



基于 Hermite 内积的量子拟循环码构造

张镇辉, 李卓*, 邢莉娟

西安电子科技大学通信工程学院, 西安 710071

E-mail: 20011110016@stu.xidian.edu.cn, lizhuo@xidian.edu.cn, ljxing@mail.xidian.edu.cn

收稿日期: 2025-03-16; 接受日期: 2025-08-06; 网络出版日期: 2025-09-30; * 通信作者

国家自然科学基金 (批准号: 61372072) 和 111 工程基金 (批准号: B08038) 资助项目

摘要 为构造高纠错性能的量子稳定子码, 本文提出一类指标为 2 的拟循环码, 给出这类拟循环码及其 Hermite 对偶码的生成元形式以及码参数. 通过推导这类拟循环码 Hermite 自正交的条件, 基于 Hermite 构造法构造出一类新的量子拟循环码. 在这类量子拟循环码中, 找到了 12 个打破当前码表纪录的二元量子稳定子码, 它们的最小距离均高于表中相同码长和维数的量子稳定子码, 这为高纠错性能量子稳定子码的构造提供了有效支持.

关键词 拟循环码 量子稳定子码 Hermite 对偶码 Hermite 构造

MSC (2020) 主题分类 94B15, 81P70

1 引言

量子纠错码通过保护量子比特信息免受量子噪声的干扰来确保量子信息传输的可靠性和量子计算的准确性, 其中量子稳定子码是量子纠错码技术研究中较为重要的码类. 因此, 量子稳定子码在减少量子噪声对量子信息处理过程的影响中起到了重要作用. 研究人员尝试通过向原始量子信息中添加冗余来使得量子信息免于量子噪声的干扰, 进而保护原始的量子信息. 然而, 由于量子信息与经典信息的特性存在较多差异, 例如, 量子态的不可克隆性、量子错误的连续性以及量子测量会破坏原有量子态等, 导致在实际中实现量子稳定子码面临许多挑战^[16]. 幸运的是, Shor^[17] 于 1995 年利用量子纠缠特性构造出了第一个二元量子稳定子码 $[[9, 1, 3]]_2$, 为量子稳定子码理论的发展作出了重大贡献.

量子稳定子码的构造要求能够构造出具有高纠错性能的量子稳定子码. 类似于经典码, 在相同的码长和维数下, 量子稳定子码的最小距离越大, 其纠错性能就越高. 因此, 高纠错性能的量子稳定子码的构造成为量子稳定子码研究中的一个重要课题. 常见的量子稳定子码的构造通过经典码来实现, 许多高纠错性能的量子稳定子码通过高纠错性能的经典码构造得到 (参见文献^[3, 13, 18, 19]). 常见的由经典码构造量子稳定子码的方法有 CSS (Calderbank-Shor-Steane) 构造法、Hermite 构造法和 Symplectic 构造法, 这些方法的本质上都是利用经典码之间的自正交关系来构造量子稳定子码.

英文引用格式: Zhang Z H, Li Z, Xing L J. The construction of quantum quasi-cyclic codes based on the Hermitian inner product (in Chinese). Sci Sin Math, 2025, 55: 1–16, doi: 10.1360/SSM-2025-0066

拟循环码作为循环码和常循环码的扩展, 与这些经典码相比, 具有更丰富的结构和更优越的性能. 文献 [12,14] 指出, 拟循环码可以达到修正的量子 Gilbert-Varshamov 界, 这表明其渐近性能优越. 并且, 通过拟循环码已经获得了许多打破现有码表纪录的经典码 [4,5], 这也展示了其在构造高纠错性能量子稳定子码方面的潜力. 2007 年, Hagiwara 和 Imai [11] 首次使用拟循环码构造了量子 LDPC (low-density parity-check) 码. 2018 年, Galindo 等 [7] 使用了一类指标为 2 的 2 生成的拟循环码, 分别研究了它在 Euclid 内积、Hermite 内积和 Symplectic 内积下的对偶码生成元形式, 通过分别确定这类拟循环码在 3 种内积下对偶包含的条件, 构造得到了 3 类量子稳定子码, 并称这类由拟循环码构造得到的量子稳定子码为量子拟循环码. 不过可惜的是, 当时的研究没能构造出打破码表纪录的量子稳定子码. 因此, 在随后的 2019 年, Ezerman 等 [6] 提出了一种构造性能优良的量子拟循环码的新方法—量子 X 构造方法, 利用拟循环码与其成分码近似自正交的关系, 成功构造出了许多打破纪录的二元量子稳定子码. 至此, 如何能够通过拟循环码构造出性能优良的量子稳定子码, 甚至是构造出打破纪录的量子稳定子码成为当前量子稳定子码构造的热点.

由于拟循环码类丰富, 近年来, 在指标为 2 的拟循环码类中, 许多研究者通过提出一类或者几类不同生成元形式的拟循环码, 构造得到了几类新的量子拟循环码, 并通过这些量子拟循环码, 得到了许多性能优良的量子稳定子码. 在 2020 年, Lv 等 [15] 通过研究一类指标为 2 的一生成的拟循环码的代数结构, 确定其在 Hermite 内积下自正交的条件, 得到了一类新的量子拟循环码. 并且, 作者通过这类量子拟循环码成功构造了许多打破码表纪录的二元量子稳定子码. 在 2022 年, Guan 等 [9,10] 提出了一类指标为 2 的二生成的拟循环码, 并且分别研究了其 Hermite 对偶码以及 Symplectic 对偶码的生成元形式, 通过给出它们在不同内积下的对偶包含条件, 最终得到了两类新的量子拟循环码, 并通过这两类量子拟循环码同样得到了许多打破码表纪录的量子稳定子码. 2023 年, Abdukhalikov 等 [1] 在 Lv 等的工作基础上, 研究了其提出的指标为 2 一生成的拟循环码的 Symplectic 对偶码生成元形式, 并且给出了其 Symplectic 自正交的条件, 得到了一类新的量子拟循环码, 并通过这类量子拟循环码构造得到了 3 个打破码表纪录的量子稳定子码.

这些研究表明, 量子拟循环码在构造高纠错性能的量子稳定子码方面具有巨大潜力. 如何通过找到合适的拟循环码来构造出更多高纠错性能的量子稳定子码仍然是当前研究的热点. 因此, 本文提出一类指标为 2 的拟循环码, 给出了其 Hermite 对偶码的参数以及生成元形式, 通过得到其 Hermite 自正交的条件, 构造得到一类新的量子稳定子码, 并在二元域上成功找到了 12 个打破码表纪录的高纠错性能的量子稳定子码.

本文余下内容结构如下. 第 2 节介绍量子稳定子码和拟循环码的一些基本概念和定义. 第 3 节首先定义一类指标为 2 的拟循环码, 给出这类拟循环码的生成元形式及码参数; 其次, 给出这类拟循环码 Hermite 对偶码的生成元形式以及码参数; 最后, 基于这类拟循环码 Hermite 自正交条件, 得到一类新的量子拟循环码. 第 4 节展示这类量子拟循环码的若干示例. 第 5 节给出这类量子拟循环码具体的构造结果以及必要的构造信息, 其中包括了 12 个打破码表纪录的二元量子稳定子码. 最后, 第 6 节给出全文总结.

2 量子稳定子码基础理论

量子稳定子码是一类重要的量子纠错码, 本节主要回顾量子稳定子码基础理论、量子稳定子码与经典码的联系以及拟循环码的基本概念. 首先介绍量子稳定子码的定义. 在本文中, 令 $\mathbb{F}_q$ 为 q 元有限

域, 其中 $q = p^r$, p 为素数, r 为正整数. $\mathbb{C}^q$ 是一个维数为 q 的复向量空间, 其中 $q = p^r$. 令

$$V_n = (\mathbb{C}^q)^{\otimes n} = \underbrace{\mathbb{C}^q \otimes \cdots \otimes \mathbb{C}^q}_n.$$

一个 $((n, K, d))_q$ 量子稳定子码是 V_n 中维数为 K 的子空间. 最小距离 d 允许其检测重量小于 d 的所有错误群中的错误, 但不能检测所有重量为 d 的错误 [13]. 若 $K = q^k$, 则 $((n, q^k, d))_q$ 量子稳定子码可写成 $[[n, k, d]]_q$ 量子稳定子码. 量子稳定子码是一个由 V_n 上合适的错误基生成的错误群的一个可交换子群的特征值为 1 的联合特征空间. 若量子稳定子码的稳定子群不包含重量小于 t 的非标量矩阵, 则称这个量子稳定子码是纯到 t 的. 若一个量子稳定子码纯到其最小距离, 则称其为纯的 [13].

本文研究的是在 Hermite 内积下拟循环码构造量子稳定子码的研究, 因此首先通过给出常见的经典码以及 Euclid 内积定义来引入 Hermite 内积以及 Hermite 对偶码的定义, 然后给出量子稳定子码的 Hermite 构造法以及相应的量子稳定子码扩展定理. 一个 $[n, k]_q$ 经典线性码 $\mathcal{C}$ 是 $\mathbb{F}_q^n$ 中一个维数为 k 的线性子空间. 向量 $\mathbf{v} \in \mathbb{F}_q^n$ 的 Hamming 重量, 记为 $wt(\mathbf{v})$, 是 $\mathbf{v}$ 中非零元素的个数. 令向量 $\mathbf{v} = (v_0, v_1, \dots, v_{n-1}) \in \mathbb{F}_q^n$ 并且 $\mathbf{u} = (u_0, u_1, \dots, u_{n-1}) \in \mathbb{F}_q^n$, 向量 $\mathbf{v}$ 与 $\mathbf{u}$ 之间的 Hamming 距离 $d_H(\mathbf{v}, \mathbf{u})$ 为

$$d_H(\mathbf{v}, \mathbf{u}) = \#\{i \in \{0, 1, \dots, n-1\} \mid v_i \neq u_i\}.$$

$\mathcal{C}$ 的最小距离等于该码中任意两个不同元素 (即不同码字) 之间的最小 Hamming 距离. 向量 $\mathbf{a} = (a_0, \dots, a_{n-1})$ 和 $\mathbf{b} = (b_0, \dots, b_{n-1})$ 在 $\mathbb{F}_{q^2}^n$ 上的 Euclid 内积和 Hermite 内积的定义分别为

$$\langle \mathbf{a}, \mathbf{b} \rangle = \sum_{i=0}^{n-1} a_i b_i$$

和

$$\langle \mathbf{a}, \mathbf{b} \rangle_h = \sum_{i=0}^{n-1} a_i^q b_i.$$

对于线性码 $\mathcal{C} \subset \mathbb{F}_{q^2}^n$, 其 Hermite 对偶码定义为

$$\mathcal{C}^{\perp_h} = \{\mathbf{a} \in \mathbb{F}_{q^2}^n \mid \langle \mathbf{a}, \mathbf{b} \rangle_h = 0, \forall \mathbf{b} \in \mathcal{C}\}.$$

量子稳定子码可通过 Hermite 自正交的经典线性码构造得到.

定理 2.1 (Hermite 构造法 [13]) 若存在一个 $[n, k, d]_{q^2}$ 经典线性码 $\mathcal{C}$ 满足 $\mathcal{C} \subseteq \mathcal{C}^{\perp_h}$, 则存在一个参数为 $[[n, n-2k, d_Q]]_q$ 的量子稳定子码, 其中 $d_Q = \min \{wt(\mathbf{x}) \mid \mathbf{x} \in \mathcal{C}^{\perp_h} \setminus \mathcal{C}\}$.

此外, 量子稳定子码也可通过以下定理从现有的量子稳定子码中扩展得到.

定理 2.2 (扩展规则 [3]) 若存在一个纯的量子稳定子码 $[[n, k, d]]_q$, 则量子稳定子码 $[[n, k-1, d]]_q$ (当 $k \geq 1$ 时) 和 $[[n+1, k, d]]_q$ (当 $k > 0$ 时) 也存在.

作为循环码的扩展, 在给出拟循环码的定义之前, 有必要回顾循环码的定义和概念. 循环码的定义如下. 对于向量 $\mathbf{c} = (c_0, \dots, c_{m-1}) \in \mathbb{F}_{q^2}^m$, 其循环移位操作 T 定义为 $T(\mathbf{c}) = (c_{m-1}, c_0, \dots, c_{m-2})$. 若 $\mathbb{F}_{q^2}^m$ 上的线性码 $\mathcal{C}$ 满足 $\mathcal{C} = T(\mathcal{C})$, 则称其为循环码. 循环码的码字可表示为多项式形式. 令 $\mathbb{F}_{q^2}[x]$ 表示 $\mathbb{F}_{q^2}$ 上的多项式环. 设 $\langle x^m - 1 \rangle$ 为由多项式 $(x^m - 1)$ 生成的 $\mathbb{F}_{q^2}[x]$ 上的理想. $\mathbb{F}_{q^2}$ 上码长为 m 的循环码可视为商环 $\mathbb{R}_m = \mathbb{F}_{q^2}[x]/\langle x^m - 1 \rangle$ 中的一个理想. 对于 $\mathbb{F}_{q^2}[x]$ 中的多项式 $g(x)$, $[g(x)]$ 表示其在 $\mathbb{R}_m$ 中的剩余类. $\mathbb{F}_{q^2}^m$ 中的向量 $\mathbf{a} = (a_0, \dots, a_{m-1})$ 与以下形式的剩余类对应:

$$[a(x)] = [a_0 + a_1x + a_2x^2 + \cdots + a_{m-1}x^{m-1}]. \quad (2.1)$$

并且向量 $T(\mathbf{a})$ 对应剩余类 $[xa(x)]$. 由于 $\mathbb{F}_{q^2}[x]$ 是主理想整环, 因此任意循环码都可由 $\mathbb{R}_m$ 中的一个元素 $[g(x)]$ 生成. 令 $g(x), s(x) \in \mathbb{F}_{q^2}[x]$, $g(x) \mid s(x)$ 表示 $g(x)$ 整除 $s(x)$. 若 $g(x)$ 和 $s(x)$ 的次数均小于 m 且 $g(x) \mid s(x)$, 则由 $[g(x)]$ 生成的循环码包含由 $[s(x)]$ 生成的循环码.

由于拟循环码是循环码的扩展, 因此其具有与循环码类似的定义. 令 l 和 m 为正整数. $\mathbb{F}_{q^2}^{lm}$ 中的向量 $\mathbf{c} = (c_{00}, c_{01}, \dots, c_{0,l-1}, c_{10}, \dots, c_{1,l-1}, \dots, c_{m-1,0}, \dots, c_{m-1,l-1})$ 的循环移位操作 T^l 定义为

$$T^l(\mathbf{c}) = (c_{m-1,0}, c_{m-1,1}, \dots, c_{m-1,l-1}, c_{00}, c_{01}, \dots, c_{0,l-1}, \dots, c_{m-2,0}, \dots, c_{m-2,l-1}).$$

若 $\mathbb{F}_{q^2}^{lm}$ 上的线性码 $\mathcal{C}$ 满足 $\mathcal{C} = T^l(\mathcal{C})$, 则称其为指标为 l 的拟循环码. 拟循环码的码字也可表示为多项式形式. 定义映射 $\phi: \mathbb{F}_{q^2}^{lm} \rightarrow \mathbb{R}_m^l$ 为

$$\phi(\mathbf{c}) = ([c_0(x)], [c_1(x)], \dots, [c_{l-1}(x)]) \in \mathbb{R}_m^l,$$

其中

$$c_j(x) = \sum_{i=0}^{m-1} c_{ij} x^i \in \mathbb{F}_{q^2}[x], \quad 0 \leq j \leq l-1.$$

指标为 l 、码长为 lm 的拟循环码可看作为 $\mathbb{R}_m^l$ 上的 $\mathbb{R}_m$ -子模. 若指标为 l 、码长为 lm 的拟循环码 $\mathcal{C}$ 由 $\mathbb{R}_m^l$ 中的 t 个元素 $\vec{a}_1(x), \vec{a}_2(x), \dots, \vec{a}_t(x)$ 生成, 其中

$$\begin{aligned} \vec{a}_1(x) &= ([a_{1,0}(x)], [a_{1,1}(x)], \dots, [a_{1,l-1}(x)]), \\ \vec{a}_2(x) &= ([a_{2,0}(x)], [a_{2,1}(x)], \dots, [a_{2,l-1}(x)]), \\ &\vdots \\ \vec{a}_t(x) &= ([a_{t,0}(x)], [a_{t,1}(x)], \dots, [a_{t,l-1}(x)]), \end{aligned}$$

则称 $\mathcal{C}$ 为 t -生成的拟循环码. 此外, $\mathcal{C}$ 的码字可表示为这些生成元的线性组合:

$$\sum_{i=1}^t [k_i(x)] \vec{a}_i(x) = \sum_{i=1}^t ([k_i(x)a_{i,0}(x)], [k_i(x)a_{i,1}(x)], \dots, [k_i(x)a_{i,l-1}(x)]),$$

其中 $k_i(x) \in \mathbb{F}_{q^2}[x]$.

在本节末引入若干必要的多项式定义, 用于定义所需要的拟循环码并支撑相关的理论证明. 设 $f(x) = f_0 + f_1x + \dots + f_{n-1}x^{n-1}$ 为 $\mathbb{F}_{q^2}[x]$ 中的多项式, 且 $f_{n-1} \neq 0$. 定义如下多项式:

$$f^q(x) = f_0^q + f_1^q x + \dots + f_{n-1}^q x^{n-1}.$$

令 $\partial f = \deg(f(x))$ 表示为多项式 $f(x)$ 的次数. 若 $\partial f < m$, 则定义以下多项式:

$$\bar{f}(x) = f(1/x) \bmod (x^m - 1).$$

当 $f(x) \mid (x^m - 1)$ 时, 定义多项式 $f'(x)$ 和 $f^\perp(x)$ 分别为

$$f'(x) = \frac{x^m - 1}{f(x)}, \quad f^\perp(x) = f' \left(\frac{1}{x} \right) x^{\partial f'}.$$

3 量子拟循环码的构造

本节首先给出一类指标为 2 拟循环码的定义, 同时给出其生成元形式和码参数; 其次, 确定其 Hermite 对偶码的生成元形式和码参数; 最后, 基于这类拟循环码 Hermite 自正交的条件, 得到一类新的量子拟循环码. 所提到的指标为 2 的拟循环码的定义如下, 这类拟循环码的生成元形式由有限域 $\mathbb{F}_{q^2}[x]$ 上的多项式 $g(x)$, $s(x)$ 和 $f(x)$ 确定.

定义 3.1 令 $g(x)$, $s(x)$ 和 $f(x)$ 为 $\mathbb{F}_{q^2}[x]$ 中的多项式, 并且 $\mathcal{C}_{q^2}(f, g, s)$ 为指标为 2、码长为 $2m$ 的拟循环码. $\mathcal{C}_{q^2}(f, g, s)$ 在 $\mathbb{F}_{q^2}$ 上的生成元为 $([g(x)], [d(x)f(x)])$ 和 $(0, [s(x)])$, 其中多项式满足:

- (1) $g(x) \mid (x^m - 1)$, $s(x) \mid (x^m - 1)$, $\partial f < m$;
- (2) $d(x) = \gcd(g(x), s(x))$.

根据拟循环码 $\mathcal{C}_{q^2}(f, g, s)$ 的生成元形式, 可进一步得出这类拟循环码的码参数, 码参数将用于量子拟循环码参数的计算.

引理 3.1 拟循环码 $\mathcal{C}_{q^2}(f, g, s)$ 的参数为 $[2m, 2m - \partial g - \partial s]$.

证明 已知 $\mathcal{C}_{q^2}(f, g, s)$ 的码长为 $2m$. 令多项式 $d(x)f(x)$ 在 $\mathbb{R}_m$ 中的剩余类决定的向量为

$$[d(x)f(x)] = [p_0 + p_1x + p_2x^2 + \cdots + p_{m-1}x^{m-1}] = (p_0, p_1, p_2, \dots, p_{m-1}).$$

其对应关系参照等式 (2.1). 设 $\mathcal{C}_1$ 为生成矩阵为 G 的线性码, G 由以下 $2m - \partial g - \partial s$ 个行向量构成:

$$\begin{aligned} ([g(x)], [d(x)f(x)]) &= (g_0, g_1, g_2, \dots, g_{\partial g-1}, \dots, 0, p_0, p_1, p_2, \dots, p_{m-1}), \\ ([xg(x)], [xd(x)f(x)]) &= (0, g_0, g_1, \dots, g_{\partial g-1}, \dots, 0, p_{m-1}, p_0, p_1, \dots, p_{m-2}), \\ &\vdots \\ ([x^{m-\partial g-1}g(x)], [x^{m-\partial g-1}d(x)f(x)]) \\ &= (0, 0, \dots, g_0, g_1, \dots, g_{\partial g-1}, p_{m-\partial g+1}, p_{m-\partial g+2}, p_{m-\partial g+3}, \dots, p_{m-\partial g}), \\ (0, [s(x)]) &= (0, 0, \dots, 0, s_0, s_1, s_2, \dots, s_{\partial s-1}, \dots, 0), \\ (0, [xs(x)]) &= (0, 0, \dots, 0, 0, s_0, s_1, \dots, s_{\partial s-1}, \dots, 0), \\ &\vdots \\ (0, [x^{m-\partial s-1}s(x)]) &= (0, 0, \dots, 0, 0, 0, \dots, s_0, s_1, \dots, s_{\partial s-1}). \end{aligned}$$

易得, G 的行向量是线性无关的, 因此 $\mathcal{C}_1$ 的维数为 $2m - \partial g - \partial s$.

若证得 (1) $\mathcal{C}_{q^2}(f, g, s)$ 中的任意码字可由生成矩阵 G 的行向量生成; (2) 由 G 生成的任意码字包含于 $\mathcal{C}_{q^2}(f, g, s)$ 中, 则可得 $\mathcal{C}_{q^2}(f, g, s)$ 的生成矩阵为 G , 并且其维数为 $(2m - \partial g - \partial s)$, 于是引理得证.

(1) 拟循环码 $\mathcal{C}_{q^2}(f, g, s)$ 的码字可表示为

$$([a(x)g(x)], [a(x)d(x)f(x) + b(x)s(x)]),$$

其中 $a(x)$ 和 $b(x)$ 是 $\mathbb{F}_{q^2}[x]$ 中的任意多项式. 根据除法算法可得

$$\begin{aligned} a(x) &= q_1(x)g'(x) + r_1(x), \\ b(x) &= q_2(x)s'(x) + r_2(x), \end{aligned}$$

其中 $\partial r_1 < m - \partial g$, $\partial r_2 < m - \partial s$. 进而, 其码字可表示为

$$\begin{aligned} & ([q_1(x)g'(x)g(x) + r_1(x)g(x)], [q_1(x)g'(x)d(x)f(x) + r_1(x)d(x)f(x) + q_2(x)s'(x)s(x) + r_2(x)s(x)]) \\ & = ([r_1(x)g(x)], [q_1(x)g'(x)d(x)f(x) + r_1(x)d(x)f(x) + r_2(x)s(x)]). \end{aligned} \quad (3.1)$$

已知 $d(x) = \gcd(g(x), s(x))$. 令 $t(x) = x^m - 1/\text{lcm}(g(x), s(x))$, $g(x) = d(x)m(x)$ 并且 $s(x) = d(x)n(x)$, 则可得 $g'(x) = t(x)n(x)$. 因此, $\mathcal{C}_{q^2}(f, g, s)$ 的码字可写成

$$\begin{aligned} & ([r_1(x)g(x)], [q_1(x)g'(x)d(x)f(x) + r_1(x)d(x)f(x) + r_2(x)s(x)]) \\ & = ([r_1(x)g(x)], [q_1(x)t(x)f(x)d(x)n(x) + r_1(x)d(x)f(x) + r_2(x)s(x)]) \\ & = ([r_1(x)g(x)], [r_1(x)d(x)f(x) + c(x)s(x)]), \end{aligned} \quad (3.2)$$

其中 $c(x) = q_1(x)t(x)f(x) + r_2(x)$. 同样地, 根据除法算法, 可得

$$c(x) = q_3(x)s'(x) + r_3(x),$$

其中 $\partial r_3 < m - \partial s$. $\mathcal{C}_{q^2}(f, g, s)$ 的码字可被写成

$$\begin{aligned} & ([r_1(x)g(x)], [r_1(x)d(x)f(x) + q_3(x)s'(x)s(x) + r_3(x)s(x)]) \\ & = ([r_1(x)g(x)], [r_1(x)d(x)f(x) + r_3(x)s(x)]), \end{aligned} \quad (3.3)$$

其中 $r_1(x)$ 和 $r_3(x)$ 是 $\mathbb{F}_{q^2}[x]$ 上的多项式, 它们的次数分别小于 $m - \partial g$ 和 $m - \partial s$. 根据生成矩阵 G 的行向量形式, 可得出 $\mathcal{C}_1$ 的码字表示形式为

$$([a_1(x)g(x)], [a_1(x)d(x)f(x) + b_1(x)s(x)]),$$

其中 $a_1(x)$ 和 $b_1(x)$ 是 $\mathbb{F}_{q^2}[x]$ 上的多项式, 它们的维数分别小于 $m - \partial g$ 和 $m - \partial s$. 因此, 可得出 $\mathcal{C}_{q^2}(f, g, s)$ 中的任意码字都可由生成矩阵 G 的行向量生成.

(2) 已知 $\mathcal{C}_{q^2}(f, g, s)$ 中的码字可表示为

$$([a(x)g(x)], [a(x)d(x)f(x) + b(x)s(x)]),$$

其中 $a(x)$ 和 $b(x)$ 是 $\mathbb{F}_{q^2}[x]$ 上的任意多项式. 易得生成矩阵为 G 的线性码 $\mathcal{C}_1$ 的任意码字都包含于 $\mathcal{C}_{q^2}(f, g, s)$.

因此可得出 G 也是 $\mathcal{C}_{q^2}(f, g, s)$ 的生成矩阵, 于是 $\mathcal{C}_{q^2}(f, g, s)$ 的维数是 $2m - \partial g - \partial s$, 引理得证. $\square$

为进一步得出拟循环码 $\mathcal{C}_{q^2}(f, g, s)$ Hermite 对偶码 $\mathcal{C}_{q^2}^{\perp_h}(f, g, s)$ 的生成元形式和码参数, 给出以下有关向量间 Hermite 内积的结论是必要的.

引理 3.2 ^[15] 令 $n(x)$, $f(x)$ 和 $h(x)$ 为 $\mathbb{F}_{q^2}[x]$ 中次数小于 m 的首一多项式, 考虑这些多项式对应于 $\mathbb{F}_{q^2}^m$ 上的由多项式决定的向量, 对应关系如等式 (2.1) 所描述, 它们的 Hermite 内积满足

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

根据引理 3.2 的证明过程容易得到, 即使不满足多项式首一条件, 引理结论仍然成立.

进一步给出定义 3.1 中拟循环码 $\mathcal{C}_{q^2}(f, g, s)$ Hermite 对偶码 $\mathcal{C}_{q^2}^{\perp_h}(f, g, s)$ 的生成元形式以及码参数.

命题 3.1 拟循环码 $\mathcal{C}_{q^2}(f, g, s)$ 在 $\mathbb{F}_{q^2}$ 上的 Hermite 对偶码 $\mathcal{C}_{q^2}^{\perp h}(f, g, s)$ 是由 $([g^{\perp q}(x)], 0)$ 和 $([-\bar{f}^q(x)\bar{t}^q(x)x^{\partial s'}], [s^{\perp q}(x)])$ 生成的拟循环码, 并且其参数为 $[2m, \partial g + \partial s]$, 其中 $t(x) = (x^m - 1)/\text{lcm}(g(x), s(x))$.

证明 设 $\mathcal{C}_2$ 为 $\mathbb{F}_{q^2}$ 上由 $([g^{\perp q}(x)], 0)$ 和 $([-\bar{f}^q(x)\bar{t}^q(x)x^{\partial s'}], [s^{\perp q}(x)])$ 生成的拟循环码. 若证得 (1) $\mathcal{C}_2$ 的维数为 $\partial g + \partial s$; (2) $\mathcal{C}_2$ 的码字与 $\mathcal{C}_{q^2}(f, g, s)$ 的码字之间的 Hermite 内积为零, 则可得 $\mathcal{C}_2$ 是 $\mathcal{C}_{q^2}(f, g, s)$ Hermite 对偶码.

(1) 类似于引理 3.1 的证明. 回顾 $[g^{\perp q}(x)]$ (或 $[s^{\perp q}(x)]$) 是由 $[g(x)]$ (或 $[s(x)]$) 生成的循环码的 Hermite 对偶码. 令多项式 $(-\bar{f}^q(x)\bar{t}^q(x)x^{\partial s'})$ 在 $\mathbb{R}_m$ 中的剩余类决定的向量为

$$[-\bar{f}^q(x)\bar{t}^q(x)x^{\partial s'}] = [v_0 + v_1x + v_2x^2 + \cdots + v_{m-1}x^{m-1}] = (v_0, v_1, v_2, \dots, v_{m-1}),$$

其对应关系参照等式 (2.1). 设 $\mathcal{C}_3$ 为生成矩阵为 G' 的线性码, 其中

$$G' = \begin{pmatrix} [g^{\perp q}(x)] & 0 \\ [xg^{\perp q}(x)] & 0 \\ \vdots & \vdots \\ [x^{\partial g-1}g^{\perp q}(x)] & 0 \\ [-\bar{f}^q(x)\bar{t}^q(x)x^{\partial s'}] & [s^{\perp q}(x)] \\ [-x\bar{f}^q(x)\bar{t}^q(x)x^{\partial s'}] & [xs^{\perp q}(x)] \\ \vdots & \vdots \\ [-x^{\partial s-1}\bar{f}^q(x)\bar{t}^q(x)x^{\partial s'}] & [x^{\partial s-1}s^{\perp q}(x)] \end{pmatrix}.$$

由于 G' 的所有行向量在 $\mathbb{F}_{q^2}^{2m}$ 上线性无关, 因此 $\mathcal{C}_3$ 的维数为 $\partial g + \partial s$.

若证得 $\mathcal{C}_2$ 中的任意码字都可由生成矩阵 G' 的行向量生成, 且生成矩阵为 G' 的线性码 $\mathcal{C}_3$ 的任意码字也包含于 $\mathcal{C}_2$ 中, 则可得 $\mathcal{C}_2$ 的维数为 $\partial g + \partial s$. 由于以下证明步骤类似于引理 3.1. 因此省略部分的细节推导, 仅展示关键的步骤和结论. $\mathcal{C}_2$ 中的码字可表示为

$$([a(x)g^{\perp q}(x) - b(x)\bar{f}^q(x)\bar{t}^q(x)x^{\partial s'}], [b(x)s^{\perp q}(x)]),$$

其中 $a(x)$ 和 $b(x)$ 是 $\mathbb{F}_{q^2}[x]$ 中的任意多项式. 令 $g''(x) = (x^m - 1)/g^{\perp q}(x)$ 并且 $s''(x) = (x^m - 1)/s^{\perp q}(x)$, 它们的次数分别为 (∂g) 和 (∂s) . 类似于等式 (3.1) 的推导, $\mathcal{C}_2$ 的码字可被写成

$$([r_1(x)g^{\perp q}(x) - q_2(x)s''(x)\bar{f}^q(x)\bar{t}^q(x)x^{\partial s'} - r_2(x)\bar{f}^q(x)\bar{t}^q(x)x^{\partial s'}], [r_2(x)s^{\perp q}(x)]),$$

其中多项式 $r_1(x)$, $q_2(x)$ 和 $r_2(x)$ 满足以下等式:

$$\begin{aligned} a(x) &= q_1(x)g''(x) + r_1(x), \\ b(x) &= q_2(x)s''(x) + r_2(x), \end{aligned}$$

这里 $\partial r_1 < \partial g$, $\partial r_2 < \partial s$. 已知 $d(x) = \text{gcd}(g(x), s(x))$, 且 $t(x) = (x^m - 1)/\text{lcm}(g(x), s(x))$. 设 $g'(x) = t(x)n(x)$ 和 $s'(x) = t(x)m(x)$, 则有 $g^{\perp q}(x) = t^q(1/x)n^q(1/x)x^{\partial g'}$ 和 $s^{\perp q}(x) = t^q(1/x)m^q(1/x)x^{\partial s'}$. 由于 $n(x)$ 和 $m(x)$ 互素, 因此 $g^{\perp q}(x)$ 和 $s^{\perp q}(x)$ 也互素, 并且有 $\text{gcd}(g^{\perp q}(x), s^{\perp q}(x)) = t^q(1/x)x^{\partial t}$. 设

$d^*(x) = \gcd(g^{\perp q}(x), s^{\perp q}(x))$, $t^*(x) = (x^m - 1)/\text{lcm}(g^{\perp q}(x), s^{\perp q}(x))$. 若 $g^{\perp q}(x) = d^*(x)m^*(x)$, 则可得 $s''(x) = t^*(x)m^*(x)$. 由于 $[\bar{t}^q(x)] = [t^q(1/x)x^m]$, 所以可得以下等式:

$$\begin{aligned} & [q_2(x)s''(x)\bar{f}^q(x)\bar{t}^q(x)x^{\partial s'}] \\ &= [q_2(x)s''(x)\bar{f}^q(x)t^q(1/x)x^m x^{\partial s'}] \\ &= [q_2(x)s''(x)\bar{f}^q(x)t^q(1/x)x^{\partial t}x^{m+\partial m}] \\ &= [q_2(x)t^*(x)m^*(x)\bar{f}^q(x)d^*(x)x^{m+\partial m}]. \end{aligned}$$

类似于等式 (3.2) 的推导, $\mathcal{C}_2$ 中的码字可表示成

$$([c(x)g^{\perp q}(x) - r_2(x)\bar{f}^q(x)\bar{t}^q(x)x^{\partial s'}], [r_2(x)s^{\perp q}(x)]),$$

其中 $c(x) = r_1(x) - q_2(x)\bar{f}^q(x)t^*(x)x^{m+\partial m}$. 类似于等式 (3.3), $\mathcal{C}_2$ 中的码字可进一步表示成

$$([r_3(x)g^{\perp q}(x) - r_2(x)\bar{f}^q(x)\bar{t}^q(x)x^{\partial s'}], [r_2(x)s^{\perp q}(x)]),$$

其中 $r_2(x)$ 和 $r_3(x)$ 是 $\mathbb{F}_{q^2}[x]$ 中次数小于 ∂s 和 ∂g 的多项式, 且 $r_3(x)$ 满足以下等式:

$$c(x) = q_3(x)g''(x) + r_3(x).$$

根据以上推导, 生成矩阵为 G' 的线性码 $\mathcal{C}_3$ 的码字可写成

$$([b_1(x)g^{\perp q}(x) - a_1(x)\bar{f}^q(x)\bar{t}^q(x)x^{\partial s'}], [a_1(x)s^{\perp q}(x)]),$$

其中 $a_1(x)$ 和 $b_1(x)$ 是 $\mathbb{F}_{q^2}[x]$ 中的多项式, 其次数分别小于 ∂s 和 ∂g . 根据 $\mathcal{C}_2$ 和 $\mathcal{C}_3$ 的码字表示形式, 可得出结论: $\mathcal{C}_2$ 中的任意码字都可由 $\mathcal{C}_3$ 的生成矩阵 G' 的行向量生成. 此外, $\mathcal{C}_2$ 中的码字可写成

$$([a(x)g^{\perp q}(x) - b(x)\bar{f}^q(x)\bar{t}^q(x)x^{\partial s'}], [b(x)s^{\perp q}(x)]),$$

其中 $a(x)$ 和 $b(x)$ 是 $\mathbb{F}_{q^2}[x]$ 中的任意多项式. 显然, $\mathcal{C}_3$ 的码字都包含于 $\mathcal{C}_2$ 中, 从而能够得出 G' 是 $\mathcal{C}_2$ 的生成矩阵, 并且 $\mathcal{C}_2$ 的维数为 $\partial g + \partial s$, 由此完成了证明的第一部分.

(2) 在证明的第二部分中, 为了简化表述, 令 $a_{21}(x) = \bar{f}^q(x)\bar{t}^q(x)x^{\partial s'}$ 且 $a_1(x), a_2(x), b_1(x)$ 和 $b_2(x)$ 为 $\mathbb{F}_{q^2}[x]$ 中的任意多项式. $\mathcal{C}_{q^2}(f, g, s)$ 中的码字可表示为

$$([a_1(x)g(x)], [a_1(x)d(x)f(x) + a_2(x)s(x)]).$$

类似地, $\mathcal{C}_2$ 中的码字可表示为

$$([b_1(x)g^{\perp q}(x) - b_2(x)a_{21}(x)], [b_2(x)s^{\perp q}(x)]).$$

上述两个码字的 Hermite 内积为

$$\begin{aligned} & \langle [a_1(x)g(x)], [b_1(x)g^{\perp q}(x) - b_2(x)a_{21}(x)] \rangle_h \\ &+ \langle [a_1(x)d(x)f(x) + a_2(x)s(x)], [b_2(x)s^{\perp q}(x)] \rangle_h, \end{aligned}$$

进一步可写成

$$\begin{aligned} & \langle [a_1(x)g(x)], [b_1(x)g^{\perp q}(x)] \rangle_h - \langle [a_1(x)g(x)], [b_2(x)a_{21}(x)] \rangle_h \\ &+ \langle [a_1(x)d(x)f(x)], [b_2(x)s^{\perp q}(x)] \rangle_h + \langle [a_2(x)s(x)], [b_2(x)s^{\perp q}(x)] \rangle_h. \end{aligned}$$

已知 $[g^{\perp q}(x)]$ (或 $[s^{\perp q}(x)]$) 是由 $[g(x)]$ (或 $[s(x)]$) 生成的循环码的 Hermite 对偶码, 因此有

$$\begin{aligned}\langle [a_1(x)g(x)], [b_1(x)g^{\perp q}(x)] \rangle_h &= 0, \\ \langle [a_2(x)s(x)], [b_2(x)s^{\perp q}(x)] \rangle_h &= 0.\end{aligned}$$

已知 $s'(x) = t(x)m(x)$, 且 $s^{\perp q}(x) = t^q(1/x)m^q(1/x)x^{\partial s'}$. 由于

$$[t^q(1/x)m^q(1/x)x^{\partial s'}] = [t^q(1/x)x^m m^q(1/x)x^m x^{\partial s'}] = [\bar{t}^q(x)\bar{m}^q(x)x^{\partial s'}],$$

所以可得 $[s^{\perp q}(x)] = [\bar{t}^q(x)\bar{m}^q(x)x^{\partial s'}]$. 由于多项式 $m(x)$ 和 $\bar{f}^q(x)$ 的次数小于 m , 根据引理 3.2, 下面的等式成立:

$$\begin{aligned}\langle [a_1(x)g(x)], [b_2(x)a_{12}(x)] \rangle_h &= \left\langle [a_1(x)d(x)m(x)], [b_2(x)\bar{f}^q(x)\bar{t}^q(x)x^{\partial s'}] \right\rangle_h \\ &= \left\langle [a_1(x)d(x)f(x)], [b_2(x)\bar{t}^q(x)\bar{m}^q(x)x^{\partial s'}] \right\rangle_h \\ &= \langle [a_1(x)d(x)f(x)], [b_2(x)s^{\perp q}(x)] \rangle_h.\end{aligned}$$

因此, $\mathcal{C}_{q^2}(f, g, s)$ 的任意码字与 $\mathcal{C}_2$ 的码字的内积为 0, 由此完成了证明的第二部分.

由于 $\mathcal{C}_2$ 的参数为 $[2m, \partial g + \partial s]$, 而 $\mathcal{C}_{q^2}(f, g, s)$ 的参数为 $[2m, 2m - \partial g - \partial s]$, 因此可得 $\mathcal{C}_2$ 是 $\mathcal{C}_{q^2}(f, g, s)$ 的 Hermite 对偶码, 其参数为 $[2m, \partial g + \partial s]$, 命题得证. $\square$

拟循环码 $\mathcal{C}_{q^2}(f, g, s)$ 包含于其 Hermite 对偶码 $\mathcal{C}_{q^2}^{\perp h}(f, g, s)$ 的条件, 即 Hermite 自正交的条件, 要求拟循环码 $\mathcal{C}_{q^2}(f, g, s)$ 中的多项式 $g(x)$, $s(x)$ 和 $f(x)$ 满足以下条件.

命题 3.2 拟循环码 $\mathcal{C}_{q^2}(f, g, s)$ 包含于其 Hermite 对偶码 $\mathcal{C}_{q^2}^{\perp h}(f, g, s)$ 的充分条件为 (1) $s^{\perp q}(x) \mid g(x)$; (2) $g^{\perp q}(x)s^{\perp q}(x) \mid s(x)$; (3) $g^{\perp q}(x)s^{\perp q}(x) \mid (g(x)s^{\perp q}(x) + d(x)f(x)\bar{f}^q(x)\bar{t}^q(x)x^{\partial s'})$.

证明 已知 $d(x) = \gcd(g(x), s(x))$. 令 $g(x) = d(x)m(x)$. 假设拟循环码 $\mathcal{C}_{q^2}(f, g, s)$ 满足命题 3.2 中的条件, 根据条件 (1) 和 (2), 可得 $s^{\perp q}(x) \mid d(x)$. 因此存在一个 $\mathbb{F}_{q^2}[x]$ 上的多项式 $a_1(x)$ 使得等式 $a_1(x)s^{\perp q}(x) = d(x)$ 成立, 并且存在一个多项式 $a_1(x)m(x)$ 使得等式 $a_1(x)m(x)s^{\perp q}(x) = d(x)m(x) = g(x)$ 成立. 根据条件 (2), 存在一个 $\mathbb{F}_{q^2}[x]$ 上的多项式 $b_1(x)$, 使得等式 $b_1(x)g^{\perp q}(x)s^{\perp q}(x) = s(x)$ 成立. 同样地, 根据条件 (3), 存在一个 $\mathbb{F}_{q^2}[x]$ 上的多项式 $c_1(x)$, 使得以下等式成立:

$$\begin{aligned}c_1(x)g^{\perp q}(x)s^{\perp q}(x) &= g(x)s^{\perp q}(x) + d(x)f(x)\bar{f}^q(x)\bar{t}^q(x)x^{\partial s'} \\ &= g(x)s^{\perp q}(x) + a_1(x)s^{\perp q}(x)f(x)\bar{f}^q(x)\bar{t}^q(x)x^{\partial s'}.\end{aligned}$$

通过约去等式两边的多项式 $s^{\perp q}(x)$, 可得以下等式:

$$c_1(x)g^{\perp q}(x) = g(x) + a_1(x)f(x)\bar{f}^q(x)\bar{t}^q(x)x^{\partial s'}.$$

由以上结论可得

$$\begin{aligned}([c_1(x)g^{\perp q}(x)], 0) &+ ([-a_1(x)f(x)\bar{f}^q(x)\bar{t}^q(x)x^{\partial s'}], [a_1(x)f(x)s^{\perp q}(x)]) \\ &= ([g(x) + a_1(x)f(x)\bar{f}^q(x)\bar{t}^q(x)x^{\partial s'} - a_1(x)f(x)\bar{f}^q(x)\bar{t}^q(x)x^{\partial s'}], [d(x)f(x)]) \\ &= ([g(x)], [d(x)f(x)]), \\ ([b_1(x)\bar{f}^q(x)\bar{t}^q(x)x^{\partial s'}g^{\perp q}(x)], 0) &+ ([-b_1(x)g^{\perp q}(x)\bar{f}^q(x)\bar{t}^q(x)x^{\partial s'}], [b_1(x)g^{\perp q}(x)s^{\perp q}(x)]) \\ &= (0, [s(x)]).\end{aligned}$$

因此, $\mathcal{C}_{q^2}(f, g, s)$ 包含于其 Hermite 对偶码 $\mathcal{C}_{q^2}^{\perp h}(f, g, s)$. 证毕. $\square$

基于以上的结论, 可通过定义 3.1 中的拟循环码 $\mathcal{C}_{q^2}(f, g, s)$ 得到一类新的量子拟循环码.

定理 3.1 若拟循环码 $\mathcal{C}_{q^2}(f, g, s)$ 的生成元为 $([g(x)], [d(x)f(x)])$ 和 $(0, [s(x)])$, 其多项式满足 $g(x)|(x^m-1)$, $s(x)|(x^m-1)$, 则 $\mathcal{C}_{q^2}(f, g, s)$ 的 Hermite 对偶码 $\mathcal{C}_{q^2}^{\perp h}(f, g, s)$ 的码参数为 $[2m, \partial g + \partial s]$, 生成元为 $([g^{\perp q}(x)], 0)$ 和 $([-\bar{f}^q(x)\bar{t}^q(x)x^{\partial s'}], [s^{\perp q}(x)])$. 若上述多项式满足 (1) $s^{\perp q}(x) | g(x)$; (2) $g^{\perp q}(x)s^{\perp q}(x) | s(x)$; (3) $g^{\perp q}(x)s^{\perp q}(x) | (g(x)s^{\perp q}(x) + d(x)f(x)\bar{f}^q(x)\bar{t}^q(x)x^{\partial s'})$, 则拟循环码 $\mathcal{C}_{q^2}(f, g, s)$ 是 Hermite 自正交的. 因此, 存在一个量子稳定子码, 其参数为

$$[[2m, 2\partial g + 2\partial s - 2m, d_Q]]_q,$$

其中 $d_Q = \min\{wt(\mathbf{x}) | \mathbf{x} \in \mathcal{C}_{q^2}^{\perp h}(f, g, s) \setminus \mathcal{C}_{q^2}(f, g, s)\}$.

证明 根据引理 3.1, 可得拟循环码 $\mathcal{C}_{q^2}(f, g, s)$ 的参数为 $[2m, 2m - \partial g - \partial s]$. 根据命题 3.1, 可得拟循环码 $\mathcal{C}_{q^2}(f, g, s)$ 的 Hermite 对偶码 $\mathcal{C}_{q^2}^{\perp h}(f, g, s)$ 的生成元形式为 $([g^{\perp q}(x)], 0)$ 和 $([-\bar{f}^q(x)\bar{t}^q(x)x^{\partial s'}], [s^{\perp q}(x)])$, 其参数为 $[2m, \partial g + \partial s]$. 因拟循环码 $\mathcal{C}_{q^2}(f, g, s)$ 的多项式满足命题 3.2 中的条件 (1) $s^{\perp q}(x) | g(x)$; (2) $g^{\perp q}(x)s^{\perp q}(x) | s(x)$; (3) $g^{\perp q}(x)s^{\perp q}(x) | (g(x)s^{\perp q}(x) + d(x)f(x)\bar{f}^q(x)\bar{t}^q(x)x^{\partial s'})$, 可得 $\mathcal{C}_{q^2}(f, g, s)$ 为自正交拟循环码, 即 $\mathcal{C}_{q^2}(f, g, s) \subseteq \mathcal{C}_{q^2}^{\perp h}(f, g, s)$. 根据定理 2.1 可得参数为 $[[2m, 2\partial g + 2\partial s - 2m, d_Q]]_q$ 的量子稳定子码, 其中

$$d_Q = \min \left\{ wt(\mathbf{x}) \mid \mathbf{x} \in \mathcal{C}_{q^2}^{\perp h}(f, g, s) \setminus \mathcal{C}_{q^2}(f, g, s) \right\}.$$

定理得证. □

4 例子

本节通过两个简单的量子拟循环码构造示例来演示量子拟循环码的构造过程. 示例中的量子拟循环码参数的计算借助了代数软件 [2].

例 4.1 令 $q = 2$, $m = 8$ 并且 w 为 $\mathbb{F}_4$ 上的一个本原元. 选取 $\mathbb{F}_4$ 上的多项式 $g(x) = x^2 + 1$, $s(x) = x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ 和 $f(x) = wx^4 + wx^3 + wx^2$, 可得一个 $\mathbb{F}_4$ 上的拟循环码 $\mathcal{C}_{q^2}(f, g, s)$.

多项式 $g(x)$ 和 $s(x)$ 满足定义 3.1 中的条件 $g(x), s(x)|(x^8 - 1)$, 且多项式 $d(x) = \gcd(g(x), s(x)) = x^2 + 1$, $t(x) = (x^8 - 1)/\text{lcm}(g(x), s(x)) = x + 1$. 基于以上多项式以及命题 3.1 的结论, 可得出 $\mathcal{C}_{q^2}(f, g, s)$ 的 Hermite 对偶码 $\mathcal{C}_{q^2}^{\perp h}(f, g, s)$ 生成元中对应的多项式

$$\begin{aligned} g^{\perp q}(x) &= x^6 + x^4 + x^2 + 1, \quad s^{\perp q}(x) = x + 1, \\ -\bar{f}^q(x)\bar{t}^q(x)x^{\partial s'} &= w^2x^{14} + w^2x^{13} + w^2x^{12} + w^2x^7 + w^2x^6 + w^2x^5. \end{aligned}$$

为验证 $\mathcal{C}_{q^2}(f, g, s)$ 的 Hermite 自正交性, 进一步计算以下多项式:

$$\begin{aligned} g^{\perp q}(x)s^{\perp q}(x) &= x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1, \\ g(x)s^{\perp q}(x) + d(x)f(x)\bar{f}^q(x)\bar{t}^q(x)x^{\partial s'} &= x^{20} + x^{14} + x^{13} + x^7 + x^3 + x^2 + x + 1. \end{aligned}$$

因上述多项式满足命题 3.2 中的条件

$$\begin{aligned} g(x) &= s^{\perp q}(x)(x + 1), \quad s(x) = g^{\perp q}(x)s^{\perp q}(x)(1), \\ g(x)s^{\perp q}(x) + d(x)f(x)\bar{f}^q(x)\bar{t}^q(x)x^{\partial s'} &= g^{\perp q}(x)s^{\perp q}(x)(x^{13} + x^{12} + x^7 + x^4 + 1), \end{aligned}$$

可得 $\mathcal{C}_{q^2}(f, g, s)$ 是一个 Hermite 自正交拟循环码.

通过对码参数的计算可得 $\mathcal{C}_{q^2}(f, g, s)$ 的参数为 $[16, 7, 8]_4$; 其 Hermite 对偶码 $\mathcal{C}_{q^2}^{\perp h}(f, g, s)$ 的参数为 $[16, 9, 4]_4$, 其重量分布为

$$w(z) = 1 + 84z^4 + 528z^6 + 1152z^7 + 5886z^8 + \cdots + 3753z^{16}.$$

根据定理 3.1 可得一个参数为 $[[16, 2, 4]]_2$ 的二元量子拟循环码.

例 4.2 令 $q = 2, m = 12$ 并且 w 为 $\mathbb{F}_4$ 上的一个本原元. 选取 $\mathbb{F}_4$ 上的多项式 $g(x) = x^3 + x^2 + x + 1$, $s(x) = x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ 和 $f(x) = w^2x$, 可得一个 $\mathbb{F}_4$ 上的拟循环码 $\mathcal{C}_{q^2}(f, g, s)$.

多项式 $g(x)$ 和 $s(x)$ 满足定义 3.1 中的条件 $g(x), s(x) \mid (x^{12} - 1)$, 且多项式 $d(x) = \gcd(g(x), s(x)) = x^3 + x^2 + x + 1$, $t(x) = (x^{12} - 1) / \text{lcm}(g(x), s(x)) = x + 1$. 基于以上多项式以及命题 3.1 的结论, 可得出 $\mathcal{C}_{q^2}(f, g, s)$ 的 Hermite 对偶码 $\mathcal{C}_{q^2}^{\perp h}(f, g, s)$ 生成元中对应的多项式

$$\begin{aligned} g^{\perp q}(x) &= x^9 + x^8 + x^5 + x^4 + x + 1, \\ s^{\perp q}(x) &= x + 1, \\ -\bar{f}^q(x)\bar{t}^q(x)x^{\partial s'} &= wx^{23} + wx^{12}. \end{aligned}$$

为验证 $\mathcal{C}_{q^2}(f, g, s)$ 的 Hermite 自正交性, 进一步计算以下多项式:

$$\begin{aligned} g^{\perp q}(x)s^{\perp q}(x) &= x^{10} + x^8 + x^6 + x^4 + x^2 + 1, \\ g(x)s^{\perp q}(x) + d(x)f(x)\bar{f}^q(x)\bar{t}^q(x)x^{\partial s'} &= x^{27} + x^{26} + x^{25} + x^{24} + x^{16} + x^{15} + x^{14} + x^{13} + x^4 + 1. \end{aligned}$$

因上述多项式满足命题 3.2 中的条件

$$\begin{aligned} g(x) &= s^{\perp q}(x)(x^2 + 1), \quad s(x) = g^{\perp q}(x)s^{\perp q}(x)(x + 1), \\ g(x)s^{\perp q}(x) + d(x)f(x)\bar{f}^q(x)\bar{t}^q(x)x^{\partial s'} &= g^{\perp q}(x)s^{\perp q}(x)(x^{17} + x^{16} + x^{13} + x^{12} + x^6 + x^4 + x^2 + 1), \end{aligned}$$

所以可得 $\mathcal{C}_{q^2}(f, g, s)$ 是一个 Hermite 自正交拟循环码.

通过对码参数的计算可得 $\mathcal{C}_{q^2}(f, g, s)$ 的参数为 $[24, 10, 4]_4$; 其 Hermite 对偶码 $\mathcal{C}_{q^2}^{\perp h}(f, g, s)$ 的参数为 $[24, 14, 4]_4$, 其重量分布为

$$w(z) = 1 + 198z^4 + 1869z^6 + 22491z^8 + \cdots + 450621z^{24}.$$

根据定理 3.1 可得一个参数为 $[[24, 4, 4]]_2$ 的二元量子拟循环码.

例 4.3 令 $q = 3, m = 15$ 并且 w 为 $\mathbb{F}_9$ 上的一个本原元. 选取 $\mathbb{F}_9$ 上的多项式 $g(x) = x^4 + w^2x^3 + w^7x^2 + w^2x + 1$, $s(x) = x^{14} + x^{13} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ 和 $f(x) = wx^8 + w^5x^7 + x^6 + w^2x^5 + w^4x^4 + w^4x^3 + w^4x + w^5$, 可得一个 $\mathbb{F}_4$ 上的拟循环码 $\mathcal{C}_{q^2}(f, g, s)$.

多项式 $g(x)$ 和 $s(x)$ 满足定义 3.1 中的条件 $g(x), s(x) \mid (x^{15} - 1)$, 且多项式

$$\begin{aligned} d(x) &= \gcd(g(x), s(x)) = x^4 + w^2x^3 + w^7x^2 + w^2x + 1, \\ t(x) &= (x^{15} - 1) / \text{lcm}(g(x), s(x)) = x + w^4. \end{aligned}$$

基于以上多项式以及命题 3.1 的结论, 可得出 $\mathcal{C}_{q^2}(f, g, s)$ 的 Hermite 对偶码 $\mathcal{C}_{q^2}^{\perp h}(f, g, s)$ 生成元中对应的多项式

$$\begin{aligned} g^{\perp q}(x) &= w^4x^{11} + w^6x^{10} + w^3x^9 + w^3x^8 + w^3x^7 + w^5x^6 + wx^5 + w^7x^4 + w^7x^3 + w^7x^2 + w^2x + 1, \\ s^{\perp q}(x) &= w^4x + 1, -\bar{f}^q(x)\bar{t}^q(x)x^{\partial s'} = x^{29} + x^{27} + x^{26} + w^2x^{25} + w^4x^{24} + w^3x^{23} + w^7x^{22} + w^5x^{15} \\ &\quad + w^4x^{13} + w^4x^{12} + w^6x^{11} + x^{10} + w^7x^9 + w^3x^8 + w^7x. \end{aligned}$$

为验证 $\mathcal{C}_{q^2}(f, g, s)$ 的 Hermite 自正交性, 进一步计算以下多项式:

$$\begin{aligned} g^{\perp q}(x)s^{\perp q}(x) &= x^{12} + wx^{11} + x^{10} + x^7 + wx^6 + x^5 + x^2 + wx + 1, \\ g(x)s^{\perp q}(x) + d(x)f(x)\bar{f}^q(x)\bar{t}^q(x)x^{\partial s'} &= w^5x^{41} + w^6x^{40} + w^7x^{39} + w^3x^{37} + w^6x^{36} + w^6x^{35} + w^6x^{34} \\ &\quad + w^2x^{33} + w^5x^{32} + w^4x^{31} + w^3x^{30} + w^5x^{29} + wx^{28} + w^5x^{27} + w^2x^{26} + w^5x^{25} + w^2x^{24} + w^6x^{23} \\ &\quad + w^7x^{21} + wx^{20} + w^6x^{19} + x^{18} + w^7x^{17} + w^6x^{16} + w^7x^{15} + w^5x^{14} + w^5x^{13} + x^{11} + w^6x^{10} + w^5x^9 \\ &\quad + w^2x^8 + w^4x^7 + x^6 + w^4x^5 + w^4x^4 + w^3x^3 + w^3x^2 + w^2x + 1. \end{aligned}$$

因上述多项式满足命题 3.2 中的条件

$$\begin{aligned} g(x) &= s^{\perp q}(x)(w^4x^3 + w^3x^2 + w^7x + 1), \\ s(x) &= g^{\perp q}(x)s^{\perp q}(x)(x^2 + w^3x + 1), \\ g(x)s^{\perp q}(x) + d(x)f(x)\bar{f}^q(x)\bar{t}^q(x)x^{\partial s'} &= g^{\perp q}(x)s^{\perp q}(x)(w^5x^{29} + w^6x^{27} + w^3x^{26} + w^2x^{24} + w^7x^{23} \\ &\quad + x^{22} + w^6x^{21} + w^6x^{20} + w^7x^{19} + w^7x^{18} + w^3x^{17} + w^3x^{16} + wx^{15} + w^2x^{13} + w^7x^{12} + w^6x^{10} \\ &\quad + w^3x^9 + w^4x^8 + wx^7 + wx^6 + w^5x^5 + w^3x^4 + w^7x^3 + wx^2 + x + 1), \end{aligned}$$

所以可得 $\mathcal{C}_{q^2}(f, g, s)$ 是一个 Hermite 自正交拟循环码.

通过对码参数的计算可得 $\mathcal{C}_{q^2}(f, g, s)$ 的参数为 $[30, 12, 12]_9$; 其 Hermite 对偶码 $\mathcal{C}_{q^2}^{\perp h}(f, g, s)$ 的参数为 $[30, 18, 9]_9$, 其重量分布为

$$w(z) = 1 + 6960z^9 + 122688z^{10} + 1638480z^{11} + \cdots + 4383181935048816z^{30}.$$

根据定理 3.1 可得一个参数为 $[[30, 6, 9]]_3$ 的三元量子拟循环码.

5 新的二元量子稳定子码

本节展示应用所提方法找到的具体参数的二元量子稳定子码, 并与现有码表中的结果进行比较. 本节比较的对象是量子稳定子码在线码表 [8]. 该码表纪录最新的最优量子稳定子码参数, 展示了量子稳定子码构造研究的最新结果, 其中结果仍在持续更新. 因此, 与该表结果对比更能突出本文研究结果的价值.

本文构造出 3 个打破码表纪录的二元量子稳定子码, 其参数分别为

$$[[126, 94, 7]]_2, \quad [[130, 92, 8]]_2, \quad [[136, 96, 8]]_2,$$

并且根据定理 2.2 扩展得到了另外的 9 个打破纪录的量子稳定子码. 它们在相同码长和维数下的最小距离均优于在线码表中列出的二元量子稳定子码. 在展示这 3 个量子稳定子码的构造细节前, 需要给出一些必要的定义和解释. 为了简化表示, 将有限域 $\mathbb{F}_4$ 中的 $0, 1, w, w^2$ 元素分别表示为 $0, 1, 2, 3$. 此外, 多项式用其升序系数序列表示, 序列的指数表示重复系数的次数. 例如, 多项式 $1 + w^2x^3 + wx^5$ 可写作 10^2302 . 在展示量子稳定子码的表格中, 上标为 $*$ 的量子稳定子码是由定理 2.2 扩展得到.

表 1 中构造出的打破码表纪录的量子稳定子码为 $[[126, 94, 7]]_2$. 构造它所用的拟循环 $\mathcal{C}_{q^2}(f, g, s)$ 是 Hermite 自正交的, 参数为 $[126, 16, 68]_4$, 构造信息为

$$g(x) = 3120320312^212^332^2301301^221213^221213^221^430^321, \quad s(x) = x^{63} - 1$$

和

$$f(x) = 0^21^20^231^20^33203.$$

根据定理 3.1, 可得到 $\mathcal{C}_{q^2}(f, g, s)$ 的 Hermite 对偶码 $\mathcal{C}_{q^2}^{\perp h}(f, g, s)$, 其参数为 $[126, 110, 7]_4$, 对应的重量分布为

$$w(z) = 1 + 50652z^7 + 1923075z^8 + 75480279z^9 + \cdots \\ + 305012918225866824479589261053031526507988039723073z^{126}.$$

因此根据定理 3.1, 可得到参数为 $[[126, 94, 7]]_2$ 的量子稳定子码. 由于码 $\mathcal{C}_{q^2}(f, g, s)$ 的最小距离为 68, 码 $\mathcal{C}_{q^2}^{\perp h}(f, g, s)$ 的最小距离为 7, $\mathcal{C}_{q^2}^{\perp h}(f, g, s)$ 的最小距离小于 $\mathcal{C}_{q^2}(f, g, s)$ 的最小距离, 因此这个量子稳定子码是纯的. 同时, 根据定理 2.2 的扩展规则能够得到另外 3 个量子稳定子码

$$[[126, 93, 7]]_2, \quad [[127, 94, 7]]_2, \quad [[127, 93, 7]]_2,$$

这些量子稳定子码相较于码表 [8] 中的相同码长和维数的量子稳定子码, 最小距离提高到了 7.

表 2 中构造出的打破码表纪录的量子稳定子码的参数为 $[[130, 92, 8]]_2$. 构造它所用的拟循环 $\mathcal{C}_{q^2}(f, g, s)$ 是 Hermite 自正交的, 参数为 $[130, 19, 66]_4$, 构造信息为

$$g(x) = 103^20^22012^21^22^20^310^2202020^210^32^21^22^21020^23^201, \quad s(x) = x^{65} - 1$$

表 1 新的量子稳定子码 $[[126, 94, 7]]_2$ 及其扩展

编号	二元量子稳定子码	码表中的量子稳定子码 [8]
1	$[[126, 94, 7]]_2$	$[[126, 94, 6]]_2$
2	$[[126, 93, 7]]_2^*$	$[[126, 93, 6]]_2$
3	$[[127, 94, 7]]_2^*$	$[[127, 94, 6]]_2$
4	$[[127, 93, 7]]_2^*$	$[[127, 93, 6]]_2$

表 2 新的量子稳定子码 $[[130, 92, 8]]_2$ 及其扩展

编号	二元量子稳定子码	码表中的量子稳定子码 [8]
1	$[[130, 92, 8]]_2$	$[[130, 92, 7]]_2$
2	$[[131, 92, 8]]_2^*$	$[[131, 92, 7]]_2$
3	$[[132, 92, 8]]_2^*$	$[[132, 92, 7]]_2$
4	$[[133, 92, 8]]_2^*$	$[[133, 92, 7]]_2$

和

$$f(x) = 0^2 131210^2 201^2 3^3 231.$$

根据定理 3.1, 可得到 $\mathcal{C}_{q^2}(f, g, s)$ 的 Hermite 对偶码 $\mathcal{C}_{q^2}^{\perp h}(f, g, s)$, 其参数为 $[130, 111, 8]_4$, 对应的重量分布为

$$\begin{aligned} w(z) = & 1 + 56151z^8 + 623424z^9 + 24005496z^{10} + \cdots \\ & + 386031974629612699731980158545447395848830081997344z^{130}. \end{aligned}$$

因此根据定理 3.1, 可得到参数为 $[[130, 92, 8]]_2$ 的量子稳定子码. 由于码 $\mathcal{C}_{q^2}(f, g, s)$ 的最小距离为 66, 码 $\mathcal{C}_{q^2}^{\perp h}(f, g, s)$ 的最小距离为 8, $\mathcal{C}_{q^2}^{\perp h}(f, g, s)$ 的最小距离小于 $\mathcal{C}_{q^2}^{\perp h}(f, g, s)$ 的最小距离, 因此这个量子稳定子码是纯的. 同时, 根据定理 2.2 的扩展规则能够得到另外 3 个量子稳定子码

$$[[131, 92, 8]]_2, \quad [[132, 92, 8]]_2, \quad [[133, 92, 8]]_2,$$

这些量子稳定子码相较于码表 [8] 中的相同码长和维数的量子稳定子码, 最小距离提高到了 8.

表 3 中构造出的打破码表纪录的量子稳定子码的参数为 $[[136, 96, 8]]_2$. 构造它所用的拟循环 $\mathcal{C}_{q^2}(f, g, s)$ 是 Hermite 自正交的, 参数为 $[136, 20, 64]_4$, 构造信息为

$$g(x) = 1203^2 21^2 032^3 020210^2 3^4 23^4 0^2 120202^3 301^2 23^2 021, \quad s(x) = x^{68} - 1$$

和

$$f(x) = 301310^2 2^3 01^4 2312^2.$$

根据定理 3.1, 可得到 $\mathcal{C}_{q^2}(f, g, s)$ 的 Hermite 对偶码 $\mathcal{C}_{q^2}^{\perp h}(f, g, s)$, 其参数为 $[136, 116, 8]_4$, 对应的重量分布为

$$\begin{aligned} w(z) = & 1 + 4662z^8 + 1549470z^9 + 57097950z^{10} + \cdots \\ & + 70354327376246914526153383899449477126944265037917319z^{136}. \end{aligned}$$

因此根据定理 3.1, 可得到参数为 $[[136, 96, 8]]_2$ 的量子稳定子码. 由于码 $\mathcal{C}_{q^2}(f, g, s)$ 的最小距离为 64, 码 $\mathcal{C}_{q^2}^{\perp h}(f, g, s)$ 的最小距离为 8, $\mathcal{C}_{q^2}^{\perp h}(f, g, s)$ 的最小距离小于 $\mathcal{C}_{q^2}^{\perp h}(f, g, s)$ 的最小距离, 因此这个量子稳定子码是纯的. 同时, 根据定理 2.2 的扩展规则能够得到另外 3 个量子稳定子码

$$[[136, 95, 8]]_2, \quad [[137, 95, 8]]_2, \quad [[137, 96, 8]]_2,$$

这些量子稳定子码相较于码表 [8] 中的相同码长和维数的量子稳定子码, 最小距离提高到了 8.

表 3 新的量子稳定子码 $[[136, 96, 8]]_2$ 及其扩展

编号	二元量子稳定子码	码表中的量子稳定子码 [8]
1	$[[136, 96, 8]]_2$	$[[136, 96, 7]]_2$
2	$[[136, 95, 8]]_2^*$	$[[136, 95, 7]]_2$
3	$[[137, 95, 8]]_2^*$	$[[137, 95, 7]]_2$
4	$[[137, 96, 8]]_2^*$	$[[137, 96, 7]]_2$

6 结论

本文提出了一类指标为 2 的拟循环码, 给出了这类拟循环码的生成元形式以及码参数. 通过研究这类拟循环码 Hermite 对偶码的代数结构, 确定了其 Hermite 对偶码的生成元形式以及码参数. 通过给出这类拟循环码在 Hermite 内积下自正交的条件后, 本文得到了一类新的量子拟循环码. 基于这类量子拟循环码, 我们找到了 12 个具体参数的打破纪录的二元量子稳定子码, 这些量子稳定子码的最小距离相较于当前码表纪录中的同码长、同维数的量子稳定子码均提高了 1, 这意味着本文构造出的量子稳定子码有着更高的纠正量子错误的能力. 这些结果表明所提方法在构造高纠错性能量子稳定子码方面是有效的. 而且根据本文证明, 本文提出的方法在未来还可能构造出更多不同有限域上的、更高码长的高纠错性能的量子稳定子码.

致谢 感谢审稿人提出的宝贵修改建议.

参考文献

- 1 Abdukhalikov K, Bag T, Panario D. One-generator quasi-cyclic codes and their dual codes. *Discrete Math*, 2023, 346: 113369
- 2 Bosma W, Cannon J, Playoust C. The Magma algebra system I: The user language. *J Symbolic Comput*, 1997, 24: 235–265
- 3 Calderbank A R, Rains E M, Shor P M, et al. Quantum error correction via codes over GF(4). *IEEE Trans Inform Theory*, 1998, 44: 1369–1387
- 4 Chen E Z. Some new binary codes with improved minimum distances. *J Algebra Comb Discrete Struct Appl*, 2018, 5: 65–70
- 5 Daskalov R, Hristov P. New binary one-generator quasi-cyclic codes. *IEEE Trans Inform Theory*, 2003, 49: 3001–3005
- 6 Ezerman M F, Ling S, Ozkaya B, et al. Good stabilizer codes from quasi-cyclic codes over F4 and F9. In: *Proceedings of the 2019 IEEE International Symposium on Information Theory*. Paris: IEEE, 2019, 2898–2902
- 7 Galindo C, Hernando F, Matsumoto R. Quasi-cyclic constructions of quantum codes. *Finite Fields Appl*, 2018, 52: 261–280
- 8 Grassl M. Bounds on the minimum distance of linear codes and quantum codes. [Http://www.codetables.de](http://www.codetables.de), 2015
- 9 Guan C, Li R, Lu L, et al. New binary quantum codes constructed from quasi-cyclic codes. *Internat J Theoret Phys*, 2022, 61: 172
- 10 Guan C, Li R, Lu L, et al. On construction of quantum codes with dual-containing quasi-cyclic codes. *Quantum Inf Process*, 2022, 21: 263
- 11 Hagiwara M, Imai H. Quantum quasi-cyclic LDPC codes. In: *Proceedings of the 2011 IEEE International Symposium on Information Theory*. St. Petersburg: IEEE, 2007, 806–810
- 12 Kasami T. A Gilbert-Varshamov bound for quasi-cycle codes of rate 1/2 (Corresp.). *IEEE Trans Inform Theory*, 1974, 20: 679
- 13 Ketkar A, Klappenecker A, Kumar S, et al. Nonbinary stabilizer codes over finite fields. *IEEE Trans Inform Theory*, 2006, 52: 4892–4914
- 14 Ling S, Sole P. Good self-dual quasi-cyclic codes exist. *IEEE Trans Inform Theory*, 2003, 49: 1052–1053
- 15 Lv J, Li R, Wang J. Quantum codes derived from one-generator quasi-cyclic codes with Hermitian inner product. *Internat J Theoret Phys*, 2020, 59: 300–312
- 16 Nielsen M A, Chuang I L. *Quantum Computation and Quantum Information*. Cambridge: Cambridge Univ Press, 2001
- 17 Shor P W. Scheme for reducing decoherence in quantum computer memory. *Phys Rev A*, 1995, 52: R2493
- 18 Steane A M. Multiple-particle interference and quantum error correction. *Proc Royal Soc London Ser A Math Phys Eng Sci*, 1996, 452: 2551–2577
- 19 Steane A M. Enlargement of Calderbank-Shor-Steane quantum codes. *IEEE Trans Inform Theory*, 1999, 45: 2492–2495

The construction of quantum quasi-cyclic codes based on the Hermitian inner product

Zhenhui Zhang, Zhuo Li & Lijuan Xing

Abstract In order to construct quantum stabilizer codes with high-error-correcting performance, in this paper, we propose a wide class of quasi-cyclic codes, providing the generator forms and code parameters of such codes and their Hermitian dual codes. By giving the conditions for the Hermitian self-orthogonality of such quasi-cyclic codes, we obtain a new class of quantum quasi-cyclic codes according to the Hermitian construction. Among this class of quantum quasi-cyclic codes, we find 12 record-breaking binary quantum stabilizer codes. Their minimum distances are higher than those of the corresponding codes in existing quantum code tables. These results demonstrate that our method provides effective support for the construction of quantum stabilizer codes with high-error-correcting performance.

Keywords quasi-cyclic code, quantum stabilizer code, Hermitian dual code, Hermitian construction

MSC(2020) 94B15, 81P70

doi: 10.1360/SSM-2025-0066