 1 的(3)证明。

定理 2 (1)LDPC 码 $C_*(2,4,2)$ 与其对偶码 $C_*^{\perp}$ 分别为几乎 3-MDS 线性码和几乎 1-MDS 线性码。

(2) LDPC 码 $C_o(2,4,2)$ 为 2-MDS 线性码。

(3) LDPC 码 $C_o(2,4,3)$ 与其对偶码 $C_o^{\perp}$ 分别为几乎 4-MDS 线性码和几乎 6-MDS 线性码。

证明 (1)由命题 5 知 $C_*(2,4,2)$ 的码长 $n=8$,最小距离 $d=4$. 下面计算其维数 k。

设 $C(2,4,2)$ 的二部图为 $\Gamma(2,4,2)$,P 和 L 分别是图 $\Gamma(2,4,2)$ 的点集和线集。首先取定图 $\Gamma(2,4,2)$ 中一点 p_0 和过 p_0 的一条直线 l_0,然后以去掉 P 中的点 p_0 和与 p_0 共线的所有点构成的点集为 P_*,并且去掉 L 中的直线 l_0 和与 l_0 相交的所有直线构成的线集为 L_*,最后以限制在 $P_*\cup L_*$ 的二部图 $\Gamma_*(2,4,2)$ 的邻接矩阵(行用线标记,列用点标记)为校验矩阵的线性码即为 LDPC 码 $C_*(2,4,2)$. 不妨取点 $p_0=(1,0,0,0)$ 以及过点 p_0 的一条直线 $l_0=\begin{pmatrix}1&0&0&0\\0&1&0&0\end{pmatrix}$。则由文献[8]的 Example 1 可得

$P_*=\{p_1=(0,0,1,0),p_2=(1,1,1,1),p_3=(0,1,1,0),p_4=(0,0,1,1),p_5=(1,0,1,0),p_6=(0,1,1,1),p_7=(1,0,1,1),p_8=(1,1,1,0)\}$

以及

$$L_*=\left\{l_1=\begin{pmatrix}0&0&1&0\\0&0&0&1\end{pmatrix},l_2=\begin{pmatrix}1&0&0&1\\0&1&1&0\end{pmatrix},l_3=\begin{pmatrix}0&0&1&0\\0&1&0&1\end{pmatrix},l_4=\begin{pmatrix}1&0&1&1\\1&0&1&0\end{pmatrix},l_5=\begin{pmatrix}0&0&1&1\\1&1&1&0\end{pmatrix},l_6=\begin{pmatrix}1&0&1&0\\1&1&1&1\end{pmatrix},l_7=\begin{pmatrix}0&1&1&0\\1&1&0&1\end{pmatrix},l_8=\begin{pmatrix}1&0&0&1\\0&1&1&1\end{pmatrix}\right\}$$

又由文献[8]可得二部图 $\Gamma_*(2,4,2)$ 的邻接矩阵(行用线标记,列用点标记)为

$$\boldsymbol{H}_*(2,4,2)=\begin{pmatrix}1&0&0&1&0&0&0&0\\0&1&1&0&0&0&0&0\\1&0&0&0&0&1&0&0\\0&0&0&0&1&0&1&0\\0&0&0&1&0&0&0&1\\0&1&0&0&1&0&0&0\\0&0&1&0&0&0&1&0\\0&0&0&0&0&1&0&1\end{pmatrix}_{8\times8}$$

且 $\boldsymbol{H}_*(2,4,2)$ 也是 $C_*(2,4,2)$ 的校验矩阵. 则对 $\boldsymbol{H}_*(2,4,2)$ 进行初等行变换并移去分量全为零的行可得 $C_*(2,4,2)$ 的一致校验矩阵

$$\boldsymbol{A}_*(2,4,2)=\begin{pmatrix}1&0&0&0&0&0&0&1\\0&1&0&0&0&0&1&0\\0&0&1&0&0&0&1&0\\0&0&0&1&0&0&0&1\\0&0&0&0&1&0&1&0\\0&0&0&0&0&1&0&1\end{pmatrix}_{6\times8}=(\mathrm{I}_6\mathrm{P})$$

注意到 $\mathrm{Rank}(\boldsymbol{A}_*(2,4,2))=6$,故由命题 2 的(1)可得 $C_*(2,4,2)$ 的维数 $k=2$,从而

$$S(C_*(2,4,2))=n-k-d+1=8-2-4+1=3$$

即 $C_*(2,4,2)$ 为 3-MDS 线性码。

又由命题 3 知 $A_*(2,4,2)$ 即为对偶码 $C_*^{\perp}(2,4,2)$ 的生成矩阵,进而由命题 2 的(2)可知 $C_*(2,4,2)$ 的对偶码 $C_*^{\perp}(2,4,2)$ 的一致校验矩阵为

$$\boldsymbol{H}_*^{\perp}(2,4,2)=(-P^{\top}I_2)=\begin{pmatrix}0&1&1&0&1&0&1&0\\1&0&0&1&0&1&0&1\end{pmatrix}_{2\times8}$$

注意到 $\mathrm{Rank}(H_*^{\perp}(2,4,2))=2$,因此由命题 2 的(1)得

$C_*^{\perp}(2,4,2)$的维数 $k^{\perp}=6$. 又 $H_o^{\perp}(2,4,2)$中任意一个列线性无关,且第 2 列和第 3 列线性相关,故由命题 1 知对偶码 $C_*^{\perp}(2,4,2)$的最小距离 $d^{\perp}=2$。于是

$$S(C_*^{\perp}(2,4,2))=n-k^{\perp}-d^{\perp}+1=8-6-2+1=1,$$

即 $C_*^{\perp}(2,4,2)$为几乎 1-MDS 线性码。

这就证明了定理 2 的(1)。

(2)由命题 6 知 $C_o(2,4,2)$的码长 $n=9$,最小距离 $d=4$。下面计算其维数 k。

设 P 是由点 $p_i(i=1,2,\cdots,9)$构成的点集,L 是由线 $l_i(l=1,2,\cdots,6)$构成的线集,其中

$$p_1=(1,0,0,0),p_2=(0,1,0,0),p_3=(0,0,1,0),$$
$$p_4=(1,1,1,1),p_5=(1,0,0,1),p_6=(0,1,1,0),$$
$$p_7=(1,1,0,0),p_8=(0,0,1,1),p_9=(0,0,0,1),$$
$$l_1=\begin{pmatrix}1&0&0&0\\0&1&0&0\end{pmatrix},l_2=\begin{pmatrix}1&0&0&0\\0&0&0&1\end{pmatrix},$$
$$l_3=\begin{pmatrix}0&1&0&0\\0&0&1&0\end{pmatrix},l_4=\begin{pmatrix}0&0&1&0\\0&0&0&1\end{pmatrix},$$
$$l_5=\begin{pmatrix}1&0&0&1\\0&1&1&0\end{pmatrix},l_6=\begin{pmatrix}1&1&0&0\\0&0&1&1\end{pmatrix},$$

于是由文献[8]可得二部图 $\Gamma_o(2,4,2)$的邻接矩阵(行用线标记,列用点标记)为

$$\boldsymbol{H}_o(2,4,2)=\begin{pmatrix}1&1&0&0&0&0&1&0&0\\1&0&0&0&1&0&0&0&1\\0&1&1&0&0&1&0&0&0\\0&0&1&0&0&0&0&1&1\\0&0&0&1&1&1&0&0&0\\0&0&0&1&0&0&1&1&0\end{pmatrix}_{6\times9}$$

且 $\boldsymbol{H}_o(2,4,2)$也是 $C_o(2,4,2)$的校验矩阵,则对 $\boldsymbol{H}_o(2,4,2)$经过初等行变换后再移去分量全为零的行可得 $C_o(2,4,2)$的一致校验矩阵

$$\boldsymbol{A}_o(2,4,2)=\begin{pmatrix}1&0&0&0&0&1&1&1&1\\0&1&0&0&0&1&0&1&1\\0&0&1&0&0&0&0&1&1\\0&0&0&1&0&0&1&1&0\\0&0&0&0&1&1&1&1&0\end{pmatrix}_{5\times9}$$
$$=(I_5\ P)$$

注意到 $\mathrm{Rank}(A_o(2,4,2))=5$,故由命题 2 的(1)可知 $C_o(2,4,2)$的维数 $k=4$,从而

$$S(C_o(2,4,2))=n-k-d+1=9-4-4+1=2$$

而 $C_o(2,4,2)$为几乎 2-MDS 线性码。

现在由命题 3 可知 $A_o(2,4,2)$即为对偶码 $C_o^{\perp}(2,4,2)$的生成矩阵,进而由命题 2 的(2)可得 $C_o(2,4,2)$的对偶码 $C_o^{\perp}(2,4,2)$的一致校验矩阵为

$$\boldsymbol{H}_o^{\perp}(2,4,2)=(-P^{\mathrm{T}}I_4)=$$
$$\begin{pmatrix}1&1&0&0&1&1&0&0&0\\1&0&0&1&1&0&1&0&0\\1&1&1&1&1&0&0&1&0\\1&1&1&0&0&0&0&0&1\end{pmatrix}_{4\times9}$$

容易计算出 $\mathrm{Rank}(H_o^{\perp}(2,4,2)=4)$,故由命题 2 的(1)知 $C_o^{\perp}(2,4,2)$的维数 $k^{\perp}=5$。又 $H_o^{\perp}(2,4,2)$中任意两个列线性无关,且第 1,2,7 列线性相关,从而由命题 1 得对偶码 $C_o^{\perp}(2,4,2)$的最小距离 $d^{\perp}=3$。从而

$$S(C_o^{\perp}(2,4,2))=n-k^{\perp}-d^{\perp}+1=9-5-3+1=2$$

即 $C_o^{\perp}(2,4,2)$为几乎 2-MDS 线性码。

综上,$C_o(2,4,2)$与其对偶码 $C_o^{\perp}(2,4,2)$均为几乎 2-MDS 线性码,从而 $C_o(2,4,2)$为 2-MDS 线性码。这就证明了定理 2 的(2)。

(3)由文献[7]的例可知 $C_o(2,4,3)$的一个校验矩阵为

$$\boldsymbol{H}_o(2,4,3)=$$
$$\begin{pmatrix}1&0&0&1&0&0&1&0&0&1&0&0&0&0&0&0\\0&1&0&0&1&0&0&1&0&0&1&0&0&0&0&0\\0&0&1&0&0&1&0&0&1&0&0&1&0&0&0&0\\1&1&1&0&0&0&0&0&0&0&0&0&1&0&0&0\\0&0&0&1&1&1&0&0&0&0&0&0&0&1&0&0\\0&0&0&0&0&0&1&1&1&0&0&0&0&0&1&0\\0&0&0&0&0&0&0&0&0&1&1&1&0&0&0&1\\0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1\end{pmatrix}_{8\times16}$$

对 $\boldsymbol{H}_o(2,4,3)$经过初等行变换后再移去分量全为零的行可得 $C_o(2,4,3)$的一致校验矩阵

$$\boldsymbol{A}_o(2,4,3)=$$
$$\begin{pmatrix}1&0&0&0&2&2&0&2&2&0&2&2&0&2&2&2\\0&1&0&0&1&0&0&1&0&0&1&0&0&0&0&0\\0&0&1&0&0&1&0&0&1&0&0&1&0&0&0&0\\0&0&0&1&1&1&0&0&0&0&0&0&0&1&0&0\\0&0&0&0&0&0&1&1&1&0&0&0&0&0&1&0\\0&0&0&0&0&0&0&0&0&1&1&1&0&0&0&1\\0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1\end{pmatrix}_{7\times16}$$

容易计算出 $\mathrm{Rank}(\boldsymbol{A}_o(2,4,3))=7$,故由命题 2 的(1)可知 $C_o(2,4,3)$的维数 $k=9$,从而

$$S(C_o(2,4,3))=n-k-d+1=16-9-4+1=4$$

即 $C_o(2,4,3)$为几乎 4-MDS 线性码。

现在由命题 3 可知 $A_o(2,4,3)$即为对偶码 $C_o^{\perp}(2,4,3)$的和矩阵,再由命题 2 可知 $C_o(2,4,3)$的对偶码 $C_o^{\perp}(2,4,3)$的一致校验矩阵为

$$\boldsymbol{H}_o^{\perp}(2,4,3)=$$
$$\begin{pmatrix}1&2&0&2&1&0&0&0&0&0&0&0&0&0&0&0\\1&0&2&2&0&1&0&0&0&0&0&0&0&0&0&0\\1&2&0&0&0&0&2&1&0&0&0&0&0&0&0&0\\1&0&2&0&0&0&2&0&1&0&0&0&0&0&0&0\\1&2&0&0&0&0&0&0&0&2&1&0&0&0&0&0\\1&0&2&0&0&0&0&0&0&2&0&1&0&0&0&0\\1&0&0&2&0&0&0&0&0&0&0&0&2&1&0&0\\1&0&0&0&0&0&2&0&0&0&0&0&2&0&1&0\\1&0&0&0&0&0&0&0&0&2&0&0&2&0&0&1\end{pmatrix}_{9\times16}$$

易知 $\mathrm{Rank}(H_o^{\perp}(2,4,3))=9$,故由命题 2 的(1)可知 $C_o^{\perp}(2,4,$

3)的维数 $k^{\perp}=7$。又 $H_o^{\perp}(2,4,3)$ 中任意3个列线性无关,且第1,2,3,13列线性相关,从而由命题1可得对偶码的最小距离 $d^{\perp}=4$。因此

$$S(C_o^{\perp}(2,4,3))=n-k^{\perp}-d^{\perp}+1=16-7-4+1=6$$

即 $C_o^{\perp}(2,4,3)$ 为几乎6-MDS线性码。

这就证明了定理2的(3)。

3 结束语

由于LDPC码的校验矩阵是一个稀疏矩阵,行数和列数都比较大,所以在通过LDPC码研究几乎 m-MDS线性码及其对偶码时,计算量往往较大.故文中只给出参数较小的一些几乎 m-MDS线性码的例子及其对偶码,这些码的对偶码的最小距离都较小.因此对LDPC码及其对偶码的研究路还很长。

参考文献:

[1] 文红,符初生. LDPC码的原理与应用[M]. 成都:电子科技大学出版社,2006.

[2] R G Gallager. Low density parity check codes[J]. IRE Trans. Inf. Theory, 1962, 8:21-28.

[3] D J C Mackay. Good error-correcting codes based on very spares matrices[J]. IEEETrans. Inform. theory, 1999, 45(2): 399-431.

[4] D J C Mackay, R N Neal. Near Shannon Limit performance of low density parity check codes[J]. Wlectromc Letters, 1996, 32: 1645-1646.

[5] P Garrett. The Mathematics of Coding Theory [M]. China Machnie Press, 2005.

[6] M A De Boer. Almost MDS Codes[J]. Des. Codes Cryptogr, 1996, 9: 143-155.

[7] S M Dodunekov, I N Landgev. On near-MDS codes[J]. J. Geom., 1995, 54: 30-43.

[8] H X Tong. NNMDS Codes[J]. J. Syst Sci Complex, 2012, 25: 617-624.

[9] Q Y Liao,H Liao. On m-MDS codes over nite elds [J]. International Journal of Computer Mathematics, 2014, 91(5): 863-871.

[10] Reinhard Diestel. Graph Theory Second Edition [M]. Springer, 2000.

[11] B Bagchi, A E Brouwer, H A Wilbrink. Notes on binary codes relate to the $O(5;q)$ generalized quadrangle for odd q [J]. Geom, Dedicata, 1991, 39: 339-355.

[12] Y N Feng, S Deng, L Wang. The minimum distances of three families of LDPC codes based on nite elds[J]. Frontiers of Mathematics in China, to appear.

[13] N S S Sastry, P Sin. The code of a regular generalized quadrangle of eveb order[J]. Proc. Sympos. Pure Math, 1998, 63: 485-496.

[14] Z X Wan. Geometry of classical groups over nite elds[M]. Science Press, Bejing, New York, 2002.

[15] P Sin, Q Xiang. On the dimensions of certain LDPC codes based on q regulai bipartite graphs [J]. IEEE Trans. Inform. Theory, 2006, 52 (8): 3735-3737.

[16] S Deng. A Class of LDPC Codes Based on Unitary and Orthogonal Space[D]. Hebei Normal University, 2013.

Several Classes of Low Density Parity Check Codes and their Dual Codes

XIE De-rong, LIAO Qun-ying

(College of Mathematics and Software Science, Sichuan Normal University, Chengdu 610066,China)

Abstract: Studying for Low density parity check (LDPC) codes and Maximal distance separate (MDS) linear codes, which are good linear codes, are interesting in recent years. Recently, MDS linear codes has been extended to m-MDS linear. In the present paper, m-MDS linear codes are extended to almost m-MDS linear codes, and by using the construction theory of LDPC codes and elementary technique, the dual codes and some properties for several classes of LDPC codes are determined. Thus then some new examples for m-MDS linear codes are obtained, where m is a nonnegative integer.

Key words: applied mathematics; coding theory; nite geometry; m-maximal distance separate linear code; low density parity check code; almost m-maximal distance separate linearcode