线性补对偶拟扭转码

姚 宇 马月娜* 吕京杰 陈 璇
(空军工程大学基础部 陕西 西安 710051)

摘 要 Saleh 等在期刊 Journal of Applied Mathematics and Computing 的第 56 卷第 1 期上发表论文“On complementary dual qusai-twist codes”[20],证明了拟扭转码在一定条件下是线性补对偶码(LCD 码)。对其中的四个关键性定理进行修正与完善,进一步给出拟扭转码是 LCD 的充分条件,并由此构造出许多具有优良参数的 LCD 码。

关键词 线性码 拟扭转码 线性补对偶码

中图分类号 O157.4 TP302.8 **文献标志码** A DOI:10.3969/j.issn.1000-386x.2024.10.052

QUASI-TWISTED LINEAR COMPLEMENTARY-DUAL CODES

Yao Yu Ma Yuena* Lü Jingjie Chen Xuan
(*Department of Basic Sciences, Air Force Engineering University, Xi'an 710051, Shaanxi, China*)

Abstract Saleh et al. published "On complementary dual qusai-twisted codes" in the first issue of Volume 56 of the important academic journal "Journal of Applied Mathematics and Computing", which proved that quasi-twisted codes are linear complementary dual (LCD) codes under certain conditions. We corrected and improved the four vital theorems, derived a sufficient condition which quasi-twisted codes are LCD, and thus constructed many LCD codes with good parameters.

Keywords Linear codes Quasi-twisted codes Linear complementary dual codes

0 引 言

线性补对偶码(LCD 码)的概念是由 Massey[1] 在 1964 年提出的。当线性码 C 与其对偶码 $C^{\perp}$ 的交集只含有零码字,即 $C\cap C^{\perp}=\{0\}$ 时,则称码 C 是 LCD 的。文献[2]证明了 LCD 码是满足渐进 Gilbert-Vashamov 界的。Guilley 等[3]发现了 LCD 码可以帮助提高敏感设备处理信息的安全性,尤其是针对所谓的边信道攻击和故障非侵入性攻击的安全性。因此一系列参数良好的 LCD 码被构造出来[4-7]。Li 等构造了几类欧式 LCD 循环码并分析了其参数的性能[8],并且研究了两类 LCD 的 BCH 码的维数与最小距离[9]。文献[10]研究了拟循环码与准负循环码在一定条件下就是 LCD 码。文献[11]给出了在 $\lambda\neq\lambda^{-1}$ 的情况下,λ-常循环码是 LCD 的充分条件。

拟扭转码作为循环码、常循环码以及拟循环码的有效推广,是一类重要的线性码,其参数是满足渐进 Gilbert-Vashamov 界的[12-13]。许多最优码和具有优良参数的 LCD 码都是通过拟循环码和拟扭转码构造出来的[10-11,14-20]。本文修改并完善了文献[20]中的四个定理的条件及证明过程,在此基础上,给出用于判断拟扭转码是 LCD 码的条件,并构造出一系列具有优良参数的 LCD 码。

1 预备知识

设 F_q^n 表示 q 元有限域 F_q 上的 n 维向量空间,其中 q 为素数幂。F_q^n 的每个非空子空间 C 都叫做一个 q 元线性码,n 叫做该码的码长,C 中的向量叫做码字。用 K 表示 C 中码字的个数,即 $K=|C|$,则 $1\leqslant K\leqslant q^n$。$k=\log_q K$ 是线性码 C 的信息位(k 为实数 $0\leqslant k\leqslant n$)即维数。对于一个 $[n,k,d]_q$ 的线性码,其中非零码字最小 Hamming 距离用 d 表示。

收稿日期:2021-03-22。国家自然科学基金项目(11801564,11901579);空军工程大学基础部创新基金项目。**姚宇**,硕士生,主研领域:量子信息,编码研究。**马月娜**,副教授。**吕京杰**,博士生。**陈璇**,硕士生。

令 F_q^* 为 F_q 中的乘法群，$\lambda \in F_q^*$，并且 λ 的阶为 $r = ord(\lambda)$。令 C_1 是码长为 n 的 q 元线性码，对任意码字 $c = (c_0, c_1, \cdots, c_{n-1}) \in C_1$，总有 $(\lambda c_{n-1}, c_0, \cdots, c_{n-2}) \in C_1$，则称 C_1 为 F_q 上的码长为 n 的 λ-常循环码。

令商环 $R_n = F_q[x]/\langle x^n - \lambda \rangle$，定义一种映射 ϕ_1 从 F_q^n 到 R_n，且 $\phi_1(c_0, c_1, \cdots, c_{n-1}) = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}$。因此一个 λ-常循环码可以被认为是 R_n 上的一个理想。因为 R_n 是主理想，所以每一个 λ-常循环码都可以由一个多项式 $g(x)$ 生成，这里的 $g(x)$ 是在 R_n 中的。当 $g(x) \mid x^n - \lambda$ 时，则称 $g(x)$ 为 λ-常循环码的生成多项式。

不仅如此，令 C_2 是码长为 $n = lm$ 的 q 元线性码，则对任意码字 $c = (c_0, c_1, \cdots, c_{m-1}, c_m, c_{m+1}, \cdots, c_{2m-1}, \cdots, c_{(l-1)m}, c_{(l-1)m+1}, \cdots, c_{lm-1}) \in C_2$，总有 $(\lambda c_{m-1}, c_0, \cdots, c_{m-2}, \lambda c_{2m-1}, c_m, \cdots, c_{2m-2}, \cdots, \lambda c_{lm-1}, c_{(l-1)m}, \cdots, c_{lm-2}) \in C_2$，则称 C_2 为 F_q 上的码长是 n 指标为 l 的 λ-拟扭转码。

定义一种映射 φ_2 从 F_q^{lm} 到 R_m^l，且 $\phi_2(c_0, c_1, \cdots, c_{m-1}, c_m, c_{m+1}, \cdots, c_{2m-1}, \cdots, c_{(l-1)m}, c_{(l-1)m+1}, \cdots, c_{lm-1}) = (c_0 + c_1 x + \cdots + c_{m-1} x^{m-1}, c_m + c_{m+1} x + \cdots + c_{2m-1} x^{m-1}, \cdots, c_{(l-1)m} + c_{(l-1)m+1} x + \cdots + c_{lm-1} x^{m-1})$。因此很容易看出，指标为 l 的 λ-拟扭转码是 R_m^l 的一个 R_m-子模。

令 C_2 为 F_q 上的码长为 n 的 λ-拟扭转码，如果 C_2 是由 r 个元素 $G_1(x), \cdots, G_r(x) \in R_m^l$ 生成的，其中 $G_i(x) = (g_{i,1}(x), g_{i,2}(x), \cdots, g_{i,l}(x))$，$1 \leqslant r \leqslant l$，则称 C_2 是 r-生成的拟扭转码。

2 重要定理的修正与完善

在讨论 r-生成的拟扭转码时，我们对文献[20]中的定理 1 与定理 2 的条件进行补充。在讨论 1-生成的拟扭转码时，我们完善文献[20]中定理 4 的条件并且修正定理 5 的条件。

2.1 r-生成的拟扭转码的情形

以下的定理 1 是文献[20]中的定理 1，其给出了当同一拟扭转码 C 拥有不同的常数 λ 时，拟扭转码 C 所具有的性质。

定理 1[20] 令 α、β 为 F_q^* 中两个不相同的元素。如果码 C 是 F_q 上码长为 $n = ml$ 的拟扭转码，且其既是 α-拟扭转码也是 β-拟扭转码，则 $C = \{0\}$ 或者 C 包含 m 个线性无关的码字。

定理 1 的结论是文献[20]中部分定理证明的基础，但是此定理缺少一个重要的条件，即 C 包含的 m 个线性无关的码字，其重量都是不超过 l 的，我们对此进行补充，见如下定理 2。

定理 2 令 α、β 为 F_q^* 中两个不相同的元素。如果码 C 是 F_q 上码长为 $n = ml$ 的拟扭转码，且其既是 α-拟扭转码也是 β-拟扭转码，当 $d_{\min}(C) \leqslant l$ 时，则 $C = \{0\}$ 或者 C 包含 m 个线性无关的码字。

证明：令码 C 是 F_q 上码长为 $n = ml$ 的拟扭转码，且其既是 α-拟扭转码也是 β-拟扭转码。当 $d_{\min}(C) \leqslant l$ 时，假定 C 是非零的，所以至少存在一个非零码字 $c_1 = (c_0, c_1, \cdots, c_{m-1}, c_m, c_{m+1}, \cdots, c_{2m-1}, \cdots, c_{(l-1)m}, c_{(l-1)m+1}, \cdots, c_{lm-1}) \in C$，假定 $c_i \neq 0$，$(m-1)l \leqslant i \leqslant ml-1$。因为 C 既是 α-拟扭转码也是 β-拟扭转码，所以有 $(\alpha c_{m-1}, c_0, \cdots, c_{m-2}, \alpha c_{2m-1}, c_m, \cdots, c_{2m-2}, \cdots, \alpha c_{lm-1}, c_{(l-1)m}, \cdots, c_{lm-2}) \in C$，并且 $(\beta c_{m-1}, c_0, \cdots, c_{m-2}, \beta c_{2m-1}, c_m, \cdots, c_{2m-2}, \cdots, \beta c_{lm-1}, c_{(l-1)m}, \cdots, c_{lm-2}) \in C$。由于 C 的线性关系，我们可以得到 $c_2 = ((\alpha-\beta)c_{m-1}, 0, \cdots, 0, (\alpha-\beta)c_{2m-1}, 0, \cdots, 0, \cdots, (\alpha-\beta)c_{lm-1}, 0, \cdots, 0) \in C$。通过码字 c_2 与它的 l 次循环移位，可得码 C 包含 m 个线性无关的码字。

例 1 令 $q = 5$，$\lambda = 2$，$m = 6$，$l = 2$，我们考虑拟扭转码 C 是由生成矩阵 $\boldsymbol{G}$ 生成的，其中：

$$\boldsymbol{G} = \begin{pmatrix} 0 & 0 & 1 & 0 & 3 & 0 & 2 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 3 & 0 & 2 & 0 & 1 & 0 & 0 \end{pmatrix}。$$

此时码 C 既是 2-拟扭转码也是 3-拟扭转码，但 C 只包含了两个线性无关的码字，而此时 $\dim(C) = 4 > l$，所以定理 1 是不完善的。

以下的定理 3 是文献[20]中的定理 2，当 r-生成的拟扭转码 C 满足其定理的条件时，则码 C 是 LCD 的。

定理 3[20] 假定 C 是 F_q 上码长为 $n = ml$ 的 λ-拟扭转码。当 $\dim(C) < m$ 或者 $\dim(C^{\perp}) < m$ 时，C 是 LCD 码。

定理 3 中的条件是不完善的，我们对定理 3 的条件进行补充，见如下定理 4。

定理 4 C 是 F_q 上码长为 $n = ml$ 的 λ-拟扭转码，当 $d_{\min}(C \cap C^{\perp}) \leqslant l$，且 $\dim(C) < m$ 或 $\dim(C^{\perp}) < m$ 时，C 是 LCD 的。

证明：由于 $C \cap C^{\perp}$ 既是 λ-拟扭转码也是 λ^{-1}-拟扭转码。根据定理 2，当 $d_{\min}(C \cap C^{\perp}) \leqslant l$ 时，有 $C \cap C^{\perp} = \{0\}$ 或者包含 m 个线性无关的码字。因为 $\dim(C \cap C^{\perp}) \leqslant \dim(C)$ 且 $\dim(C \cap C^{\perp}) \leqslant \dim(C^{\perp})$，所以当 $\dim(C) < m$ 或者 $\dim(C^{\perp}) < m$ 时 $\dim(C \cap C^{\perp}) < m$，而这与 $C \cap C^{\perp}$ 包含 m 个线性无关的码字相矛盾。所以 C 是 LCD 码。

接下来，给出一个仅满足定理 3 条件的拟扭转码，但其并不是 LCD 码的反例。

例 2　令 $q=5,\lambda=2,m=6,l=2$,对多项式 $x^6-2=(x^2+2)(x^2+x+2)(x^2+4x+2)$ 进行分解。我们考虑拟扭转码是由 $(g(x),f(x)g(x))$ 生成的,其中 $g(x)$、$f(x)$ 是 R_m^l 中的首一多项式,并且 $g(x)\mid x^m-\lambda$,$\gcd(f(x),(x^m-\lambda)/g(x))=1$。此时令 $g(x)=x^2+2$,$f(x)=2x^2+1$,我们可得到一个参数为 $[12,4,4]_5$ 的拟扭转码 C。易得,$\dim(C)=4<m$。按照定理 3,拟扭转码 C 应当是 LCD 的,但是 $C\cap C^{\perp}$ 的生成矩阵为:

$$\begin{pmatrix}0&0&1&0&3&0&2&0&1&0&0&0\\0&0&0&1&0&3&0&2&0&1&0&0\end{pmatrix}$$

因此得出 $C\cap C^{\perp}\neq\{0\}$,所以定理 3 是不完善的。

2.2　1-生成的拟扭转码的情形

根据定理 4 可知,当拟扭转码是 1-生成的且 $d_{\min}(C\cap C^{\perp})\leqslant l$ 时,它总是 LCD 的,因此考虑极大 1-生成的拟扭转码,即 $\dim(C)=m$ 的 1-生成的拟扭转码。接下来对 $l>2$ 的情况进行讨论。

定理 5[20]　令 C 是码长 $n>2m$ 的极大 1-生成的拟扭转码。那么 C 是 LCD 码或者是自正交码。

定理 5 是文献[20]中的定理 4,下面对其进行完善,见如下定理 6。

定理 6　令 C 是极大 1-生成的拟扭转码,其码长为 $n>2m$ 即 $l>2$。当 $d_{\min}(C\cap C^{\perp})\leqslant l$ 时,C 是 LCD 码或者是自正交码。

证明:因为 C 是极大 1-生成的拟扭转码,所以 $\dim(C)=m$。根据定理 2,假定 $C\cap C^{\perp}\neq\{0\}$,当 $d_{\min}(C\cap C^{\perp})\leqslant l$ 时,则 $C\cap C^{\perp}$ 包含 m 个线性无关的码字,即 $\dim(C\cap C^{\perp})\geqslant m$。因为 $\dim(C\cap C^{\perp})\leqslant\dim(C)=m$。所以 $\dim(C\cap C^{\perp})=m$。进而 $\dim(C\cap C^{\perp})=\dim(C)$,由此得知 $C\cap C^{\perp}=C$。又因为 $\dim(C^{\perp})=n-\dim(C)=(l-1)m>m$,因此 C 是自正交的。

下面给出一个反例,当仅满足文献[20]中定理 4 的条件时,拟扭转码既不是 LCD 的也不是自正交的。

例 3　令 $q=5,\lambda=2,m=6,l=3$,多项式 $x^6-2=(x^2+2)(x^2+x+2)(x^2+4x+2)$,我们考虑拟扭转码 C 是由 $(g(x),f_1(x)g(x),f_2(x)g(x))$ 生成的,其中 $g(x)$、$f_1(x)$、$f_2(x)$ 是 R_m^l 中的首一多项式,并且 $g(x)\mid x^m-\lambda$,$\gcd(f_i(x),(x^m-\lambda)/g(x))=1,i=\{1,2\}$。此时令 $g(x)=1,f_1(x)=x^3+1,f_2(x)=3x^3+1$ 我们可得到一个参数为 $[18,6,4]_5$ 的拟扭转码 C。依据定理 5,拟扭转码 C 应当是 LCD 码或者是自正交码。但 $C\cap C^{\perp}$ 的生成矩阵为 $(\boldsymbol{I}_{3\times3},\boldsymbol{I}_{3\times3},3\boldsymbol{I}_{3\times3},2\boldsymbol{I}_{3\times3},2\boldsymbol{I}_{3\times3},4\boldsymbol{I}_{3\times3})$,其中 $\boldsymbol{I}_{3\times3}$ 是三阶单位矩阵,显而易见 $C\cap C^{\perp}\neq\{0\}$ 且 C 不是自正交的,易得定理 5 是不完善的。

以下的定理 7 是文献[20]中的定理 5,其给出了拟扭转码 C 是 LCD 的条件。

定理 7[20]　令 C 是码长 $n>2m$ 的极大 1-生成的拟扭转码,其生成矩阵为 $\boldsymbol{G}=(G_1,G_2,\cdots,G_l)$,其中:

$$\boldsymbol{G}_i=\begin{pmatrix}a_{i0}&a_{i1}&\cdots&a_{im-1}\\\lambda a_{im-1}&a_{i0}&\cdots&a_{im-2}\\\vdots&\vdots&&\vdots\\\lambda a_{i1}&\lambda a_{i2}&\cdots&a_{i0}\end{pmatrix}$$

如果至少存在一个 $j,0\leqslant j\leqslant m-1$,$\sum_{i=1}^{l}a_{ij}^2\neq0(\bmod q)$,则 C 是 LCD 码。

我们对定理 7 进行完善与改正,并给出一个极大 1-生成的拟扭转码是 LCD 码的充分条件,见如下定理 8。

定理 8　令 C 是码长为 $n>2m$ 的极大 1-生成的拟扭转码。当 $d_{\min}(C\cap C^{\perp})\leqslant l$ 且其生成矩阵为 $\boldsymbol{G}=(G_1,G_2,\cdots,G_l)$ 时,其中:

$$\boldsymbol{G}_i=\begin{pmatrix}a_{i0}&a_{i1}&\cdots&a_{im-1}\\\lambda a_{im-1}&a_{i0}&\cdots&a_{im-2}\\\vdots&\vdots&&\vdots\\\lambda a_{i1}&\lambda a_{i2}&\cdots&a_{i0}\end{pmatrix}$$

若 $\sum_{i=1}^{l}\sum_{j=0}^{m-1}a_{ij}^2\neq0(\bmod q)$,则 C 是 LCD 码。

证明:根据定理 6,当 $d_{\min}(C\cap C^{\perp})\leqslant l$ 且其码长 $n>2m$ 时 C 是 LCD 或者是自正交码。我们假定 C 是自正交码,则它满足 $G\boldsymbol{G}^{\perp}=0$。所以生成矩阵 $\boldsymbol{G}$ 第一行与自身的内积必定等于 0,即 $\sum_{i=1}^{l}\sum_{j=0}^{m-1}a_{ij}^2=0(\bmod q)$。所以当 $\sum_{i=1}^{l}\sum_{j=0}^{m-1}a_{ij}^2\neq0(\bmod q)$ 时,C 是 LCD 码。

定理 8 补充了一个重要条件 $d_{\min}(C\cap C^{\perp})\leqslant l$,并将定理 7 中的"至少存在一个 $j,0\leqslant j\leqslant m-1$,$\sum_{i=1}^{l}a_{ij}^2\neq0(\bmod q)$"修改为"$\sum_{i=1}^{l}\sum_{j=0}^{m-1}a_{ij}^2\neq0(\bmod q)$"。针对定理 7,我们举出一个反例进行说明。

例 4　我们令 $q=5,\lambda=2,m=6,l=3$,多项式 $x^6-2=(x^2+2)(x^2+x+2)(x^2+4x+2)$,我们考虑拟扭转码是由 $(g(x),f_1(x)g(x),f_2(x)g(x))$ 生成的。此时我们令 $g(x)=1,f_1(x)=x^3+1,f_2(x)=3x^4+1$,可得到一个参数为 $[18,6,5]_5$ 的拟扭转码 C,其生成矩阵为:

$$\left(\begin{array}{c|cccccccccccc} \boldsymbol{I}_{6\times6} & 1&0&0&1&0&0&1&0&0&0&3&0\\ &0&1&0&0&1&0&0&1&0&0&0&3\\ &0&0&1&0&0&1&1&0&1&0&0&0\\ &2&0&0&1&0&0&0&1&0&1&0&0\\ &0&2&0&0&1&0&0&0&1&0&1&0\\ &0&0&2&0&0&1&0&0&0&1&0&1 \end{array}\right)$$

其中 $\boldsymbol{I}_{6\times6}$ 是六阶单位矩阵。易得 $1+1+1=3\neq0(\bmod 5)$。按照定理 7,拟扭转码 C 应是 LCD 的。而 $C\cap C^{\perp}$ 的生成矩阵为(1 0 3 0 3 2 1 1 2 1 3 0 4 0 1 2 1 2)。

显然 $C\cap C^{\perp}\neq\{0\}$,所以定理 7 的条件有误。

3 构造优良参数的 LCD 码

为了构造参数优良的 LCD 码,本节给出一个 $l=2$ 的极大 1-生成的拟扭转码是 LCD 的充分条件,见定理 9。

定理 9 令 C 是码长为 $n=2m$ 的极大 1-生成的拟扭转码,当 $d_{\min}(C\cap C^{\perp})\leqslant l$ 时,C 是 LCD 码。

证明:根据定理 2,当 $d_{\min}(C\cap C^{\perp})\leqslant l$ 时,$C\cap C^{\perp}=\{0\}$ 即 C 是 LCD 的或者 $C\cap C^{\perp}$ 包含 m 个重量至多为 l 的线性无关的码字。假定 C 不是 LCD 的,因此 $\dim(C\cap C^{\perp})\geqslant m$。又因为 $\dim(C\cap C^{\perp})\leqslant\dim(C)=m$。所以我们可以得到 $\dim(C\cap C^{\perp})=\dim(C^{\perp})=\dim(C)=m$,进而可以得出 $C\cap C^{\perp}=C=C^{\perp}$,这与 $\lambda\neq\lambda^{-1}$ 相矛盾。因此 C 是 LCD 码。

根据定理 4、定理 6、定理 8 和定理 9,我们可以得到许多参数优良 LCD 码。例 4 和例 5 给出构造过程,表 1 给出部分构造结果。

例 5 令 $q=5,\lambda=2,m=6,l=3$,多项式 $x^6-2=(x^2+2)(x^2+x+2)(x^2+4x+2)$,考虑拟扭转码是由 $(g(x),f_1(x)g(x),f_2(x)g(x))$ 生成的,选择 $g(x)=1,f_1(x)=x^4+x^3+1,f_2(x)=4x^5+x^4+2x^3+x^2+x+1$,可以得到一个参数为 $[18,6,10]_5$ 的拟扭转码 C。根据定理 6,拟扭转码 C 是 LCD 码或者是自正交码,而 $C\cap C^{\perp}=\{0\}$,所以拟扭转码 C 是 LCD 的。根据码表[21],码 C 是最优的。

例 6 令 $q=5,\lambda=2,m=7,l=3$,多项式 $x^7-2=(x+2)(x^6+3x^5+4x^4+2x^3+x^2+3x+4)$,考虑拟扭转码是由 $(g(x),f_1(x)g(x),f_2(x)g(x))$ 生成的。选择 $g(x)=1,f_1(x)=x^4+x^3+x^2+1,f_2(x)=4x^5+2x^4+x^3+2x^2+x+1$,由此可得到一个参数为 $[21,7,11]_5$ 的拟扭转码 C。此时码 C 的生成矩阵为:

$$\left(\begin{array}{c|cccccccccccc} \boldsymbol{I}_{7\times7} & 1&0&1&1&1&0&0&1&1&2&1&2&4&0\\ &0&1&0&1&1&1&0&0&1&1&2&1&2&4\\ &0&0&1&0&1&1&1&3&0&1&1&2&1&2\\ &2&0&0&1&0&1&1&4&3&0&1&1&2&1\\ &2&2&0&0&1&0&1&2&4&3&0&1&1&2\\ &2&2&2&0&0&1&0&4&2&4&3&0&1&1\\ &0&2&2&2&0&0&1&2&4&2&4&3&0&1 \end{array}\right)$$

其中 $\boldsymbol{I}_{7\times7}$ 是七阶单位矩阵。因为 $\sum_{i=1}^{l}\sum_{j=0}^{m-1}a_{ij}^2=2(\bmod q)$ 所以根据定理 8,拟扭转码 C 是 LCD 的。依据码表[21],码 C 的参数是已知最优的。

表 1 中列出由定理 4 和定理 9 得到的 1-生成的拟扭转码 C,C 也是 LCD 码并且具有最优的参数。拟扭转码 C 是由 $(g(x),f(x)g(x))$ 生成的,并且其常数为 $\lambda=2$。记 x^3+x+1 为 $1^2 01$。

表 1 最优 LCD 码

m	q	$g(x),f(x)$	最优 LCD 码
6	5	$434^2 1,1$	$[12,2,10]_5$
6	5	211,1021	$[12,4,8]_5$
6	5	$1,1^5 4$	$[12,6,6]_5$
7	5	$21,101^2$	$[14,6,7]_5$
7	5	$1,101^2 21$	$[14,7,6]_5$
8	5	$1,10^2 1^3 21^2$	$[16,8,7]_5$
9	5	$20^2 1,10141^2$	$[18,6,10]_5$
8	7	$52^2 351,1$	$[16,3,12]_7$
8	7	$4^3 21,10^3 15$	$[16,4,11]_7$
8	7	$6231,101^2 16$	$[16,5,10]_7$
8	7	$31,10^2 213$	$[16,7,8]_7$
8	7	$1,10^2 1^3 21^2$	$[16,8,7]_7$
9	7	$1,10^2 1^3 216$	$[18,9,8]_7$
10	7	1,123424631	$[20,10,9]_7$

4 结 语

本文修正并完善了文献[20]中四个重要定理,给出了拟扭转码是 LCD 的充分条件,并构造出许多具有优良参数的 LCD 码。本文的研究局限于元域的拟扭转码的构造,在后续的研究中,我们将会进一步讨论元域上,基于厄米特内积的拟扭转码是 LCD 码所满足的条件以及码的参数。

参 考 文 献

[1] Massey J L. Reversible codes[J]. Information and Control,

1964,7(3):369 – 380.
[2] Sendrier N. Linear codes with complementary duals meet the Gilbert-Varshamov bound[J]. Discrete Mathematics,2004,285(1 – 3):345 – 347.
[3] Carlet C, Guilley S. Complementary dual codes for counter-measures to side-channel attacks[J]. Mathematics of Communications,2016,10(1):131 – 150.
[4] Yang X, Massey J L. The necessary and sufficient condition for a cyclic code to have a complementary dual[J]. Discrete Mathematics,1994,126(1 – 3):391 – 393.
[5] Dougherty S, Kim J L, Ozkaya B, et al. The combinatorics of LCD codes: Linear programming bound and orthogonal matrices[J]. International Journal of Information and Coding Theory,2017,4(2 – 3):116 – 128.
[6] Lv L D, Li R H, Guo L, et al. Maximal entanglement entanglement-assisted quantum codes constructed from linear codes[J]. Quantum Information Processing,2015,14:165 – 182.
[7] 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.
[8] Li C J, Ding C S, Li S X. LCD cyclic codes over finite fields[J]. IEEE Transactions on Information Theory,2017,63(7):4344 – 4356.
[9] Li S X, Li C J, Ding C S, et al. Two families of LCD BCH codes[J]. IEEE Transactions on Information Theory,2017,63(9):5699 – 5717.
[10] Esmaeili M, Yari S. On complementary-dual quasi-cyclic codes[J]. Finite Fields and Their Applications,2009,15(3):375 – 386.
[11] Dinh H Q. On repeated-root constacyclic codes of length 4ps[J]. Asian-European Journal of Mathematics,2013,6(2):1350020.
[12] Kasami T. A Gilber-Vashamov bound for quasi-cyclic codes of rate 1/2[J]. IEEE Transactions on Information Theory,1974,20(5):679.
[13] Ling S, Solé P. Good self-dual quasi-cyclic codes exist[J]. IEEE Transactions on Information Theory,2003,49(4):1052 – 1053.
[14] Siap I, Aydin N, Ray-Chaudhuri D K. New ternary quasi-cyclic codes with better minimum distances[J]. IEEE Transactions on Information Theory,2000,46(4):1554 – 1558.
[15] Aydin N, Ray-Chaudhuri D K. Quasi-cyclic codes over Z/sub 4/ and some new binary codes[J]. IEEE Transactions on Information Theory,2002,48(7):2065 – 2069.
[16] Chen E Z. An explicit construction of 2-generator quasi-twisted codes[J]. IEEE Transactions on Information Theory,2008,54(12):5770 – 5773.
[17] Daskalov R, Hristov P. New binary one-generator quasi-cyclic codes[J]. IEEE Transactions on Information Theory,2003,49(11):3001 – 3005.
[18] Daskalov R, Hristov P. New quasi-twisted degenerate ternary linear codes[J]. IEEE Transactions on Information Theory,2003,49:2259 – 2263.
[19] Chen E Z. New quasi-cyclic codes from simplex codes[J]. IEEE Transactions on Information Theory,2007,53(3):1193 – 1196.
[20] Saleh A, Esmaeili M. On complementary dual quasi-twisted codes[J]. Journal of Applied Mathematics and Computing,2018,56(1):115 – 129.
[21] Grassl M. Bounds on the minimum distance of linear codes[EB/OL]. [2021 – 03 – 22]. https://www.researchgate.net/publication/258239682_Bounds_on_the_minimum_distance_of_linear_codes.

(上接第 281 页)

[7] Carminati A, Starke R A, Oliveira R S. Combining loop unrolling strategies and code predication to reduce the worst-case execution time of real-time software[J]. Applied Computing and Informatics,2017,13(2):184 – 193.
[8] 郭恒亮,柴晓楠,韩林,等. Canny 边缘检测在飞腾平台的实现与优化[J]. 计算机工程,2021,47(7):37 – 43.
[9] 李睿婷. 高性能 X-DSP 指令流水线部件设计实现与软硬件协同验证[D]. 长沙:国防科学技术大学,2014.
[10] 鲁庆男. 面向向量处理器的 QR 分解算法设计与实现[D]. 长沙:国防科学技术大学,2015.
[11] 崔建伟,王冬青,刘金燕. 基于高斯模糊的单幅图像去雾算法[J]. 自动化与仪器仪表,2021(1):9 – 11,16.
[12] Sano A, Nishio T, Masuda T, et al. Denoising PET images for proton therapy using a residual U-net[J]. Biomedical Physics & Engineering Express,2021,7(2):25014.
[13] 吴冰. 基于医疗超声图像的实时图像处理算法的研究[D]. 哈尔滨:哈尔滨工业大学,2010.
[14] 毛义坪,马茂源. 基于高斯拉普拉斯算子的多聚焦图像融合[J]. 计算机应用与软件,2019,36(10):216 – 221.
[15] 朱发强. 基于多核 DSP 的红外告警信息处理系统设计[D]. 西安:西安电子科技大学,2018.
[16] 沈肖雅,葛俊祥,王奇. 一种稳健自适应波束形成算法[J]. 中国电子科学研究院学报,2019,14(4):373 – 380.
[17] Aslam A, Khan E, Beg M. Improved edge detection algorithm for brain tumor segmentation[J]. Procedia Computer Science,2015,58:430 – 437.
[18] 张美迪. 面向并行程序的高访存效率 DMA 部件设计[D]. 西安:西安电子科技大学,2018.
[19] 李海玲,张昊. 卷积边界扩展研究与实现[J]. 微型电脑应用,2018,34(10):47 – 49.