# 关于欧几里得、厄米和辛拟循环互补对偶码

关超峰、李瑞虎、马智

arXiv:2301.00945v4 [cs.IT] 7 Jul 2023

摘要

线性互补对偶码（LCD）与其对偶码的交集仅含零向量。本文提出了 LCD 码的一种新刻画，使我们能够从码字层面判断线性码是否具有互补对偶性。此外，我们确定了单生成元准循环码在欧几里得、厄米和辛内积下成为 LCD 码的充分必要条件。最后，我们构造了许多参数优异的欧几里得、厄米和对称 LCD 码，其中一些改进了文献中的结果。值得注意的是，我们构造了一个辛 LCD $[28,6]_2$ 码，其辛距离为 10；它对应一个迹厄米加法互补对偶 $(14, 3, 10)_4$ 码，性能优于最优的四元厄米 LCD $[14,3,9]_4$ 码。

关键词：准循环码、欧几里得、厄米、辛、互补对偶码。

AMS 分类（MSC 2020）：94B05、15B05、12E10

## 1 引言

线性互补对偶码（LCD）与其对偶码的交集仅含零码字。LCD码已广泛应用于数据存储、通信系统、消费电子和密码学领域 [1,2]。在 [1], Massey 证明，LCD码为双用户二进制加法信道提供了一种最优的线性编码方案。在 [2], Carlet 等人研究了二元 LCD 码在抵御侧信道攻击和故障注入攻击方面的应用。鉴于 LCD码的重要应用，已有大量研究聚焦于 LCD码 [4–11]。

值得注意的是， [12], Carlet 等人证明， $\mathbb{F}_q$-码（ $q \geq 4$）等价于欧几里得 LCD 码，而 $\mathbb{F}_{q^2}$-码（ $q \geq 3$）等价于厄米 LCD 码。因此，目前大多数关于 LCD 码的研究都集中在小有限域上。Bouyuklieva [13], Harada[14], Ishizuka 等人 [15,16], Li 等人 [17,18], 以及 wang 等人 [19] 构造了许多优良的 LCD 码，并建立了若干短长度 LCD 码表。此外，Shi 等人 [20,21] 引入了适用于安全应用且至今仍有意义的加性互补对偶码（ACD）。由于 [22], 二元辛内积与四元迹厄米内积等价，因此， $\mathbb{F}_2^{2n}$-辛 LCD 码等价于 $\mathbb{F}_4^n$-迹厄米 LCD 码。因此，辛 LCD 码的构造

也具有重要意义。Xu 等人 [23] 构造了一类辛 LCD MDS 码。在 [24], Huang 等人构造了一些具有良好性质的低维拟循环辛 LCD 码，其定义在 $\mathbb{F}_{2^r}$上。

在 [25], Yang 和 Massey 给出了循环码成为欧几里得 LCD 码的充分必要条件。Esmaeili 等人 [26] 研究了准循环码成为欧几里得 LCD 码的充分条件，并提出了一种构造准循环欧几里得 LCD 码的方法。在 [27], G¨uneri 等人利用准循环码的级联结构，研究了具有欧几里得和厄米互补对偶的准循环码，并得到了指数二的一类单生成元拟循环码成为 LCD 码的充分必要条件。随后，Alahmadi 等人 [28] 提出了指数为 $t$的一类单生成元多重负循环码（拟扭曲码的一个子类，其扭曲常数为 $-1$）成为欧几里得 LCD 码的充分必要条件。然而，如何从准循环码构造 LCD 码仍有许多重要问题有待解决。其中最关键的问题之一是确定准循环码成为 LCD 码的充分必要条件，以便更高效地构造准循环 LCD 码。

本文的主要目标是研究拟循环欧几里得、厄米和辛 LCD 码。我们确定了单生成元拟循环码成为欧几里得、厄米和辛 LCD 码的充分必要条件。更准确地说，我们回答以下两个问题：

1. 哪些多项式可用于构造准循环 LCD 码？2. 如何使用多项式构造准循环 LCD 码?

首先，我们给出 LCD 码的一种新刻画，使得可以在码字层面研究 LCD 码。随后，通过分解准循环码的码字空间，我们得到了在欧几里得、厄米和辛内积下这些码与其对偶码仅有平凡交集的充分必要条件。最后，我们提出一种利用准循环码构造 LCD 码的实用方法，并构造了许多优良的拟循环欧几里得、厄米和辛 LCD 码。

本文结构安排如下。第 2 节介绍准循环码以及欧几里得、厄米和辛 LCD 码的预备知识和背景。第 3 节和第 4 节分别从码字的角度重新描述 LCD 码，并确定准循环码在欧几里得、厄米和辛内积下成为 LCD 码的充分必要条件。我们还构造了许多优良的拟循环欧几里得、厄米和辛 LCD 码。最后，我们在第 5 节给出总结性评述。本文中的所有计算均使用代数计算机系统 Magma [29] 完成。

## 2 预备知识

本节介绍准循环码、欧几里得、厄米和辛 LCD 码的一些基本概念。更多细节请参阅标准手册 [30, 31]。

## 2.1 线性码基础

本文中， $p$ 是一个素数， $\mathbb{F}_q$ 是阶为 $q$的有限域，其中 $q = p^r$对某个正整数 $r$成立。定义在 $\mathbb{F}_q$ 上的 $[\ell n, k]_q$ 线性码 $\mathscr{C}$ 是$\mathbb{F}_q^{\ell n}$的一个维数为 $k$的线性子空间。设 $\boldsymbol{u} = (u_0, u_1, \ldots, u_{\ell n-1}) \in \mathscr{C}$，则 $\boldsymbol{u}$的汉明重量为$\mathsf{w}_H(\boldsymbol{u}) = \#\{i \mid u_i \neq 0, 0 \leq i \leq \ell n - 1\}$。若 $\mathscr{C}$的最小汉明距离为$d_H = \min\{\mathsf{w}_H(\boldsymbol{u}) \mid \boldsymbol{u} \in \mathscr{C} \backslash \{\mathbf{0}\}\}$，则$\mathscr{C}$可写为 $[\ell n, k, d_H]_q$。若 $\ell$为偶数，令 $N = \ell n/2$，则 $\boldsymbol{u}$的辛重量为$\mathsf{w}_s(\boldsymbol{u}) = \#\{i \mid (u_i, u_{N+i}) \neq (0, 0)\ 0 \leq i \leq N - 1\}$。类似地，若 $\mathscr{C}$的最小辛重量为 $d_s(\mathscr{C}) = \min\{\mathsf{w}_s(\boldsymbol{u}) \mid \boldsymbol{u} \in \mathscr{C} \setminus \{\mathbf{0}\}\}$，则将 $\mathscr{C}$记为 $[\ell n, k, d_s]_q^s$。

$\boldsymbol{x} = (x_0, \ldots, x_{\ell n-1})$与 $\boldsymbol{y} = (y_0, \ldots, y_{\ell n-1})$的欧几里得内积定义为：

$$\langle \boldsymbol{x}, \boldsymbol{y} \rangle_e = \sum_{i=0}^{\ell n-1} x_i y_i. \tag{1}$$

类似地， $\boldsymbol{x}$与 $\boldsymbol{y} \in \mathbb{F}_{q^2}^{\ell n}$ 的厄米内积定义为：

$$\langle \boldsymbol{x}, \boldsymbol{y} \rangle_h = \sum_{i=0}^{\ell n-1} x_i y_i^q. \tag{2}$$

如果 $\ell$ 为偶数，则 $\boldsymbol{x}$与 $\boldsymbol{y} \in \mathbb{F}_q^{\ell n}$的辛内积为：

$$\langle \boldsymbol{x}, \boldsymbol{y} \rangle_s = \sum_{i=0}^{N-1} \left( x_i y_{N+i} - x_{N+i} y_i \right). \tag{3}$$

$\mathscr{C}$的欧几里得对偶码为 $\mathscr{C}^{\perp_e} = \{\boldsymbol{v} \in \mathbb{F}_q^{\ell n} \mid \langle \boldsymbol{u}, \boldsymbol{v} \rangle_e = 0, \forall \boldsymbol{u} \in \mathscr{C}\}$；如果 $\ell n$为偶数，则 $\mathscr{C}$的辛对偶码为$\mathscr{C}^{\perp_s} = \{\boldsymbol{v} \in \mathbb{F}_q^{\ell n} \mid \langle \boldsymbol{u}, \boldsymbol{v} \rangle_s = 0, \forall \boldsymbol{u} \in \mathscr{C}\}$；如果 $q = p^2$，则 $\mathscr{C}$的厄米对偶码为 $\mathscr{C}^{\perp_h} = \{\boldsymbol{v} \in \mathbb{F}_{q^2}^{\ell n} \mid \langle \boldsymbol{u}, \boldsymbol{v} \rangle_h = 0, \forall \boldsymbol{u} \in \mathscr{C}\}$。当且仅当$\mathscr{C} \cap \mathscr{C}^{\perp_*} = \{\mathbf{0}\}$时， $\mathscr{C}$是一个LCD码，其中“$\perp_*$”表示欧几里得、厄米或辛对偶码之一。

## 2.2 准循环码基础

循环码是一类在移位算子 $\tau_1$下封闭的线性码。对于 $\boldsymbol{x} = (x_0, x_1, \ldots, x_{n-1}) \in \mathbb{F}_q^n$，记 $\tau_1(\boldsymbol{x}) = (x_{n-1}, x_0, \ldots, x_{n-2})$。若 $\mathscr{C} = \tau_1(\mathscr{C})$，则称 $\mathscr{C}$为循环码。设 $\mathbb{R} = \mathbb{F}_q[x]/\langle x^n - 1 \rangle$，并定义映射 $\varphi_1$如下：

$$\begin{aligned} \varphi_1 : \mathbb{F}_q^n &\to \mathbb{R} \\ (c_0, c_1, \ldots, c_{n-1}) &\mapsto c_0 + c_1 x + \cdots + c_{n-1} x^{n-1} \end{aligned} \tag{4}$$

显然， $\varphi_1$ 是 $\mathbb{F}_q$-模的一个同构，而长度为 $n$ 的循环码 $\mathscr{C}$ 是商环 $\mathbb{R}$的一个理想。此外，循环码 $\mathscr{C}$ 可由 $x^n - 1$的一个首一因子 $g(x)$生成。多项式 $g(x)$称为 $\mathscr{C}$的生成多项式， $\mathscr{C}$的维数为 $n - deg(g(x))$。令 $h(x) = x^n - 1/g(x)$，且 $\tilde{h}(x) = x^{\deg(h(x))} h(x^{-1})$，

则 $\mathscr{C}$ 的欧几里得对偶码是一个循环码，其生成多项式为$g^{\perp_e}(x) = \tilde{h}(x)$。令 $g^q(x)$ $= g_0^q + g_1^q x + g_2^q x + \cdots + g_{n-1}^q x^{n-1}$。若 $\mathscr{C}$是 $\mathbb{F}_{q^2}$上的循环码，则 $\mathscr{C}$ 的厄米特对偶码是由 $g^{\perp_h}(x) = \tilde{h}^q(x)$生成的循环码。

令 $\boldsymbol{x} = (x_0, x_1, \ldots, x_{\ell n-1}) \in \mathbb{F}_q^{\ell n}$，且 $\tau_2(\boldsymbol{x}) = (x_{n-1}, x_0, \ldots, x_{n-2}, x_{2n-1}, x_n, \ldots, x_{2n-2}, \cdots\cdots,$ $x_{n\ell-1}, x_{(n-1)\ell}, , x_{n\ell-2})$。若 $\mathscr{C} = \tau_2(\mathscr{C})$，则称线性空间 $\mathscr{C} \subset \mathbb{F}_q^{\ell n}$ 为指标为 $\ell$ 的准循环码。定义一个 $\mathbb{F}_q$-模同构 $\varphi_2$，将 $\mathbb{F}_q^{\ell n}$ 映射到 $\mathbb{R}^\ell$，

$$\begin{aligned}&\varphi_2 : \mathbb{F}_q^{\ell n} \to \mathbb{R}^\ell = \mathbb{R} \oplus \mathbb{R} \oplus \cdots \oplus \mathbb{R}\\&\left(c_0, \ldots, c_{n-1}, c_n, \ldots, c_{2n-1}, \ldots, c_{\ell(n-1)}, \ldots, c_{\ell n-1}\right)\\&\mapsto \left(c_0(x), c_1(x), \ldots, c_{\ell-1}(x)\right),\end{aligned}$$

其中 $c_i(x) = \sum_{t=0}^{n-1} c_{i,\ t} x^t, i = 0, 1, \ldots, \ell - 1$。从代数角度看，准循环码 $\mathscr{C}$ 是 $\mathbb{R}^\ell$ 的一个子模。

## 3 互补对偶码的新刻画

本节将从码字的角度给出 LCD 码的新刻画，为后续证明奠定基础。首先，我们约定内积的表示法，其中“$l$”表示欧几里得或厄米内积之一，而“$*$”表示欧几里得、厄米或辛积之一。

引理 3.1. 设 $\mathscr{C}$ 是 $\mathbb{F}_q$ 上的线性码，则 $\mathscr{C}$ 在内积“$*$”下是 LCD码，当且仅当 $\forall c_1 \in \mathscr{C} \setminus \{\mathbf{0}\}$, $\exists c_2 \in \mathscr{C}, \langle c_1, c_2\rangle_* \neq 0$ 成立。

证明. 显然，$\mathscr{C} \cap \mathscr{C}^{\perp_*} = \{\mathbf{0}\}$ 等价于 $\forall c_1 \in \mathscr{C} \setminus \{\mathbf{0}\}$, $c_1 \notin \mathscr{C}^{\perp_*}$。此外，$c_1 \notin \mathscr{C}^{\perp_*}$ 等价于 $\exists c_2 \in \mathscr{C}, \langle c_1, c_2\rangle_* \neq 0$，因此 $\mathscr{C}$ 是 LCD 等价于 $\forall c_1 \in \mathscr{C} \setminus \{\mathbf{0}\}, \exists c_2 \in \mathscr{C}, \langle c_1, c_2\rangle_* \neq 0$。□

为便于表述，我们给出以下定义。

定义 3.2. 设 $\mathscr{C}_1$ 和 $\mathscr{C}_2$ 是 $\mathbb{F}_q$上的线性码，若满足以下条件：

$$\begin{cases} \forall c_1 \in \mathscr{C}_1 \setminus \{\mathbf{0}\}, \exists c_2 \in \mathscr{C}_2, \langle c_1, c_2\rangle_* \neq 0, \\ \forall c_2 \in \mathscr{C}_2 \setminus \{\mathbf{0}\}, \exists c_1 \in \mathscr{C}_1, \langle c_1, c_2\rangle_* \neq 0, \end{cases} \tag{5}$$

则称 $\mathscr{C}_1$ 和 $\mathscr{C}_2$ 在内积“$*$”下彼此完全非正交。

引理 3.3. 设 $\mathscr{C}_1$ 和 $\mathscr{C}_2$ 是 $\mathbb{F}_q$上的线性码，则 $\mathscr{C}_1$ 和 $\mathscr{C}_2$ 彼此完全非正交，当且仅当 $\mathscr{C}_1 \cap \mathscr{C}_2^{\perp_*} = \{\mathbf{0}\}$ 和 $\mathscr{C}_1^{\perp_*} \cap \mathscr{C}_2 = \{\mathbf{0}\}$。

证明. 根据对偶码的定义，此引理成立。□

引理 3.4. 设 $\mathscr{C}_1$ 和 $\mathscr{C}_2$ 为两个循环码，分别由 $g_1(x)$ 和$g_2(x)$生成，其中 $g_1(x) \mid x^n - 1$ 且 $g_2(x) \mid x^n - 1$，则 $\mathscr{C}_1$ 和 $\mathscr{C}_2$ 彼此完全欧几里得非正交，当且仅当 $g_1(x) = \tilde{g}_1(x)$ $= g_2(x)$； $\mathscr{C}_1$ 和 $\mathscr{C}_2$ 彼此完全厄米非正交，当且仅当 $g_1(x) = \tilde{g}_1^q(x) = g_2(x)$。

证明. 设 [30]、 $\mathscr{C}_1 \cap \mathscr{C}_2^{\perp_l}$和 $\mathscr{C}_1^{\perp_l} \cap \mathscr{C}_2$ 均为循环码，分别由 $lcm(g_1(x)g_2^{\perp_l}(x))$ 和 $lcm(g_1^{\perp_l}(x)\ g_2(x))$生成。此外，$\mathscr{C}_1 \cap \mathscr{C}_2^{\perp_l} = \{\mathbf{0}\}$ 和 $\mathscr{C}_1^{\perp_l} \cap \mathscr{C}_2 = \{\mathbf{0}\}$ 推出 $lcm(g_1(x)\, g_2^{\perp_l}(x)) \equiv 0 \pmod{x^n - 1}$ 以及 $lcm(g_1^{\perp_l}(x)\ g_2(x)) \equiv 0 \pmod{x^n - 1}$。因此分两种情况：第一种是 $\tilde{g}_2(x) \mid g_1(x)$ 和 $\tilde{g}_1(x) \mid g_2(x) \iff g_1(x) = \tilde{g}_1(x) = g_2(x)$。第二种是 $\tilde{g}_2^q(x) \mid g_1(x)$ 和 $\tilde{g}_1^q(x) \mid g_2(x) \iff g_1(x) = \tilde{g}_1^q(x) = g_2(x)$。至此，证明完成。 □

## 4 准循环互补对偶码

本节从引理 3.1 出发，确定在欧几里得、厄米和辛内积下，单生成元准循环码成为 LCD 码的充分必要条件。

为便于表述，下面说明一些符号。令 $g(x) = g_0 + g_1x + g_2x + \cdots + g_{n-1}x^{n-1} \in \mathbb{R}$, $[g(x)]$ 表示由 $\mathbb{F}_q^n$ 中 $g(x)$ 的系数定义的向量，即 $[g(x)] = [g_0, g_1, g_2, \cdots, g_{n-1}]$，且 $\bar{g}(x) = x^n g(x^{-1})$。

为了确定系数向量形式下不同多项式之间的欧几里得内积和厄米内积，以下两个引理至关重要。

引理4.1. ( *[32]*) 设 $f(x)$、 $g(x)$ 和 $h(x)$ 是 $\mathbb{R}$ 中的多项式。则它们之间的欧几里得内积满足以下等式：

$$\langle [f(x)g(x)], [h(x)] \rangle_e = \langle [g(x)], [\bar{f}(x)h(x)] \rangle_e. \tag{6}$$

引理4.2。（ *[33]*）设 $f(x)$、 $g(x)$ 和 $h(x)$ 是 $\mathbb{R}$ 中的首一多项式。则 $\mathbb{F}_{q^2}^n$ 中向量的厄米内积满足以下等式：

$$\langle [f(x)g(x)], [h(x)] \rangle_h = \langle [g(x)], [\bar{f}^q(x)h(x)] \rangle_h. \tag{7}$$

定义 4.3。设 $g(x)$ 和 $f_j(x)$ 是 $\mathbb{R}$ 中的首一多项式，且 $g(x) \mid (x^n - 1)$, $0 \le j \le \ell - 1$。若 $\mathscr{C}$ 是由（$[g(x)f_0(x)]$, $[g(x)f_1(x)]$, $\cdots$, $[g(x)f_{\ell-1}(x)]$）生成的准循环码，则称 $\mathscr{C}$ 为指标为 $\ell$ 的单生成元拟循环码。$\mathscr{C}$ 的生成矩阵 $G$ 具有以下形式：

$$G = (G_0, G_1, \cdots, G_{\ell-1}), \tag{8}$$

其中， $G_j$ 是分别由 $[g(x)f_j(x)]$, 生成的 $n \times n$ 个循环矩阵。

定理 4.4。若 $\mathscr{C}$ 是定义 4.3 中的单生成元拟循环码，则 $\mathscr{C}$ 为欧几里得 LCD 码的充分必要条件为

$$\begin{cases} g(x) = \tilde{g}(x), \\ gcd(\sum_{i=0}^{\ell-1} f_i(x)\bar{f}_i(x), \frac{x^n-1}{g(x)}) = 1. \end{cases} \tag{9}$$

证明。设 $a(x)$,$b(x)$ 是 $\mathbb{R}$ 中任意多项式，则 $\mathscr{C}$ 中任意两个码字可表示为 $\boldsymbol{c_1} = ([a(x)g(x)f_0(x)], [a(x)g(x)f_1(x)], \cdots, [a(x)g(x)f_{\ell-1}(x)])$ 和 $\boldsymbol{c_2} =$

$([b(x)g(x)f_0(x)], [b(x)g(x)f_1(x)], \cdots, [b(x)g(x)f_{\ell-1}(x)])$，分别。 $c_1$ 与 $c_2$ 的欧几里得内积可表示为：

$$\begin{aligned}\langle \boldsymbol{c_1}, \boldsymbol{c_2}\rangle_e &= \sum_{i=0}^{\ell-1}\langle [a(x)g(x)f_i(x)], [b(x)g(x)f_i(x)]\rangle_e \\ &= \sum_{i=0}^{\ell-1}\langle [a(x)g(x)f_i(x)\bar{f}_i(x)], [b(x)g(x)]\rangle_e \\ &= \langle [a(x)g(x)\sum_{i=0}^{\ell-1} f_i(x)\bar{f}_i(x)], [b(x)g(x)]\rangle_e.\end{aligned}$$

由引理 3.1 和 3.4 可知，$\mathscr{C}_{\ell-1}$是欧几里得 LCD 码的充分必要条件是 $g(x) = \tilde{g}(x)$ 和 $gcd(\sum_{i=0} f_i(x)\ \bar{f}_i(x)\ \frac{x^n-1}{g\ x}\ ()\ ) = 1$，因此定理得证。

□

在 $[27, 28],$ 中，还给出了一类单生成元负循环码成为欧几里得 LCD 码的充分必要条件，如下所示。

引理 4.5. ( *[27, 28]*) 设 $\mathscr{C}_n$ 是一个指标为$t$、由 $(1, a_1(x) \ldots, a_{t-1}(x))$ 生成的单生成元负循环码，且 $a_i(x) \in \mathbb{F}_q[x]/\langle x^n + 1\rangle$。对于 $gcd(n, q) = 1$， $\mathscr{C}_n$ 是欧几里得 LCD 码的充分必要条件为

$$gcd\left(1 + \sum_{y=1}^{t-1} a_y(x)a_y\left(-x^{n-1}\right), x^n + 1\right) = 1. \tag{10}$$

值得注意的是，$[27, 28]$ 中的结果简化了准循环码的结构，因此引理 4.5 只能构造码率为 $1/t$、长度为 $tn$的欧几里得 LCD 码，其中 $gcd(n, q) = 1$。相比之下，根据引理 4.4 改变 $g(x)$，可以构造长度和维数非常灵活的 LCD 码。为便于比较，我们给出以下例子。

例 4.6。令 $q = 3$ 和 $n = 13$，在 $[28]$ 中只能构造出一个欧几里得 LCD $[26, 13, 8]_3$ 码。这里，利用引理 4.4，选择不同的理想，我们得到九个参数为
$[26, 4, 15]_3$, $[26, 7, 13]_3$, $[26, 8, 11]_3$, $[26, 9, 10]_3$,
$\mathbf{[26, 12, 9]_3}$, $\mathbf{[26, 13, 8]_3}$, $\mathbf{[26, 14, 7]_3}$, $[26, 15, 6]_3$, $\mathbf{[26, 20, 4]_3}$ 的优良欧几里得 LCD 码。加粗的码是根据 $[34]$ 得出的最优或已知最佳码。此外，我们在附录 A 中给出了这些码的构造方法。

为了展示我们方法的有效性，我们还构造了 17 个新的二元欧几里得 LCD 码，其参数列于表 1。为节省篇幅，详细的构造方法见附录 B。

由于厄米内积与欧几里得内积形式相似，采用类似的方法即可得到单生成元准循环码为厄米 LCD 码的充分必要条件。因此，我们给出以下定理，不再证明。

表 1：新的二元拟循环欧几里得 LCD 码

| No. | 我们的 LCD 码 | $[17,19]$ 中的最佳 LCD 码 |
|---|---|---|
| 1 | $[39,13,12]_2$ | $[39,13,11]_2$ |
| 2 | $[44,11,16]_2$ | $[44,11,15]_2$ |
| 3 | $[44,12,15]_2$ | $[44,12,14]_2$ |
| 4 | $[44,22,9]_2$ | $[44,22,8]_2$ |
| 5 | $[45,12,16]_2$ | $[45,12,15]_2$ |
| 6 | $[45,13,15]_2$ | $[45,13,14]_2$ |
| 7 | $[45,22,10]_2$ | $[45,22,9]_2$ |
| 8 | $[45,23,9]_2$ | $[45,23,8]_2$ |
| 9 | $[46,23,10]_2$ | $[46,23,9]_2$ |
| 10 | $[46,24,9]_2$ | $[46,24,8]_2$ |
| 11 | $[49,15,15]_2$ | $[49,15,14]_2$ |
| 12 | $[50,8,21]_2$ | $[50,8,20]_2$ |
| 13 | $[50,15,16]_2$ | $[50,15,14]_2$ |
| 14 | $[50,16,15]_2$ | $[50,16,14]_2$ |
| 15 | $[51,8,22]_2^\star$ | - |
| 16 | $[51,16,16]_2^\star$ | - |
| 17 | $[51,17,15]_2^\star$ | - |

*由于可以从这些码导出新的二元 LCD 码，因此它们也是新的。

定理 4.7. 若 $\mathscr{C}$ 是定义 4.3 中的单生成元拟循环码，则 $\mathscr{C}$ 为厄米 LCD 码的充分必要条件为

$$\begin{cases} g(x) = \tilde{g}^q(x), \\ gcd(\sum_{i=0}^{\ell-1} f_i(x)\bar{f}_i^q(x), \frac{x^n-1}{g(x)}) = 1. \end{cases} \tag{11}$$

令 $\{0,1,w,w^2\}$ 表示 $\mathbb{F}_4$ 中的元素，其中 $w$ 满足 $w^2+w+1=0$。我们还构造了一些良好的四元拟循环厄米 LCD 码，其中六个是新的。详情见表 2。

定理 4.8. 若 $\mathscr{C}$ 是定义 4.3 中的单生成元拟循环码，且 $\ell$ 为偶数。令 $m=\ell/2$，则 $\mathscr{C}$ 是辛 LCD 码当且仅当满足以下方程。

$$\begin{cases} g(x) = \tilde{g}(x), \\ gcd(\sum_{j=0}^{m-1} (f_j(x)\bar{f}_{m+j}(x) - f_{m+j}(x)\bar{f}_j(x)), \frac{x^n-1}{g(x)}) = 1. \end{cases} \tag{12}$$

证明。设 $a(x)$,$b(x)$ 是 $\mathbb{R}$ 中的任意多项式，则 $\mathscr{C}$ 中任意两个码字可表示为 $\boldsymbol{c_1} = ([a(x)g(x)f_0(x)], [a(x)g(x)f_1(x)], \cdots, [a(x)g(x)f_{\ell-1}(x)])$ 和 $\boldsymbol{c_2} =$

表 2：良好的四元拟循环厄米特LCD码

| No. | 我们的 LCD 码 | 构造 |
|---|---|---|
| 1 | $[10,4,6]_4$ | $x+1, wx^3+x^2+wx+w^2$ |
| 2 | $[14,6,7]_4$ | $x+1, w^2x^5+w^2x^4+wx^2+x+1$ |
| 3 | $[14,7,6]_4$ | $1, x^4+x^3+wx^2+x+1$ |
| 4 | $[18,5,10]_4$ | $x^4+x^3+wx^2+wx+w, wx^2+wx+wx$ |
| 5 | $[20,8,9]_4$ | $x^2+1,\quad x^7+w^2x^5+x^4+wx^3+wx^2;$ |
| 6 | $\mathbf{[20,8,9]_4}$ | 缩短 $[21,9,9]_4$ |
| 7 | $\mathbf{[21,9,9]_4}$ | 缩短 $[22,10,9]_4$ |
| 8 | $\mathbf{[22,9,9]_4}$ | 扩展 $[21,9,9]_4$ |
| 9 | $\mathbf{[22,10,9]_4}$ | $x+1,\quad wx^9+w^2x^7+w^2x^6+wx^5+w^2x^4+wx^3+x+w;$ |
| 10 | $\mathbf{[23,10,9]_4}$ | 扩展 $[22,10,9]_4$ |
| 11 | $\mathbf{[22,11,8]_4}$ | $1, wx^{10}+x^9+w^2x^8+w^2x^6+x^5+x^4+x^3+x^2+w^2x+w^2$ |

注：本表中所有准循环 LCD 码均以生成元 $([g(x)],([g(x)f(x)])$ 给出。参见参考文献 [35], 。加粗的码是新的四元厄米特 LCD 码；其余码的最小距离达到文献 [35] 中已知的最佳下界。

$([b(x)g(x)f_0(x)],[b(x)g(x)f_1(x)],\cdots,[b(x)g(x)f_{\ell-1}(x)])$。辛内积 $c_1$ 与 $c_2$ 可表示为:

$$\begin{aligned}
\langle \boldsymbol{c_1}, \boldsymbol{c_2}\rangle_s = &\ \boldsymbol{c_1}\cdot\begin{pmatrix} 0 & I_{mn} \\ -I_{mn} & 0 \end{pmatrix}\cdot \boldsymbol{c_2}^T \\
= &\ \sum_{j=0}^{m-1}\langle [a(x)g(x)f_j(x)],[b(x)g(x)f_{m+j}(x)]\rangle_e \\
&-\sum_{j=0}^{m-1}\langle [a(x)g(x)f_{m+j}(x)],[b(x)g(x)f_j(x)]\rangle_e \\
= &\ \sum_{j=0}^{m-1}\langle [a(x)g(x)f_j(x)\bar{f}_{m+j}(x)],[b(x)g(x)]\rangle_e \\
&-\sum_{j=0}^{m-1}\langle [a(x)g(x)f_{m+j}(x)\bar{f}_j(x)],[b(x)g(x)]\rangle_e \\
= &\ \langle [a(x)g(x)\sum_{j=0}^{m-1}(f_j(x)\bar{f}_{m+j}(x)-f_{m+j}(x)\bar{f}_j(x))],[b(x)g(x)]\rangle_e.
\end{aligned}$$

由引理 3.1 和 3.4 可知，对于 $\mathscr{C}$，其为辛 LCD 码的充分必要条件是$_{m-1}^{-}$ $g(x) = \tilde{g}(x)$ 和 $gcd(\sum(f_j(x)f_{m+j}(x) -_{j=0} f_{m+j}(x)\bar{f}_j(x))\frac{x^n-1}{g(x)})=1$，因此定理得证。

□

定理 4.8 确定了偶指标单生成元准循环码成为辛 LCD 码的充分必要条件。在 [24], Huang 等人还通过推导 $\mathscr{C}$ 与其辛对偶码 $\mathscr{C}^{\perp_s}$之间的关系，确定了由 $([g(x)],[g(x)f(x)])$ 生成的准循环码 $\mathscr{C}$成为辛 LCD 码的条件。

引理 4.9.（*[24],* 定理 3.1）设 $\mathscr{C}(f,g)$ 是 $\mathbb{F}_q$ 上长度为 $2n$、由 $(g(x)\ f(x)g(x))$ 生成的准循环码，其中 $gcd\left(g(x)\ g^{\perp}(x)\right)=1$, $h(x)\mid g^{\perp}(x)$, $\gcd(h(x)\ \bar{f}(x)\ -f(x))=1$。则 $\mathscr{C}(f,g)$ 是辛 LCD 码。

然而，引理 4.9 仅给出了一个充分条件。根据定理 4.8， $\mathscr{C}(f,g)$ 是辛 LCD 码的充分必要条件如下式所示。

$$\begin{cases} g(x) = \tilde{g}(x), \\ gcd(f(x) - \bar{f}(x), \frac{x^n-1}{g(x)}) = 1. \end{cases} \tag{13}$$

由于二元辛内积与四元迹厄米内积等价，构造性能优于四元厄米 LCD 码的迹厄米 ACD 码，是辛 LCD 码的一项重要动机。以下两个例子展示了如何构造性能优于四元 LCD 码的迹厄米 ACD 码。更多内容请参阅 [36]。

例 4.10. 设 $q = 2$, $n = 7$, $\ell = 4$。令 $g(x) = x + 1$, $f_1(x) = x^5 + x^3 + x^2$,$f_2(x) = x^4 + x^3$, $f_3(x) = x^6 + x^5 + x^4 + x$。容易验证， $g(x) = \tilde{g}(x)$， $1gcd(\sum_{j=0}(f_j(x)\ \bar{f}_{1+j}(x) - f_{1+j}(x)\ \bar{f}_j(x))\ \frac{x^n-1}{g\ x}(\ )\ ) = 1$，因此 $([g(x)f_0(x)], [g(x)f_1(x)], [g(x)f_2(x)], [g(x)f_3(x)])$ 可以生成一个 1 生成元拟循环辛 LCD 码。然后，利用 Magma [29] ，我们可以计算得到该码的参数为 $[28, 6, 10]_2^s$，其辛重量分布为 $\mathrm{w}_s(z) = 1 + 35z^{10} + 21z^{11} + 7z^{13}$。因此，存在一个参数为 $(14, 3, 10)_4$ 的迹厄米 ACD 码。值得注意的是， [37] 中长度为 14、维数为 3 的最优厄米 LCD 码的参数为 $[14, 3, 9]_4$,，所以我们的辛构造性能更好。

例 4.11. 令 $q = 2, n = 21, , \ell = 2$。令 $g(x) = x^3+1$, $f_0(x) = x^{18}+x^{16}+x^{15}+x^{14}+x^{13}+x^{12}+x^8+x^7+x^3+1$, $f_1(x) = x^{20}+x^{19}+x^{18}+x^{15}+x^{14}+x^9+x^7+x^5+x^3+x^2+1$。容易验证， $g(x) = \tilde{g}(x)$， $gcd(f_0(x)\bar{f}_1(x) - f_1(x)\ \bar{f}_0(x)\ \frac{x^n-1}{g\ x}(\ )\ ) = 1$，因此，$([g(x)f_0(x)], [g(x)f_1(x)])$ 可以生成一个 1-生成元拟循环辛 LCD 码。然后，使用 Magma [29] ，我们可以计算出该码的参数为 $[42, 18, 9]_2^s$，其辛重量分布为 $\mathrm{w}_s(z) = 1 + 448z^9 + 1344z^{10} + 3906z^{11} + 9051z^{12} + 18753z^{13} + \cdots + 609z^{21}$。因此，存在一个参数为 $(21, 9, 9)_4$的迹厄米 ACD 码。值得注意的是， [16] 中已知的最佳厄米 LCD 码在长度为 21、维数为 9 时，参数为 $[21, 9, 8]_4$, ，所以我们的辛构造性能更好。

## 5 结论

在本文中，我们提出了 LCD 码的一种新刻画，使我们能够从码字层面确定线性码的互补对偶性。此外，基于这一结果，我们确定了关于欧几里得、厄米和辛内积的单生成元准循环码成为 LCD 码的充分必要条件。最后，我们构造了许多欧几里得、厄米和辛准循环 LCD 码，以说明准循环码可用于构造优良的 LCD 码。

未来，一个可能的延伸方向是研究 $h$ 生成元准循环码成为 LCD 码的充分必要条件。另一方面，构造优于最优厄米特 LCD 码的迹厄米 ACD 码，将是一个有趣且具有挑战性的问题。

## 利益冲突

作者声明，与本文内容相关的利益冲突。

## 数据存放信息

如有合理需要，可向作者索取我们的数据。

## 参考文献

[1]J. L. Massey，《具有互补对偶的线性码》，《离散数学》，第 106 卷，第 337–342 页，1992 年。[2] C. Carlet 和 S. Guilley，《用于应对侧信道攻击的互补对偶码》，《通信数学进展》，第 10 卷，第 1 期，第 131 页，2016 年。[3] N. Sendrier，《具有互补对偶的线性码达到 Gilbert–Varshamov 界》，《离散数学》，第 285 卷，第 1–3 期，第 345–347 页，2004 年。[4] C. Li、C. Ding 和 S. Li，《有限域上的 LCD 循环码》，《IEEE 信息论汇刊》，第 63 卷，第 7 期，第 4344–4356 页，2017 年。[5] S. T. Dougherty、J.-L. Kim、B. Ozkaya、L. Sok 和 P. Sol´e，《LCD 码组合学：线性规划界与正交矩阵》，《国际信息与编码理论杂志》，第 4 卷，第 2–3 期，第 116–128 页，2017 年。[6] L. Galvez、J. L. Kim、N. Lee、Y. G. Roe 和 B.-S. Won，《二元 LCD 码的一些界》，《密码学与通信》，第 10 卷，第 4 期，第 719–728 页，2018 年。[7] C. Carlet、S. Mesnager、C. Tang 和 Y. Qi，《欧几里得与厄米特 LCD MDS 码》，《设计、编码与密码学》，第 86 卷，第 11 期，第 2605–2618 页，2018 年。[8] C. Li，《由循环码构造的厄米特 LCD 码》，《设计、编码与密码学》，第 86 卷，第 10 期，第 2261–2278 页，2018 年。[9] M. Araya、M. Harada 和 K. Saito，《四元厄米特线性互补对偶码》，《IEEE 信息论汇刊》，第 66 卷，第 5 期，第 2751–2759 页，2019 年。

[10] Y. Li、S. Zhu 和 E. Mart´anez-Moro，《两种经典传播规则的核及其应用》，《IEEE 信息论汇刊》，第 1–1 页，2023 年。[11] S. Li、M. Shi 和 J. Wang，《一种构造小核形式自对偶码的改进方法》，《设计、编码与密码学》，第 1–21 页，2023 年。[12] C. Carlet、S. Mesnager、C. Tang、Y. Qi 和 R. Pellikaan，《有限域上的线性码等价于 LCD 码》，《IEEE 信息论汇刊》，第 64 卷，第 4 期，第 3010–3017 页，2018 年。[13] S. Bouyuklieva，《最优二元 LCD 码》，《设计、编码与密码学》，第 89 卷，第 11 期，第 2445–2461 页，2021 年。[14] M. Harada，《二元 LCD 码、三元 LCD 码和四元厄米特 LCD 码的构造》，《设计、编码与密码学》，第 89 卷，第 10 期，第 2295–2312 页，2021 年。[15] K. Ishizuka 和 K. Saito，《自对偶码与 LCD 码的构造》，《通信数学进展》，第 17 卷，第 1 期，2023 年。[16] K. I shizuka，《四元厄米特 LCD 码的构造》，《密码学与通信》，第 1–13 页，2022 年。[17] S. Li、M. Shi 和 H. Liu，《小有限域上最优 LCD 码的若干构造》，ArXiv，第 abs/2206.04936 卷，2023 年。[18] S. Li、M. Shi 和 H. Liu，《关于指数 t 的 Toeplitz 码和等距码》，《离散数学》，第 346 卷，第 113484 页，2023 年。[19] G. Wang、S. Liu 和 H. Liu，《最优二元 LCD 码的新构造》，ArXiv，第 abs/2302.00906 卷，2023 年。[20] M. Shi、N. Liu、J.-L. Kim 和 P. Sol´e，《上的加性互补对偶码》，《设计、编码与密码学》，第 91 卷，第 1 期，第 273–284 页，2023 年。.[21] M. Shi、N. Liu、F. Ozbudak 和 P. Sol´e，《上的加性循环互补对偶码》，《有限域及其应用》，第 83 卷，第 102087 页，2022 年。[22] A. R. Calderbank、E. M. Rains、P. Shor 和 N. J. Sloane，《通过 GF (4) 上的码实现量子纠错》，《IEEE 信息论汇刊》，第 44 卷，第 4 期，第 1369–1387 页，1998 年。[23] H. Xu 和 W. Du，《辛 LCD MDS 码的构造》，《马来西亚数学科学学会通报》，第 44 卷，第 5 期，第 3377–3390 页，2021 年。[24] X. Huang、J. Li 和 S. Huang，《由准循环码构造辛 LCD MDS 码》，《通信数学进展》，第 16 卷，第 4 期，第 779–790 页，2022 年。

[25] X. Yang 和 J. L. Massey，“循环码具有互补对偶的条件”，《离散数学》，第 126 卷，第 391–393 页，1994 年。[26] M. Esmaeili 和 S. Yari，“关于互补对偶准循环码”，《有限域及其应用》，第 15 卷，第 375–386 页，2009 年。.[27] C. G¨uneri、B. Ozkaya 和 P. Sol´e，“准循环互补对偶码”，《有限域及其应用》，第 42 卷，第 67–80 页，2016 年。.[28] A. Alahmadi、C. G¨uneri、B. Ozkaya、H. Shoaib 和 P. Sole，“关于互补对偶多重负循环码”，《密码学与通信》，第 12 卷，第 101–113 页，2020 年。[29] W. Bosma、J. Cannon 和 C. Playoust，“Magma 代数系统 I：用户语言”，《符号计算学报》，第 24 卷，第 3–4 期，第 235–265 页，1997 年。[30] W. C. Huffman 和 V. Pless，《纠错码基础》。英国：剑桥大学出版社，2003 年。[31] W. C. Huffman、J. L. Kim 和 P. Sol´e，《编码理论简明百科全书》。Chapman and Hall/CRC出版社，2021 年。[32] C. Galindo、F. Hernando 和 R. Matsumoto，“量子码的准循环构造”，《有限域及其应用》，第 52 卷，第 261–280 页，2018 年。[33] J. Lv、R. Li 和 J. Wang，“由具有厄米内积的单生成元准循环码导出的量子码”，《国际理论物理学杂志》，第 59 卷，第 1 期，第 300–312 页，2020 年。[34] M. Grassl，“线性码和量子码最小距离的界限”。在线可查 http://www.codetables.de。访问日期：2022.12.30。[35] K. Ishizuka，“四元厄米 LCD 码的构造”，ArXiv 预印本 arXiv:2207.00801，2022 年。[36] C. Guan、R. Li、Y. Liu 和 Z. Ma，“某些四元加性码优于相应的线性码”，IEEE 信息论汇刊，2023 年。[37] M. Araya、M. Harada 和 K. Saito，“四元厄米特线性互补对偶码”，IEEE 信息论汇刊，第 66 卷，第 5 期，第 2751–2759 页，2020 年。

## 附录

本附录中所有生成元为 $([g(x)], [g(x)f(x)])$ 或 $([g(x)], [g(x)f_1(x)\ \ [g(x)f_2(x)])$ 的准循环码，使用 Magma 记法 `QuasiCyclicCode(2*n, [g(x)],[g(x)*f(x)])`or `QuasiCyclicCode(3*n, [g(x)],[g(x)*`$f_1$`(x)],[g(x)*`$f_2$`(x)])`，即可直接得到相应的 LCD 码。

A：生成 例 4.6 中三元拟循环欧几里得LCD码的生成元

例 4.6 中生成元为 $([g(x)], [g(x)f(x)])$ 的三元拟循环欧几里得LCD码。令 $\{0,1,2\}$ 表示 $\mathbb{F}_3$ 中的元素。设 $n=13$、 $q=3$ ，指标为 $\ell=2$。详情如下。

1. $[26,4,15]_3$: $g(x) = 2x^9+2x^8+x^7+x^6+2x^5+x^4+2x^3+2x^2+x+1$; $f(x) = 2x^3+x^2+2x+1$; 2. $[26,6,13]_3$及其对偶码 $[26,20,4]_3$: $g(x) = 2x^7+2x^5+2x^4+x^3+x^2+1$; $f(x) = x^5+2x^4+x^2+2x+1$; 3. $[26,7,13]_3$: $g(x) = 2x^6+2x^5+x^4+x^2+2x+2$; $f(x) = x^6+2x^5+2x^4+2x^3+2x$; 4. $[26,8,11]_3$: $g(x) = x^5+x^4+x^3+2x^2+2x+2$; $f(x) = x^7+x^6+x^5+2x^4+x^3+1$; 5. $[26,9,10]_3$: $g(x) = x^4+2x^3+2x+1$; $f(x) = 2x^8+2x^7+2x^6+2x^5+2x^4+x^2+x+2$; 6. $[26,12,9]_3$及其对偶码 $[26,14,7]_3$: $g(x) = x+2$; $f(x) = 2x^{11}+2x^{10}+x^7+2x^5+2x^3+x^2+2x+2$; 7. $[26,13,8]_3$: $g(x) = 1$; $f(x) = x^{12}+x^9+2x^7+2x^6+2x^5+2x^4+2x^3+x^2+2x$; 8. $[26,11,7]_3$及其对偶码 $[26,15,6]_3$: $g(x) = x^2+x+1$; $f(x) = 2x^{10}+2x^9+x^7+2x^6+x^5+2x^2+x+1$;

B：表 1 中二元拟循环欧几里得 LCD 码的生成元

1. $[39,13,12]_2$: $n=13$, $\ell=3$, $g(x)=1$, $f_1(x) = x^{12}+x^7+x^3+x+1$, $f_2(x) = x^{12}+x^{11}+x^9+x^8+x^5+x^3+x^2$。 2. $[45,12,16]_2$: $n=15$, $\ell=3$, $g(x) = x^3+1$, $f_1(x) = x^{14}+x^{11}+x^{10}+x^8+x^7+x^6+x^4+x$, $f_2(x) = x^{13}+x^{11}+x^9+x^3+x^2+1$;。 3. $[45,13,15]_2$: $n=15$, $\ell=3$, $g(x) = x^2+x+1$, $f_1(x) = x^{13}+x^4+x^3+x$, $f_2(x) = x^{14}+x^{12}+x^{11}+x^9+x^5+x^4+x^3+x$; 4. $[44,22,9]_2$: $n=22$, $\ell=2$, $g(x)=1$, $f(x) = x^{20}+x^{18}+x^{17}+x^{16}+x^{14}+x^{12}+x^{10}+x^9+x^8+x^6+x^4+x^3$; 5. $[46,23,10]_2$: $n=23$, $\ell=2$, $g(x)=1$, $f(x) = x^{18}+x^{16}+x^{13}+x^{12}+x^{11}+x^{10}+x^9+x^6+x^5+x$; 6. $[46,22,10]_2$及其对偶码 $[46,24,9]_2$: $n=23$, $\ell=2$, $g(x) = x+1$, $f(x) = x^{22}+x^{19}+x^{17}+x^{15}+x^{14}+x^{13}+x^{11}+x^6+x^4+x^3+x+1$; 7. $[51,8,22]_2$: $n=17$, $\ell=3$, $g(x) = x^9+x^6+x^5+x^4+x^3+1$, $f_1(x) = x^{16}+x^{15}+x^{14}+x^{12}+x^{11}+x^8+x^2$, $f_2(x) = x^{16}+x^{15}+x^{13}+x^{11}+x^9$;

8. $[51, 16, 16]_2$: $n = 17$, $\ell = 3$, $g(x) = x + 1$, $f_1(x) = x^{15} + x^{14} + x^{12} + x^{11} + x^9 + x^8 + x^5 + x^4 + x^3 + x$, $f_2(x) = x^{15} + x^{14} + x^{13} + x^6 + x^5 + x^4 + x^3 + x^2$;

9. $[51, 17, 15]_2$: $n = 17$, $\ell = 3$, $g(x) = 1$, $f_1(x) = x^{15} + x^{14} + x^{10} + x^8 + x^7 + x^6 + x^5 + x^3$, $f_2(x) = x^{14} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^6 + x^5$;