由 n-to-1 映射构造的自正交极小码

Qin Du、Ziling Heng 和 Jun Zhang

arXiv:2611.32192v1 [cs.IT] 24 Nov 2026

摘要

自正交码是构造量子纠错码的核心，而极小码能够导出秘密共享方案，其访问结构可由码字的支撑集读出。因此，兼具自正交性与极小性的码可同时发挥这两种作用，使同一个码族能够同时构造量子码和秘密共享方案。有限域上由 n-to-1 映射导出的线性码，是此类码的自然来源，近年来受到广泛关注；然而，其参数和重量分布仍难以确定：对于大多数高次数函数，无法直接计算其 Walsh 谱，而极小性与自正交性的分析恰恰依赖于这些重量。我们借助斜多项式环的代数理论来解决这一难题。利用斜多项式的右最大公因子，我们确定了与 n-to-1 映射相关的线性化多项式的核空间维数，进而得到相应码的重量分布。借助这一方法，我们研究了两个新构造的 n-to-1 函数族以及一个已知函数族，并得到了由此产生的码的精确重量分布；此外，我们还证明这些码均为极小且自正交。因而，每个函数族都能同时导出量子纠错码和秘密共享方案，且其参数和访问结构均已明确确定。本研究为确定由 n-to-1 映射导出的线性码参数提供了新的视角。

索引词

n-到-1 映射、斜多项式环、自正交码、极小码。

I. 引言

长度为 v 、维数为 κ 且定义在有限域 $\mathbb{F}_q$ 上的线性码，被定义为 $\mathbb{F}_q^v$ 的 κ 维线性子空间。通常将其称为 $[v, \kappa, d]$ 码，其中 d 表示最小汉明距离。 $[v, \kappa, d]$ 线性码 $\mathcal{C}$ 的重量分布是序列 $(A_i)_{i=0}^{v}$，其中 A_i 表示汉明重量为 i 的码字数量。重量分布是一个基本不变量，它不仅决定了该码的检错和纠错能力，还与其许多组合性质和代数性质密切相关。

随着现代通信、数据存储、分布式计算和密码系统的快速发展，对高效且可靠的编码方案的需求日益迫切。有限域上的线性码因其线性结构和易于实现而得到广泛研究。具有特殊重量分布和良好正交性质的线性码一直是研究的重点。少重量线性码已在密码学和组合设计 [2], [39] 中得到广泛应用。因此，新线性码的构造及其重量分布的确定，均具有理论和实际意义。

过去几十年来，人们提出了多种构造线性码的方法，由此得到许多参数优良且具有有趣重量分布的码族 [2], [7], [8], [10], [11], [13], [34]。特别是，研究人员利用

Q. Du 和 Z. Heng 任职于中国西安 710064 长安大学理学院，同时也任职于中国西安 710071 西安电子科技大学综合业务网国家重点实验室；J.ZhangiswiththeCollegeofMathematicsandStatistics, Chongqing University, Chongqing 401331, China（电子邮箱：15535565189@163.com、zilingheng@chd.edu.cn、jun zhang@cqu.edu.cn）。（通讯作者：*Ziling Heng*）Z. Heng 的研究部分得到了国家自然科学基金（项目编号：12271059）和陕西省自然科学基础研究计划（项目编号：2026JC-YXQN-030）的资助。J. Zhang 的研究得到了国家自然科学基金（项目编号：12441105）的资助。

有限域上的多种特殊密码函数构造了具有最优参数的线性码，例如（弱正则）弯曲函数[34], 二次密码函数 [36], [40],弱正则平台函数 [27], [28],（几乎）完美非线性（APN 或 PN）函数 [10], 以及 n-对-1 函数 [18], [25], 等。这种方法的核心挑战在于选择合适的函数来构造码，而选择的根本目标是赋予所得码优良的代数性质和组合性质。在这些性质中，极小性和自正交性已成为两个十分活跃的研究课题，因为它们在密码学、通信系统和数据存储中有广泛的应用。

极小码的特征在于任一码字都不覆盖另一码字，这使其成为构造秘密共享方案和安全多方计算协议的基础 [39]。自Ashikhmin-Barg充分条件 [1], 提出以来，关于极小码的判定标准得到了广泛研究；此后，研究重点逐渐转向完整刻画。在这一方向上，Heng、Ding和Zhou通过码字的汉明重量，为有限域上的线性码成为极小码建立了一个充要条件，并基于该条件构造了若干族二元和三元极小码 [14]。从另一角度来看，Tang等人利用切割阻挡集，从射影几何的视角对极小码进行了完整刻画 [35]。这些成果共同推动了极小性判定标准理论框架的发展。

与此同时，自正交码是线性码的一个重要子类。它们与组合设计、量子纠错码 [3], 、线性互补对偶码 [15], 和秘密共享方案 [4]密切相关。因此，过去几十年来，大量研究致力于探索其结构特征及显式构造。例如，有研究对由组合设计得到的自正交码进行了探讨 [12]。近年来，研究人员利用特殊密码函数（如弱正则Bent函数和plateaued函数）构造了自正交码 [15], [17]。

在已知的数学工具中，有限域上的 n 对一映射对于在编码理论中构造良好的线性码非常重要。据我们所知，利用二对一函数构造线性码的研究可追溯至 [5], [6]。继 [26], 的一项重要工作之后，Li 等人进一步研究了特征2有限域上的二对一映射，并通过构造 I 和构造 II 将其应用于构造具有新参数的二元线性码 [19]。下面回顾这两种线性码构造方法。设 $\mathbb{F}_{2^m}$ 为含有 2^m 个元素的有限域，且 $\mathbb{F}_{2^m}^*:=\mathbb{F}_{2^m}\setminus\{0\}$。设 $f(x)$ 是从 $\mathbb{F}_{2^m}$到 $\mathbb{F}_{2^m}$的函数，且 $D(f)=\{f(x):\ x\in\mathbb{F}_{2^m}\}\setminus\{0\}=\{d_1,d_2,\cdots,d_l\}$, 其中$l=|D(f)|$。设 $\mathrm{Tr}_{2^m/2}$ 为从 $\mathbb{F}_{2^m}$ 到 $\mathbb{F}_2$的迹函数。构造 I 如下:

$$\mathcal{C}_f=\left\{\mathbf{c}_{a,b}=\left(\mathrm{Tr}_{2^m/2}(ax+bf(x))\right)_{x\in\mathbb{F}_{2^m}^*}:a,b\in\mathbb{F}_{2^m}\right\}.$$

构造 II 如下给出

$$\mathcal{C}_{D(f)}\ =\ \left\{\mathbf{c}_b=\left(\mathrm{Tr}_{2^m/2}\left(bd_1\right),\mathrm{Tr}_{2^m/2}\left(bd_2\right),\cdots,\mathrm{Tr}_{2^m/2}\left(bd_l\right)\right):b\in\mathbb{F}_{2^m}\right\}.$$

2023年，Mesnager 等人基于构造 III [25], 构造了若干族新的二元最小线性码，这些码来自二对一映射，其形式为

$$\tilde{\mathcal{C}}_{D(f)}\ =\ \left\{\tilde{\mathbf{c}}_{a,b}=\left(\mathrm{Tr}_{2^m/2}(ad_i+bd_j)\right)_{(d_i,d_j)\in D(f)\times D(f)}:a,b\in\mathbb{F}_{2^m}\right\},$$

其中， $D(f)^2$ 表示笛卡尔积。随后，在2024年，Ren´e Rodr´ıguez-Aldama [33] 将这项研究拓展到具有任意素特征 p 的有限域，并通过构造 II 利用 t 对一函数构造了两族无穷的 p 元线性码。最近，Li 等人 [22] 在 $\mathbb{F}_{2^m}$ 上构造了形如 $f(x)=cx+\mathrm{Tr}^{2^{2m}/2^m}(h(x))$ 的新二对一函数，并通过构造 I 获得了具有新参数的二元线性码，丰富了该方向的研究体系。

自正交性和极小性分别服务于不同的应用——量子纠错码和秘密共享方案——但同时具备这两种性质的线性码具有重要意义。自正交码可通过 CSS 构造 [3], 导出量子纠错码，而

极小码则可通过 Yuan 和 Ding 的构造方法 [39],导出一种秘密共享方案，其访问结构由其码字的支集决定；因此，同时具备这两种性质的码可以兼用于这两种构造。在既需要量子纠错又要求特定访问结构的场景中——例如基于 CSS 的量子秘密共享，其中单个自正交码既提供量子码，也提供用于推导访问结构的经典数据——使用一个码族即可替代两个。因此，有必要构造同时具备自正交性和极小性的线性码。

因此，本文的主要目的是从 n-到-1 映射构造这类码的新族。由有限域上的 n-到-1 映射产生的线性码是这类码的一个自然来源，近年来已受到广泛关注，但其参数和重量分布仍然难以确定：对于大多数高次数函数，无法直接计算 Walsh 谱，而极小性和自正交性的分析正是建立在这些重量之上的。

为解决这一问题，我们采用一种基于斜多项式环代数理论的方法。具体而言，通过对斜多项式环上的多项式使用右最大公因式方法，我们确定了与 n-到-1 映射相关的线性化多项式的核空间维数。在此方法的基础上，我们进一步完全确定了基于构造 I 的三个线性码族的精确重量分布；这些线性码族分别由两个新构造的 n-到-1 映射族和一个已知族产生。此外，我们证明所得码既是具有三个非零重量的极小线性码，也是自正交线性码。本文构造的三类自正交极小码可以按照 [39], 中的方法用于秘密共享方案以及量子码。

本文其余部分安排如下。第二节介绍相关预备知识。第三节构造两个新的 n 对 1 映射族，然后研究基于构造 I、由这两个新的 n 对 1 映射族以及一个已知映射族构造的线性码的重量分布、自正交性和极小性。第四节总结本文的主要结果并得出结论。

II. 预备知识

本节介绍用于给出主要结果的一些预备知识。首先定义如下记号。

- q：素数 p 的幂；
- $\mathbb{F}_q$：含有 q 个元素的有限域；
- $\mathbb{F}_{q^m}$：$\mathbb{F}_q$ 的 m 次有限扩域，其中 m 是正整数；
- $\mathbb{F}_{q^m}^*$：$\mathbb{F}_{q^m}$的乘法群；
- $\mathbb{F}_{q^m}[x]$：有限域 $\mathbb{F}_{q^m}$上的多项式环；

- $\times$：集合的笛卡尔积；
- $\#A$：集合 A的基数；
- $\mathrm{Tr}_{q^m/q}(x) = \sum_{i=0}^{m-1} x^{q^i}$：从 $\mathbb{F}_{q^m}$ 到 $\mathbb{F}_q$的迹函数；

- $\ker(f(x)) = \{x \in \mathbb{F}_q : f(x) = 0\}$：将 f映射到 $\mathbb{F}_q$上的同态的核；
- $\dim_{\mathbb{F}_2}(K)$：$\mathbb{F}_2$-向量空间 K的维数；
- $\mathrm{wt}(\mathbf{c})$：向量$\mathbf{c}$的汉明重量；
- $d(\mathcal{C})$：码 $\mathcal{C}$ 的最小距离。

A. n-对-1映射

n-对-1 映射的定义见 [29] ，如下所示。

定义 1. *[29]* 设 A和 B 为有限集。若满足以下任一条件，则称函数 $f: A \to B$ 为 n-对-1 映射：

1) 如果 n 整除$\#A$，那么 $b \in B$ 中的每个元素在 A中都有 n 个原像或0 个原像 .

2) 如果 n 不整除$\#A$，那么除了唯一一个元素之外， B中的每个元素在 A中都有 n 个原像或0个原像。 B 中的这个特殊元素在 A中恰好有$\#A$模 n 个原像。

下面，我们回顾有限域上的一个已知的 n-对-1映射，如下所示 .

引理1. *[22]* 设 k 为奇正整数， $q=2^k$ 且 $c\in\mathbb{F}_{q^2}$ 满足 $c^{q-1}=\omega$，其中 $\omega^3=1$。则 $f(x)=cx+\mathrm{Tr}_{q^2/q}\left(x^6+x^{2q+4}\right)$ 在 $\mathbb{F}_{q^2}$上是2对1 映射。

B. 迹函数

从 $\mathbb{F}_{q^m}$ 到 $\mathbb{F}_q$ 的迹函数定义为

$$\mathrm{Tr}_{q^m/q}(\alpha)=\alpha+\alpha^q+\alpha^{q^2}+\cdots+\alpha^{q^{m-1}}.$$

它是一个满射的 $\mathbb{F}_q$-线性映射，也是编码理论、密码学和序列设计中的基础工具。具体而言，它已被广泛用于构造循环码、特殊类别的线性码、密码函数以及各种具有低相关性的序列。

Le理 lemma 2. 从 $\mathbb{F}_{q^m}$ 到 $\mathbb{F}_q$ 的迹函数满足以下性质 :

(1) $Tr^{q^m/q}(\alpha+\beta)=Tr^{q^m/q}(\alpha)+Tr^{q^m/q}(\beta)$ 对所有 α、$\beta\in\mathbb{F}_{q^m}$均成立；*(2)* $Tr^{q^m/q}(c\alpha)=cTr^{q^m/q}(\alpha)$ 对任意 $c\in\mathbb{F}_q$ 和 $\alpha\in\mathbb{F}_{q^m}$均成立；*(3)* $Tr^{q^m/q}(\alpha^q)=Tr^{q^m/q}(\alpha)$ 对所有 $\alpha\in\mathbb{F}_{q^m}$均成立；*(4)* 对于属于 $\mathbb{F}_q$的每个元素 α，$Tr^{q^m/q}(\alpha)=m\alpha$ 均成立。

C. 二次函数与沃尔什变换

引言中已经介绍了几种线性码的构造方法。下文的讨论基于构造 I。该方法利用函数f : $\mathbb{F}_{2^m}\to\mathbb{F}_{2^m}$ 定义了一个在 $\mathbb{F}_2$ 上的线性码，如下所示:

$$\mathcal{C}_f=\left\{\mathbf{c}_{a,b}=\left(\mathrm{Tr}_{2^m/2}(ax+bf(x))\right)_{x\in\mathbb{F}_{2^m}^*}\mid a,b\in\mathbb{F}_{2^m}\right\},\tag{1}$$

其中 $f(0)=0$，且 m 为正整数。为研究该码的参数，只需确定Walsh变换 $W_f(a,b)$，其定义为

$$W_f(a,b)=\sum_{x\in\mathbb{F}_{2^m}}(-1)^{\mathrm{Tr}_{2^m/2}(ax+bf(x))}.$$

特别地，我们关注当 f是二次函数，即 f的代数次数为 2 时， $W_f(a,\ b)$ 的值分布。

引理*3.* *[18]* 设 $\varphi(x):=Tr^{2^m/2}(Q(x))$，其中 $Q(x)$ 表示一个从 $\mathbb{F}_{2^m}$ 到 $\mathbb{F}_{2^m}$的二次函数，且满足 $Q(0)=0$。其对应的对称双线性映射定义为 $B_\varphi(x,y)=\varphi(x+y)+\varphi(x)+\varphi(y)$。 B_φ的核记为 V_φ，它构成 $\mathbb{F}_{2^m}$ 的一个 $\mathbb{F}_2$-子空间，定义如下:

$$V_\varphi=\{y\in\mathbb{F}_{2^m}:B_\varphi(x,y)=0\ \textit{for all}\ x\in\mathbb{F}_{2^m}\}.$$

φ 的秩定义为 $Rank(\varphi)=m-$ 维数$_{\mathbb{F}_2}(V_\varphi)$。则 $\varphi(y)=$ 迹$^{2^m/2}(Q(y))$ 在 V_φ上是线性的，且

$$\Sigma_{x\in\mathbb{F}_{2^m}}(-1)^{\varphi(x)}=\begin{cases}\pm2^{\frac{m+d'}{2}} & if\ \varphi\ vanishes\ on\ V_\varphi,\\ 0 & otherwise,\end{cases}$$

其中 $d'=$ 维数 (V_φ)。

设 f是一个从 $\mathbb{F}_{2^m}$到 $\mathbb{F}_{2^m}$的二次函数，满足 $f(0)=0$。对于$\varphi_{a,b}(x)=\mathrm{Tr}^{2^m/2}(ax+bf(x))$和 $\varphi_b(x)=\mathrm{Tr}^{2^m/2}(bf(x))$，分别记为 $a,b\in\mathbb{F}_{2^m}$。注意，对于任意非零的 $b\in\mathbb{F}_{2^m}$，$\varphi_{a,b}(x)$和 $\varphi_b(x)$具有相同的关联对称双线性映射。因此，引理4给出以下结果。

引理4. *[18]* 设 f是一个从 $\mathbb{F}_{2^m}$到 $\mathbb{F}_{2^m}$的二次函数，满足 $f(0)=0$。则有

$$W_f(a,b)=\Sigma_{x\in\mathbb{F}_{2^m}}(-1)^{\varphi_{a,b}(x)}=\begin{cases}\pm 2^{\frac{m+d_b}{2}} & \textit{if } \varphi_{a,b} \textit{ vanishes on } V_{\varphi_b},\\ 0 & \textit{otherwise},\end{cases}$$

其中，d_b表示 φ_b的核 V_{φ_b}的维数。

D. 带自同构 σ的斜多项式环

定义2. *[37]* 设 σ是 $\mathbb{F}_{q^k}$相对于 $\mathbb{F}_q$的 *Frobenius*自同构，并用 $\mathbb{F}_{q^k}[x;\sigma]$表示 $\mathbb{F}_{q^k}$上的所有斜多项式的集合。这类多项式的加法按通常方式定义，而乘法则通过分配律并结合以下规则定义

$$(ax^i)(bx^j)=a\sigma^i(b)x^{i+j}=ab^{q^i}x^{i+j},\quad a,b\in\mathbb{F}_{q^k}. \tag{2}$$

在这些运算下，$\mathbb{F}_{q^k}[x;\sigma]$构成一个环，称为带自同构$\sigma$的 $\mathbb{F}_{q^k}$上的斜多项式环。

定义3. *[30]* 当 $F(x)=D_1(x)D_2(x)$时，我们称 $D_2(x)$为 $F(x)$的右因子，称 $D_1(x)$为其左因子。

令 $F(x)=a_0x^{m_1}+a_1x^{m_1-1}+\cdots+a_{m_1}$和 $G(x)=b_0x^{m_2}+a_0x^{m_2-1}+\cdots+b_{m_2}\in\mathbb{F}_{q^k}[x;\ \sigma]$和$m_1\geq m_2$。差异

$$F_1(x)=F(x)-a_0\sigma^{m_1-m_2}(b_0^{-1})x^{m_1-m_2}G(x) \tag{3}$$

的次数是 低于 m_1。由此可知，总是可以执行右除法

$$F(x)=Q(x)G(x)+R(x),$$

其中 $Q(x)$的次数为 m_1-m_2，而 $R(x)$的次数不超过 m_2-1。利用上述带余数的右除法应用右欧几里得算法，可求得 $F(x)$和 $G(x)$的右最大公因子，记为 gcrd($F(x)$ $G(x)$)。具体而言，如果

$$\begin{aligned}F(x)&=Q_0(x)G(x)+F_1(x),\\ G(x)&=Q_1(x)F_1(x)+F_2(x),\\ &\vdots\\ F_{t-2}(x)&=Q_{t-1}(x)F_{t-1}(x)+F_t(x),\\ F_{t-1}(x)&=Q_t(x)F_t(x),\end{aligned}$$

那么 $=F_t(x)$是 gcrd($F(x)$ $G(x)$)。

E. 线性化多项式

在线性化多项式的理论和应用中，下面介绍的线性化多项式都非常重要。这些多项式的一个实用特点是其根集的结构，这有助于确定其根。与通常一样，令 q 表示一个素数幂。

定义4。 *[23]*形式为

$$L(x)=\sum_{i=0}^{r}\alpha_i x^{q^i},$$

系数取自 $\mathbb{F}_q$的扩域 $\mathbb{F}_{q^m}$ 的多项式，称为 $\mathbb{F}_{q^m}$上的 q-线性化多项式，或 q-多项式。

定义 5。 *[23]* 多项式

$$L(x)=\sum_{i=0}^{r}\alpha_i x^{q^i} \quad \textit{and} \quad l(x)=\sum_{i=0}^{r}\alpha_i x^i \tag{4}$$

over $\mathbb{F}_{q^m}$ 称为彼此的 q-伴随多项式。更具体地说， $l(x)$ 是 $L(x)$的常规 q-伴随多项式，而 $L(x)$ 是 $l(x)$ 的线性化 q-伴随多项式。

引理 5。 *[23, 第 112–114]* 页设 $L(x)$ 是 $\mathbb{F}_{q^m}$上的线性化多项式。将其核记为

$$K=\ker L=\{x\in\mathbb{F}_{q^m}\mid L(x)=0\}.$$

核 K 构成一个 $\mathbb{F}_q$-线性子空间。设 维数$_{\mathbb{F}_q}K=t$。则 K 的基数满足$|K|=q^t$。此外，还具有以下性质。

1) 如果 α 属于 L的像集 $\mathrm{Im}(L)$ ，则方程 $L(x)=\alpha$ 恰有 q^t 个解。*2)* 如果 α 不包含于 $\mathrm{Im}(L)$中，则该方程无解。

下面的引理为确定线性化多项式的根的数量提供了一个有用工具。

引理6。 *[37]* 对于任意线性化多项式 L（x）$\in\mathbb{F}_{q^m}[x]$，记其伴随多项式为 l（x）。则 L（x）在 $\mathbb{F}_{q^m}$ 中的根的数量等于 q^ℓ，当且仅当 $\deg(\mathrm{gcrd}(l$（x） $x^m-1))=\ell$。

F. 自正交码与极小线性码

对于素数幂 q 和正整数 n，两个向量 $\boldsymbol{c}$ =(c_1，……， c_v) 和 $\boldsymbol{c}'$ =(c_1'，……， c_v') $\in\mathbb{F}_q^v$之间的（汉明）距离，是它们取值不同的坐标数。 q-元 $[v,\kappa,d]$码 $\mathcal{C}$ 是 $\mathbb{F}_q^v$ 的一个 κ维子空间，且最小距离为 d。 $\mathcal{C}$ 中的向量称为码字。 $\mathcal{C}$的对偶码记为 $\mathcal{C}^\perp$，定义为

$$\mathcal{C}^\perp:=\left\{x\in\mathbb{F}_q^v\mid x\cdot y=0 \text{ for all } y\in\mathcal{C}\right\},$$

这是一个 $[v,v-\kappa]$ 码，其中 $\cdot$ 表示标准点积。如果 $\mathcal{C}\subseteq\mathcal{C}^\perp$，则称 $\mathcal{C}$ 为自正交码，即对于任意码字 $\mathbf{a}$，$\mathbf{b}\in\mathcal{C}$，都有$\mathbf{a}\cdot\mathbf{b}=0$。特别地，如果 $\mathcal{C}=\mathcal{C}^\perp$，则称 $\mathcal{C}$ 为自对偶码。下面给出线性码成为自正交码的一个充分条件。

引理7。 *[16]* 设 $\mathcal{C}$ 是一个二元线性码。如果 $\mathcal{C}$ 中的每个码字的汉明重量都能被4整除，那么 $\mathcal{C}$ 是自正交的，即 $\mathcal{C}\subseteq\mathcal{C}^\perp$。

向量$\mathbf{u}$ =（u_1， u_2，……， u_v）的支集 $\in\mathbb{F}_q^v$，记作 Supp(u)，定义为其非零坐标的索引集合，即 Supp(u) $=\{1\le i\le v\mid u_i\neq 0\}$。如果 Supp(v) $\subseteq$ Supp(u)，则称向量$\mathbf{u}$ 覆盖另一个向量$\mathbf{v}$，记作$\mathbf{v}\preceq\mathbf{u}$。线性码 $\mathcal{C}$ 中的码字$\mathbf{c}$ 称为极小的，如果它所覆盖的唯一其他码字是其数量倍 $a\mathbf{c}$，且 $a\in\mathbb{F}_q$。如果线性码 $\mathcal{C}$ 中的每个码字都是极小的，则称该码极小。下面的定理给出了线性码为极小码的一个充分条件。

引理8。 *[7]* 设 $\mathcal{C}$ 是定义在 $\mathbb{F}_q$上的线性码。令 $w_{\min}$ 和 $w_{\max}$ 分别表示 $\mathcal{C}$中非零码字的最小汉明重量和最大汉明重量。若

$$\frac{w_{\min}}{w_{\max}}>\frac{q-1}{q}, \tag{5}$$

于是 $\mathcal{C}$ 是极小的。

G. 普莱斯幂矩

对于一个在 $\mathbb{F}_q$上的 $[v,\kappa,d]$ 线性码 $\mathcal{C}$，$\mathbf{c}_i=(c_1,\ c_2,\ \cdots,\ c_v)$ 的重量定义为非零 c_i的数量。用 A_i 表示 $\mathcal{C}$中重量为 i的码字数量，用 B_i 表示 $\mathcal{C}^{\perp}$中重量为 i 的码字数量。对于 $q=2$，前四个 Pless幂矩如下所示[16]:

$$\begin{aligned}
\sum_{j=0}^{v} A_j &= 2^{\kappa},\\
\sum_{j=0}^{v} jA_j &= 2^{\kappa-1}\left(v-B_1\right),\\
\sum_{j=0}^{v} j^2A_j &= 2^{\kappa-2}\left(v(v+1)-2(v+1)B_1+2B_2\right),\\
\sum_{j=0}^{v} j^3A_j &= 2^{\kappa-3}\left[v\left(v^2+3v-4\right)-\left(3v^2+3v-6\right)B_1+(3v-6)B_2-6B_3\right].
\end{aligned}$$

普莱斯幂矩为确定线性码对偶码的最小重量提供了一种强有力的工具。

III. 由 n-到-1 映射构造的新线性码族

本节采用三类 n-到-1映射（其中两类是新构造的，另一类是已知的），构造三个具有三种重量的自正交极小码族。

设 f 是一个从 $\mathbb{F}_{2^m}$ 到其自身的映射，且 $f(0)=0$。设 $\mathcal{C}_f$ 是方程（1）中定义的线性码。显然，$\mathcal{C}_f$ 的维数至多为 $2m$。为确定 $\mathcal{C}_f$的维数，只需计算满足对所有 $x\in\mathbb{F}_{2^m}$，$\mathrm{Tr}^{2^m/2}(ax+bf(x))$均为零的有序对$(a,\ b)$的个数。等价地，由于$f(0)=0$，我们有 $\dim(\mathcal{C}_f)=2m-\dim_{\mathbb{F}_2}(K_1)$，其中

$$K_1=\left\{(a,b)\in\mathbb{F}_{2^m}^2:W_f(a,b)=2^m\right\}. \tag{6}$$

码字的汉明重量$\mathbf{c}_{a,\ b}\in\mathcal{C}_f$ 由下式给出

$$\begin{aligned}
\mathrm{wt}(\mathbf{c}_{a,b}) &= \#\left\{x\in\mathbb{F}_{2^m}^*:\mathrm{Tr}_{2^m/2}(ax+bf(x))=1\right\}\\
&= 2^m-\#\left\{x\in\mathbb{F}_{2^m}:\mathrm{Tr}_{2^m/2}(ax+bf(x))=0\right\}\\
&= 2^m-\frac{1}{2}\sum_{x\in\mathbb{F}_{2^m}}\sum_{y\in\mathbb{F}_2}(-1)^{y\mathrm{Tr}_{2^m/2}(ax+bf(x))}\\
&= 2^{m-1}-\frac{1}{2}\sum_{x\in\mathbb{F}_{2^m}}(-1)^{\mathrm{Tr}_{2^m/2}(ax+bf(x))}\\
&= 2^{m-1}-\frac{1}{2}W_f(a,b),
\end{aligned} \tag{7}$$

其中，第三个等式源于加性特征的众所周知的正交关系 [23]。

下面，我们研究 $\mathcal{C}_f$的对偶码的最小距离，并证明对于 $m>1$，$\mathcal{C}_f$ 始终是一个射影码。

引理9。设 $f(x)$ 是一个从 $\mathbb{F}_{2^m}$到自身的函数，满足 $f(0)=0$对于 $m>1$成立。则$\mathcal{C}_f^{\perp}$的最小距离满足 $d\left(\mathcal{C}_f^{\perp}\right)\geq 3$。

证明。向量 $\boldsymbol{\omega}=(\omega_x)^{x\in\mathbb{F}_{2^m}^*}$ 属于 $\mathcal{C}_f^{\perp}$ 当且仅当

$$\sum_{x\in\mathbb{F}_{2^m}^*}\omega_x\,\mathrm{Tr}_{2^m/2}(ax+bf(x))=0,\quad \forall\, a,b\in\mathbb{F}_{2^m},$$

这等价于

$$\mathrm{Tr}_{2^m/2}\left(a\sum_{x\in\mathbb{F}_{2^m}^*}\omega_x x+b\sum_{x\in\mathbb{F}_{2^m}^*}\omega_x f(x)\right)=0 \tag{8}$$

对所有 $a,b\in\mathbb{F}_{2^m}$。注意 $\omega_x\in\{0,1\}$。假设 $\mathcal{C}_f^{\perp}$ 包含一个重量为一的码字。则存在 $x_0\in\mathbb{F}_{2^m}^*$ 使得 $\omega_{x_0}=1$ 且所有其他项均为零。方程（8）于是给出

$$\mathrm{Tr}_{2^m/2}\big(ax_0+bf(x_0)\big)=0 \text{ for all } a,b\in\mathbb{F}_{2^m}.$$

取 $b=0$，我们得到 $\mathrm{Tr}_{2^m/2}(ax_0)=0$ 对所有 $a\in\mathbb{F}_{2^m}$。等价地，$x_0\mathbb{F}_{2^m}\subseteq\ker(\mathrm{Tr}_{2^m/2})$，这是不可能的，因为 $\dim_{\mathbb{F}_2}\ker(\mathrm{Tr}_{2^m/2})=m-1<m$。现在假设 $\mathcal{C}_f^{\perp}$ 包含一个重量为二的码字，其支集为两个不同元素 $x_1,x_2\in\mathbb{F}_{2^m}^*$。方程（8）于是给出

$$\mathrm{Tr}_{2^m/2}\big(a(x_1+x_2)+b(f(x_1)+f(x_2))\big)=0,\ \forall\, a,b\in\mathbb{F}_{2^m}.$$

取 $b=0$，我们得到 $\mathrm{Tr}_{2^m/2}(a(x_1+x_2))=0$ 对所有 $a\in\mathbb{F}_{2^m}$。由于 $x_1\neq x_2$，我们有 $x_1+x_2\neq 0$。因此 $(x_1+x_2)\mathbb{F}_{2^m}\subseteq\ker(\mathrm{Tr}_{2^m/2})$，这是不可能的，因为 $\dim_{\mathbb{F}_2}\ker(\mathrm{Tr}_{2^m/2})=m-1<m$。consequently，$\mathcal{C}_f^{\perp}$ 不包含重量小于三的非零码字，因此 $d(\mathcal{C}_f^{\perp})\geq 3$。 □

A. $f(x)=\mathrm{Tr}^{q^l/q}\left(x^{2q+2}\right)+cx$的情形

在本小节中，我们研究线性码 $\mathcal{C}_f$，其中 $f(x)=\mathrm{Tr}_{q^l/q}\left(x^{2q+2}\right)+cx$，且 $c\in\mathbb{F}_q^*$为偶正整数，$q=2^k$为奇正整数。首先，我们证明 $f(x)$是一个四对一映射或置换多项式。

定理1。设 $q=2^k$ 为偶正整数，且设 l 为奇正整数。定义$f(x)=\mathrm{Tr}_{q^l/q}\left(x^{2q+2}\right)+cx$，其中 $c\in\mathbb{F}_q^*$。则以下结论成立。

1) 若 $c^{\frac{q-1}{3}}=1$，则 $f(x)$是 $\mathbb{F}_{q^l}$上的一个4对1映射。*2)* 若 $c^{\frac{q-1}{3}}\neq 1$，则 $f(x)$是 $\mathbb{F}_{q^l}$上的一个置换多项式。

证明。我们分析方程 $f(x)=e$ 的解，即

$$\mathrm{Tr}_{q^l/q}\left(x^{2q+2}\right)+cx=e \tag{9}$$

对于任意元素 $e\in\mathbb{F}_{q^l}$。令 $u:=cx+e$。则方程（9）推出 $u=\mathrm{Tr}^{q^l/q}(x^{2q+2})\in\mathbb{F}_q$以及当 $c\neq 0$时—的 $x=\frac{u+e}{c}$。由于 $u\in\mathbb{F}_q$ 和 $c\in\mathbb{F}_q^*$，因此

$$x^{2q+2}=\left(\frac{u+e}{c}\right)^{2q+2}=\frac{u^4+\left(e^2+e^{2q}\right)u^2+e^{2q+2}}{c^4}.$$

将其代入方程（9）并应用引理 2，我们得到

$$u=\frac{u^4+\left(e^2+e^{2q}\right)u^2+e^{2q+2}}{c^4}=\frac{u^4}{c^4}+\mathrm{Tr}_{q^l/q}\left(e^2+e^{2q}\right)\frac{u^2}{c^4}+\frac{\mathrm{Tr}_{q^l/q}\left(e^{2q+2}\right)}{c^4}.$$

重新整理上述方程可得关于 u 的四次方程:

$$u^4+c^4u+\mathrm{Tr}_{q^l/q}\left(e^{2q+2}\right)=0.$$

由于 u^4+c^4u 是一个 $\mathbb{F}_2$-线性化多项式，引理 5 表明，方程 $u^4+c^4u+\mathrm{Tr}_{q^l/q}\left(e^{2q+2}\right)=0$ 的解的个数只有两种可能：要么无解，要么其解的个数等于齐次方程 $u^4+c^4u=0$ 的解的个数。因此，接下来只需研究 $u^4+c^4u=0$ 在 $\mathbb{F}_q$ 中的解。显然，$u=0$ 是 $u^4+c^4u=0$ 的平凡解。对于$u\in\mathbb{F}_q^*$，我们有 $u^3+c^4=0$，当且仅当 c^4 是 $\mathbb{F}_q^*$ 中的立方元时，该方程才有解。由于 k 是偶数，我们有 $3\mid 2^k-1$，这意味着 $\mathbb{F}_q^*$ 中存在一个三次子群。因此，如果 c^4 是一个

$\mathbb{F}_q^*$中的立方剩余，则方程 $u^3+c^4=0$ 在 $\mathbb{F}_q^*$中有三个不同的非零解；若 c^4 不是 $\mathbb{F}_q^*$中的立方剩余，则方程 $u^3+c^4=0$ 没有非零解。令 N 表示方程 $u^4+c^4u+\mathrm{Tr}^{q^l/q}(e^{2q+2})=0$ 在 $\mathbb{F}_q$中的不同根的数量。基于以上讨论，我们推导出

$$N=\begin{cases}1 & \text{if } c^{\frac{4(q-1)}{3}}\neq 1,\\ 4 & \text{if } c^{\frac{4(q-1)}{3}}=1.\end{cases}$$

注意，$c^{\frac{4(q-1)}{3}}=1$ 当且仅当。由于映射 $u=cx+e$ 是仿射变换，$\mathbb{F}_{q^l}$ 中 $f(x)$ 的解的数量与上述情况相同。 □

注记 1. 在定理*1*中，我们假设 l 为奇数且 k 为偶数。若 l 为奇数，$c^{\frac{q-1}{3}}\neq 1$, k 为偶数，且 $k\neq 0$ (模 3)，则已在 *[20,* 定理 *3.4]* 中证明，$f(x)$ 是 $\mathbb{F}_{q^l}$的置换。然而，定理*1*的第 *2)* 条并无 $k\neq 0$(模 3)的限制。此外，我们还研究了 l为奇数、 k为偶数且 $c^{\frac{q-1}{3}}=1$的情况。若 l为偶数且 $c\in\mathbb{F}_{q^2}^*$，则 $f(x)$是 $\mathbb{F}_{q^l}$的置换，这已在 *[20,*定理 *3.1]*中证明。

现在我们研究由 n-to-1 映射 $f(x)$ 构造的 $\mathcal{C}_f$ 的参数、重量分布、极小性和自正交性。为此，我们需要以下引理。

引理10. 设 $m=lk$ *and* $q=2^k$，其中 l 是奇数正整数，且 k 是正整数。那么有

$$\dim_{\mathbb{F}_2}(\ker(L_b))=k,$$

其中 $L_b(y):=\mathrm{Tr}^{2^m/2^k}(b)y^2+\mathrm{Tr}^{2^m/2^k}(b)y^{2q^2}$，其中 $\mathrm{Tr}^{2^m/2^k}(b)\neq 0$ 是关于$y\in\mathbb{F}_{2^m}$的 2-线性化多项式。

证明. $L_b(y)$ 的传统2伴随多项式为 $l_{a,b}(y)=\mathrm{Tr}^{2^m/2^k}(b)y+\mathrm{Tr}^{2^m/2^k}(b)y^{2k+1}$。根据引理6，我们需要确定

$$\mathrm{gcrd}\left(\mathrm{Tr}_{2^m/2^k}(b)y^{2k+1}+\mathrm{Tr}_{2^m/2^k}(b)y, y^{kl}-1\right).$$

设 $B:=\mathrm{Tr}^{2^m/2^k}(b)$ 和 $l=2t+1$。注意到 $y^{lk}-1=y^{lk}+1$。那么我们有一个右除法:

$$y^{kl}+1=\left(B^{-1}\right)^{2^{k(l-2)}-1}y^{k(l-2)-1}\left(By^{2k+1}+By\right)+y^{k(l-2)}+1.$$

由于 $y^{k(l-2)}+1$ 的次数不小于 $2k+1$，我们需要继续应用右除法算法，直到余式的次数不超过 $2k$。我们得到

$$\begin{aligned}
y^{k(l-2)}+1 &= \left(B^{-1}\right)^{2^{k(l-4)}-1}y^{k(l-4)-1}\left(By^{2k+1}+By\right)+y^{k(l-4)}+1,\\
y^{k(l-4)}+1 &= \left(B^{-1}\right)^{2^{k(l-6)}-1}y^{k(l-6)-1}\left(By^{2k+1}+By\right)+y^{k(l-6)}+1,\\
&\vdots\\
y^{5k}+1 &= \left(B^{-1}\right)^{2^{3k}-1}y^{3k-1}\left(By^{2k+1}+By\right)+y^{3k}+1,\\
y^{3k}+1 &= \left(B^{-1}\right)^{2^{k}-1}y^{k-1}\left(By^{2k+1}+By\right)+y^{k}+1.
\end{aligned}$$

于是，我们得到最终表达式

$$y^{kl}+1=\sum_{i=1}^{t}\left(B^{-1}\right)^{2^{k(l-2i)-1}}y^{k(l-2i)-1}\left(By^{2k+1}+By\right)+y^k+1.$$

类似地，我们有

$$\begin{aligned}
By^{2k+1}+By &= By^{k+1}\left(y^k+1\right)+By^{k+1}+By,\\
By^{k+1}+By &= By\left(y^k+1\right).
\end{aligned}$$

由此我们得出结论:

$$\gcd\left(\mathrm{Tr}_{2^m/2^k}(b)y^{2k+1}+\mathrm{Tr}_{2^m/2^k}(b)y,\ y^{kl}-1\right)=y^k+1.$$

最后，由引理6可得所需结论。 □

定理 2。 设 $f(x)=\mathrm{Tr}^{q^l/q}\left(x^{2q+2}\right)+cx\in\mathbb{F}_{q^l}[x]$，其中 $q=2^k$, l 为奇数， k 为正整数，且$c\in\mathbb{F}_q^*$。设 $m=kl$。则 $\mathcal{C}_f$ 是一个二元线性码，其参数为

$$\left[2^{lk}-1,\ k(l+1),\ 2^{lk-1}-2^{\frac{lk+k}{2}-1}\right]$$

其重量分布见表 I。若 $k(l-1)\geq 4$，则 $\mathcal{C}_f$ 是极小码。若 $k(l+1)\geq 6$，则 $\mathcal{C}_f$ 是自正交码。

表 I: 定理 2 中 $\mathcal{C}_f$ 的重量分布

重量	频数
0	1
$2^{kl-1}-2^{\frac{kl+k}{2}-1}$	$2^{\frac{kl+k}{2}-1}-2^{\frac{kl-k}{2}-1}+2^{kl-1}-2^{kl-k-1}$
2^{kl-1}	$2^{kl-k}+2^{kl+k}-2^{kl}-1$
$2^{kl-1}+2^{\frac{kl+k}{2}-1}$	$2^{\frac{kl-k}{2}-1}-2^{\frac{kl+k}{2}-1}+2^{kl-1}-2^{kl-k-1}$

证明。 根据公式（7），我们首先需要计算任意 $a,b\in\mathbb{F}_{2^m}$ 对应的 Walsh 变换 $W_f(a,b)$。我们有

$$W_f(a,b)=\sum_{x\in\mathbb{F}_{2^m}}(-1)^{\mathrm{Tr}_{2^m/2}\left(ax+b\left(\mathrm{Tr}_{2^m/2^k}\left(x^{2q+2}\right)+cx\right)\right)}=\sum_{x\in\mathbb{F}_{2^m}}(-1)^{\mathrm{Tr}_{2^m/2}(Q(x))},$$

其中 $Q(x):=ax+b\left(\mathrm{Tr}^{2^m/2^k}\left(x^{2q+2}\right)+cx\right)$。现在我们化简 $\mathrm{Tr}^{2^m/2}(Q(x))$:

$$\begin{aligned}
&\mathrm{Tr}_{2^m/2}(Q(x))\\
=\ &\mathrm{Tr}_{2^m/2}\left(ax+b\left(\mathrm{Tr}_{2^m/2^k}\left(x^{2q+2}\right)+cx\right)\right)\\
=\ &\mathrm{Tr}_{2^m/2}\left(ax+bcx+bx^{2q+2}+\left(b^{\frac{1}{q}}x^{2q+2}\right)^q+\cdots+\left(b^{\frac{1}{q^{l-1}}}x^{2q+2}\right)^{q^{l-1}}\right)\\
=\ &\mathrm{Tr}_{2^m/2}\left((a+bc)x+\left(b+b^{\frac{1}{q}}+\cdots+b^{\frac{1}{q^{l-1}}}\right)x^{2q+2}\right)\\
=\ &\mathrm{Tr}_{2^m/2}\left((a+bc)x+\mathrm{Tr}_{2^m/2^k}\left(b^{\frac{1}{q^{l-1}}}\right)x^{2q+2}\right)\\
=\ &\mathrm{Tr}_{2^m/2}\left((a+bc)x+\mathrm{Tr}_{2^m/2^k}(b)\,x^{2q+2}\right).
\end{aligned}$$

如果 $\mathrm{Tr}^{2^m/2^k}(b)=0$，那么我们有

$$W_f(a,b)=\sum_{x\in\mathbb{F}_{2^m}}(-1)^{\mathrm{Tr}_{2^m/2}((a+bc)x)}=\begin{cases}2^m & \text{if } a+bc=0,\\ 0 & \text{if } a+bc\neq 0.\end{cases}$$

若 $\mathrm{Tr}^{2^m/2^k}(b)\neq 0$，则 $\varphi_{a,\ b}(x):=\mathrm{Tr}^{2^m/2}(Q(x))$ 的双线性形式为

$$\begin{aligned}
&B_{\varphi_{a,b}}(x,y)\\
=\ &\varphi_{a,b}(x+y)+\varphi_{a,b}(x)+\varphi_{a,b}(y)\\
=\ &\mathrm{Tr}_{2^m/2}\left(\mathrm{Tr}_{2^m/2^k}(b)x^{2q}y^2+\mathrm{Tr}_{2^m/2^k}(b)x^2y^{2q}\right)\\
=\ &\mathrm{Tr}_{2^m/2}\left(\left(\left(\mathrm{Tr}_{2^m/2^k}(b)\right)^q y^{2q^2}+\mathrm{Tr}_{2^m/2^k}(b)y^2\right)x^{2q}\right)\\
=\ &\mathrm{Tr}_{2^m/2}\left(L_b(y)x^{2q}\right),
\end{aligned}$$

其中 $L_b(y) = \mathrm{Tr}^{2^m/2^k}(b)y^2 + \mathrm{Tr}^{2^m/2^k}(b)y^{2q^2}$。记

$$V_{\varphi_b} = \ker(L_b) = \{y \in \mathbb{F}_{2^m} : L_b(y) = 0\}.$$

根据引理10，我们有 $\dim_{\mathbb{F}_2}(V_{\varphi_b}) = k$。应用引理4，我们随后推得，当 $\mathrm{Tr}^{2^m/2^k}(b) \neq 0$ 时，$W_f(a, b) \in \left\{0, \pm 2^{\frac{m+k}{2}}\right\}$。综合这两种情况，对于所有 $a, b \in \mathbb{F}_{2^m}$，我们得到 $W_f(a, b) \in \left\{0, \overline{2^m}, \pm 2^{\frac{m+k}{2}}\right\}$。

回顾一下，$\dim(\mathcal{C}_f) = 2m - \dim_{\mathbb{F}_2}(K_1)$，其中 K_1 在公式（6）中定义。注意，$W_f(a, b) = 2^m$ 当且仅当 $a + bc = 0$ 且 $\mathrm{Tr}^{2^m/2^k}(b) = 0$，这得到 2^{m-k} 解对 (a, b)。于是 $\dim_{\mathbb{F}_2}(K_1) = m - k$，因此 $\dim(\mathcal{C}_f) = m + k$。

由公式（7），我们有

$$\mathrm{wt}(\mathbf{c}_{a,b}) \in \left\{2^{m-1},\ 0,\ 2^{m-1} - 2^{\frac{m+k}{2}-1},\ 2^{m-1} + 2^{\frac{m+k}{2}-1}\right\}.$$

根据引理9和前三个Pless幂矩，我们可以容易地得到 $\mathcal{C}_f$ 在表I中的重量分布。

根据引理8，将最小非零重量 $w_{\min} = 2^{kl-1} - 2^{\frac{kl+k}{2}-1}$ 和最大非零重量 $w_{\max} = 2^{kl-1} + 2^{\frac{kl+k}{2}-1}$ 代入公式（5），我们推得，当 $k(l-1) \geq 4$ 时，$\mathcal{C}_f$ 是极小的。根据引理7，我们进一步推得，当 $k(l+1) \geq 6$ 时，$\mathcal{C}_f$ 是自正交的。 □

B. $f(x) = cx + \mathrm{Tr}^{q^2/q}(x^6 + x^{2q+4})$ 的情形

在本小节中，我们研究由函数 $f(x) = \mathrm{Tr}_{q^2/q}\left(x^6 + x^{2q+4}\right) + cx$ 构造的 $\mathcal{C}_f$ 的参数、重量分布、极小性和自正交性，其中 $c \in \mathbb{F}_q^*$ 和 $q = 2^k$，且 k 为奇数正整数。根据引理1，在一定条件下，该映射在 $\mathbb{F}_{q^2}$ 上是2-1映射。为了陈述主要结果，我们需要以下引理。

引理 11。设 $m = 2k$ 和 $q = 2^k$，其中 k 是奇数正整数。则有

$$\dim_{\mathbb{F}_2}(\ker(L_b)) = k + 1,$$

其中 $L_b(y) := \left(b^{2^{k+1}} + b^2\right) y^{2^{k+3}} + \left(b^{2^k} + b\right) y^{2^{k+1}} + \left(b^{2^{k+1}} + b^2\right) y^{2^3} + \left(b^{2^k} + b\right) y^2$ 是一个 2-线性化多项式，并且对于 $y \in \mathbb{F}_{2^m}$ 有 $b^{2^{k+1}} + b^2 \neq 0$。

证明。( ) 的传统 2 $L_b\ y$ $l_b\ y = \left(b^{2^{k+1}} + b^2\right) y^{k+3} + \left(b^{2^k} + b\right) y^{k+1} +$ - $\left(b^{2^{k+1}} + b^2\right) y^3 + \left(b^{2^k} + b\right) y$ 6,

伴随式为 ( )。根据引理，我们需要确定

$$\mathrm{gcrd}\left(l_b(y), y^{2^k} - 1\right).$$

注意到 $y^{2^k} - 1 = \left(y^k + 1\right)^2$。令 $A := b^{2^k} + b$ 且 $k = 2t + 1$。则 $l_b(y) = A^2 y^{k+3} + A y^{k+1} + A^2 y^3 + A y$。我们有

$$A^2 y^{k+3} + A y^{k+1} + A^2 y^3 + A y = A^2 y^3 \left(y^k + 1\right) + A y^{k+1} + A y.$$

由于 $A y^{k+1} + A y$ 的次数不小于 k，我们必须继续应用右除法算法，直到余式的次数不超过 $k - 1$。由于

$$A y^{k+1} + A y = A y \left(y^k + 1\right),$$

我们得到如下表达式

$$l_b(y) = \left(A^2 y^3 + A y\right) \left(y^k + 1\right).$$

因此，我们有

$$\mathrm{gcrd}\left(l_b(y), y^{2^k} - 1\right) = \mathrm{gcrd}\left(\left(A^2 y^3 + A y\right), y^k + 1\right) \left(y^k + 1\right).$$

接下来，只需确定最大公因子 $\left(A^2y^3+Ay,\ y^k+1\right)$。我们进行右除法:

$$y^k+1=\left(A^{-2}\right)^{2^{k-3}}y^{k-3}\left(A^2y^3+Ay\right)+\left(A^{-1}\right)^{2^{k-3}}y^{k-2}+1.$$

类似地，通过进行右除法，直到余式的次数小于 3，我们得到

$$\begin{aligned}y^k+1=&\left(\sum_{i=1}^{t}\left(\prod_{j=1}^{i-1}\left(A^{-1}\right)^{2^{k-2j-1}}\right)\left(A^{-2}\right)^{2^{k-2i-1}}y^{k-2i-1}\right)\left(A^2y^3+Ay\right)\\&+\left(A^{-1}\right)^{2^{k-3}+\cdots+2^{k-2t-1}}y+1.\end{aligned}\tag{10}$$

这些步骤容易引起混淆，因此我们将详细阐述证明。记 $2^{k-3}+\cdots+2^{k-2t-1}=2^{\frac{2^{k-1}-1}{3}}=s$，则

$$A^2y^3+Ay\ =\ \left(A^{2+4s}y^2+A^{2+4s}A^{2s}y\right)\left(\left(A^{-1}\right)^s y+1\right)+\left(A^{2^k}+A\right)y.\tag{11}$$

由于 $A=b^{2^k}+b$ 和 $A^{2^k}=b+b^{2^k}$，因此我们有 $A^{2^k}+A=0$。结合方程 (10) 和 (11) 得到

$$\operatorname{gcrd}\left(A^2y^3+Ay,y^k+1\right)=\left(A^{-1}\right)^s y+1.$$

最后，我们得出

$$\operatorname{gcrd}\left(l_b(y),y^{2k}-1\right)=\left(\left(A^{-1}\right)^s y+1\right)\left(y^k+1\right).$$

根据引理6，所需结论得证。 □

定理 3. 设 $f(x)=\mathrm{Tr}^{q^2/q}\left(x^6+x^{2q+4}\right)+cx\in\mathbb{F}_{q^2}[x]$，其中 $q=2^k$，k 为奇数，且 $c\in\mathbb{F}_q^*$。令$m=2k$。则 $\mathcal{C}_f$ 是一个参数为

$$\left[2^{2k}-1,3k,2^{2k-1}-2^{\frac{3k+1}{2}-1}\right]$$

以及表 *II* 中的重量分布。若 $k\geq 5$，则 $\mathcal{C}_f$ 是极小的。若 $k\geq 3$，则 $\mathcal{C}_f$ 是自正交的。

表 II：定理 3 中 $\mathcal{C}_f$ 的重量分布

Weight	Frequency
0	1
$2^{2k-1}-2^{\frac{3k+1}{2}-1}$	$2^{2k-2}+2^{\frac{3k-1}{2}-1}-2^{k-2}-2^{\frac{k-1}{2}-1}$
2^{2k-1}	$2^{3k}-2^{2k-1}+2^{k-1}-1$
$2^{2k-1}+2^{\frac{3k+1}{2}-1}$	$2^{2k-2}-2^{\frac{3k-1}{2}-1}-2^{k-2}+2^{\frac{k-1}{2}-1}$

证明。 根据公式（7），我们首先需要计算任意 $a,b\in\mathbb{F}_{2^m}$ 的 Walsh变换 $W_f(a,b)$。我们有

$$\begin{aligned}W_f(a,b)\ &=\ \sum_{x\in\mathbb{F}_{2^m}}(-1)^{\mathrm{Tr}_{2^m/2}\left(ax+b\left(\mathrm{Tr}_{q^2/q}\left(x^6+x^{2q+4}\right)+cx\right)\right)}\\&=\ \sum_{x\in\mathbb{F}_{2^m}}(-1)^{\mathrm{Tr}_{2^m/2}(Q(x))},\end{aligned}$$

其中 $Q(x):=ax+b\left(\mathrm{Tr}^{q^2/q}\left(x^6+x^{2q+4}\right)+cx\right)$。现在我们来简化 $\mathrm{Tr}^{2^m/2}(Q(x))$:

$$\begin{aligned}&\mathrm{Tr}_{2^m/2}(Q(x))\\=\ &\mathrm{Tr}_{2^m/2}\left(ax+b\left(\mathrm{Tr}_{2^m/2^k}\left(x^6+x^{2q+4}\right)+cx\right)\right)\\=\ &\mathrm{Tr}_{2^m/2}\left(ax+bcx+bx^6+bx^{6q}+bx^{2q+4}+bx^{4q+2}\right)\\=\ &\mathrm{Tr}_{2^m/2}\left((a+bc)x+bx^{2^2+2}+b^{2^k}x^{2^2+2}+bx^{2^{k+1}+2^2}+b^{2^k}x^{2^{k+1}+2^2}\right)\\=\ &\mathrm{Tr}_{2^m/2}\left((a+bc)x+\left(b^{2^k}+b\right)x^{2^2+2}+\left(b^{2^k}+b\right)x^{2^{k+1}+2^2}\right).\end{aligned}$$

如果 $b^{2^k}+b=0$，那么我们有

$$W_f(a,b)=\sum_{x\in\mathbb{F}_{2^m}}(-1)^{\mathrm{Tr}_{2^m/2}((a+bc)x)}=\begin{cases}2^m & \text{if } a+bc=0,\\ 0 & \text{if } a+bc\neq 0.\end{cases}$$

若 $b^{2^k}+b\neq 0$，则 $\varphi_{a,b}(x):=\mathrm{Tr}^{2^m/2}(Q(x))$ 的双线性形式为

$$\begin{aligned}
& B_{\varphi_{a,b}}(x,y)\\
= \;& \varphi_{a,b}(x+y)+\varphi_{a,b}(x)+\varphi_{a,b}(y)\\
= \;& \mathrm{Tr}_{2^m/2}\left(\left(b^{2^k}+b\right)x^{2^2}y^2+\left(b^{2^k}+b\right)x^2y^{2^2}+\left(b^{2^k}+b\right)x^{2^{k+1}}y^4+\left(b^{2^k}+b\right)x^4y^{2^{k+1}}\right)\\
= \;& \mathrm{Tr}_{2^m/2}\left(\left(\left(b^{2^k}+b\right)y^{2^{k+1}}+\left(b^{2^{k+1}}+b^2\right)y^{2^{k+3}}+\left(b^{2^{k+1}}+b^2\right)y^{2^3}+\left(b^{2^k}+b\right)y^2\right)x^{2^{k+2}}\right)\\
= \;& \mathrm{Tr}_{2^m/2}\left(L_b(y)x^{2^{k+2}}\right),
\end{aligned}$$

其中 $L_b(y)=\left(b^{2^k}+b\right)y^{2^{k+1}}+\left(b^{2^{k+1}}+b^2\right)y^{2^{k+3}}+\left(b^{2^{k+1}}+b^2\right)y^{2^3}+\left(b^{2^k}+b\right)y^2$。记

$$V_{\varphi_b}=\ker\left(L_b\right)=\left\{y\in\mathbb{F}_{2^m}:L_b(y)=0\right\},$$

由引理11，$\mathbb{F}_2$ V_{φ_b} $=k+1$ 4，W_f a b $\in$可 $\left\{0\ \pm 2^{\frac{m+k+1}{2}}\right\}$ $b^{2^k}+b\neq 0$ W_f a b $\in\left\{0\ 2^m\ \pm 2^{\frac{m+k+1}{2}}\right\}$得 dim ( ) 。应用引理，我们进而推出 (,) ,当.....时。综合这两种情况，对于所有 $a,b\in\mathbb{F}_{2^m}$，可得 (,) ,,。

回想一下，$\dim(\mathcal{C}_f)=2m-\dim_{\mathbb{F}_2}(K_1)$，其中 K_1 由公式（6）定义。注意，$W_f(a,\ b)=2^m$ 当且仅当 $a+bc=0$ 且 $\mathrm{Tr}^{2^m/2^k}(b)=0$，由此得到 2^{m-k} 个解对（$a,\ b$）。于是 $\dim_{\mathbb{F}_2}(K_1)=m-k$，因此 $\dim(\mathcal{C}_f)=m+k$。

由公式（7），我们有

$$\mathrm{wt}(\mathbf{c}_{a,b})\in\left\{2^{m-1},\ 0,\ 2^{m-1}-2^{\frac{m+k+1}{2}-1},\ 2^{m-1}+2^{\frac{m+k+1}{2}-1}\right\}.$$

根据引理9和前三个Pless幂矩，我们可以轻松得到 $\mathcal{C}_f$ 的重量分布，如表II所示。

根据引理8，将最小非零重量 $w_{\min}=2^{2k-1}-2^{\frac{3k+1}{2}-1}$和最大非零重量 $w_{\max}=2^{2k-1}+2^{\frac{3k+1}{2}-1}$代入公式（5），可推得当 $k\geq 5$时，$\mathcal{C}_f$是极小的。根据引理7，我们进一步推得，只要 $k\geq 2$，$\mathcal{C}_f$ 就是自正交的。

证明完毕。 □

C. f（x）$=\mathrm{Tr}_{q^l/q}\left(c_1x+c_2x^{\frac{q+q^2}{2}}\right)+c_3x^{2^i}$的情形

在本小节中，我们研究 $\mathcal{C}_f$for $f(x)=\mathrm{Tr}_{q^l/q}\left(c_1x+c_2x^{\frac{q+q^2}{2}}\right)+c_3x^{2^i}$ 的线性码，其中 $i\in\mathbb{Z}$、$c_1\in\mathbb{F}_{q^l}$ $c_2\in\mathbb{F}_q$ $c_3\in\mathbb{F}_q^*$ f x q 1，以及。在本节中，我们首先证明 ( ) 要么是一个 -to- 映射、一个 $2^{\gcd(i,k)}$-to-1 映射，要么是一个置换多项式，然后利用 $f(x)$ 构造一个具有三个非零重量的线性码族。

定理4。设 $q=2^k$，其中 k是一个正整数。定义 $f(x)=\mathrm{Tr}_{q^l/q}\left(c_1x+c_2x^{\frac{q+q^2}{2}}\right)+c_3x^{2^i}$，其中 $i\in\mathbb{Z}$且 $c_1\in\mathbb{F}_{q^l}$、$c_2\in\mathbb{F}_q$、$c_3\in\mathbb{F}_q^*$。则以下结论成立。***(1)*** 若 $\mathrm{Tr}^{q^l/q}(c_1)=lc_2$，则 $f(x)$ 是 $\mathbb{F}_{q^l}$上的置换多项式。

(2) 若 $\mathrm{Tr}^{q^l/q}(c_1) \neq lc_2$，则 $f(x)$ 如下：

$$\begin{cases} \textit{a } q\textit{-to-}1 \textit{ mapping over } \mathbb{F}_{q^l} & \textit{if } i=0 \textit{ and } c_3+\mathrm{Tr}_{q^l/q}(c_1)+lc_2=0, \\ \textit{a permutation polynomial over } \mathbb{F}_{q^l} & \textit{if } i=0 \textit{ and } c_3+\mathrm{Tr}_{q^l/q}(c_1)+lc_2\neq 0, \\ \textit{a } 2^{\gcd(i,k)}\textit{-to-}1 \textit{ mapping over } \mathbb{F}_{q^l} & \textit{if } i>0 \textit{ and } \left(\dfrac{lc_2+\mathrm{Tr}_{q^l/q}(c_1)}{(c_3)^{1/2^i}}\right)^{\frac{2^m-1}{\gcd(2^i-1,\,2^m-1)}}=1, \\ \textit{a permutation polynomial over } \mathbb{F}_{q^l} & \textit{if } i>0 \textit{ and } \left(\dfrac{lc_2+\mathrm{Tr}_{q^l/q}(c_1)}{(c_3)^{1/2^i}}\right)^{\frac{2^m-1}{\gcd(2^i-1,\,2^m-1)}}\neq 1. \end{cases}$$

证明。我们分析方程 $f(x)=e$ 对所有 $e\in\mathbb{F}_{q^l}$ 的解。令 $u:=c_3x^{2^i}+e$，$\mathrm{Tr}^{q^l/q}\left(c_1x+c_2x^{\frac{q^2+q}{2}}\right)\in\mathbb{F}_q$。由于 $c_3\neq 0$，有 $x=\left(\frac{u+e}{c_3}\right)^{\frac{1}{2^i}}$。由于 $u,\ c_2\in\mathbb{F}_q,\ c_3\in\mathbb{F}_q^*$，我们得到

$$x^{\frac{q^2+q}{2}} = \left(\frac{u+e}{c_3}\right)^{\frac{q^2+q}{2^{i+1}}} = \left(\frac{u^2+\left(e^{q^2}+e^q\right)u+e^{q^2+q}}{(c_3)^2}\right)^{\frac{1}{2^{i+1}}}.$$

将上述表达式代入 $f(x)=e$，得到

$$\begin{aligned} u = & \mathrm{Tr}_{q^l/q}\left(c_2\left(\frac{u^2+\left(e^{q^2}+d^q\right)u+e^{q^2+q}}{(c_3)^2}\right)^{\frac{1}{2^{i+1}}}+c_1\left(\frac{u+e}{c_3}\right)^{\frac{1}{2^i}}\right) \\ = & \frac{\mathrm{Tr}_{q^l/q}(c_1)}{(c_3)^{\frac{1}{2^i}}}u^{\frac{1}{2^i}}+\frac{\mathrm{Tr}_{q^l/q}\left(c_1e^{\frac{1}{2^i}}\right)}{(c_3)^{\frac{1}{2^i}}}+\frac{lc_2}{(c_3)^{\frac{1}{2^i}}}u^{\frac{1}{2^i}}+\frac{c_2\left(\mathrm{Tr}_{q^l/q}\left(e^{q^2}+e^q\right)\right)^{\frac{1}{2^{i+1}}}}{(c_3)^{\frac{1}{2^i}}}u+\frac{c_2\mathrm{Tr}_{q^l/q}\left(e^{\frac{q^2+q}{2^{i+1}}}\right)}{(c_3)^{\frac{1}{2^i}}} \\ = & \frac{lc_2+\mathrm{Tr}_{q^l/q}(c_1)}{(c_3)^{\frac{1}{2^i}}}u^{\frac{1}{2^i}}+\frac{\mathrm{Tr}_{q^l/q}\left(c_1e^{\frac{1}{2^i}}\right)}{(c_3)^{\frac{1}{2^i}}}+\frac{c_2\mathrm{Tr}_{q^l/q}\left(e^{\frac{q^2+q}{2^{i+1}}}\right)}{(c_3)^{\frac{1}{2^i}}}. \end{aligned}$$

由于最大公因数 $\left(2^i,\ 2^k-1\right)=1$，映射 $u\to u^{2^i}$ 在 $\mathbb{F}_{2^k}$ 上是双射，且该变换保持原函数的根的数量不变。然后重新整理方程（12）得到

$$u^{2^i} = \frac{lc_2+\mathrm{Tr}_{q^l/q}(c_1)}{(c_3)^{\frac{1}{2^i}}}u+\frac{\mathrm{Tr}_{q^l/q}\left(c_1e^{\frac{1}{2^i}}\right)}{(c_3)^{\frac{1}{2^i}}}+\frac{c_2\mathrm{Tr}_{q^l/q}\left(e^{\frac{q^2+q}{2^{i+1}}}\right)}{(c_3)^{\frac{1}{2^i}}}. \tag{12}$$

现在我们考虑以下情况。

情形 1 $i=0$。

方程（12）可改写为

$$\left(c_3+\mathrm{Tr}_{q^l/q}(c_1)+lc_2\right)u+\mathrm{Tr}_{q^l/q}(c_1e)+c_2\mathrm{Tr}_{q^l/q}\left(e^{\frac{q^2+q}{2}}\right)=0. \tag{13}$$

由上述关系可知，若 $c_3+\mathrm{Tr}^{q^l/q}(c_1)+lc_2=0$，则对所有 $u\in\mathbb{F}_q$，方程（13）在 $\mathrm{Tr}^{q^l/q}\ c_1e\ +c_2$ —— $f\ x$ q $\mathrm{Tr}^{q^l/q}\ c_1e\ +()\ \mathrm{Tr}$ c_2 $\mathrm{Tr}^{q^l/q}\left(e^{\frac{q^2+q}{2}}\right)$ —— 0 时均成立，且 $()$ 有不同的解。当 $\mathrm{Tr}\ ()\ \mathrm{Tr}^{q^l/q}\left(e^{\frac{q^2+q}{2}}\right)\neq 0$ 时，方程（）不成立，且 $()$ 无解。因此，$()$ 是一个 -to- 映射。若 $c_3+\mathrm{Tr}^{q^l/q}(c_1)+lc_2\neq 0$，则方程（13）恰有一个解，因此 $f(x)$ 是 $\mathbb{F}_{q^l}$ 上的置换多项式。

情形 2 $i>0$。

由于 l 是偶整数，方程（12）可以重排为

$$(c_3)^{\frac{1}{2^i}} u^{2^i} + \mathrm{Tr}_{q^l/q}(c_1)\, u + \mathrm{Tr}_{q^l/q}\left(c_1 e^{\frac{1}{2^i}}\right) + c_2 \mathrm{Tr}_{q^l/q}\left(e^{\frac{q^2+q}{2^{i+1}}}\right) = 0. \tag{14}$$

根据引理 5，方程（14）在 $\mathbb{F}_{2^k}$ 中的解数只有两种可能：要么无解，要么其解数等于齐次方程的解数

$$(c_3)^{\frac{1}{2^i}} u^{2^i} + \mathrm{Tr}_{q^l/q}(c_1)\, u = 0. \tag{15}$$

方程（15）得出 $u = 0$ 或

$$u^{2^i-1} = \frac{\mathrm{Tr}_{q^l/q}(c_1)}{(c_3)^{\frac{1}{2^i}}}. \tag{16}$$

若 $\mathrm{Tr}_{q^l/q}(c_1) = 0$，则方程（15）恰有一个解 $u = 0$。因此，$f(x)$ 是一个置换多项式。若 $\mathrm{Tr}_{q^l/q}(c_1) \neq 0$ 且 $\left(\mathrm{Tr}_{q^l/q}\left(c_1^{\frac{1}{2^i}}\right)\right)^{\frac{2^m-1}{2^i-1}} (c_3)$ 最大公因数$\left(,2^m-1\right) = 1$，则方程（16）有 $\gcd\left(2^i-1, 2^k-1\right)$ 个不同的非零解，这意味着 $f(x)$ 是一个 $2^{\gcd(i.k)}$-对-1 映射。若 $\left(\mathrm{Tr}_{q^l/q}\left(c_1^{\frac{1}{2^i}}\right)\right)^{\gcd\left(2^i-1\right)} (c_3)^{\frac{2^m-1}{2^m-1}}, 2^m-1\right) \neq 1$ 且 $\mathrm{Tr}_{q^l/q}(c_1) \neq 0$，则方程（16）无解，这意味着 $f(x)$ 是一个置换多项式。

当 l 是奇数正整数时，方程（12）可重写为

$$(c_3)^{\frac{1}{2^i}} u^{2^i} + \left(c_2 + \mathrm{Tr}_{q^l/q}(c_1)\right) u + \mathrm{Tr}_{q^l/q}\left(c_1 e^{\frac{1}{2^i}}\right) + c_2 \mathrm{Tr}_{q^l/q}\left(e^{\frac{q^2+q}{2^{i+1}}}\right) = 0. \tag{17}$$

根据引理 5，方程（17）在 $\mathbb{F}_{2^k}$ 中的解数只有两种可能：要么无解，要么其解数等于齐次方程的解数

$$(c_3)^{\frac{1}{2^i}} u^{2^i} + \left(c_2 + \mathrm{Tr}_{q^l/q}(c_1)\right) u = 0. \tag{18}$$

由方程（18）可得 $u = 0$ 或

$$u^{2^i-1} = \frac{c_2 + \mathrm{Tr}_{q^l/q}(c_1)}{(c_3)^{\frac{1}{2^i}}}. \tag{19}$$

若 $c_2 + \mathrm{Tr}_{q^l/q}(c_1) = 0$，则方程（18）恰有一个解 $u = 0$。因此，$f(x)$ 是置换多项式。若 $c_2 + \mathrm{Tr}_{q^l/q}(c_1) \neq 0$ 且 $\left(^{c_2+}\mathrm{Tr}_{q^l/q}(c_1)\,(c_3)^{\frac{1}{2^i}}\right)$ 最大公因数$\left(2^i-1, 2^m-1\right) = 1$，则方程有 $\gcd\left(2^i-1, 2^k-1\right)$ 个不同的非零解，这意味着 $f(x)$ 是一个 $2^{\gcd(i.k)}$-对-1 映射。若 $c_2 + \mathrm{Tr}_{q^l/q}(c_1) \neq 0$ 且 $\left(^{c_2+}\mathrm{Tr}_{q^l/q}\left(c_1^{\frac{1}{2^i}}\right)\right)^{\frac{2^m-1}{2^i-1}} (c_3)$ $\gcd\left(,2^m-1\right) \neq 1$，则方程（19）无解，这意味着 $f(x)$ 是置换多项式。 (19)

□

注2. 定理*4*假设 l 是正整数，$c_1 \in \mathbb{F}_{q^l}$、$c_2 \in \mathbb{F}_q$和 $c_3 \in \mathbb{F}_q^*$。如果 l 是奇数，$i = 0$、$c_2 = 1$、$c_1 = 0$和 $c_3 \in \mathbb{F}_q \setminus \{0, 1\}$，我们的函数 $f(x)$ 退化为

$$f(x) = c_3 x + \mathrm{Tr}_{q^l/q}\left(x^{\frac{q+q^2}{2}}\right).$$

已在 *[20, 定理 3.5]* 中证明，这个退化的 $f(x)$ 是 $\mathbb{F}_{q^l}$上的置换多项式。然而，定理*4*并未施加 l 为奇数的限制。此外，除了置换多项式之外，我们还研究 n-*to*-1映射性质，具体确定 $f(x)$ 成为 q-*to*-1 映射或 $2^{\gcd(i,k)}$-*to*-1 映射的条件。

现在我们研究 $\mathcal{C}_f$的参数、重量分布、极小性和自正交性； $\mathcal{C}_f$是由定理4中的 n-to-1映射 $f(x)$构造的。为此，我们需要以下引理。

引理 12 $m = lk$ $q = 2^k$ k l L_b y $= \left({}_{2^{m}/2^{k}}\ b\ c_2 \right)^2 y^{q^3} +$.设 *and*，其中，均为正整 $\left({}_{2^{m}/2^{k}}\ b\ c_2 \right)^2 y^{q}$ 2 ${}_{2^{m}/2^{k}}\ b\ c_2 \neq 0$ $y \in \mathbb{F}_{2^m}$ 数。设():Tr()Tr()是一个 -线性化多项式，且Tr()对成立。则有

$$\dim_{\mathbb{F}_2}(\ker(L_b)) = \begin{cases} k & \textit{if } l \textit{ is odd,} \\ 2k & \textit{if } l \textit{ is even.} \end{cases}$$

证明。 $L_b(y)$的传统2伴随多项式为 $l_b(y) = \left(\mathrm{Tr}^{2^m/2^k}(b)c_2\right)^2 \left(y^k + y^{3k}\right)$。根据引理6，我们需要确定

$$\mathrm{gcrd}\left(\left(\mathrm{Tr}_{2^m/2^k}(b)c_2\right)^2 \left(y^k + y^{3k}\right), y^{kl} - 1\right).$$

令 $D := \left(\mathrm{T}\ \mathrm{r}_{2^m/2^k}(b)c_2\right)^2$。注意到 $y^{lk} - 1 = y^{lk} + 1$。于是我们进行右除法:

$$y^{kl} + 1 = \left(D^{-1}\right)^{2^{k-3}} y^{k(l-3)}\left(Dy^{3k} + Dy^k\right) + y^{k(l-2)} + 1.$$

由于 $y^{k(l-2)} + 1$ 的次数不小于 $3k$，我们需要继续应用右除法算法，直到余式的次数不超过 $3k - 1$。当 l 为奇数时，记 $l = 2t + 1$。仿照引理10和引理11中的计算方法，可得

$$y^{kl} + 1 = \sum_{i=1}^{t} \left(D^{-1}\right)^{2^{k(l-2i-1)}} y^{k(l-2i-1)} \left(Dy^{3k} + Dy^k\right) + y^k + 1$$

and

$$Dy^{3k} + Dy^k \ = \ \left(Dy^{2k} + Dy^k\right)\left(y^k + 1\right).$$

由此可得

$$\mathrm{gcrd}\left(\left(\mathrm{Tr}_{2^m/2^k}(b)c_2\right)^2 \left(y^k + y^{3k}\right), y^{kl} - 1\right) = y^k + 1.$$

当 l 为偶数时，记 $l = 2t$。可得

$$y^{kl} + 1 = \sum_{i=1}^{t-1} \left(D^{-1}\right)^{2^{k(l-2i-1)}} y^{k(l-2i-1)} \left(Dy^{3k} + Dy^k\right) + y^{2k} + 1$$

and

$$Dy^{3k} + Dy^k \ = \ Dy^k\left(y^{2k} + 1\right).$$

由此可得

$$\mathrm{gcrd}\left(\left(\mathrm{Tr}_{2^m/2^k}(b)c_2\right)^2 \left(y^k + y^{3k}\right), y^{kl} - 1\right) = y^{2k} + 1.$$

因此，由引理6可得所需结论。 □

定理 5. 设 $f(x) = \text{迹}_{q^l/q}\left(c_1 x + c_2 x^{\frac{q+q^2}{2}}\right) + c_3 x^{2^i} \in \mathbb{F}_{q^l}[x]$，其中 $q = 2^k$、 $i \in \mathbb{Z}$以及 $c_1 \in \mathbb{F}_{q^l}$、 $c_2 \in \mathbb{F}_q$ $c_3 \in \mathbb{F}_q^*$ $m = kl$ ，。设。则以下结论成立。

1) 若 l 为奇数，则 $\mathcal{C}_f$ 是一个参数为

$$\left[2^{lk} - 1, lk + k, 2^{lk-1} - 2^{\frac{lk+k}{2}-1}\right]$$

以及表 *III* 中的重量分布。如果 $k\,(l-1) \geq 4$，则 $\mathcal{C}_f$ 是极小的。如果 $k\,(l+1) \geq 6$，则 $\mathcal{C}_f$ 是自正交的。

2）如果 l 为偶数，则 $\mathcal{C}_f$ 是一个参数为

$$\left[2^{lk}-1, lk+k, 2^{lk-1}-2^{\frac{lk+2k}{2}-1}\right]$$

以及表 *IV* 中的重量分布。若 $k(l-2) \geq 4$，则 $\mathcal{C}_f$ 是极小的。若 $k(l+2) \geq 6$，则 $\mathcal{C}_f$ 是自正交的。

表 III：定理 5 中 $\mathcal{C}_f$ 的重量分布（ l为奇数）

重量	频数
0	1
$2^{lk-1}-2^{\frac{lk+k}{2}-1}$	$2^{lk-2}+2^{\frac{lk+k}{2}-2}-2^{lk-k-1}-2^{\frac{lk-k}{2}-1}$
2^{lk-1}	$2^{lk+k-1}-2^{lk-1}+2^{lk-k}-1$
$2^{lk-1}+2^{\frac{lk+k}{2}-1}$	$2^{lk-2}-2^{\frac{lk+k}{2}-2}-2^{lk-k-1}+2^{\frac{lk-k}{2}-1}$

表IV：定理 5 中 $\mathcal{C}_f$ 的重量分布（ l为偶数）

重量	频率
0	1
$2^{lk-1}-2^{\frac{lk+2k}{2}-1}$	$2^{lk-2}-2^{\frac{lk+2k}{2}-2}-2^{lk-k-1}+2^{\frac{lk-k}{2}-1}$
2^{lk-1}	$2^{lk+k-1}-2^{lk-k-1}+2^{lk-2k}-1$
$2^{lk-1}+2^{\frac{lk+2k}{2}-1}$	$2^{lk-2}+2^{\frac{lk+2k}{2}-2}-2^{lk-k-1}-2^{\frac{lk-k}{2}-1}$

证明。 根据公式（7），我们首先需要计算任意 $a, b \in \mathbb{F}_{2^m}$ 下的 Walsh 变换 $W_f(a,b)$。我们有

$$\begin{aligned} W_f(a,b) &= \sum_{x\in\mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}_{2^m/2}\left(ax+b\left(\mathrm{Tr}_{q^l/q}\left(c_1x+c_2x^{\frac{q+q^2}{2}}\right)+c_3x^{2^i}\right)\right)} \\ &= \sum_{x\in\mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}_{2^m/2}(Q(x))}. \end{aligned}$$

其中 $Q(x) := ax + b\left(\mathrm{Tr}_{q^l/q}\left(c_1x + c_2x^{\frac{q+q^2}{2}}\right) + c_3x^{2^i}\right)$。现在我们利用迹函数的性质，将 $\mathrm{Tr}_{2^m/2}(Q(x))$ 化简如下：

$$\begin{aligned} & \mathrm{Tr}_{2^m/2}\left(Q(x)\right) \\ = \ & \mathrm{Tr}_{2^m/2}\left(ax + b\left(\mathrm{Tr}_{q^l/q}\left(c_1x + c_2x^{\frac{q+q^2}{2}}\right) + c_3x^{2^i}\right)\right) \\ = \ & \mathrm{Tr}_{2^m/2}\left(ax + (bc_3)^{\frac{1}{2^i}}x + \left(bc_1x + b^{\frac{1}{q}}c_1x + \cdots + b^{\frac{1}{q^{l-1}}}c_1x\right)\right. \\ & \left. + \left(bc_2x^{\frac{q+q^2}{2}} + b^{\frac{1}{q}}c_1x^{\frac{q+q^2}{2}} + \cdots + b^{\frac{1}{q^{l-1}}}c_1x^{\frac{q+q^2}{2}}\right)\right) \\ = \ & \mathrm{Tr}_{2^m/2}\left(\left(a + (bc_3)^{\frac{1}{2^i}} + \mathrm{Tr}_{q^l/q}(b)c_1\right)x + \left(\mathrm{Tr}_{q^l/q}(b)c_2\right)^2 x^{q^2+q}\right). \end{aligned}$$

若 $\mathrm{Tr}_{q^l/q}(b)c_2 = 0$，则我们有

$$\begin{aligned} W_f(a,b) &= \sum_{x\in\mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}_{2^m/2}\left(\left(a+\mathrm{Tr}_{2^m/2^k}(b)c_1+(c_3b)^{\frac{1}{2^i}}\right)x\right)} \\ &= \begin{cases} 2^m & \text{if } a+\mathrm{Tr}_{2^m/2^k}(b)c_1+(c_3b)^{\frac{1}{2^i}}=0, \\ 0 & \text{if } a+\mathrm{Tr}_{2^m/2^k}(b)c_1+(c_3b)^{\frac{1}{2^i}}\neq 0. \end{cases} \end{aligned}$$

如果 $\mathrm{Tr}_{q^l/q}(b)c_2 \neq 0$，则 $\varphi_{a,b}(x) := \mathrm{Tr}_{2^m/2}(Q(x))$ 的双线性形式为

$$\begin{aligned} & B_{\varphi_{a,b}}(x,y) \\ = \ & \varphi_{a,b}(x+y)+\varphi_{a,b}(x)+\varphi_{a,b}(y) \\ = \ & \mathrm{Tr}_{2^m/2}\left(\left(\mathrm{Tr}_{2^m/2^k}(b)c_2\right)^2 x^{q^2}y^q+\left(\mathrm{Tr}_{2^m/2^k}(b)c_2\right)^2 x^q y^{q^2}\right) \\ = \ & \mathrm{Tr}_{2^m/2}\left(\left(\mathrm{Tr}_{2^m/2^k}(b)c_2\right)^2\left(y^q+y^{q^3}\right)x^{q^2}\right) \\ = \ & \mathrm{Tr}_{2^m/2}\left(L_b(y)x^{q^2}\right), \end{aligned}$$

其中 $L_b(y) = \left(\mathrm{Tr}_{2^m/2^k}(b)c_2\right)^2\left(y^q+y^{q^3}\right)$。记

$$V_{\varphi_b} = \ker(L_b) = \{y \in \mathbb{F}_{2^m} : L_b(y) = 0\}.$$

接下来，我们分别讨论 l 为奇数和偶数的情形。

1）由引理12，当 l为奇数时，有 $\dim_{\mathbb{F}_2}(V_{\varphi_b}) = k$。应用引理4，我们进而推出，只要 $\mathrm{Tr}_{q^l/q}(b)c_2 \neq 0$，就有 $W_f(a,b) \in \left\{0, \pm 2^{\frac{m+k}{2}}\right\}$。结合这两种情形，对于所有 $a,b \in \mathbb{F}_{2^m}$，可得 $W_f(a,b) \in \left\{0, 2^m, \pm 2^{\frac{m+k}{2}}\right\}$。回顾一下，$\dim(\mathcal{C}_f) = 2m - \dim_{\mathbb{F}_2}(K_1)$，其中 K_1由公式（6）定义。注意，$W_f(a,b) = 2^m$当且仅当 $a + \mathrm{Tr}_{2^m/2^k}(b)c_1 + (c_3 b)^{\frac{1}{2^i}} = 0$且 $\mathrm{Tr}_{2^m/2^k}(b)c_2 = 0$，由此得到 2^{m-k}个解对 (a,b)。于是 $\dim_{\mathbb{F}_2}(K_1) = m-k$，因此 $\dim(\mathcal{C}_f) = m+k$。由公式（7），我们有

$$\mathrm{wt}(\mathbf{c}_{a,b}) \in \left\{2^{m-1},\ 0,\ 2^{m-1}-2^{\frac{m+k}{2}-1},\ 2^{m-1}+2^{\frac{m+k}{2}-1}\right\}.$$

根据引理9和前三个Pless幂矩，我们可以轻松得到表 III 中 $\mathcal{C}_f$ 的重量分布。由引理8，将最小非零重量 $w_{\min} = 2^{kl-1} - 2^{\frac{kl+k}{2}-1}$ 和最大非零重量 $w_{\max} = 2^{kl-1} + 2^{\frac{kl+k}{2}-1}$ 代入方程（5）中，可推得当 $k(l-1) \geq 4$ 时，$\mathcal{C}_f$ 是极小的。根据引理7，我们进一步推得，只要 $k(l+1) \geq 6$，$\mathcal{C}_f$ 就是自正交的。

2）由引理12，当 l 为偶数时，我们有 $\dim_{\mathbb{F}_2}(V_{\varphi_b}) = 2k$。应用引理4，进而可推得，只要 $\mathrm{Tr}_{q^l/q}(b)c_2 \neq 0$，$W_f(a,b) \in \left\{0, \pm 2^{\frac{m+2k}{2}}\right\}$。结合这两种情况，对于所有 a，$b \in \mathbb{F}_{2^m}$，我们得到 $W_f(a,b) \in \left\{0,\ 2^m,\ \pm 2^{\frac{m+2k}{2}}\right\}$。回顾一下，$\dim(\mathcal{C}_f) = 2m - \dim_{\mathbb{F}_2}(K_1)$，其中 K_1 在公式（6）中定义。注意，当且仅当 $a + \mathrm{Tr}_{2^m/2^k}(b)c_1 + (c_3 b)^{\frac{1}{2^i}} = 0$ 且 $\mathrm{Tr}_{2^m/2^k}(b)c_2 = 0$ 时，$W_f(a,b) = 2^m$，由此得到 2^{m-k} 个解对 (a,b)。于是 $\dim_{\mathbb{F}_2}(K_1) = m-k$，因此 $\dim(\mathcal{C}_f) = m+k$。根据公式（7），我们有

$$\mathrm{wt}(\mathbf{c}_{a,b}) \in \left\{2^{m-1},\ 0,\ 2^{m-1}-2^{\frac{m+2k}{2}-1},\ 2^{m-1}+2^{\frac{m+2k}{2}-1}\right\}.$$

根据引理9和前三个 Pless幂矩，我们可以轻松得到表IV中 $\mathcal{C}_f$的重量分布。根据引理8，将最小非零重量$w_{\min} = 2^{kl-1} - 2^{\frac{kl+2k}{2}-1}$ 和最大非零重量代入方程（5）中，可推得当 $k(l-2) \geq 4$时，$\mathcal{C}_f$ 是极小的。根据引理7，我们进一步推得，只要 $k(l+2) \geq 6$，$\mathcal{C}_f$ 就是自正交的。

证明至此完成。 □

IV. 总结

在本文中，我们从三类n到1映射构造了三族三重量二元线性码。主要贡献总结如下。

1) 我们提出了两个新的 n-对-1 映射族，分别由 $f(x) = \mathrm{Tr}^{q^l/q}(x^{2q+2}) + cx$ (定理1) 和 $f(x) = \mathrm{Tr}_{q^l/q}\left(c_1 x + c_2 x^{\frac{q+q^2}{2}}\right) + c_3 x^{2^i}$ (定理4) 给出。

2) 利用新构造的两个 n-对-1 映射族和一个已知族，我们构造了三个三重量射影二元线性码族。借助斜多项式环的代数理论，明确确定了它们的参数和重量分布。此外，我们还证明了这些码的极小性和自正交性。

这些二元码既是极小码，又是自正交码，因此在量子码和具有良好访问结构 [3], [39] 的秘密共享方案中具有重要应用。此外，在 [2] 框架下，我们的三重量码可用于构造关联方案。与 [8], [11], [22]，相比，本文得到的三重量码具有新的参数。根据这些码的重量分布和 Pless幂矩，可以轻易推导出这些码的对偶码最小距离为三。因此，可以验证这些对偶码相对于著名的球填充界几乎达到了距离最优。

要计算本文所构造线性码的重量分布，关键在于确定相应线性化多项式的零点个数。根据 [23, 第 118], 页，我们知道，$G(x) = 0$ 在 $\mathbb{F}_{q^m}$ 中有 q^ℓ 个根，当且仅当

$$\deg\left(\gcd\left(\sum_{i=0}^{m-1}\lambda_i x^i,\, x^m-1\right)\right)=\ell,$$

其中 $G(x) = \sum_{i=0}^{m-1}\lambda_i x^{q^i} \in \mathbb{F}_q[x]$ 是一个 q-线性化多项式。然而，该结果要求 $G(x)$的系数属于 $\mathbb{F}_q$，而我们基于引理6的方法适用于更一般的情形$G(x) \in \mathbb{F}_{q^m}[x]$。因此，本文为确定由 n对1映射导出的线性码的参数提供了新的视角。

致谢

作者感谢吴宝峰博士提供引理6，这为本文研究方法的形成提供了帮助。

参考文献

[1] A. Ashikhmin 和 A. Barg，《线性码中的极小向量》，*IEEE* 信息论汇刊，第 44 卷，第 5 期，第 2010–2017 页，1998 年 9 月。[2] A. R. Calderbank 和 J. M. Goethals，《三重量码与关联方案》，*Philips* 研究杂志，第 39 卷，第 4/5 期，第 143–152 页，1984 年 12 月。[3] A. R. Calderbank、E. M. Rains、P. Shor 和 N. J. Sloane，《基于 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 7 月。[4] R. dela Cruz、A. Meyer 和 P. Sole，《Massey 秘密共享方案的扩展》，载于*IEEE* 信息论研讨会论文集，2010 年 8 月，第 1–5 页。[5] C. Ding，《从布尔函数构造二元线性码》，离散数学，第 339 卷，第 9 期，第 2288–2303 页，2016 年 9 月。[6] C. Ding，《来自若干 2-设计的线性码》，*IEEE* 信息论汇刊，第 61 卷，第 6 期，第 3265–3275 页，2015 年 6 月。[7] C. Ding、Z. Heng 和 Z. Zhou，《二元极小线性码》，*IEEE* 信息论汇刊，第 64 卷，第 10 期，第 6536–6545 页，2018 年 6 月。[8] C. Ding、C. Li、N. Li 和 Z. Zhou，《三重量循环码及其重量分布》，离散数学，第 339 卷，第 2 期，第 415–427 页，2016 年 2 月。[9] C. Ding 和 X. Wang，《一种基于编码理论的新型系统认证码构造》，理论计算机科学，第 330 卷，第 1 期，第 81–99 页，2005 年 1 月。[10] K. Ding 和 C. Ding，《一类二重量码和三重量码及其在秘密共享中的应用》，*IEEE* 信息论汇刊，第 61 卷，第 11 期，第 5835–5842 页，2015 年 11 月。[11] K. Ding 和 C. Ding，《具有三种重量的二元线性码》，*IEEE* 通信快报，第 18 卷，第 11 期，第 1879–1882 页，2014 年 11 月。[12] M. Dzhumalieva-Stoeva、I. G. Bouyukliev 和 V. Monev，《从组合设计构造自正交码》，信息传输问题，第 48 卷，第 3 期，第 250–258 页，2012 年。

[13] Z. Heng、M. Yang 和 Y. Ming，《一族具有局部性 2 的自正交可除码》，离散数学，第 348 卷，第 10 期，文章编号 114185，2025年。[14] Z. Heng、C. Ding 和 Z. Zhou，《有限域上的极小线性码》，有限域及其应用，第 54 卷，第 176–196 页，2018 年 11 月。[15] Z. Heng、D. Li 和 F. Liu，《由弱正则弯曲函数构造的三元自正交码及其在 LCD码中的应用》，设计、码与密码学，第 91 卷，第 12 期，第 3891–3913 页，2023年。[16] W. C. Huffman 和 V. Pless，《纠错码基础》。英国剑桥：剑桥大学出版社，2003 年。[17] W. Jin、K. Li 和 L. Qu，《若干违反 Ashikhmin-Barg条件的自正交极小线性码新类》，IEEE 信息论汇刊，第 71 卷，第 10 期，第 7699–7714 页，2025 年 10 月。[18] K. Li、C. Li、T. Helleseth 和 L. Qu，《由二对一函数构造的少重量二元线性码》，IEEE 信息论汇刊，第 67 卷，第 7 期，第 4263–4275 页，2021 年 7 月。[19] K. Li、S. Mesnager 和 L. Qu，《关于 $\mathbb{F}_2^n$ 上的二对一映射的进一步研究》，IEEE 信息论汇刊，第 67 卷，第 6 期，第 3486–3496 页，2021 年 6 月。[20] K. Li、L. Qu、X. Chen 等，《形如 $cx+\mathrm{Tr}^{q^l/q}(x^a)$的置换多项式及偶特征有限域上的置换三项式》，密码学通信，第 10 卷，第 3 期，第 531–554 页，2018 年。[21] X. Li 和 Z. Heng，《从 p-可除码构造自正交码》，IEEE 信息论汇刊，第 70 卷，第 12 期，第 8562–8586 页，2024 年 12 月。[22] Y. Li、K. Li 和 Q. Zhang，《 $\mathbb{F}_{2^n}$ 上的二对一映射新构造及其在二元线性码中的应用》，离散数学，第 349 卷，第 7 期，文章编号 114256，2026 年 7 月。[23] R. Lidl 和 H. Niederreiter，《有限域》。英国剑桥：剑桥大学出版社，2008 年。[24] S. Mesnager，《基于一般构造，由弱正则弯曲函数构造的少重量线性码》，密码学通信，第 9 卷，第 1 期，第 71–84 页，2017 年 1 月。[25] S. Mesnager、L. Qian、X. Cao 和 M. Yuan，《由二对一函数构造的若干族二元最小线性码》，IEEE 信息论汇刊，第 69 卷，第 5 期，第 3285–3301 页，2023 年 5 月。[26] S. Mesnager 和 L. Qu，《关于有限域上的二对一映射》，IEEE 信息论汇刊，第 65 卷，第 12 期，第 7884–7895 页，2019 年 12 月。[27] S. Mesnager 和 A. Sinak，《由弱正则平台函数构造的若干类少重量极小线性码》，IEEE 信息论汇刊，第 66 卷，第 4 期，第 2296–2310 页，2020 年 4 月。[28] S. Mesnager、A. Sinak 和 O. Yayla，《具有少量重量的极小线性码及其秘密共享》，国际信息安全科学杂志，第 8 卷，第 3 期，第 44–52 页，2019 年 1 月。[29] T. Niu、K. Li、L. Qu 和 C. Li，《有限域上 n-对一映射的刻画与构造》，有限域及其应用，第 85 卷，文章编号 102130，2023 年 1 月。[30] O. Ore，《非交换多项式理论》，数学年刊，第 34 卷，第 480–508 页，1933 年。[31] O. Ore，《关于一类特殊多项式》，美国数学会汇刊，第 35 卷，第 559–584 页，1933 年。[32] V. Pless，《纠错码重量分布的幂矩恒等式》，信息与控制，第 6 卷，第 2 期，第 147–152 页，1963 年 6 月。[33] R. Rodr´ıguez-Aldama，《由 t-对一映射构造的 $\mathbb{F}_p$ 上的少重量线性码》，有限域及其应用，第 100 卷，文章编号 102496，2024 年 12 月。[34] C. Tang、N. Li、Y. Qi、Z. Zhou 和 T. Helleseth，《由弱正则弯曲函数构造的二重量或三重量线性码》，IEEE 信息论汇刊，第 62 卷，第 3 期，第 1166–1176 页，2016 年 3 月。[35] C. Tang、Y. Qiu、Q. Liao 和 Z. Zhou，《极小线性码作为切割阻挡集的完整刻画》，IEEE 信息论汇刊，第 67 卷，第 6 期，第 3690–3700 页，2021 年 6 月。[36] C. Tang、C. Xiang 和 K. Feng，《由非齐次二次函数构造的少重量线性码》，设计、码与密码学，第 83 卷，第 3 期，第 691–714 页，2017 年 6 月。[37] B. Wu 和 Z. Liu，《有限域上线性化多项式再探》，有限域及其应用，第 22 卷，第 79–100 页，2013 年 7 月。[38] C. Xie 和 Z. Heng，《 n-对一映射在差族和最优恒重码中的应用》，IEEE 信息论汇刊，第 72 卷，第 11 期，第 8890–8908 页，2026 年。[39] J. Yuan 和 C. Ding，《来自三类线性码的秘密共享方案》，IEEE 信息论汇刊，第 52 卷，第 1 期，第 206–212 页，2006 年 1 月。[40] Z. Zhou、N. Li、C. Fan 和 T. Helleseth，《由二次弯曲函数构造的二重量或三重量线性码》，设计、码与密码学，第 81 卷，第 2 期，第 283–295 页，2016 年 11 月。