arXiv:2601.03492v1 [cs.IT] 7 Jan 2026

厄米 L　　CD 有限链环上的 2-拟阿贝尔码

Sanjit Bhowmick[1] 和 Kuntal Deka[1]

2026年1月8日

摘要

本文介绍了有限域上的一类厄米特 LCD 2-拟阿贝尔码，并全面枚举了相对最小重量较小的这类码。我们证明，这类码在有限域上是渐近良好的。此外，我们将分析推广到有限链环，刻画了该背景下的 2-拟阿贝尔码，并证明有限链环上同样存在渐近良好的厄米特 LCD 2-拟阿贝尔码。

关键词： 有限链环、指标为2的拟阿贝尔码、渐近良好、厄米特 LCD 码。**2020 AMS 分类代码：** 94B05；94B65。

1 引言

具有互补对偶的线性码（LCD码）是一类与其相应对偶码交集为平凡集的线性码，由 Massey 提出 [24]。他给出了 LCD码的代数刻画，并证明了渐近良好的 LCD码的存在性。他还证明，二元LCD码为双用户二元加法信道提供了最优的线性编码方案。Sendrier 证明了 LCD码达到 Gilbert-Varshamov界（[29]）。除此之外，这些码在理论和应用领域都具有重要意义，尤其可用于防御嵌入式密码系统中的被动和主动侧信道攻击 [6, 7]。除密码学外，LCD码还应用于通信系统、消费电子产品和数据存储领域。这些广泛的应用促使人们对构造此类码的方法进行了大量研究 [8, 9, 10]。

有限域上的本原BCH码族并非渐近良好。循环码是否渐近良好仍是一个悬而未决的问题（见 [22]）。相比之下，早已证明2-准循环码是渐近良好的，如 [11, 12, 23]所示。在[16], 中，有人引入了具有特定指标的准循环码，并已证明这类码是渐近良好的。最近，Fan和Lin [13] 证明了存在许多达到 Gilbert-Varshamov界的渐近良好的拟阿贝尔码。二面体群码，它们并非

*[1]印度理工学院古瓦哈提分校电子与电气工程系，阿萨姆邦，781039，印度。电子邮箱：sanjitbhowmick@rnd.iitg.ac.in；kuntaldeka@iitg.ac.in

阿贝尔的，与循环群码十分相似。Bazzi和Mitter [2] 证明了二元二面体群码是渐近良好的。此外，在 [14], Fan和Lin进一步证明，具有理想数学性质的任意有限域上的二面体群码也是渐近良好的。

20世纪90年代，人们发现许多二元非线性码都可以表示为环上线性码的格雷像 $\mathbb{Z}_4$ （见 [17]）。这一发现引发了人们对有限交换链环上线性码研究的日益浓厚的兴趣 [18, 27, 28]。近年来，有限交换环上的 LCD 码得到了广泛研究 [3, 4, 5, 20, 21]。最近，Zhang 等人证明，有限域上的厄米自对偶 2-拟阿贝尔码是渐近良好的（见 [31]）。另一方面，Zhang 等人证明，有限域上的欧几里得 LCD2-拟阿贝尔码是渐近良好的（见 [32]）。因此，一个自然的问题是：有限交换链环上是否存在渐近良好的厄米 LCD2-拟阿贝尔码？受上述研究和这一问题的启发，我们研究有限交换链环上的厄米 LCD2-拟阿贝尔码。首先，我们构造了一类特殊的任意有限域上的厄米 LCD2-拟阿贝尔码（定理3.1）。随后，我们统计这类码的数量（定理3.7），并估计相对最小重量较低的码所占比例（定理3.15）。这两项结果导出了本文的结论（定理3.17）。最后，我们证明，任意有限链环上都存在渐近良好的 LCD2-拟阿贝尔码（定理4.12）。

本文的结构安排如下。在第2节，我们回顾有限链环的伽罗瓦扩张这一概念，以及有限链环上的阿贝尔码及其厄米对偶的一些必要事实。第3 节讨论有限域上的厄米 LCD 2-拟阿贝尔码。此外，我们构造并计数一类有限域上的厄米 LCD 码。进一步地，我们证明有限域上存在渐近良好的厄米 LCD 2-拟阿贝尔码。在第4节，我们给出有限链环上厄米 LCD2-拟阿贝尔码的刻画。最后，我们证明有限链环上存在渐近良好的厄米 LCD 2-拟阿贝尔码。

2 一些预备知识

在全文中，我们将 $\mathcal{S}$ 和 $\mathcal{R}$ 记为两个有限交换链环（链环是指其所有理想构成一个链），并将 $\mathbb{F}_q$ 记为一个有限域，其中 q 为素数幂。设 G 为一个阶为奇数 $n \geq 7$ 且满足最大公约数 $\{n, q\} = 1$ 的有限阿贝尔群。进一步假设链环 $\mathcal{S}$ 的极大理想为 $\mathfrak{m}$，其幂零指数为 s （即 $\mathfrak{m}^s = 0$ ，但 $\mathfrak{m}^{s-1} \neq 0$）。如果 $\mathcal{S}$ 是 $\mathcal{R}$ 的环扩张，记作 $\mathcal{S}|\mathcal{R}$，则称 $\mathcal{R}$ 是 $\mathcal{S}$ 的子环且 $1_{\mathcal{R}} = 1_{\mathcal{S}}$。若 $\mathcal{S}|\mathcal{R}$ 是一个二次伽罗瓦扩张，则当 $\mathcal{S}$ 同构于 $^{\mathcal{R}[x]}$ （f （x）） 时，其中 f 是 $\mathcal{R}$ 上的二次首一基本多项式。与该伽罗瓦扩张对应的群 $\mathrm{Aut}_{\mathcal{R}}$（$\mathcal{S}$）由所有环自同构 σ 构成，这些环自同构作用在 $\mathcal{S}$ 上并且在 $\mathcal{R}$ 上恒等。进一步假设环 $\mathcal{S}$ 和 $\mathcal{R}$ 的剩余域分别为 $\mathbb{F} = \mathbb{F}_{q^2}$ 和 $\mathbb{F}_q$。根据 [25, 定理 XV.2], ，我们有 $\mathrm{Aut}^{\mathbb{F}_q}$（$\mathbb{F}$） $\equiv$ $\mathrm{Aut}_{\mathcal{R}}$ （$\mathcal{S}$）。环 $\mathcal{S}$ 可视为一个自由的 $\mathcal{R}$- 模，其秩为 2，且 $\mathrm{rank}_{\mathcal{R}}$ （$\mathcal{S}$） $=|$ $\mathrm{Aut}_{\mathcal{R}}$ （$\mathcal{S}$） $|$。设 $\mathcal{S}|\mathcal{R}$ 为一个二次有限链环伽罗瓦扩张，并令 σ 表示 $\mathrm{Aut}_{\mathcal{R}}$（$\mathcal{S}$）中阶为 2 的一个生成元。

我们引入一个非退化的 σ-半双线性型

$$\langle\ ,\ \rangle\ :\ \mathcal{S}^n \times \mathcal{S}^n \to \mathcal{S} \text{ is defined as}$$
$$\langle \mathbf{u}, \mathbf{v}\rangle_\sigma = \sum_{j=1}^{n} u_j \sigma(v_j),\ \text{where},\ \mathbf{u} = (u_1, u_2, \ldots, u_n) \text{ and } \mathbf{v} = (v_1, v_2, \ldots, v_n).$$

我们称 线性码 C 是 $\mathcal{S}$ 的子模，且 $\mathcal{S}^n$ 的相应 σ-对偶为 C

$$C^{\perp_\sigma} = \{\mathbf{u} \in \mathcal{S}^n \mid \langle \mathbf{u}, \mathbf{c}\rangle_\sigma = 0\ \forall\ \mathbf{c} = (c_1, c_2, \ldots, c_n) \in C\}.$$

$\mathcal{S}$ 上的线性码称为厄米线性补对偶（H-LCD）码，若它与其 σ-对偶的交仅含零元。

$\mathcal{S}$上的 G 的群环记作 $\mathcal{S}G$，由所有有限个 G的元素的 $\mathcal{S}$-线性组合构成，即

$$\mathcal{S}G = \left\{ \sum_{g\in G} a_g g \mid a_g \in \mathcal{S} \right\}.$$

$\mathcal{S}G$ 的数乘、加法和乘法算子分别定义为 $k\mathsf{a} = \sum_{g\in G}(ka_g)g$、$\mathsf{a} + \mathsf{b} = \sum_{g\in G}(a_g + b_g)g$和 $\mathsf{ab} = \sum_g$, $_{h\in G} a_g b_{g^{-1}h} h$，其中 $k \in \mathcal{S}$，$\mathsf{a} = \sum_{g\in G} a_g g$ 属于 $\mathcal{S}G$，且 $\mathsf{b} = \sum_{g\in G} b_g g$属于 $\mathcal{S}G$。于是 $\mathcal{S}G$ 是一个群环，其单位元为 $1 = 1_\mathcal{S} 1_G$，其中 $1_\mathcal{S}$ 和 $1_\mathcal{G}$ 分别表示环 $\mathcal{S}$ 和群 G的单位元。注意，由于 $\mathcal{S}$ 和 G 都是有限的， $\mathcal{S}G$ 是一个有限交换环。因此，根据 [25, 定理 VI.2 和定理 VI.2]的证明， $\mathcal{S}G$ 可以唯一分解为

$$\mathcal{S}G = \mathcal{S}Ge'_0 \oplus \mathcal{S}Ge'_1 \oplus \cdots \oplus \mathcal{S}Ge'_t, \tag{1}$$

其中，每个 e'_i 都是幂等元， $e'_i e'_j = 0$，对于 $1 \le i \ne j \le t$，且 $\sum_{i=1}^{t} e'_i = 1$。 $\mathcal{S}G$ 的每个元素$\mathbf{a}$ $= \sum_{g\in G} a_g g$都可以视为 $\mathcal{S}$上的一个长度为 n的字 $(a_g)_{g\in G}$ ，因此$\mathbf{a}$ 的汉明重量记为$wt_H(\mathbf{a})$，定义为

$$wt_H(\mathbf{a}) = wt_H((a_g)_{g\in G}) = \mid \{a_g \in \mathcal{S} \mid a_g \ne 0\ \forall\ g \in G\} \mid .$$

现在，我们引入厄米内积 $\langle,\ \rangle_H$ ，定义如下

$$\langle\ ,\ \rangle_H\ :\ \mathcal{S}G \times \mathcal{S}G \to \mathcal{S} \text{ is defined by}$$
$$\left\langle \sum_{g\in G} a_g g, \sum_{h\in G} b_h h \right\rangle_H = \sum_{g\in G} a_g \sigma(b_g),\ \text{for all } \sum_{g\in G} a_g g, \sum_{h\in G} b_h h \in \mathcal{S}G.$$

如果代码 $\mathfrak{C}$ 是 $\mathcal{S}G$ 的阿贝尔代码，则称其为阿贝尔的，当且仅当 $\mathfrak{C}$是 $\mathcal{S}G$的一个理想。利用上述厄米内积， $\mathcal{S}G$ 的厄米对偶 $\mathfrak{C}$定义为

$$\mathfrak{C}^{\perp_H} = \{\mathbf{a} = \sum_{g\in G} a_g g \in \mathcal{S}G \mid \langle \mathbf{a}, \mathbf{c}\rangle_H = 0 \text{ for all } \mathbf{c} \in \mathfrak{C}\}.$$

我们称一个阿贝尔 如果 $\mathfrak{C}$ 为 $\mathcal{S}G$ ，则称其为厄米 LCD，当且仅当 $\mathfrak{C} \cap \mathfrak{C}^{\perp_H} = \{0\}$。接下来，我们考虑一个

映射 $\phi:\ \mathcal{S}G \to \mathcal{S}$，其定义为 $\sum_{g\in G} a_g g \mapsto a_{1_G}$。显然，$\phi$ 是一个满环同态。此外，容易观察到 $\langle \mathbf{a},\ \mathbf{b}\rangle_H = \phi(\mathbf{a}\widehat{\sigma}(\mathbf{b}))$，其中映射 $\widehat{\sigma}:\ \mathcal{S}G \to \mathcal{S}G$ 定义为 $\mathbf{a} = \sum_{g\in G} a_g g \mapsto \widehat{\sigma}(\mathbf{a}) = \sum_{g\in G} \sigma(a_g) g^{-1}$。可以立即验证，$\widehat{\sigma}$ 是 $\mathcal{S}G$上的环自同构。存在一个从 $\mathcal{S}$ 到 $\mathbb{F}$的自然满环同态，即定义 $\pi:\ \mathcal{S} \to \mathbb{F}$ 为 $r \mapsto \pi(r) = r + \mathbf{m}$，其中任意 $r \in \mathcal{S}$均成立。自然地，我们将此映射扩展为 $\pi: \mathcal{S}G \to \mathbb{F}G$，其定义为 $r \mapsto \pi(r)$，其中任意 $r \in \mathcal{S}G$均成立。

根据马施克定理（[1]，并且在条件 最大公约数$\{n, q\} = 1$ 下，$\mathbb{F}G$ 可唯一分解为

$$\mathbb{F}G = \mathbb{F}Ge_0 \oplus \mathbb{F}Ge_1 \oplus \mathbb{F}Ge_2 \oplus \cdots \oplus \mathbb{F}Ge_r \oplus \mathbb{F}Ge_{r+1} \oplus \cdots \oplus \mathbb{F}Ge_{r+s}, \tag{2}$$

其中每个 e_i 都是本原幂等元，且 $e_i e_j = 0$ 适用于 $i \neq j$ 和 $1 = \sum_1^{r+s} e_i$。可以验证，$\mathbb{F}Ge_i$ 是 $\mathbb{F}$ 上的向量空间，因此可写为

$$\mu_q(n) = \min\{\dim_{\mathbb{F}} \mathbb{F}Ge \ \big|\ e \in E \setminus \{e_0\}\},$$

更多细节请参见 [15, 引理 II.2]。注意，$\mathbb{F}G$上的限制映射，即 $\tau := \widehat{\sigma}\,|_{\mathbb{F}G}:\ \mathbb{F}G \to \mathbb{F}G$，是 $\mathbb{F}G$ 上的一个自同构，其定义为 $\alpha = \sum_{g\in G} \alpha_g g \mapsto \alpha^\tau = \sum_{g\in G} \alpha_g^q g^{-1}$。此外，我们将记号固定为

- $E = \{e_0\} \cup \{e_1, e_2, \ldots, e_r\} \cup \{e_{r+1}, e_{r+1}^\tau, \ldots, e_{r+s}, e_{r+s}^\tau\}$, where $e_0^\tau = e_0$, $e_i^\tau = e_i$, for $i = 1, 2, \ldots, r$, and $e_{r+j}^\tau \neq e_{r+j}$, for $j = 1, 2, \ldots, s$.
- $E^* = E \setminus \{e_0\} = \{e_1, e_2, \ldots, e_r\} \cup \{e_{r+1}, e_{r+1}^\tau, \ldots, e_{r+s}, e_{r+s}^\tau\}$.
- $\widehat{e}_{r+j} = e_{r+j} + e_{r+j}^\tau$, where $j = 1, 2, \ldots, s$.
- $\widehat{E} = \{e_0, e_1, \ldots, e_r, \widehat{e}_{r+1}, \ldots, \widehat{e}_{r+s}\}$.
- $\widehat{E}^\dagger = \widehat{E} \setminus \{e_0\} = \{e_1, \ldots, e_r, \widehat{e}_{r+1}, \ldots, \widehat{e}_{r+s}\}$.
- $\mathcal{A}_i = \mathbb{F}Ge_i$, for $i = 0, 1, \ldots, r+s$.
- $\widehat{\mathcal{A}}_{r+j} = \mathbb{F}Ge_i + \mathbb{F}G\widehat{e}_{r+j}$, for $j = 1, \ldots, s$.
- $\mathcal{I}^\tau = \{a \in \mathcal{I} \mid a^\tau = a\}$, where $\mathcal{I}$ is an ideal of $\mathbb{F}G$.

此外，我们注意到，τ 在 $\mathcal{A}_{r+j}$ 上的限制诱导出映射 $\mathcal{A}_{r+j} = \mathbb{F}Ge_{r+j} \to \mathcal{A}_{r+j}^\tau = \mathbb{F}Ge_{r+j}^\tau$，因为 $a \mapsto a^\tau$ 是一个 $\mathbb{F}$-线性同构。可以立即验证，$\mathcal{A}_{r+j} + \mathcal{A}_{r+j}^\tau$ 在自同构 τ下是不变的。现在，我们给出一个见于 [31]的引理。

引理 2.1. *[31, 引理 2.2]* 我们沿用上文所述的记号。则有以下结论

a) $(\mathbb{F}Ge_0)^\tau = \mathbb{F}_q e_0$;

b) $(\mathbb{F}G)^\tau$ 是 $\mathbb{F}_q$ 上的向量空间，并且$(\mathbb{F}G)^\tau$ 可唯一分解为

$$(\mathbb{F}G)^\tau = \mathbb{F}_q e_0 \bigoplus (\oplus_{i=1}^r (\mathbb{F}Ge_i)^\tau) \bigoplus \left(\oplus_{j=1}^s (\mathbb{F}G\widehat{e}_{r+j})^\tau\right);$$

c) 维数$_{\mathbb{F}_q}(\mathbb{F}G)^\tau = n$;

d) $(\mathbb{F}G\widehat{e}_{r+j})^\tau = \{a + a^\tau \mid a \in \mathbb{F}Ge_{r+j}\}$ 以及 维数$_{\mathbb{F}_q}(\mathbb{F}G\widehat{e}_{r+j})^\tau =$维数$_{\mathbb{F}_q}\mathbb{F}Ge_{r+j}$，其中 $j = 1$，……，s;

e) $\dim_{\mathbb{F}_q}(\mathbb{F}Ge_i)^\tau = \frac{1}{2}\dim_{\mathbb{F}_q}\mathbb{F}Ge_i$, *for* $i = 1, \ldots, r$.

此外，记

$$\begin{aligned}
&k_e = \dim_{\mathbb{F}}\mathbb{F}Ge \text{ for all } e \in \widehat{E} \setminus \{e_0\},\\
&k_i = k_{e_i}, \text{ for } i = 1, 2, \ldots, r;\\
&k_{r+j} = k_{\widehat{e}_{r+j}} \text{ and } k_{r+j} \text{ is even for } j = 1, 2, \ldots, s;\\
&\dim_{\mathbb{F}}\mathbb{F}Ge_{r+j} = \dim_{\mathbb{F}}\mathbb{F}Ge_{r+j}^\tau \text{ for } j = 1, 2, \ldots, s.
\end{aligned}$$

3 厄米特 LCD 2-拟阿贝尔码

本节的主要目标是构造一类定义在 $\mathbb{F}$上的厄米特-LCD 2-拟阿贝尔群码。令

$$(\mathbb{F}G)^2 := \mathbb{F}G \times \mathbb{F}G = \{(a, b) \mid a, b \in \mathbb{F}G\}$$

这是一个 $\mathbb{F}G$-模。$(\mathbb{F}G)^2$ 的任意 $\mathbb{F}G$-子模 $\mathcal{C}$ 称为定义在 $\mathbb{F}$上的 2-拟阿贝尔码。我们进一步自然地扩展 $(\mathbb{F}G)^2$ 中的厄米内积。因此，以类似的方式，我们定义 $\mathbb{F}G$关于 $\mathbb{F}$ 的厄米特对偶码。对于任意 a, $b \in \mathbb{F}G$，记 $\mathcal{C}_{a,\ b}$ 如下

$$\mathcal{C}_{a,b} := \{s(a, b) \mid s \in \mathbb{F}G\}.$$

显然，$\mathcal{C}_{a,\ b}$ 是由 $(a,\ b)$ 生成的 $(\mathbb{F}G)^2$ 的 $\mathbb{F}G$-子模。记作 $\mathbb{F}^\times = \mathbb{F} \setminus \{0\}$。

定理 3.1. 对于任意 a，$b \in \mathbb{F}G$，且若 $aa^\tau + bb^\tau = \lambda$，其中 $\lambda \in \mathbb{F}^\times$，则 $\mathcal{C}_{a,b}$ 是一个厄米 *LCD*2-准阿贝尔码，即 $\mathcal{C}_{a,b} \cap \mathcal{C}_{a}^{\perp_H}{}_{,b} = \{0\}$.

证明。令 $s(a,\ b) \in \mathcal{C}_{a,\ b} \cap \mathcal{C}_{a\ b}^{\perp_H}{}_{,}$，可得 $(sa,\ sb) \in \mathcal{C}_{a\ b}^{\perp_H}{}_{,}$，这意味着 $\langle (sa,\ sb), (s_1a,\ s_1b)\rangle_H = 0$, 对所有$s_1 \in \mathbb{F}G$均成立。因此，$\langle sa,\ s_1a\rangle_H + \langle sb,\ s_1b\rangle_H = 0$对所有 $s_1 \in \mathbb{F}G$均成立。由此可得，对于所有 $s_1 \in \mathbb{F}G$，$\phi\,|_{\mathbb{F}G}(ss_1^\tau(aa^\tau + bb^\tau))$ =0。根据假设，对于所有 $s_1 \in \mathbb{F}G$，$\phi\,|_{\mathbb{F}G}(ss_1^\tau) = 0$。这意味着 $s = 0$。因此结论立即成立。 □

推论 3.2. 对于满足 $\beta\beta^\tau = \lambda - 1 \in \mathbb{F}^\times$ 的 $\beta \in \mathbb{F}G$ 和 $\lambda \in \mathbb{F}^\times$，$\mathcal{C}_{1,\ \beta} = \{s(1,\ \beta) \mid s \in \mathbb{F}G\}$ 是一个码率为 $1/2$ 的厄米 *LCD* 2-准阿贝尔码。

证明。应用定理 3.1，取 $a = 1$ 和 $b = \beta$，即可立即得到结论。对于另一部分，我们定义映射 $\varrho : \mathcal{C}_{1,\ \beta} \to \mathbb{F}G$，使得对所有 $s \in \mathbb{F}G$，$s(\mathbf{1},\ \beta) \mapsto s$。容易验证，$\varrho$ 是 $\mathcal{C}_{1,\ \beta}$ 与 $\mathbb{F}G$ 之间的一个 $\mathbb{F}G$-模同构。因此，我们得出所需结论。 □

利用上述推论3.2，我们将构造一类满足条件 $\lambda \in \mathbb{F}^\times$ 和 $\lambda - 1 \in \mathbb{F}^\times$的厄米特 LCD 码。

下文中我们始终记

$$\mathcal{D}_\lambda = \left\{ \mathcal{C}_{1,\beta} \,\middle|\, \beta \in \mathbb{F}G,\ \beta\beta^\tau = \lambda - 1 \right\}, \tag{3}$$

这就是所有厄米 LCD 2-拟阿贝尔码的集合，参见推论 3.2。我们始终假设δ 是一个实数，且满足 $0 \le \delta \le 1 - q^{-1}$，并令

$$\mathcal{D}_\lambda^{\le\delta} = \left\{ \mathcal{C}_{1,\beta} \,\middle|\, \mathcal{C}_{1,\beta} \in \mathcal{D},\ \Delta(\mathcal{C}_{1,\beta}) = \tfrac{wt_H(\mathcal{C}_{1,\beta})}{2n} \le \delta \right\} \tag{4}$$

and

$$\widehat{\mathcal{D}}_\lambda = \left\{ \beta \in \mathbb{F}G \,\middle|\, \beta\beta^\tau = \lambda - 1 \right\}. \tag{5}$$

可以立即验证 $\left|\mathcal{D}_\lambda\right| = \left|\widehat{\mathcal{D}}_\lambda\right|$。为估计 $\widehat{\mathcal{D}}_\lambda$，我们引入以下引理。

引理 3.3. 对于 $\beta \in \mathbb{F}G$ 和 $\lambda \in \mathbb{F}^\times$， $\beta\beta^\tau = \lambda - 1$ 当且仅当

$$\begin{cases} \beta\beta^\tau e_0 = (\lambda-1)e_0 & \\ \beta\beta^\tau e_i = (\lambda-1)e_i & for\ 1 \le i \le r \\ \beta\beta^\tau \widehat{e}_{r+j} = (\lambda-1)\widehat{e}_{r+j} & for\ 1 \le j \le s. \end{cases}$$

证明。 其证明是一个直接的练习。 □

此外，我们用以下集合表示

$$\mathcal{I}_0 = \{\alpha \in \mathbb{F}Ge_0 \mid \alpha\alpha^\tau = (\lambda-1)e_0\}; \tag{6}$$

$$\mathcal{I}_i = \{\alpha \in \mathbb{F}Ge_i \mid \alpha\alpha^\tau = (\lambda-1)e_i\} \text{ for all } i = 1, 2, \ldots, r; \tag{7}$$

$$\mathcal{I}_{r+j} = \{\alpha \in \mathbb{F}G\widehat{e}_{r+j} \mid \alpha\alpha^\tau = (\lambda-1)\widehat{e}_{r+j}\} \text{ for all } j = 1, 2, \ldots, s. \tag{8}$$

引理 3.4。 设 $\mathcal{I}_0$ 为方程 (6)中定义的集合。则当 $\left|\mathcal{I}_0\right| = \begin{cases} q+1 \text{ 时，} & \lambda - 1 \in \mathbb{F}_q^*; \\ \text{当 } 0 \text{ 时，} & \lambda - 1 \notin \mathbb{F}_q^*. \end{cases}$

证明。 根据方程（6），可得

$$\begin{aligned} \left|\mathcal{I}_0\right| &= \left|\{\alpha \in \mathbb{F}Ge_0 \mid \alpha\alpha^\tau = (\lambda-1)e_0\}\right| \\ &= \left|\{\nu e_0 \in \mathbb{F}Ge_0 \mid \nu e_0(\nu e_0)^\tau = (\lambda-1)e_0\}\right| \\ &= \left|\{\nu \in \mathbb{F} \mid \nu\nu^\tau = (\lambda-1)\}\right|. \end{aligned}$$

因此，

$$\left|\mathcal{I}_0\right| = \left|\{\nu \in \mathbb{F} \mid \nu\nu^\tau = (\lambda-1)\}\right| = \begin{cases} q+1 & \text{if } \lambda - 1 \in \mathbb{F}_q^*, \\ 0 & \text{if } \lambda - 1 \notin \mathbb{F}_q^*. \end{cases}.$$

这是因为映射 $\nu \mapsto \nu^{q+1}$ from $\mathbb{F}_{q^2}^* \to \mathbb{F}_q^*$ 是一个核的大小为 $q+1$ 的满射群同态。

□

引理 3。 **5.** L且 $\mathcal{I}_i$ 是方程 (7)中定义的集合。则 $\left|\mathcal{I}_i\right| = q^{k_i} + 1$，对 $i = 1, 2, \ldots\ldots, r$。

证明。 应用引理2.1，我们得出 $(\mathbb{F}Ge_i)^\tau$ 是 $\mathbb{F}Ge_i$ 的子域，其 $\dim(\mathbb{F}Ge_i)^\tau = \frac{1}{2}\dim \mathbb{F}Ge_i$。注意到，$\tau$ 在 $\mathbb{F}Ge_i$ 上是 $\mathbb{F}Ge_i$ 的伽罗瓦自同构。这意味着 τ 的阶等于 2。因此，对于所有 $\alpha \in \mathbb{F}Ge_i$、$i = 1, 2, \ldots\ldots, r$，我们得到 $\alpha^\tau = \alpha^{q_i^k}$。于是，对于$i = 1, 2, \ldots\ldots, r$，有 $\left|\mathcal{I}_i\right| = q^{k_i} + 1$（见 [30, 定理 7.16 和推论 7.17]）。

□

引理 3.6。 令 $\mathcal{I}_{r+j}$ 为方程 (8)中定义的集合。则 $\left|\mathcal{I}_{r+j}\right| = q^{k_{r+j}} - 1$，其中 $j = 1, 2, \ldots\ldots, s$。

证明。 为证明该结果，假设 $\alpha = \beta + \gamma$，其中 $\beta \in \mathbb{F}Ge_{r+j}$ 和 $\gamma \in \mathbb{F}Ge_{r+j}^\tau$。于是，

$$\begin{aligned}\mathcal{I}_{r+j} &= \{\beta + \gamma \in \mathbb{F}G\widehat{e}_{r+j} \mid (\beta+\gamma)(\beta+\gamma)^\tau = (\lambda-1)\widehat{e}_{r+j}\} \\ &= \{\beta + \gamma \in \mathbb{F}G\widehat{e}_{r+j} \mid \beta\gamma^\tau + \beta^\tau\gamma = (\lambda-1)e_{r+j} + (\lambda-1)e_{r+j}^\tau\} \\ &= \{\beta + (\lambda-1)(\beta^{-1})^\tau e_{r+j}^\tau \mid \beta \in (\mathbb{F}Ge_{r+j})^\times\}\end{aligned}$$

因此，对于 $j = 1, 2, \ldots\ldots, s$，有 $\left|\mathcal{I}_{r+j}\right| = q^{k_{r+j}} - 1$，证毕。

□

此外，我们有以下定理。

定理 3.7。 $\mathcal{D}_\lambda$ 的基数为

$$\left|\mathcal{D}_\lambda\right| = (q+1)\prod_{i=1}^{r}(q^{k_i}+1)\prod_{j=1}^{s}(q^{k_{r+j}}-1). \tag{9}$$

证明。 这可由引理 3.4、3.5和 3.6立即得到。

□

引理 3.8. *[15, 引理 IV.7]*对于 $q \geq 2$，以及 $l_1, l_2, \ldots, l_m$，满足 $l_i \geq$对数$_q m$，其中 i =1、2、. . .、 m，则

a) $\prod_{i=1}^{m}(q^{l_i}-1) \geq q^{\sum_{i=1}^{m} l_i} - 2$;

b) $\prod_{i=1}^{m}(q^{l_i}+1) \leq q^{\sum_{i=1}^{m} l_i} + 2$.

推论 3.9. 对于 对数 $\frac{q\ n}{\mu_q\ n}() \leq 1$，我们有 $\left|\mathcal{D}_\lambda\right| \geq q^{n-2}$。

证明。 注意到 $n = 1 + r + s$，我们有 对数$_q(r+s)$ $<$ 对数$_q n \leq \mu_q(n)$。显然， 对数$_q(r+s)$ $< k_e$ 当$\mu_q(n) \leq k_e$。由此并应用定理 3.7 和引理 3.8，我们得出$\left|\mathcal{D}_\lambda\right| \geq q^{n-2}$。

□

接下来，对于 $a \in \mathbb{F}G$，我们记

$$\widehat{E}_a = \left\{ e \mid e \in \widehat{E},\ ea \neq 0 \right\},\ \ \widehat{E}_a^{\dagger} = \left\{ e \mid e \in \widehat{E}^{\dagger},\ ea \neq 0 \right\};$$
$$L_a = \oplus_{e \in \widehat{E}_a^{\dagger}} \mathbb{F}Ge \leq \mathbb{F}G;\ \ \ell_a = \sum_{e \in \widehat{E}_a^{\dagger}} n_e,\ \text{hence},\ \dim L_a = \ell_a.$$

对于满足 $\mu_q(n) \leq \ell < n$ 的整数 ℓ，我们记为，
$\Omega_\ell = \left\{ J \leq \mathbb{F}G \mid \text{存在一个子集 } \mathcal{S} \subseteq \widehat{E}_a^{\dagger},\ \text{使得 } J = \oplus_{e \in \mathcal{S}} \mathbb{F}Ge,\ \dim J = \ell \right\}$；$J \in \Omega_\ell$，我们记 $\tilde{J} = \mathbb{F}Ge_0 + J$，$\tilde{J}^* = \left\{ a \mid a \in \tilde{J},\ L_a = J \right\}$，因此，$\dim \tilde{J} = \ell + 1$，$\ell_a = \ell$；$\mathcal{D}_{a,b} = \left\{ \mathcal{C}_{1,\beta} \mid (a,\ b) \in \mathcal{C}_{1,\ \beta} \right\}$.

引理 3.10。若 $\mathcal{D}_{a,\ b} \neq \emptyset$，则 $\widehat{E}_a = \widehat{E}_b$，且 $\mathcal{D}_{a,\ b} \leq q^{n+3-\ell_a}$。

证明。为证明该结果，假设 $\beta = \sum_{e \in \widehat{E}} \beta_e$，其中 $\beta_e \in \mathbb{F}Ge$ 对 $e \in E$ 和 $\mathcal{C}_{1,\ \beta} \in \mathcal{D}_{a,\ b}$成立。这意味着对于某个 $u \in \mathbb{F}G$，有 $(a,\ b) = u(1,\ \beta)$。由此得到 $a = u$ 和 $b = u\beta$，从而可推出 $b = a\beta$。因此，对于所有 $e \in E$，$eb = ea\beta = ea\beta_e$。此外，我们得出：当且仅当 $\beta_e\beta_e^{\tau} = (\lambda - 1)e$且 $e\beta = ea\beta_e$，对于所有 $e \in \widehat{E}$，$\mathcal{C}_{1,\ \beta} \in \mathcal{D}_{a,\ b}$成立。于是，$\widehat{E}_a = \widehat{E}_b$和$\left|\mathcal{D}_{a,\ b}\right| = \prod_{e \in \widehat{E}} \left|\{\beta_e \mid \beta_e\beta_e^{\tau} = (\lambda - 1)e,\ eb = ea\beta_e\}\right|$。

情形 1：$e = e_0$。应用引理 3.4，我们至多有 $q + 1$ 种 β_e的选择。

情形 2：$e \in \widehat{E}_a^{\dagger}$。由于 $\widehat{E}_a^{\dagger} = \widehat{E}_b^{\dagger}$，因此 $ea \neq 0$ 和 $eb \neq 0$。

子情形 2.1：$e = e_i$，其中某个 i 满足 $1 \leq i \leq r$。我们得出 $\mathbb{F}Ge$ 是有限域且 $eb = ea\beta_e$，由此得到 $\beta_e = (ea)^{-1}(e\beta)$。因此，$\beta_e$ 只有一种选择。

子情形 2.2：$e = \widehat{e}_i = e_{r+j} + e_{r+j}^{\tau}$，其中某个 j 满足 $1 \leq j \leq s$。假设 $\beta_e = c_e + d_e$，其中 $c_e \in \mathbb{F}Ge_{r+j}$，且 $d_e \in \mathbb{F}Ge_{r+j}^{\tau}$。因此，$\beta_e\beta_e^{\tau} = (\lambda - 1)e$ 当且仅当 $c_e d_e^{\tau} = (\lambda - 1)^{e_{r+j}}$，且 $eb = ea\beta_e$ 当且仅当 $be_{r+j} = ae_{r+j}c_e$, $be_{r+j}^{\tau} = ae_{r+j}^{\tau}d_e$. 。若 $ea \neq 0$，则有 $e_{r+j}a \neq 0$ 或 $e_{r+j}^{\tau}a \neq 0$。在这两种情况下，我们都得出 β_e 只有一种选择。

情况 3：$e \in \widehat{E}^{\dagger} - \widehat{E}_a^{\dagger}$。我们有 $eb = ea = 0$。因此，$eb = ea\beta_e$。因此，β_e 的选择数至多为 $\max\{q^{k_e} - 1, q^{k_e} + 1\} = q^{k_e} + 1$，这可直接由引理 3.5 和 3.6得出。因此，我们得出

$$\left|\mathcal{D}_{a,b}\right| \leq (q+1) \prod_{e \in \widehat{E}^{\dagger} - \widehat{E}_a^{\dagger}} (q^{k_e} + 1).$$

此外，我们注意到 $\sum_{e \in \widehat{E}^{\dagger} - \widehat{E}_a^{\dagger}} k_e = n - 1 - \ell_a$。应用引理 3.10，可得

$$\left|\mathcal{D}_{a,b}\right| \leq (q+1) \prod_{e \in \widehat{E}^{\dagger} - \widehat{E}_a^{\dagger}} (q^{k_e} + 1) \leq (q+1) q^{\sum_{e \in \widehat{E}^{\dagger} - \widehat{E}_a^{\dagger}} k_e + 2} \leq q^{n+3-\ell_a}.$$

证明至此完成。 □

引理 3.11。 我们有如下关系。

$$\mathcal{D}_{\lambda}^{\leq\delta} \subseteq \bigcup_{\mu_q \leq \ell < n} \bigcup_{J \in \Omega_\ell} \bigcup_{(a,b) \in (\tilde{J}^* \times \tilde{J}^*)^{\leq\delta}} \mathcal{D}_{a,b}.$$

证明。为了证明该结论，我们假设 $\mathcal{C}_{1,\beta} \in \mathcal{D}_{\lambda}^{\leq\delta}$，由此得到 $0 < wt_H(\mathcal{C}_{1,\beta}) \leq 2n\delta$ 和 $\beta\beta^\tau = \lambda - 1$。因此，存在一个非零元素 (a,b) 属于 $\mathcal{C}_{1,\beta}$，使得 $0 < wt_H(a,b) \leq 2n\delta$。因此，由引理 3.10 可得 $\widehat{E}_a^\dagger = \widehat{E}_b^\dagger$。若可能，假设 $\widehat{E}_a^\dagger = \widehat{E}_b^\dagger = \emptyset$，这意味着对于所有 $e \in \widehat{E}_a^\dagger$，都有 $ea = eb = 0$，也就是说 a, b 属于 $\mathbb{F}Ge_0$。那么，存在 $\mathbb{F}$ 的非零元素 ν_a, ν_b，使得 $a = \nu_a e_0$ 且 $b = \nu_b e_0$。因此，$wt_H(a,b) = 2n$，这与 $wt_H(a,b) < 2n$ 矛盾。因此，$\widehat{E}_a^\dagger = \widehat{E}_b^\dagger \neq \emptyset$。接下来，令~我们设 $J = \oplus_{e \in \widehat{E}_a^\dagger} \mathbb{F}Ge = \oplus_{e \in \widehat{E}_b^\dagger} \mathbb{F}Ge$, $J = J + \mathbb{F}Ge_0$，且 $\dim_{\mathbb{F}} J = \ell$，则 $\mu_q(n) \leq \ell < n$。因此，$J \in \Omega_\ell$ 且 $a, b \in \tilde{J}^*$。于是，对于 $(a,d) \in (\tilde{J}^* \times \tilde{J}^*)^{\leq\delta}$，有 $\mathcal{C}_{1,\beta} \in \mathcal{D}_{a,b}$。 □

引理 3.12。 Ω_ℓ 的基数为

$$\left|\Omega_\ell\right| < n^{\frac{\ell}{\mu_q(n)}}.$$

证明。 该结果可由 Ω_ℓ 的定义直接得到。 □

接下来，我们定义 q-熵函数，记为 $h_q(\delta)$，其表达式为 $h_q(\delta) = \delta \log_q(q-1) - \delta \log_q \delta - (1-\delta)\log_q(1-\delta)$。注意，$h_q(\delta)$ 在区间 $[0, 1-q^{-1}]$ 内递增且为凹函数，其中 $h_q(0) = 0$ 且 $h_q(1-q^{-1}) = 1$。

引理 3.13。 *[15, 引理 IV.6]* 对于 $\mathbb{F}G$ 的理想 I，有 $I \times I \leq (\mathbb{F}G)^2$，且 $\left|I \times I\right|^{\leq\delta} \leq q^{h_q(\delta)\text{维数}_{\mathbb{F}}(I \times I)}$。

引理 3.14。 对于 $\mu_q(n) \leq \ell < n$ 和 $I \in \Omega_\ell$，有 $\left|\bigcup_{(a,b) \in (\tilde{J}^* \times \tilde{J}^*)^{\leq\delta}} \mathcal{D}_{a,b}\right| \leq q^{n+3-2\ell[\frac{1}{2}-h_q(\delta)]+2h_q(\delta)}$。

证明。 应用引理 3.13，我们得到

$$\begin{aligned}
\left|\bigcup_{(a,b) \in (\tilde{J}^* \times \tilde{J}^*)^{\leq\delta}} \mathcal{D}_{a,b}\right| &\leq \sum_{(a,b) \in (\tilde{J}^* \times \tilde{J}^*)^{\leq\delta}} \left|\mathcal{D}_{a,b}\right| \\
&\leq \sum_{(a,b) \in (\tilde{J}^* \times \tilde{J}^*)} q^{n+3-\ell} \quad \text{by Lemma 3.10} \\
&= \left|(\tilde{J}^* \times \tilde{J}^*)^{\leq\delta}\right| q^{n+3-\ell} \\
&\leq q^{n+3-2\ell[\frac{1}{2}-h_q(\delta)]+2h_q(\delta)}.
\end{aligned}$$

证明至此完成。 □

定理 3.15。 对于 $\frac{1}{2} - h_q(\delta) - \log_{\mu_q(n)} q^n > 0$，我们有 $\left|\mathcal{D}_\lambda^\delta\right| \leq q^{n+4-2\mu_q(n)\left[\frac{1}{2}-h_q(\delta)-\frac{\log_q n}{\mu_q(n)}\right]}$。

证明。 首先，我们得出 $\ell \geq \mu_q(n)$ 以及 $\frac{1}{2} - h_q(\delta) - \text{对数}_{\mu_q(n)} q^n > 0$。这意味着 $2h_q(\delta) \leq 1$。应用引理 3.11、3.12 和 3.14，结论立即成立。 □

引理 3.16。 *[14,* 引理 *II.6]* 存在无穷多个与 q 互素的正奇整数 $n_1, n_2, \ldots$，使得 极限$_{i\to\infty}$ 对数$_{\mu_q}{}^{q^{n_i}}{}_{n_i}$ $() = 0$，具体而言 $\mu_q(n_i) \longrightarrow\infty$ 当 $i \to \infty$ 时。

现在，我们准备证明，存在一类定义在 $\mathbb{F}$上的厄米 LCD 2-拟阿贝尔码，它们是渐近良好的。

定理 3.17。 设 n_i （如引理 *3.16* 中所定义），且设阿贝尔群 G_i 的阶为奇数n_i，其中 $i = 1, 2, \ldots$ ...，存在厄米特 *LCD* 2-拟阿贝尔码 $\mathcal{C}_i$，使得码序列$\mathcal{C}_1, \mathcal{C}_2, \ldots$ 是渐近良好的。

证明。为证明这些结果，令我们假设$\mathcal{D}_{\lambda, i}$ （按公式（3）中的定义）是对于 $i = 1, 2, \ldots$的厄米 LCD 2-拟阿贝尔码集合。由于 $\lim_{i\to\infty} \log_{\mu_q}{}^{q^{n_i}}{}_{n_i}() = 0$，因~~此~~我们选择 $\epsilon > 0$ 使得$\frac{1}{2} - h_q(\delta) - \log_{\mu_q}{}^{q^{n}}{}_{n}() > \epsilon > 0$ 且 $\log_{\mu_q}{}^{q^{n_i}}{}_{n_i}() \leq 1$。~~应~~用推论 3.9 和定理 3.15，我们得到

$$\frac{|\mathcal{D}_{\lambda,i}^{\leq\delta}|}{|\mathcal{D}_{\lambda,i}|} \leq \frac{q^{n_i+4-2\mu_q(n_i)[\frac{1}{2}-h_q(\delta)-\frac{\log_q n_i}{\mu_q(n_i)}]}}{q^{n_i-2}} = q^{-2\mu_q(n_i)[\frac{1}{2}-h_q(\delta)-\frac{\log_q n}{\mu_q(n)}]+6}.$$

取 $\mu_q(n_i) \to \infty$，我们有

$$\lim_{i\to\infty} \frac{|\mathcal{D}_{\lambda,i}^{\leq\delta}|}{|\mathcal{D}_{\lambda,i}|} \leq \lim_{i\to\infty} q^{-2\mu_q(n_i)[\frac{1}{2}-h_q(\delta)-\frac{\log_q n_i}{\mu_q(n_i)}]+6} = 0.$$

因此，我们可以取 $\mathcal{C}_i \in \mathcal{D}_{\lambda,\, i} \setminus \mathcal{D}_{\lambda\, i}^{\leq\delta}$，对于 $i = 1, 2, \ldots$，存在厄米 LCD 2-拟阿贝尔码$\mathcal{C}_i$，其长度为 n_i，对于 $i = 1, 2, \ldots$，使得 $n_i \to \infty$，并且我们得到

i) 长度为 $2n_i \to \infty$ 的码 $\mathcal{C}_i$；

ii) 码率 $R(\mathcal{C}_i) = \frac{1}{2}$；-

iii) 对所有 $i = 1, 2, \ldots$，相对最小距离 $\triangle(\mathcal{C}_i) > \delta$。

因此，我们称码序列 $\mathcal{C}_1, \mathcal{C}_2, \ldots$ 是渐近良好的 . □

4 有限链环上的厄米 LCD 2-拟阿贝尔码

本节首先刻画有限链环上的厄米 LCD 2-拟阿贝尔码。现在，我们回顾有限链环上的厄米 LCD 2-拟阿贝尔码的性质。接下来，$(\mathcal{SG})^2 := \{(a, b) : a, b \in \mathcal{SG}\} = \mathcal{SG} \times \mathcal{SG}$。任意 $\mathcal{SG}$-子模 $\mathfrak{C}$ of $(\mathcal{SG})^2$ 均称为 $\mathcal{S}$ 上的 2-拟阿贝尔码。对于任意 $(a, b) \in (\mathcal{SG})^2$,，我们将 2-拟阿贝尔码 $\mathfrak{C}_{c,d}$ 记为 $\mathfrak{C}_{c,d} = \{(uc, ud) : u \in \mathcal{SG}\}$。此外，若 2- 拟阿贝尔码 $\mathfrak{C}_{c,d}$ 满足 $\mathfrak{C}_{c,d} \cap \mathfrak{C}_c^{\perp_H}{}_{,d} = \{0\}$，则称其为厄米 LCD 码。这里，$\mathfrak{C}_c^{\perp_H}{}_{,d} = \{(x, y) \in (\mathcal{SG})^2 : \langle (x, y), (uc, ud)\rangle = \langle x, uc\rangle + \langle y, ud\rangle = \phi(x\widehat{\sigma}(uc)) + \phi(y\widehat{\sigma}(ud)) = \phi(\widehat{\sigma}(u)(x\widehat{\sigma}(c) + y\widehat{\sigma}(d))) = 0 \ \forall\ u(c, d) \in \mathfrak{C}_{c,d}\}$，其中 $\phi : \mathcal{SG} \to \mathcal{S}$ 为 $\sum_{g} a_g g \mapsto a_{g0}$。我们还回顾一下$\in G$ 自然满环同态 $\mathcal{S}$ 到 $\mathbb{F}$，即 $\pi : \mathcal{S} \to \mathbb{F}$ 由 $r \mapsto \pi(r) = r + \mathbf{m}$，对任意 $r \in \mathcal{S}$均成立。自然地，我们将此映射扩展为 $\pi : \mathcal{SG} \to \mathbb{F}G$ 由 $r \mapsto \pi(r) = r + \mathrm{J}(\mathcal{SG})$，对任意 $r \in \mathcal{SG}$均成立，其中 $\mathrm{J}(\mathcal{SG})$ 是 $\mathcal{SG}$ 的雅各布森根。

定义 4.1. r 的元素称为 $\mathcal{S}G$ 的单位元，若 $\pi(r)$ 是 $\mathbb{F}G$ 的单位元。

接下来，我们给出以下命题，该命题由 [25]得到。

命题 4.1。 设 M 是一个有限生成右 $\mathcal{S}$-模，其雅各布森根为 $J(\mathcal{S})$，且 $\mathcal{S}$。若$MJ(\mathcal{S}) = M$，则 $M = 0$.

引理 4.2。 设 $\mathfrak{C}_{c,d}$ 是一个定义在 $\mathcal{S}$上的2-拟阿贝尔码。若 $\pi(\mathfrak{C}_{c,d})$是厄米 *LCD* 码，则$\mathfrak{C}_{c,d}$ 也是厄米 *LCD* 码。

证明。为证明该结果，设 $x \in \mathfrak{C}_{c,d} \cap \mathfrak{C}_{c\,d}^{\perp_H}$, 。于是 $\pi(x) \in \pi(\mathfrak{C}_{c,d}) \cap \pi(\mathfrak{C}_{c\,d}^{\perp_H},)$。由于 $\pi(\mathfrak{C}_{c\,d}^{\perp_H},) \subseteq \pi(\mathfrak{C}_{c,d})^{\perp_H}$ ，且根据假设， $\pi(\mathfrak{C}_{c,d})$ 是厄米 LCD 码，因此 $\pi(x) = 0$，即 $x \in \ker(\pi) = \mathfrak{C}_{c,d} \cap \mathfrak{C}_{c}^{\perp_H},_d \cdot \mathrm{J}(\mathcal{S}G)$, 其中 $\mathrm{J}(\mathcal{S}G)$ 是 $\mathcal{S}G$ 的雅各布森根。因此，$\mathfrak{C}_{c,d} \cap \mathfrak{C}_{c}^{\perp_H},_d = \left(\mathfrak{C}_{c,d} \cap \mathfrak{C}_{c,d}^{\perp_H}\right) \cdot \mathrm{J}(\mathcal{S}G)$。由于该交集是有限生成的 $\mathcal{S}G$-模，根据命题 4.1，它必为零。因此，$\mathfrak{C}_{c,d}$ 是厄米 LCD 码。

□

此外，我们给出以下引理。

引理 4.3. 设 $\mathcal{S}G$ 是一个雅各布森根为 $J(\mathcal{S}G)$ 的有限交换环。那么存在一个非零元素 $m \in J(\mathcal{S}G)$, 使得对所有 $\alpha \in J(\mathcal{S}G)$，均有 $\alpha m = 0$ 。

证明。 由于 $\mathcal{S}G$ 是有限交换环，其雅各布森根 $\mathrm{J}(\mathcal{S}G)$ 是一个幂零理想。设 g 是满足 $\mathrm{J}(\mathcal{S}G)^g = 0$，但 $\mathrm{J}(\mathcal{S}G)^{g-1} \neq 0$ 的最小正整数。于是 $\mathrm{J}(\mathcal{S}G)^{g-1} \subseteq \mathrm{J}(\mathcal{S}G)$，并且对于任意 $m \in \mathrm{J}(\mathcal{S}G)^{g-1}$ 和 $\alpha \in \mathrm{J}(\mathcal{S}G)$, 有 $\alpha m \in \mathrm{J}(\mathcal{S}G)^g = 0$。因此，任意非零 $m \in \mathrm{J}(\mathcal{S}G)^{g-1}$ 都满足对所有 $\alpha \in \mathrm{J}(\mathcal{S}G)$， $\alpha m = 0$ 。

□

定理 4.4。 设 $\mathfrak{C}_{c,d}$ 是 $\mathcal{S}$ 上的2-准阿贝尔码，且 $\pi(\mathfrak{C}_{c}^{\perp},d) = \pi(\mathfrak{C}_{c,d})^{\perp}$。那么 $\mathfrak{C}_{c,d}$ 是 $\mathcal{S}$ 上的厄米 *LCD* 码，当且仅当 $\pi(\mathfrak{C}_{c,d})$是 $\mathbb{F}$上的厄米 *LCD* 码。

证明。 由引理 4.3可知，若 $\pi(\mathfrak{C}_{c,d})$ 是 $\mathbb{F}$上的厄米 LCD 码，则 $\mathfrak{C}_{c,d}$ 也是。

反过来，假设 $\mathfrak{C}_{c,d} \cap \mathfrak{C}_{c}^{\perp}{}^{H},_d = 0$。令 $x \in \pi(\mathfrak{C}_{c,d}) \cap \pi(\mathfrak{C}_{c\,d}^{\perp}{}^{H},)$。那么存在 $c \in \mathfrak{C}_{c,d}$和 $d \in \mathfrak{C}_{c\,d}^{\perp}{}^{H}$, 使得 $\pi(c) = \pi(d) = x$，这意味着 $c - d \in (\mathcal{S}G)^2\mathrm{J}(\mathcal{S}G)$。由引理 4.3，存在一个非零的 $m \in \mathrm{J}(\mathcal{S}G)$，使得 $(c - d)m = 0$，因此 $cm = dm \in \mathfrak{C}_{c,d} \cap \mathfrak{C}_{c}^{\perp}{}^{H},_d = 0$。于是，$cm = 0$\$ $whichimplies$\$$c \in (\mathcal{S}G)^2\mathrm{J}(\mathcal{S}G)$。若 $c \notin (\mathcal{S}G)^2\mathrm{J}(\mathcal{S}G)$，则 $cm \neq 0$，由此得出矛盾。因此， $x = \pi(c) = 0$，从而得出 $\pi(\mathfrak{C}_{c,d}) \cap \pi(\mathfrak{C}_{c\,d}^{\perp_H},) = \{0\}.$ 。因此， $\pi(\mathfrak{C}_{c,d})$ 是 $\mathbb{F}$上的厄米 LCD 码。

□

现在，我们给出 2-准阿贝尔码为厄米 LCD 码的刻画。

定理 4.5. 设 $(c, d) \in (\mathcal{S}G)^2$. 若 $\pi(c\hat{\sigma}(c) + d\hat{\sigma}(d))$是 $\mathbb{F}G$中的单位，则 $\mathcal{S}$ 上的2-准阿贝尔码 $\mathfrak{C}_{c,d}$ 是厄米 *LCD* 码。

证明。假设 $u(c, d) \in \mathfrak{C}_{c,d} \cap \mathfrak{C}_{c}^{\perp},_d$。那么，对于所有 $u'(c, d) \in \mathcal{R}G$，我们有 $\langle u(c, d)\ u'(c, d)\rangle = \phi(u\bar{u}'(c\bar{c} + dd))$ $= 0$. 由于 $\pi(c\hat{\sigma}(c) + d\hat{\sigma}(d))$ 是一个单位，这意味着对于所有 $u' \in \mathcal{S}G$， $\phi(u\bar{u}') = 0$, 因此 $u = 0$。所以，$\mathfrak{C}_{c,d}$ 是厄米 LCD。 □

为了研究有限链环上某类 2-拟阿贝尔码的厄米特 LCD 渐近性质，我们考虑一族特定的码，记为 code $\mathfrak{C}_{1,\ d}$ 在 $\mathcal{C}_{a,\ b}$ 中。回顾一下，若某个$\mathcal{S}$-模 $\mathfrak{C}_{c,\ d}$ 与某个 $t>0$ 的 $\mathcal{S}^t$ 同构，则称其为自由模。

引理 4.6。 $\mathfrak{C}_{1,\ d}$ 是一个自由 $\mathcal{S}G$ 模。

证明。 定义映射 $\varphi:\mathfrak{C}_{1,\ d}\to\mathcal{S}G$ ，使得 $\varphi(u(1,\ d))=u$ ，对所有 $u\in\mathcal{S}G$ 均成立。显然，该映射是一个$\mathcal{S}G$-模同构。因此，作为 $\mathcal{S}G$-模，$\mathfrak{C}_{1,\ d}\cong\mathcal{S}G$ ，于是 $\mathfrak{C}_{1,\ d}$ 是自由的。 □

定理 4.7。 设 $\mathfrak{C}_{1,\ d}$ 是有限域 $\mathcal{S}$ 上的一个2-拟阿贝尔码。那么，$\mathfrak{C}_{1,\ d}$ 是厄米 *LCD*，当且仅当 $\pi(\mathfrak{C}_{1,\ d})$ 是有限域 $\mathbb{F}$ 上的厄米 *LCD*。

证明。 应用引理 4.6，可得 $\mathfrak{C}_{1,\ d}$ 是一个自由 $\mathcal{R}G$ 模。众所周知，对于 $\mathfrak{C}_{1,\ d}$ 是一个自由$\mathcal{S}G$ 模，$\mathfrak{C}_{1\,d}^{\perp_H}$，也是自由的 $\mathcal{S}G$ 模。因此，$\pi\left(\mathfrak{C}_{1,d}^{\perp_H}\right)=\pi\left(\mathfrak{C}_{1,\ d}\right)^{\perp_H}$。由此并应用定理 4.4，即可得到所需结果。

□

推论 4.8. 若 $d\in\mathcal{R}G$ 满足 $\pi(1+d\hat{\sigma}(d))$ 是 $\mathbb{F}G\setminus\{1\}$中的一个单位，则 $\mathfrak{C}_{1,d}$ 是一个厄米 *LCD*，码率为1 2。 –

证明。 应用定理4.5，可推得 $\mathfrak{C}_{1,d}$ 是一个厄米 LCD。对于另一部分，应用引理4.6，容易看出秩$_{\mathcal{S}}\mathfrak{C}_{1,\ d}$ =秩$_{\mathcal{S}}\mathcal{S}G$。因此，码率等于1 2。 – □

在下述定理中，我们给出一种构造有限链环上的 2-拟阿贝尔码的方法，该方法基于链环 $\mathcal{S}$的剩余域 $\mathbb{F}$ 上的 2-拟阿贝尔码 $\mathcal{S}$ 。

定理 4.9. 设 $\mathcal{C}_{1,\beta}=[2n,k,d]$ 是 $\mathbb{F}$上的一个2-拟阿贝尔码。那么存在 $d\in\mathcal{S}G$ 使得 $\mathfrak{C}_{1,d}=[2n,k,d]$ 是 $\mathcal{S}$上的一个2-拟阿贝尔码，其中 $\pi(d)=\beta$且 $\pi\left(\mathfrak{C}_{1,d}\right)=\mathcal{C}_{1,\beta}$。

证明。为证明这一点，我们定义映射 $\iota:(\mathbb{F}G)^2\to(\mathcal{S}G)^2$ by $(a,b)\mapsto(a,b)$，对于所有 $a,b\in\mathbb{F}G$，这是一个包含映射。在此映射下，$\mathcal{C}_{1,\beta}$ 嵌入于 $(\mathcal{S}G)^2$, ，即 $\iota(\mathcal{C}_{1,\beta})$ 是 $(\mathcal{S}G)^2$ 的一个 $\mathcal{S}G$-模。另一方面，$\pi:\ \mathcal{S}G\to\mathbb{F}G$ 是一个满环同态，因此对于 $\beta\in\mathbb{F}G$，存在 $d\in\mathcal{S}G$ 使得 $\pi(d)=\beta$ 且 $\pi\left(\mathfrak{C}_{1,d}\right)=\mathcal{C}_{1,\beta}$。应用引理 4.6可得，$\iota(\mathcal{C}_{1,\beta})$ 和 $\mathfrak{C}_{1,d}$ 都是自由的 $\mathcal{S}G$-模。因此，$\mathfrak{C}_{1,d}=[2n,k,d]$ 是一个 $\mathcal{S}$ 上的 2-拟阿贝尔码。 □

引理 4.10。 *[26]* 若 I 是 $\mathcal{S}$ 中的一个理想，且 G 是一个有限群，则 $\frac{\mathcal{S}G}{IG}\cong\frac{\mathcal{S}}{I}G$。

引理 4.11. 若 f 是 $\mathbb{F}G$中的一个幂等元，则存在元素 f' 属于 $\mathcal{S}G$ ，使得$\pi(f')=f$。

证明。 由于 $\mathbf{m}$是t he m的极大理想 $\mathcal{S}$ 且它是双边理想，通过应用引理 4.10，我们得到

$$\frac{\mathcal{S}G}{\mathbf{m}G}\cong\frac{\mathcal{S}}{\mathbf{m}}G\cong\mathbb{F}G$$

以及 $\frac{\mathcal{S}G}{\mathbf{m}^iG}\cong\frac{\mathcal{S}}{\mathbf{m}^i}G$，其中 $1\le i\le s$，且 $\mathbf{m}^s=0$，但 $\mathbf{m}^{s-1}\neq0$。

我们将用归纳法证明这一点。通过归纳，我们定义幂等元 f_i 如下

$$f_i \in \frac{\mathcal{S}G}{\mathbf{m}^i G}.$$

若 $i=1$，在此情形下，我们令 $f_1=f$，则此引理成立。

若 $i>1$，令 f_{i-1} 为 $\mathcal{S}G$ $\mathbf{m}^{i-1}G$ 中的一个幂等元。考虑 $\mathcal{S}G$ $\mathbf{m}^i G$ 中的一个元素 $\overline{h}$，其像为 f_{i-1}，且属于 $\mathcal{S}G$ $\overline{\mathbf{m}^{i-1}G}$ $\mathbf{m}^i G$。容易验证，$h-h^2$ 属于 $\overline{\mathbf{m}^{i-1}G}$ $\mathbf{m}^i G$。因此，$(h-h^2)^2=0$。

现在，我们令 $f_i=(3h^2-2h^3)$。此外，

$$\begin{aligned} f_i^2-f_i &= (3h^2-2h^3)(3h^2-2h^3-1) = h^2(3-2h)(3h^2-2h^3-1) \\ &= (2h-3)(1+2h)(h-h^2)^2 = 0. \end{aligned}$$

此引理对所有 i 均成立。由于 $\mathbf{m}^s=0$，因此 $f'=f_s$。 □

根据等式（1），

$$\begin{aligned} \mathcal{S}G = &\ \mathcal{S}Ge_0' \bigoplus \mathcal{S}Ge_1' \bigoplus \cdots \bigoplus \mathcal{S}Ge_t, \quad \text{it follows that} \\ \mathbb{F}G = &\ \mathbb{F}Ge_0 \bigoplus \mathbb{F}Ge_1 \bigoplus \cdots \bigoplus \mathbb{F}Ge_t, \end{aligned}$$

反过来，根据引理 4.11 和 [19, 定理 10。2]结合等式（2），我们得出

$$\begin{aligned} \mathcal{S}G = &\ \mathcal{S}Ge_0 \bigoplus \left(\bigoplus_{i=1}^{r} \mathcal{S}Ge_i \right) \bigoplus \left(\bigoplus_{j=1}^{s} \mathcal{S}G\widehat{e}_{r+j} \right), \quad \text{if and only if} \\ \mathbb{F}G = &\ \mathbb{F}Ge_0 \bigoplus \left(\bigoplus_{i=1}^{r} \mathbb{F}Ge_i \right) \bigoplus \left(\bigoplus_{j=1}^{s} \mathbb{F}G\widehat{e}_{r+j} \right) \end{aligned}$$

接下来，我们称厄米 LCD 码序列 $\mathcal{C}_1$，$\mathcal{C}_2$，.....在有限域 $\mathbb{F}$上渐近良好。此外，应用定理 4.7 和 4.9，存在厄米特 LCD 2- 拟阿贝尔码 $\mathfrak{C}_i$，长度为 $(\mathcal{S}G)^2$，$i=1$，2，.....，使得码序列 $\mathfrak{C}_1$，$\mathfrak{C}_2$，.....满足以下条件：

i) 码 $\mathfrak{C}_i$ 的长度为 $2n_i \to \infty$;

ii) 码率 $R(\mathfrak{C}_i) = R(\mathcal{C}_i) = \frac{1}{2}$; -

iii) 对所有 $i=1$，2，.....，相对最小距离 $\triangle(\mathfrak{C}_i) = \triangle(\mathcal{C}_i) > \delta$

因此，根据上述讨论，我们在以下定理中给出有限链环上渐近良好的厄米特 LCD 2-拟阿贝尔码类。

定理 4.12。设 $n_1, n_2, \ldots$ 为与 q 互素的正奇整数，且 G_i 是有限阶为 n_i 的阿贝尔群，其中 $i=1$，2, ... 则存在厄米 *LCD* 2-拟阿贝尔码 $\mathfrak{C}_i$，其参数为 $(\mathcal{S}G)^2, i=1,2,\ldots$，使得码序列 $\mathfrak{C}_1, \mathfrak{C}_2, \ldots$ 渐近良好。

证明。应用定理4.7 和 4.9，我们得到 $\mathfrak{C}_i$ 厄米 LCD2-拟阿贝尔码 over 有限域

链环。由此并应用定理 3.17，结论立即成立。 □

致谢

作者谨向副编辑和各位审稿人致以诚挚谢意，感谢他们细致的审阅和富有见地的建议，这些意见极大地提升了本文的质量。我们也衷心感谢印度理工学院古瓦哈提分校的支持。

参考文献

[1] J. L. Alperin，B. Bell。《群表示论》。*Springer-Verlag*，瑞士沙姆，1995。[2] L. M. J. Bazzi，S .K. Mitter。基于群作用的一些随机化码构造。*IEEE* 信息论汇刊，**52**(7):3210–3219，2007。[3] S. Bhowmick，A. F. Tabue，E. Martínez-Moro，R. Bandi，S. Bagchi。有限交换Frobenius环上是否存在非自由 LCD码？载于《设计、码与密码学》，**88**，825–840，2020。[4] S. Bhowmick，S. Bagchi，R. Bandi。关于 $\mathbb{Z}_4$上的 LCD码。载于《印度纯粹与应用数学杂志》，2024，https://doi.org/10.1007/s13226-024-00563-x。[5] S. Bhowmick，A. F. Tabue，J. Pal。关于有限交换环上码的 ℓ-DLIP。载于《离散数学》，**347**(4)，113853，2024。[6] J. Bringer，C. Carlet，H. Chabanne，S. Guilley和H. Maghrebi。正交直和掩码——一种适用于智能卡的码内计算范式，内置侧信道攻击和故障攻击防护。载于《信息安全理论与实践：物联网安全保障，*WISTP 2014*，希腊克里特岛，会议论文集》，《计算机科学讲义》第8501卷，第40–56页。Springer，2014。[7] 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》，**10**(1):131–150，2016。[8] C. Carlet，S. Mesnager，C. Tang，Y. Qi和R. Pellikaan。 $\mathbb{F}_q$ 上的线性码等价于 $q > 3$的 LCD码。*IEEE* 信息论汇刊，**64**(4):3010–3017，2018。[9] C. Carlet，S. Mesnager，C. Tang和Y. Qi。欧几里得 LCD MDS码与厄米 LCD MDS码。《设计、码与密码学》，**86**(11):2605–2618，2018。[10] C. Carlet，S. Mesnager，C. Tang和Y. Qi。关于 σ-LCD码。*IEEE* 信息论汇刊，**65**(3):1694–1704，2019。[11] C. L. Chen，W. W. Peterson，E. J. Weldon Jr. 关于准循环码的一些结果。《信息与控制》，**15**(5):407–423，1969。[12] V. V. Chepyzhov。线性准循环码和近线性循环码最小距离的新下界。《问题信息传输》，**28**(1):39–51，1992。

[13] Y. Fan，L. Lin。随机拟阿贝尔码的阈值。《IEEE 信息论汇刊》，61(1): 82–90，2015。[14] Y. Fan，L. Lin。有限域上的二面体群码。《IEEE 信息论汇刊》，67(8): 5016–5025，2021。[15] Y. Fan，L. Lin。自对偶2-拟阿贝尔码。《IEEE 信息论汇刊》，68(10): 6417–6425，2022。[16]Y. Fan，L. Lin。指标为 1 1 3 的准循环码。《IEEE 信息论汇刊》，62(11): 6342–6347，2016。[17] A. R. Hammons，P. V. Kumar，A. R. Calderbank，N. J. A. Sloane和P. Solé。Kerdock码、Preparata码、Goethals码及相关码的 $\mathbb{Z}_4$-线性。《IEEE 信息论汇刊》，40:301–319，1994。[18] T. Honold，I. Landjev。《有限链环上的线性码》。《组合电子期刊》，7:1–22，2000。[19] B. Huppert，N. Blackburn。《有限群 II》。Springer，柏林，1982。[20] X. Liu和H. Liu。有限链环上的 LCD码。《有限域应用》，34，1–19，2015。[21] X. Liu和H. Liu。有限链环上的 σ-LCD码。《设计、码与密码学》，88，727–746，2020。[22] C. Martínez-Pérez，W. Willems。循环码类是否渐近良好? 《IEEE 信息论汇刊》，52:696–700，2006。[23] C. Martínez-Pérez，W. Willems。自对偶双偶2-拟循环传递码渐近良好。《IEEE 信息论汇刊》，53:4302–4308，2007。[24] J. L. Massey。具有互补对偶的线性码。《离散数学》，106-107:337–342，1992。[25] B. R. McDonald。《含幺有限环》。Marcel Dekker Inc.，纽约，1974。[26] C. P. Miles和S. K. Sehgal。《群环导论》。Kluwer Academic Publishers，2001。[27] G. H. Norton，A. Sălăgean。有限链环上线性码与循环码的结构。《应用代数、工程、通信与计算》，10: 489–506，2000。[28] G. H. Norton，A. Sălăgean。有限链环上线性码与循环码的结构。《IEEE 信息论汇刊》，46:(4)1060–1067，2000。[29] N. Sendrier。具有互补对偶的线性码达到Gilbert-Varshamov界。《离散数学》，285:345-347，2004。[30] Z. Wan。《有限域与伽罗瓦环》。World Scientific Publishing Co Pte Ltd，2011。[31] G. Zhang，L. Lin，C. Qin和R. Li。厄米特自对偶2-拟阿贝尔码。《有限域应用》，94: 102357，2024。

[32] G. Zhang、L. Lin 和 X. Liu. 有限域上渐近良好的 LCD 2-拟阿贝尔码。《离散数学》，**348(1)**：114224，2025。