Advances in Applied Mathematics 应用数学进展, **2023, 12(8), 3507-3517**
Published Online August 2023 in Hans. https://www.hanspub.org/journal/aam
https://doi.org/10.12677/aam.2023.128349

Hans汉斯

一类基于向量布尔函数构造的极小二元线性码

吴 昊

西北师范大学数学与统计学院，甘肃 兰州

收稿日期：2023年7月1日；录用日期：2023年7月23日；发布日期：2023年8月1日

摘 要

线性码在数据储存、通信、密码学和组合数学等方面都有着重要的应用，其中的极小线性码可以用来构造具有良好访问结构的秘密共享方案. 本文利用向量布尔函数构造了一类新的二元线性码，并且利用布尔函数的密码学性质研究了线性码的长度，维数和重量分布. 结论表明，所构造的线性码最小距离更大且为宽极小码. 此外，本文将现有的一些结果推广到一般情形.

关键词

线性码，极小码，向量布尔函数，重量分布

Minimal Binary Linear Codes from a Class of Vectorial Boolean Functions

Hao Wu

College of Mathematics and Statistics, Northwest Normal University, Lanzhou Gansu

Received: Jul. 1^{st}, 2023; accepted: Jul. 23^{rd}, 2023; published: Aug. 1^{st}, 2023

Abstract

The applications of linear codes in data storage, communication, cryptography and combinatorial mathematics have been of great importance over the years, among which minimal linear codes can be used to construct secret sharing schemes with good access structure. In this paper, we construct a new class of binary linear codes using vectorial Boolean functions, and study the length, dimension and weight distribution

文章引用: 吴昊. 一类基于向量布尔函数构造的极小二元线性码[J]. 应用数学进展, 2023, 12(8): 3507-3517.
DOI: 10.12677/aam.2023.128349

of linear codes using the cryptographic properties of Boolean functions. The results show that the constructed linear codes have larger minimum distance and are wide minimal codes. At the same time, this article extends some existing results to general situations.

Keywords

Linear Code, Minimal Code, Vectorial Boolean Function, Weight Distribution

1. 引言

编码理论可以被用来解决密码学中的某些困难问题. 为了满足工程技术中的实际需要, 编码理论自创立以来就获得了快速地发展. 在编码理论中, 线性码是一类具有优良性质且便于实现的码. 因其具有良好的代数性质, 在很多场合都有着非常重要的应用. 线性码不但能够被用于数字通信系统和存储系统, 并且在秘密共享方案 [1,2]、认证码 [3]、关联方案 [4] 等方面也有着广泛应用, 因此受到大量学者的关注并成为密码学研究的热点课题. 此外, 具有某些特殊性质的线性码也一直都是编码理论研究的重点. 例如, 极小线性码就是一类特殊的线性码, 在这类线性码中, 所有的非零码字都是极小码字. 这一性质使得极小线性码可被用于构造译码算法 [5] 和多用户通信方案. 在编码理论和密码学中, 构造新的拥有特殊参数的极小线性码是一个有趣的研究课题. 在极小线性码的研究中人们得到, 任何二元线性码若 $w_{\min}/w_{\max} > 1/2$, 则其为极小码 [5], 其中 $w_{\max}$ 和 $w_{\min}$ 分别为线性码的最大重量和最小重量. 目前已有不少线性码基于这个条件被证明是极小线性码, 参见 [2,6–10]. 然而, 只有少数几类满足 $w_{\min}/w_{\max} \leq 1/2$ 的极小二元线性码被提出 [11,12], 以及满足 $w_{\min}/w_{\max} \leq (q-1)/q$ 的奇特征极小线性码被提出 [13,14], 其中 q 为奇素数的幂. 在通常情况下, 构造一类满足条件 $w_{\min}/w_{\max} < 1/2$ 的极小二元线性码是一个困难问题.

过去的三十年里, 由 (向量) 布尔函数设计二元线性码一直是重要的研究课题, 并且已经获得了许多具有良好参数的二元线性码, 见文献 [6,15] 等. 一般来说, 由 (向量) 布尔函数构造的二元线性码有两种结构. 第一种构造 [6] 基于一些高非线性度布尔函数 (如 Bent 函数和半 Bent 函数) 的支撑. 第二种构造 [16,17] 基于高非线性度的向量布尔函数, 例如完全非线性 (PN) 函数和几乎 Bent (AB) 函数.

受上述文章的启发, 本文旨在基于由向量布尔函数构造线性码的一般结构来构造一类新的极小二元线性码, 且这类码满足 $w_{\min}/w_{\max} \leq 1/2$. 首先, 介绍有关于向量布尔函数和极小线性码的概念并且研究了 Plateaued 函数的密码学性质. 其次, 给出基于向量布尔函数构造二元线性码的两种一般方式及它们之间的关系, 并将文献 [18] 中的部分内容推广到更一般的情形, 证明了当参数取特殊

值时, 可以构造出最小距离较大的极小码, 且这类码满足 $w_{\min}/w_{\max} \leq 1/2$.

本文第 2 节介绍向量布尔函数, Walsh-Hadamard 变换, 线性码的参数以及极小线性码的有关预备知识; 第 3 节论述基于向量布尔函数构造二元线性码的两种一般方式和它们之间的关系, 并具体给出极小线性码的构造和证明; 第 4 节则是对本文工作的总结.

2. 基础知识

本节介绍关于向量布尔函数, Walsh-Hadamard 变换, 线性码的参数以及极小线性码的一些基本概念和已有结论.

2.1. 向量布尔函数和Walsh-Hadamard变换

给定两个整数 n 和 m, 从向量空间 $\mathbb{F}_2^n$ 到 $\mathbb{F}_2^m$ 的映射称为 (n,m)-函数. 当不强调 n 和 m 的具体值时, 通常称之为向量值函数, 也称为向量布尔函数. 特别地, 当 $m=1$ 时, 即映射 $f:\mathbb{F}_2^n \to \mathbb{F}_2$, 称为 n 元布尔函数. 给定一个 (n,m)-函数 F, 就有 m 个 n 元布尔函数 $f_1, f_2, \cdots, f_m$, 使得对任意 $\mathbf{x}=(x_1,x_2,\cdots,x_n)\in\mathbb{F}_2^n$, 均有 $F(\mathbf{x})=(f_1(x), f_2(x), \cdots, f_m(x))$. 这时 $f_1, f_2, \cdots, f_m$ 称为 F 的分量函数, 特别地, f_i 称为 F 的第 i 个分量函数, 其中 $1\leq i\leq m$. 显然, 布尔函数 $\mathbf{a}\cdot F$ 称为 F 的分量函数, 其中 $\mathbf{a}\in\mathbb{F}_2^{m*}$. 如果用有限域 $\mathbb{F}_{2^m}$ 的元素来表示向量空间 $\mathbb{F}_2^{m*}$ 的每个元素, 那么 F 的分量函数 f_α 可以表示为 $\mathrm{tr}_1^m(\alpha F)$, 其中 $\alpha\in\mathbb{F}_{2^m}^*$, $\mathrm{tr}_1^m(x)=\sum_{i=0}^{m-1}x^{2^i}$ 是从 $\mathbb{F}_{2^m}$ 到 $\mathbb{F}_2$ 的迹函数.

下面给出向量布尔函数的 Walsh-Hadamard 变换.

设 F 是一个 (n,m)-函数, F 在点 $(\mathbf{u},\mathbf{v})\in\mathbb{F}_2^n\times\mathbb{F}_2^m$ 处的 Walsh-Hadamard 变换定义为

$$W_F(\mathbf{u},\mathbf{v})=\sum_{\mathbf{x}\in\mathbb{F}_2^n}(-1)^{\mathbf{u}\cdot F(\mathbf{x})+\mathbf{v}\cdot\mathbf{x}}.$$

由上式可知, 向量布尔函数在 $(\mathbf{u},\mathbf{v})\in\mathbb{F}_2^n\times\mathbb{F}_2^m$ 处的 Walsh-Hadamard 变换就是布尔函数 $\mathbf{u}\cdot F(\mathbf{x})$ 在 $\mathbf{v}$ 处的 Walsh-Hadamard 变换, 即 $W_F(\mathbf{u},\mathbf{v})=W_{\mathbf{u}\cdot F(\mathbf{x})}(\mathbf{v})$.

为方便起见, 本文中使用 $\hat{f}(\mathbf{x})$ 表示布尔函数 f 在点 $\mathbf{x}\in\mathbb{F}_2^n$ 处的 Walsh-Hadamard 变换, $\mathcal{B}_n$ 表示所有 n 元布尔函数的集合. 设 $f\in\mathcal{B}_n$, f 的支撑定义为 $\mathrm{supp}(f)=\{\mathbf{x}\in\mathbb{F}_2^n : f(\mathbf{x})=1\}$. 如下引理给出了布尔函数的 Walsh-Hadamard 变换与其支撑之间的关系.

引理 1. [19] 符号如上所示. 若用 $\|\mathrm{supp}(f)\|$ 表示集合 $\mathrm{supp}(f)$ 中所含元素的个数, 则 f 在点 $\mathbf{a}\in\mathbb{F}_2^n$ 处的 Walsh 变换满足

$$\hat{f}(\mathbf{a})=\begin{cases}2^n-2\|\mathrm{supp}(f)\|, & \mathbf{a}=\mathbf{0},\\ -2\sum\limits_{\mathbf{x}\in\mathrm{supp}(f)}(-1)^{\mathbf{a}\cdot\mathbf{x}}, & \text{其他}.\end{cases}$$

另外, 根据 Walsh-Hadamard 变换的定义, 设布尔函数 $f\in\mathcal{B}_n$, 易得

$$\sum_{\mu\in\mathbb{F}_2^n}\hat{f}^2(\mu)=2^{2n}, \tag{1}$$

这便是 Parseval 公式, 显然 $\max_{\mu\in\mathbb{F}_2^n}|\hat{f}(\mu)|\geq 2^{n/2}$, 当且仅当 n 为偶数并且对于任意的 $\mu\in\mathbb{F}_2^n$, $|\hat{f}(\mu)|=2^{n/2}$ 时, 上述不等式取等号. 此时, 称 f 为 Bent 函数.

定义 1. 设 n 和 r 为两奇偶性相同的正整数, 满足 $0\leq r\leq n$. 如果对任意的 $\mu\in\mathbb{F}_2^n$, 布尔函数 $f\in\mathbb{F}_2^n$ 的 Walsh-Hadamard 变换满足 $\hat{f}(\mu)\in\{0,\pm 2^{(n+r)/2}\}$, 那么称布尔函数 f 为 r-Plateaued 函数.

显然, 0-Plateaued 函数对应的布尔函数为 Bent 函数, 1-Plateaued 函数对应的布尔函数为 AB 函数, n-Plateaued 函数对应的布尔函数为仿射函数.

2.2. 线性码的参数和极小线性码

设 n 为正整数, $\mathbb{F}_2^n$ 表示有限域 $\mathbb{F}_2$ 上的 n 维向量空间. $\mathbb{F}_2^n$ 的一个 k 维子空间 C 称为码长为 n, 维数为 k 的 $[n,k,d]$ 二元线性码. 其中极小距离 d 定义为

$$d=\min_{\mathbf{a}\neq\mathbf{b}\in C} d_H(\mathbf{a},\mathbf{b}),$$

上式中 d_H 表示向量 $\mathbf{a}=(a_1,a_2,\cdots,a_n)\in C$ 和 $\mathbf{b}=(b_1,b_2,\cdots,b_n)\in C$ 之间的汉明距离, 即 $d_H(\mathbf{a},\mathbf{b})=\|\{1\leq i\leq n: a_i\neq b_i\}\|$. 码 C 中的每个向量 $\mathbf{c}$ 称为码字, 则对于给定码字 $\mathbf{a}=(a_1,a_2,\cdots,a_n)\in C$, 汉明重量 $wt(\mathbf{a})$ 定义为码字中非零坐标的个数. 显然, 任何二元线性码的最小汉明距离都等于该码中非零码字的最小汉明重量.

设 A_i 表示 C 中汉明重量为 i 的码字的个数, 多项式 $1+A_1z+A_2z^2+\cdots+A_nz^n$ 称为码 C 的重量计数器, 序列 $(1,A_1,A_2,\cdots,A_n)$ 称为码 C 的重量分布. 若在 $(1,A_1,A_2,\cdots,A_n)$ 中, $A_i\neq 0$ $(1\leq i\leq n)$ 的个数为 t, 则称码 C 为 t 重码. 码字 $\mathbf{c}=(c_0,c_1,\cdots,c_{n-1})\in C$ 的支撑定义为

$$\mathrm{supp}(\mathbf{c})=\{0\leq i\leq n-1: c_i\neq 0\}.$$

则码字 $\mathbf{c}$ 的汉明重量 $wt(\mathbf{c})$ 满足

$$wt(\mathbf{c})=\|\mathrm{supp}(\mathbf{c})\|.$$

若对任意向量 $\mathbf{u},\mathbf{v}\in\mathbb{F}_2^n$, 都有 $\mathrm{supp}(\mathbf{v})\subseteq\mathrm{supp}(\mathbf{u})$, 则称 $\mathbf{u}$ 覆盖 $\mathbf{v}$, 记为: $\mathbf{v}\preceq\mathbf{u}$. 若线性码 C 的一个非零码字 $\mathbf{c}$ 只覆盖它的纯量倍数, 则称 $\mathbf{c}$ 是一个极小向量.

定义 2. 若线性码 C 中任意码字都是极小向量, 则称 C 是极小线性码, 简称极小码.

3. 极小二元线性码的构造

本节中, 首先简单介绍引言中提到的由 (向量) 布尔函数构造二元线性码的两种一般方式, 并给出两者之间的关系. 其次, 利用向量布尔函数构造一类新的宽极小二元线性码, 即 $w_{\min}/w_{\max}<1/2$, 并确定了其长度、维数以及参数取特殊值时的重量分布.

最近, Ding 在 [6] 中提出了一种使用单变量多项式表示从布尔函数的支撑设计线性码的方法. 对于给定的 $f\in\mathcal{B}_m$, 定义集 $D=\{x\in\mathbb{F}_{2^m}: f(x)\neq 0\}$ 称为 f 的支撑, 并且用 n_f 表示 D 的大小. 令 $D=\{d_1,d_2,\cdots,d_{n_f}\}$, 则 Ding [6] 定义了一个长度为 n_f, 维数为 m 的二元线性码 C_D :

$$C_D=\{c_\alpha:\alpha\in\mathbb{F}_{2^m}\},\tag{2}$$

其中 $c_\alpha=(\mathrm{tr}_1^m(\alpha d_1),\mathrm{tr}_1^m(\alpha d_2),\cdots,\mathrm{tr}_1^m(\alpha d_{n_f}))$, $\mathrm{tr}_1^m(x)=\sum_{i=0}^{m-1}x^{2^i}$ 是 $\mathbb{F}_{2^m}$ 到 $\mathbb{F}_2$ 的迹函数.

引理 2. [15] 符号定义如上. 如果对于任意 $\alpha\in\mathbb{F}_{2^m}^*$, 都有 $2n_f\neq-\hat{f}(\alpha)$, 则由 (2) 式定义的 C_D 是一个长度为 n_f, 维数为 m 的二元线性码, 其重量分布由以下多重集给出

$$\left\{\left\{\frac{2n_f+\hat{f}(\alpha)}{4}:\alpha\in\mathbb{F}_{2^m}^*\right\}\right\}\cup\{\{0\}\}. \tag{3}$$

注意到, 通过选取 $\mathbb{F}_{2^m}$ 在 $\mathbb{F}_2$ 上的某组恰当的基, 向量空间 $\mathbb{F}_2^m$ 与有限域 $\mathbb{F}_{2^m}$ 同构. 如果 $(\lambda_1,\lambda_2,\ldots,\lambda_m)$ 是 $\mathbb{F}_{2^m}$ 在 $\mathbb{F}_2$ 上的一组基, 那么 $\mathbb{F}_2^m$ 的每个向量 $\mathbf{x}=(x_1,x_2,\ldots,x_m)$ 都可以由元素 $x_1\lambda_1+x_2\lambda_2+\ldots+x_m\lambda_m\in\mathbb{F}_{2^m}$ 表示. 有限域 $\mathbb{F}_2^m$ 可被视为 $\mathbb{F}_2$ 上的 m 维向量空间. 此外, 它的每个元素都可以由长度为 m 的二元向量表示. 现在从向量空间的角度重新描述这个一般结构. 设 $D=\{\mathbf{d}_1,\mathbf{d}_2,\ldots,\mathbf{d}_n\}$ 是 $\mathbb{F}_2^m$ 上的非空子集, 则 $\mathbb{F}_2$ 上长度为 n 的线性码 C_D 定义为

$$C_D=\{(\mathbf{a}\cdot\mathbf{d}_1,\mathbf{a}\cdot\mathbf{d}_2,\ldots,\mathbf{a}\cdot\mathbf{d}_n),\mathbf{a}\in\mathbb{F}_2^m\}. \tag{4}$$

其中, 集合 D 称为码 C_D 的定义集.

1998 年, Ashikhmin 和 Barg [5] 给出了一般线性码中极小向量的基本性质, 并利用线性码的最大重量 $w_{\max}$ 和最小重量 $w_{\min}$ 给出了判别线性码为极小码的充分条件, 即如果 $w_{\min}/w_{\max}>1/2$, 任何二元线性码 C 都是极小的, 其中 $w_{\min}=\min\{wt(\mathbf{c}):\mathbf{0}\neq\mathbf{c}\in C\}$ 且 $w_{\max}=\max\{wt(\mathbf{c}):\mathbf{c}\in C\}$. 该条件在本文中称为 Ashikhmin-Barg 条件. 一般称满足 Ashikhmin-Barg 条件的极小线性码为窄极小码, 其他的极小码称为宽极小码.

实际上, 关于窄极小码的研究已经相当广泛 [2,6–10]. 然而, 宽极小码仅在很少的文章中被提及 [11,12]. 这两类宽极小码是从 [16,17] 中考虑的码中探索而来的. 首先回顾一下 [11,12,16,17] 中考虑的线性码. 设 $f\in\mathcal{B}_n$, $f(\mathbf{0})=0$, 则

$$\mathcal{C}_f=\{(uf(\mathbf{x})+\mathbf{v}\cdot\mathbf{x})_{\mathbf{x}\in\mathbb{F}_2^m\backslash\{\mathbf{0}\}}:u\in\mathbb{F}_2,\mathbf{v}\in\mathbb{F}_2^m\}, \tag{5}$$

其中 $f(\mathbf{x})\neq\mathbf{v}\cdot\mathbf{x}$.

引理 3. [12] 由 (5) 式定义的二元线性码长度为 2^m-1 , 维数为 $m+1$, 重量分布由以下多重集合的并给出:

$$\left\{2^{m-1}-\frac{1}{2}\hat{f}(\alpha):\alpha\in\mathbb{F}_2^m\right\}\cup\left\{2^{m-1}:\alpha\in\mathbb{F}_2^{m*}\right\}\cup\{0\}. \tag{6}$$

在本文中, 为了证明由 (5) 式定义的二元线性码 C_f 是极小的, 并且满足 $w_{\min}/w_{\max}\leq1/2$, 引入如下引理.

引理 4. [18] 若 (2) 式中定义的长度为 n 维数为 m 的线性码 C_D 和 (5) 式中定义的长度为 2^m-1 维数为 $m+1$ 的线性码 C_f 使用相同的 m 元布尔函数 f, 即 C_D 的定义集等于 $\mathrm{supp}(f)$, 其中函数 f 用于构造线性码 C_f, 则 C_f 中的码字满足 $w_{\min}/w_{\max}\leq1/2$ 当且仅当 C_D 中的码字满足以下三个条件:

(1) 对于任意的 $\alpha\in\mathbb{F}_2^m\backslash\{\mathbf{0}\}$, 有 $wt(\mathbf{c}_\alpha)\neq n$,

(2) 对于任意的 $\alpha\neq\beta\in\mathbb{F}_2^m\backslash\{\mathbf{0}\}$, 有 $wt(\mathbf{c}_\alpha)+wt(\mathbf{c}_\beta)-n\neq2^{m-2}$ 和 $wt(\mathbf{c}_\alpha)-wt(\mathbf{c}_\beta)\neq2^{m-2}$,

(3) 对于任意的 $\alpha\in\mathbb{F}_2^m\backslash\{\mathbf{0}\}$, 有 $\frac{\min\{2^{m-1},2^{m-1}-2wt(c_\alpha)+n,n\}}{\max\{2^{m-1},2^{m-1}-2wt(c_\alpha)+n,n\}}\leq\frac{1}{2}$.

下面给出本文的主要结论和证明.

定理 1. 设 F 为 $\mathbb{F}_{2^k}$ 上的 r-Plateaued 函数, $0 \le r \le n$, 且 $F(0)=0$. f 是一个 $2k+1$ 元布尔函数, 其支撑定义为

$$\begin{aligned}\mathrm{supp}(f) =& \{(1,x,y) : x,y \in \mathbb{F}_{2^k}\} \backslash \{(1,x,x) : x \in \mathbb{F}_{2^k}\} \\ &\cup \{(0,x,y) : x,y \in \mathbb{F}_{2^k}\} \backslash \{(0,x,F(x)) : x \in \mathbb{F}_{2^k}\}.\end{aligned}$$

令定义集 $D = \mathrm{supp}(f)$, 则 C_D 的码长为 $2^{2k+1}-2^{k+1}$, 维数为 $2k+1$, 码字的汉明重量由下面多重集合给出

$$\bigcup_{i=1}^{3}\bigcup_{j=-1}^{1}\left\{2^{2k}-i2^{k-1}+j2^{\frac{k+r-2}{2}}, 0 \le r \le n\right\}.$$

C_f 的码长为 $2^{2k+1}-1$, 维数为 $2k+2$, 码字的汉明重量由下面多重集合给出

$$\bigcup_{i=-1}^{1}\bigcup_{j=-1}^{1}\left\{2^{2k}+i2^{k}+j2^{\frac{k+r}{2}}, 0 \le r \le n\right\}.$$

证明 由定义集的选取以及码的定义可知, 线性码 C_D 的长度为 $n = \| \mathrm{supp} \| = 2^{2k+1}-2^{k+1}$, 维数为 $2k+1$.

对任意的 $\mathbf{v} \in \mathbb{F}_2^k \backslash \{\mathbf{0}\}$, 令 $U = \{\mathbf{x} \in D : \mathbf{v}\cdot\mathbf{x} \ne 0\}$, 由引理 1, C_D 中任何非零码字$\mathbf{c_v} = (\mathbf{v}\cdot\mathbf{x})_{\mathbf{x}\in D}$ 的汉明重量 $wt(\mathbf{c_v})$ 计算如下:

$$\begin{aligned}wt(\mathbf{c_v}) = \|U\| &= n - \frac{1}{2}\sum_{\mathbf{x}\in D}\sum_{y\in\mathbb{F}_2}(-1)^{y(\mathbf{v}\cdot\mathbf{x})} \\ &= \frac{n}{2} - \frac{1}{2}\sum_{\mathbf{x}\in D}(-1)^{\mathbf{v}\cdot\mathbf{x}} \\ &= \frac{n}{2} - \frac{1}{2}\sum_{\mathbf{x}\in \mathrm{supp}(f)}(-1)^{\mathbf{v}\cdot\mathbf{x}} \\ &= \frac{2n+\hat{f}(\mathbf{v})}{4}.\end{aligned} \tag{7}$$

当 $v \ne 0$ 时, 定义 tr_1^k 为 $\mathbb{F}_{2^k}$ 到 $\mathbb{F}_2$ 的绝对迹函数. 设 $\mathbf{v} = (v_1, \mathbf{v}_2, \mathbf{v}_3) \in \mathbb{F}_2 \times \mathbb{F}_2^k \times \mathbb{F}_2^k$.

$$\begin{aligned}\hat{f}(\mathbf{v}) &= \hat{f}(v_1, \mathbf{v}_2, \mathbf{v}_3) \\ &= \sum_{(x_1,\mathbf{x}_2,\mathbf{x}_3)\in\mathbb{F}_2\times\mathbb{F}_2^k\times\mathbb{F}_2^k}(-1)^{f(x_1,\mathbf{x}_2,\mathbf{x}_3)+v_1\cdot x_1+\mathbf{v}_2\cdot\mathbf{x}_2+\mathbf{v}_3\cdot\mathbf{x}_3} \\ &= \sum_{(x_1,x_2,x_3)\in\mathbb{F}_2\times\mathbb{F}_{2^k}\times\mathbb{F}_{2^k}}(-1)^{f(x_1,x_2,x_3)+v_1\cdot x_1+\mathrm{tr}_1^k(v_2x_2)+\mathrm{tr}_1^k(v_3x_3)} \\ &= -2\sum_{(x_1,x_2,x_3)\in\mathrm{supp}(f)}(-1)^{v_1\cdot x_1+\mathrm{tr}_1^k(v_2x_2)+\mathrm{tr}_1^k(v_3x_3)} \\ &= -2\Bigg(\sum_{(1,x,y)\in\mathbb{F}_2\times\mathbb{F}_{2^k}\times\mathbb{F}_{2^k}}(-1)^{v_1+\mathrm{tr}_1^k(v_2x+v_3y)} + \sum_{(0,x,y)\in\mathbb{F}_2\times\mathbb{F}_{2^k}\times\mathbb{F}_{2^k}}(-1)^{\mathrm{tr}_1^k(v_2x+v_3y)} \\ &\quad - \sum_{(1,x,x)\in\mathbb{F}_2\times\mathbb{F}_{2^k}\times\mathbb{F}_{2^k}}(-1)^{v_1+\mathrm{tr}_1^k(v_2+v_3)x} - \sum_{(0,x,F(x))\in\mathbb{F}_2\times\mathbb{F}_{2^k}\times\mathbb{F}_{2^k}}(-1)^{\mathrm{tr}_1^k(v_2x+v_3F(x))}\Bigg).\end{aligned}$$

由 (7) 式可知, $wt(\mathbf{c_v})$ 的值依赖于布尔函数 f 在点 $\mathbf{v}\in\mathbb{F}_2^k$ 处的 Walsh 谱值. 下面基于 v_1,v_2,v_3 的不同取值分类讨论 f 在点 $\mathbf{v}$ 处的 Walsh 谱值.

(1) 若 $v_1=0$, $v_2\in\mathbb{F}_{2^k}$, $v_3\neq 0$, 则

当 $v_2+v_3=0$ 时, $\hat{f}(\mathbf{v})=\begin{cases}2^{k+1},\\ 2^{k+1}-2^{\frac{k+r+2}{2}},\\ 2^{k+1}+2^{\frac{k+r+2}{2}};\end{cases}$

当 $v_2+v_3\neq 0$ 时, $\hat{f}(\mathbf{v})=\begin{cases}0,\\ -2^{\frac{k+r+2}{2}},\\ 2^{\frac{k+r+2}{2}}.\end{cases}$

(2) 若 $v_2\neq v_3=0$, 即 $v_2+v_3\neq 0$, 则无论 v_1 是否为零都有 $\hat{f}(\mathbf{v})=0$.

(3) 若 $v_1=1$, $v_2=0$, $v_3=0$, 即 $v_2+v_3=0$, 则 $\hat{f}(\mathbf{v})=0$.

(4) 若 $v_1=1$, $v_2\in\mathbb{F}_{2^k}$, $v_3\neq 0$, 则

当 $v_2+v_3=0$ 时, $\hat{f}(\mathbf{v})=\begin{cases}-2^{k+1},\\ -2^{k+1}-2^{\frac{k+r+2}{2}},\\ -2^{k+1}+2^{\frac{k+r+2}{2}};\end{cases}$

当 $v_2+v_3\neq 0$ 时, $\hat{f}(\mathbf{v})=\begin{cases}0,\\ -2^{\frac{k+r+2}{2}},\\ 2^{\frac{k+r+2}{2}}.\end{cases}$

将上述结果代入 (7) 式,

$$wt(\mathbf{c_v})\in\Big\{0,2^{2k}-2^{k-1},2^{2k}-2^k,2^{2k}-3\cdot 2^{k-1},2^{2k}-2^{k-1}-2^{\frac{k+r-2}{2}},2^{2k}-2^{k-1}+2^{\frac{k+r-2}{2}},\\ 2^{2k}-2^k-2^{\frac{k+r-2}{2}},2^{2k}-2^k+2^{\frac{k+r-2}{2}},2^{2k}-3\cdot 2^{k-1}-2^{\frac{k+r-2}{2}},2^{2k}-3\cdot 2^{k-1}+2^{\frac{k+r-2}{2}}\Big\}.$$

同理, 将上述 Wlash 谱值代入 (6) 式可得码 C_f 中码字的汉明重量. □

定理 2. 符号如上所示, 则当 $r=1$, 即 F 为 $\mathbb{F}_{2^k}$ 上的 AB 函数时, C_D 是一类参数为 $[2^{2k+1}-2^{k+1},2k+1,2^{2k}-3\cdot 2^{k-1}-2^{\frac{k-1}{2}}]$ 的二元线性码, 其重量分布如表 1所示; C_f 是一类参数为 $[2^{2k+1}-1,2k+2,2^{2k}-2^k-2^{\frac{k+1}{2}}]$ 的宽极小码, 其重量分布如表 2所示.

Table 1. The weight distribution of C_D for $r=1$

表 1. $r=1$ 时 C_D 的重量分布

重量	频数
0	1
$2^{2k}-2^{k-1}$	2^{k-1}
$2^{2k}-2^{k-1}-2^{\frac{k-1}{2}}$	$2^{k-2}-2^{\frac{k-3}{2}}$
$2^{2k}-2^{k-1}+2^{\frac{k-1}{2}}$	$2^{k-2}+2^{\frac{k-3}{2}}$
$2^{2k}-2^k$	$2^{2k}-1$
$2^{2k}-2^k-2^{\frac{k-1}{2}}$	$2(2^k-2)(2^{k-2}-2^{\frac{k-3}{2}})$
$2^{2k}-2^k+2^{\frac{k-1}{2}}$	$2(2^k-2)(2^{k-2}+2^{\frac{k-3}{2}})$
$2^{2k}-3\cdot 2^{k-1}$	2^{k-1}
$2^{2k}-3\cdot 2^{k-1}-2^{\frac{k-1}{2}}$	$2^{k-2}-2^{\frac{k-3}{2}}$
$2^{2k}-3\cdot 2^{k-1}+2^{\frac{k-1}{2}}$	$2^{k-2}+2^{\frac{k-3}{2}}$

证明 首先确定 $r=1$ 时 C_D 的重量分布. 记 $S_f=\{\alpha\in\mathbb{F}_2^k:\hat{f}(\alpha)\neq 0\}$. 由 (1) 式

$$\sum_{\alpha\in\mathbb{F}_2^k}\hat{f}^2(\alpha)=2^{k+1}\|S_f\|=2^{2k},$$

可得 $\|S_f\|=2^{k-1}, \|\overline{S_f}\|=2^k-2^{k-1}=2^{k-1}$, 其中 $\overline{S_f}=\mathbb{F}_2^k\backslash S_f$. 设 $S_f^{(+)}:=\{\alpha\in\mathbb{F}_2^k:\hat{f}(\alpha)>0\}$, $S_f^{(-)}:=\{\alpha\in\mathbb{F}_2^k:\hat{f}(\alpha)<0\}$, 则根据定义

$$\|S_f^{(+)}\|+\|S_f^{(-)}\|=\|S_f\|=2^{k-1}. \tag{8}$$

Table 2. The weight distribution of C_f for $r=1$

表 2. $r=1$ 时 C_f 的重量分布

重量	频数
0	1
$2^{2k}-2^k$	2^{k-1}
$2^{2k}-2^k+2^{\frac{k+1}{2}}$	$2^{k-2}-2^{\frac{k-3}{2}}$
$2^{2k}-2^k-2^{\frac{k+1}{2}}$	$2^{k-2}+2^{\frac{k-3}{2}}$
2^{2k}	$3\cdot 2^{2k}-2$
$2^{2k}+2^{\frac{k+1}{2}}$	$2(2^k-2)(2^{k-2}-2^{\frac{k-3}{2}})$
$2^{2k}-2^{\frac{k+1}{2}}$	$2(2^k-2)(2^{k-2}+2^{\frac{k-3}{2}})$
$2^{2k}+2^k$	2^{k-1}
$2^{2k}+2^k+2^{\frac{k+1}{2}}$	$2^{k-2}-2^{\frac{k-3}{2}}$
$2^{2k}+2^k-2^{\frac{k+1}{2}}$	$2^{k-2}+2^{\frac{k-3}{2}}$
$2^{2k+1}-2^{k+1}$	1

由布尔函数 f 在点 $\alpha\in\mathbb{F}_2^k$ 处的 Walsh 变换定义可得

$$\sum_{\alpha\in\mathbb{F}_2^k}\hat{f}(\alpha)=\sum_{\mathbf{x}\in\mathbb{F}_2^k}(-1)^{f(\mathbf{x})}\sum_{\alpha\in\mathbb{F}_2^k}(-1)^{\alpha\cdot\mathbf{x}}=2^k(-1)^{f(\mathbf{0})}=2^k,$$

则 $2^{\frac{k+1}{2}}\cdot\|S_f^{(+)}\|+(-2^{\frac{k+1}{2}})\cdot\|S_f^{(-)}\|+0\cdot\|S_f\|=2^k$, 即

$$2^{\frac{k+1}{2}}(\|S_f^{(+)}\|-\|S_f^{(-)}\|)=2^k. \tag{9}$$

由 (8) 式和 (9) 式解得 $\|S_f^{(+)}\|=\frac{1}{2}(2^{k-1}+2^{\frac{k-1}{2}})$, $\|S_f^{(-)}\|=\frac{1}{2}(2^{k-1}-2^{\frac{k-1}{2}})$.

下面仅确定定理 1 的第一种情形, 即满足条件 (1) 的汉明重量的码字个数. 其他情形同理可证, 不再赘述. 以下用 $\gamma(a)$ 表示汉明重量为 a 的码字频数.

(a) 当 $v_2+v_3=0$ 即 $v_2=v_3\neq 0$ 时,
$\gamma(2^{2k}-2^{k-1})=\|\overline{S_f}\|=2^{k-1}$,
$\gamma(2^{2k}-2^{k-1}+2^{\frac{k-1}{2}})=\|S_f^{(+)}\|=2^{k-2}+2^{\frac{k-3}{2}}$,
$\gamma(2^{2k}-2^{k-1}-2^{\frac{k-1}{2}})=\|S_f^{(-)}\|=2^{k-2}-2^{\frac{k-3}{2}}$.

(b) 当 $v_2+v_3\neq 0$ 时,

$\gamma(2^{2k}-2^k)=(2^k-2)\|\overline{S_f}\|=(2^k-2)2^{k-1}$,

$\gamma(2^{2k}-2^k+2^{\frac{k-1}{2}})=(2^k-2)\|S_f^{(+)}\|=(2^k-2)(2^{k-2}+2^{\frac{k-3}{2}})$,

$\gamma(2^{2k}-2^k-2^{\frac{k-1}{2}})=(2^k-2)\|S_f^{(-)}\|=(2^k-2)(2^{k-2}-2^{\frac{k-3}{2}})$.

注意到, 当 $v_1=1$, $v_2\in\mathbb{F}_{2^k}$, $v_3\neq 0$ 且 $v_2+v_3\neq 0$ 时, 重量对应的码字个数与情形 (b) 相同.

同理, 当 $r=1$ 时, C_f 的重量分布可类似确定. 其中, 由引理 1 和引理 3 可得

$$\widehat{f}(0)=2^m-2\|\operatorname{supp}(f)\|=2^{2k+1}-2(2^{2k+1}-2^{k+1})=2^{k+2}-2^{2k+1},$$

$$wt(c_v)=2^{m-1}-\frac{1}{2}\hat{f}(0)=2^{2k}-\frac{1}{2}(2^{k+2}-2^{2k+1})=2^{2k+1}-2^{k+1}.$$

码 C_f 中其他码字的汉明重量及重量分布与 C_D 类似, 这里不再详细证明.

下面讨论 C_D 的极小性, 首先由定理 1 可知, C_D 的码长 $n=2^{2k+1}-2^{k+1}$, 维数 $m=2k+1$. 则对于任意的 $\mathbf{u}\neq\mathbf{v}\in\mathbb{F}_2^{2k+1}\backslash\{\mathbf{0}\}$, 由上述码字的汉明重量可得,

$$wt(\mathbf{c_v})\neq n, wt(\mathbf{c_v})-wt(\mathbf{c_u})\neq 2^{m-2},$$

$$wt(\mathbf{c_v})+wt(\mathbf{c_u})-n\neq 2^{m-2}.$$

并且容易验证, 对于任意的 $\mathbf{v}\in\mathbb{F}_2^{2k+1}\backslash\{\mathbf{0}\}$, 有

$$\frac{\min\left\{2^{2k},2^{2k}-2wt\left(\mathbf{c_v}\right)+n,n\right\}}{\max\left\{2^{2k},2^{2k}-2wt\left(\mathbf{c_v}\right)+n,n\right\}}<\frac{1}{2}.$$

因此, 由引理 4 可以确定一类参数为 $[2^{2k+1}-1,2k+2,2^{2k}-2^k-2^{\frac{k+1}{2}}]$ 的宽极小二元线性码. □

引理 5. [20] 令 $D_1\subseteq D_2$ 是元素在 $\mathbb{F}_2^m$ 中的两个多重集合, 且 $\operatorname{rank}(D_1)=\operatorname{rank}(D_2)=m$, 其中 $\operatorname{rank}(D_i)$ 表示 D_i 中元素构成矩阵的秩, $i=1,2$. 若 C_{D_1} 是极小码, 则 C_{D_2} 也是极小码.

注记 1. 符号如上所示. 令定义集

$$D'=\{(1,x,y):x,y\in\mathbb{F}_{2^k}\}\backslash\{(1,0,0)\}$$

$$\cup\{(0,x,y):x,y\in\mathbb{F}_{2^k}\}\backslash\{(0,x,F(x)):x\in\mathbb{F}_{2^k}\},$$

当 $r=1$ 即 F 为 $\mathbb{F}_{2^k}$ 上的 AB 函数, $F(0)=0$ 时. 则显然有 $D'\subseteq D$, 其中 D 为定理 1 中的定义集. 由引理 5, $C_{D'}$ 为一极小二元线性码, 这与文献 [18] 的结论一致, 但证法有所不同.

4. 总结

本文首先通过对向量布尔函数设计线性码的两种一般构造之间的关系进行分析, 通过选取合适的定义集, 构造了一类新的极小二元线性码. 并利用向量布尔函数的密码学性质确定了码的长度, 维数和汉明重量. 然后, 当参数取特殊值时, 确定了码的重量分布. 特别地, 本文所构造的极小码均为宽极小码, 即不满足 Ashikhmin-Barg 条件. 最后, 本文推广了文献 [18] 的部分结果. 结果表明, 这些线性码可以用来构造具有良好访问结构的秘密共享方案.

参考文献

[1] Anderson, R., Ding, C., Helleseth, T., *et al.* (1998) How to Build Robust Shared Control Systems. *Designs, Codes and Cryptography*, **15**, 111-124. https://doi.org/10.1023/A:1026421315292

[2] Ding, K. and Ding, C. (2015) A Class of Two-Weight and Three-Weight Codes and Their Applications in Secret Sharing. *IEEE Transactions on Information Theory*, **61**, 5835-5842. https://doi.org/10.1109/TIT.2015.2473861

[3] Ding, C. and Wang, X. (2005) A Coding Theory Construction of New Systematic Authentication Codes. *Theoretical Computer Science*, **330**, 81-99. https://doi.org/10.1016/j.tcs.2004.09.011

[4] Delsarte, P. and Levenshtein, V.I. (1998) Association Schemes and Coding Theory. *IEEE Transactions on Information Theory*, **44**, 2477-2504. https://doi.org/10.1109/18.720545

[5] Ashikhmin, A. and Barg, A. (1998) Minimal Vectors in Linear Codes. *IEEE Transactions on Information Theory*, **44**, 2010-2017. https://doi.org/10.1109/18.705584

[6] Ding, C. (2015) Linear Codes from Some 2-Designs. *IEEE Transactions on Information Theory*, **61**, 3265-3275. https://doi.org/10.1109/TIT.2015.2420118

[7] Heng, Z. and Yue, Q. (2015) A Class of Binary Linear Codes with at Most Three Weights. *IEEE Communications Letters*, **19**, 1488-1491. https://doi.org/10.1109/LCOMM.2015.2455032

[8] Heng, Z., Yue, Q. and Li, C. (2016) Three Classes of Linear Codes with Two or Three Weights. *Discrete Mathematics*, **339**, 2832-2847. https://doi.org/10.1016/j.disc.2016.05.033

[9] Tang, C., Li, N., Qi, Y., *et al.* (2016) Linear Codes with Two or Three Weights from Weakly Regular Bent Functions. *IEEE Transactions on Information Theory*, **62**, 1166-1176. https://doi.org/10.1109/TIT.2016.2518678

[10] Tang, C., Qi, Y. and Huang, D. (2015) Two-Weight and Three-Weight Linear Codes from Square Functions. *IEEE Communications Letters*, **20**, 29-32. https://doi.org/10.1109/LCOMM.2015.2497344

[11] Chang, S. and Hyun, J.Y. (2018) Linear Codes from Simplicial Complexes. *Designs, Codes and Cryptography*, **86**, 2167-2181. https://doi.org/10.1007/s10623-017-0442-5

[12] Ding, C., Heng, Z. and Zhou, Z. (2018) Minimal Binary Linear Codes. *IEEE Transactions on Information Theory*, **64**, 6536-6545. https://doi.org/10.1109/TIT.2018.2819196

[13] Bartoli, D. and Bonini, M. (2019) Minimal Linear Codes in Odd Characteristic. *IEEE Transactions on Information Theory*, **65**, 4152-4155. https://doi.org/10.1109/TIT.2019.2891992

[14] Bonini, M. and Borello, M. (2021) Minimal Linear Codes Arising from Blocking Sets. *Journal of Algebraic Combinatorics*, **53**, 327-341. https://doi.org/10.1007/s10801-019-00930-6

[15] Ding, C. (2016) A Construction of Binary Linear Codes from Boolean Functions. *Discrete Mathematics*, **339**, 2288-2303. https://doi.org/10.1016/j.disc.2016.03.029

[16] Carlet, C. and Ding, C. (2007) Nonlinearities of S-Boxes. *Finite Fields and Their Applications*, **13**, 121-135. https://doi.org/10.1016/j.ffa.2005.07.003

[17] Wadayama, T., Hada, T., Wakasugi, K., *et al.* (2001) Upper and Lower Bounds on Maximum Nonlinearity of n-Input m-Output Boolean Function. *Designs, Codes and Cryptography*, **23**, 23-34. https://doi.org/10.1023/A:1011207501748

[18] Tang, D. and Li, X. (2020) A Note on Theminimal Binary Linear Code. *Cryptography and Communications*, **12**, 375-388. https://doi.org/10.1007/s12095-019-00412-3

[19] Li, X. and Yue, Q. (2020) Four Classes of Minimal Binary Linear Codes with $w_{min}/w_{max} < 1/2$ Derived from Boolean Functions. *Designs, Codes and Cryptography*, **88**, 257-271. https://doi.org/10.1007/s10623-019-00682-1

[20] Lu, W., Wu, X. and Cao, X. (2021) The Parameters of Minimal Linear Codes. *Finite Fields and Their Applications*, **71**, Article 101799. https://doi.org/10.1016/j.ffa.2020.101799