两类极小二元线性码的构造

杜小妮* 胡金霞 金文刚 孙彦中
(西北师范大学数学与统计学院 兰州 730070)

摘 要：线性码在数据存储、信息安全以及秘密共享等领域具有重要的作用。而极小线性码是设计秘密共享方案的首选码，设计极小线性码是当前密码与编码研究的重要内容之一。该文首先选取恰当的布尔函数，研究了函数的Walsh谱值分布，并利用布尔函数的Walsh谱值分布构造了两类极小线性码，确定了码的参数及重量分布。结果表明，所构造的码是不满足Ashikhmin-Barg条件的极小线性码，可用作设计具有良好访问结构的秘密共享方案。

关键词：布尔函数；Walsh变换；2元线性码
中图分类号：TN918.2; TTP391 **文献标识码**：A **文章编号**：1009-5896(2022)10-3643-07
DOI: 10.11999/JEIT210720

Construction of Two Classes of Minimal Binary Linear Codes

DU Xiaoni HU Jinxia JIN Wengang SUN Yanzhong
(*College of Mathematics and Statistics*, *Northwest Normal University*, *Lanzhou* 730070, *China*)

Abstract: Linear codes play an important role in data storage, information security and secret sharing. Minimal linear codes are the first choice to design secret sharing schemes, so the design of minimal linear codes is one of the important contents of current cryptosystem and coding theory. In this paper, the Walsh spectrum distribution of the selected Boolean functions is studied, and two kinds of minimal linear codes are obtained by using the Walsh spectrum distribution of the functions, then the weight distribution of the codes are determined. The results show that the constructed codes are minimal linear codes that do not satisfy the Ashikhmin-Barg condition, and can be used to design secret sharing schemes with good access structure.

Key words: Boolean functions; Walsh transform; Binary linear codes

1 引言

线性码因其具有良好的代数结构、易于描述和加解密等特性，在通信、数据存储、信息安全和密码学等领域具有广泛的应用。特别地，极小线性码是一类特殊的线性码，在构造具有良好访问结构的秘密共享方案[1,2]和两方安全计算[3,4]中起着重要的作用。线性码的重量分布既能说明码的纠错能力，又可用来计算信息在传输过程中发生错误的概率，因而确定线性码的重量分布问题是编码理论中的一个重要课题，但确定一般线性码的重量分布是非常困难的。

布尔函数作为一类重要的密码学函数在编码密码领域有着广泛的应用，如利用布尔函数的Walsh谱值分布来构造极小线性码、雷德-穆勒(Reed-Muller, RM) 码[5]和Kerdock码[6]等。1972 年，Baumert等人[7]首次提出了基于定义集构造具有较低重量线性码的方法，随后，学者们基于该方法设计了多类低重线性码[8,9]。2016年，Ding[10]通过选取合适的定义集，提出了利用布尔函数的Walsh谱值分布研究2元线性码的方法。2018年，Chang等人[11]提出了一类不满足Ashikhmin-Barg条件的极小2元线性码。随后，Heng等人[12]构造了一类不满足Ashikhmin-Barg条件的无限族极小3元线性码，并给出了判断极小线性码的充分必要条件。同年， Ding等人[13]得到了3类不满足Ashikhmin-Barg条件的无限族极小2元码，并给出了码的重量分布，且提出了新的判断极小线性码的充要条件。2020年，Mesnager等人[14]利用特征函数的性质，进一步推广了文献[13]的结果。

受上述文献的启发，本文利用所设计的布尔函数的Walsh谱值分布构造了两类极小2元线性码。具体地，首先得到了给定的Maiorana-McFarland类布尔函数中某些特殊函数的Walsh谱值分布，利用文献[13]中的方法，以布尔函数的Walsh变换为工具，构造了第1类极小2元线性码，并确定了其参

收稿日期：2021-07-16；改回日期：2022-04-03；网络出版：2022-04-22
*通信作者： 杜小妮 ymLdxn@126.com
基金项目：国家自然科学基金(61772022, 62172337)
Foundation Items: The National Natural Science Foundation of China (61772022, 62172337)

数和重量分布。其次，利用文献[14]中的方法，结合特征函数的性质，构造了第2类极小2元线性码，确定了码的参数和重量分布。结果表明，本文所构造的这两类码均是不满足Ashikhmin-Barg条件的极小2元线性码，可用于设计具有良好访问结构的秘密共享方案。

本文的组织结构如下，第2节主要介绍有限域中的一些定义和基本事实；第3节给出了两类线性码的构造；最后，总结全文。

2 预备知识

本节介绍一些基本的概念和已有的结论。

设m为正整数，$\boldsymbol{F}_2^m$表示有限域$\boldsymbol{F}_2$上的m维向量空间，B_m表示$\boldsymbol{F}_2^m \sim \boldsymbol{F}_2$上的布尔函数集合。有限域$\boldsymbol{F}_2$上$n$维空间$\boldsymbol{F}_2^n$的一个$k$维子空间称为码长为$n$，维数为$k$的$[n,k,d]$2元线性码，其中$d$表示码的最小汉明重量，码$\boldsymbol{C}$中的每一个向量$\boldsymbol{c}$称为码字。设$A_i$表示码$\boldsymbol{C}$中汉明重量为$i$的码字的个数，$1+A_1z+A_2z^2+\cdots+A_nz^n$定义为码$\boldsymbol{C}$的重量计数器，序列$(1,A_1,A_2,\cdots,A_n)$称为码$\boldsymbol{C}$的重量分布。若在$(1,A_1,A_2,\cdots,A_n)$中，使得$A_i\neq 0(1\le i\le n)$的个数为$t$，则称码$\boldsymbol{C}$为$t$重码。码字$\boldsymbol{c}=(c_0,c_1,\cdots,c_{n-1})\in\boldsymbol{C}$的支撑集定义为

$$\text{Suppt}\,(c)=\{0\le i\le n-1:c_i\neq 0\} \tag{1}$$

根据定义可知，码字c的汉明重量$\text{wt}(\boldsymbol{c})$满足

$$\text{wt}(\boldsymbol{c})=|\text{Suppt}\,(\boldsymbol{c})| \tag{2}$$

若对任意的向量$\boldsymbol{u},\boldsymbol{v}\in\boldsymbol{F}_2^n$，有$\text{Suppt}\,(\boldsymbol{v})\subseteq\text{Suppt}\,(\boldsymbol{u})$，则称$\boldsymbol{u}$覆盖$\boldsymbol{v}$。若码$\boldsymbol{C}$的一个非0码字$c$只覆盖它的纯量倍数，则称$\boldsymbol{c}$是一个极小向量。若码$\boldsymbol{C}$中的所有码字均是极小向量，则称线性码$\boldsymbol{C}$是极小线性码。

下述引理给出了利用码的重量分布判别极小线性码的充分条件。

引理1[15] (Ashikhmin-Barg条件)设$w_{\min}$和$w_{\max}$分别表示线性码$\boldsymbol{C}$的最小和最大非0重量。如果$w_{\min}/w_{\max}>1/2$，则$\boldsymbol{C}$是$\boldsymbol{F}_2$上的极小线性码。

接下来介绍Krawchouk多项式及其性质。这些结果及其证明过程详见文献[16]。

设m是正整数，x是一个非0变量，则Krawchouk多项式定义为

$$P_k(x,m)=\sum_{j=0}^{k}(-1)^j\begin{pmatrix}x\\j\end{pmatrix}\begin{pmatrix}m-x\\k-j\end{pmatrix} \tag{3}$$

其中，$0\le k\le m$。在不引起歧义的前提下，简记$P_k(x)=P_k(x,m)$，显然有

$$(1+z)^{m-x}(1-z)^x=\sum_{k=0}^{m}P_k(x)z^k \tag{4}$$

引理2[16] 设$\boldsymbol{u},\boldsymbol{v}\in F_2^m$且汉明重量为$\text{wt}(\boldsymbol{u})=i$，$0\le i\le m$，则$\sum_{\text{wt}(\boldsymbol{v})=k}(-1)^{\boldsymbol{u}\cdot\boldsymbol{v}}=P_k(i)$。

设$f(\boldsymbol{x})\in B_m$，对任意的$\boldsymbol{w}\in\boldsymbol{F}_2^m$，$f(\boldsymbol{x})$的Walsh变换定义为

$$\hat{f}(\boldsymbol{w})=\sum_{\boldsymbol{x}\in\boldsymbol{F}_2^m}(-1)^{f(\boldsymbol{x})+\boldsymbol{w}\cdot\boldsymbol{x}} \tag{5}$$

其中，$\boldsymbol{w}\cdot\boldsymbol{x}$是$\boldsymbol{w}$和$\boldsymbol{x}$的内积。若将$f(\boldsymbol{x})$看作只有0和1的实值函数，则与$f(\boldsymbol{x})$相关的Walsh变换可定义为

$$\tilde{f}(\boldsymbol{w})=\sum_{\boldsymbol{x}\in\boldsymbol{F}_2^m}f(x)(-1)^{\boldsymbol{w}\cdot\boldsymbol{x}} \tag{6}$$

显然，这两种Walsh变换之间有如式(7)的关系

$$\hat{f}(\boldsymbol{w})=\begin{cases}2^m-2\tilde{f}(\boldsymbol{0}), & \boldsymbol{w}=\boldsymbol{0}\\ -2\tilde{f}(\boldsymbol{w}), & \boldsymbol{w}\neq\boldsymbol{0}\end{cases} \tag{7}$$

$f(\boldsymbol{x})$的Walsh变换是多重集$\left\{\left\{\hat{f}(\boldsymbol{w}):\boldsymbol{w}\in\boldsymbol{F}_2^m\right\}\right\}$。$f(\boldsymbol{x})$的支撑定义为

$$\text{Suppt}(f)=\{\boldsymbol{x}\in\boldsymbol{F}_2^m:f(\boldsymbol{x})=1\} \tag{8}$$

设$f(\boldsymbol{x})\in\boldsymbol{B}_m$，满足$f(\boldsymbol{0})=0$，且至少存在1个$\boldsymbol{b}\in\boldsymbol{F}_2^m$使得$f(\boldsymbol{b})=1$。定义线性码$C_f$为

$$C_f=\left\{(\boldsymbol{u}f(\boldsymbol{x})+\boldsymbol{v}\cdot\boldsymbol{x})_{\boldsymbol{x}\in\boldsymbol{F}_2^m\setminus\{\boldsymbol{0}\}}:\boldsymbol{u}\in\boldsymbol{F}_2,\boldsymbol{v}\in\boldsymbol{F}_2^m\right\} \tag{9}$$

下述引理给出了当函数f的Walsh变换的值确定时，线性码C_f的重量分布。

引理3[13] 若对所有的$\boldsymbol{w}\in\boldsymbol{F}_2^m$有$f(\boldsymbol{x})\neq\boldsymbol{w}\cdot\boldsymbol{x}$，则式(9)中定义的2元码$C_f$长为$2^m-1$，维数为$m+1$，$C_f$的重量分布由式(10)的多重集给出

$$\begin{aligned}&\left\{2^{m-1}+\tilde{f}(\boldsymbol{\omega}):\boldsymbol{\omega}\in\mathbb{F}_2^m\setminus\{\boldsymbol{0}\}\right\}\cup\left\{\tilde{f}(\boldsymbol{0})\right\}\\&\quad\cup\left\{2^{m-1}:\boldsymbol{\omega}\in\mathbb{F}_2^m\setminus\{\boldsymbol{0}\}\right\}\cup\{0\}\\&=\left\{2^m-\hat{f}(\boldsymbol{\omega})\Big/2:\omega\in\mathbb{F}_2^m\right\}\\&\quad\cup\left\{2^{m-1}:\boldsymbol{\omega}\in\mathbb{F}_2^m\setminus\{\boldsymbol{0}\}\right\}\cup\{0\}\end{aligned} \tag{10}$$

下述引理给出了判定式(9)所构造的码是否为极小码的充要条件。

引理4[13] 式(9)中定义的C_f是极小码当且仅当对任意的$\boldsymbol{a},\boldsymbol{b}\in\boldsymbol{F}_2^m,\boldsymbol{a}\neq\boldsymbol{b}$，有

$$\hat{f}(\boldsymbol{a})\pm\hat{f}(\boldsymbol{b})\neq 2^m \tag{11}$$

3 主要结论及证明

本节将利用一般的Maiorana-McFarland类布尔函数和特征函数的性质，得到了两类不满足Ashikhmin-Barg条件的极小2元线性码。

3.1 第1类极小2元线性码

设m是任意正整数，s和t是满足$s+t=m$的两

个正整数。一般Maiorana-McFarland类函数形式为

$$f(\boldsymbol{x},\boldsymbol{y})=\phi(\boldsymbol{x})\cdot\boldsymbol{y}+g(\boldsymbol{x}) \tag{12}$$

其中，$\boldsymbol{x}\in\boldsymbol{F}_2^s$, $\boldsymbol{y}\in\boldsymbol{F}_2^t$, ϕ是从$\boldsymbol{F}_2^s$到$\boldsymbol{F}_2^t$的任意映射，g是$\boldsymbol{F}_2^s$上任意的布尔函数。对于式 (12) 定义的布尔函数，显然对任意的$(\boldsymbol{a}_1,\boldsymbol{a}_2)\in\boldsymbol{F}_2^s\times\boldsymbol{F}_2^t$，有

$$\hat{f}(\boldsymbol{a}_1,\boldsymbol{a}_2)=\begin{cases}2^t\displaystyle\sum_{\boldsymbol{x}\in\phi^{-1}(\boldsymbol{a}_2)}(-1)^{g(\boldsymbol{x})+\boldsymbol{a}_1\cdot\boldsymbol{x}}, & \boldsymbol{a}_2\in\mathrm{Im}\phi\\ 0, & \boldsymbol{a}_2\notin\mathrm{Im}\phi\end{cases} \tag{13}$$

其中，$\mathrm{Im}\phi=\{\phi(\boldsymbol{x}):\boldsymbol{x}\in\boldsymbol{F}_2^s\}$, $\phi^{-1}(\boldsymbol{a}_2)=\{\boldsymbol{x}:\phi(\boldsymbol{x})=\boldsymbol{a}_2,\boldsymbol{x}\in\boldsymbol{F}_2^s\}$。

引理5[13]　设$\boldsymbol{U}$和$\boldsymbol{V}$分别为$\boldsymbol{F}_2^s$和$\boldsymbol{F}_2^t$的子集且$2^s-|\boldsymbol{U}|\le 2^t-|\boldsymbol{V}|$，$\phi$是从$F_2^s\backslash\boldsymbol{U}$到$F_2^t\backslash\boldsymbol{V}$的嵌入映射，则对于式 (12) 中的布尔函数，有

$$\hat{f}(\boldsymbol{a}_1,\boldsymbol{a}_2)=\begin{cases}2^t(-1)^{g(\phi^{-1}(\boldsymbol{a}_2))+\boldsymbol{a}_1\cdot\phi^{-1}(\boldsymbol{a}_2)}, & \boldsymbol{a}_2\in\mathrm{Im}\phi\backslash\boldsymbol{V}\\ 2^t\displaystyle\sum_{\boldsymbol{x}\in\phi^{-1}(\boldsymbol{a}_2)}(-1)^{g(\boldsymbol{x})+\boldsymbol{a}_1\cdot\boldsymbol{x}}, & \boldsymbol{a}_2\in\mathrm{Im}\phi\cap\boldsymbol{V}\\ 0, & \boldsymbol{a}_2\notin\mathrm{Im}\phi\end{cases} \tag{14}$$

下文中，令$m\ge 11$是一个奇整数，$s=\dfrac{m+1}{2}$, $t=\dfrac{m-1}{2}$, $\boldsymbol{U}=\{\boldsymbol{x}\in\boldsymbol{F}_2^s:\mathrm{wt}(\boldsymbol{x})\ge 3\}$, $\boldsymbol{V}=\{\boldsymbol{0}\}$且满足$2^s-|\boldsymbol{U}|\le 2^t-|\boldsymbol{V}|$。为讨论方便，记$A(i)=2i^2-3i-2si+\dfrac{s^2+s}{2}+1$，其中整数$1\le i\le s$。

引理6　符号如上所示，则有

$$\sum_{\boldsymbol{x}\in\boldsymbol{U}}(-1)^{\boldsymbol{a}_1\cdot\boldsymbol{x}}=\begin{cases}2^s-1-\frac{s(s+1)}{2}, & \mathrm{wt}(\boldsymbol{a}_1)=0\\ -A(i), & \mathrm{wt}(\boldsymbol{a}_1)=i\end{cases} \tag{15}$$

其中，$\boldsymbol{a}_1\in\boldsymbol{F}_2^s$。

证明　当$\mathrm{wt}(\boldsymbol{a}_1)=0$时，有

$$\sum_{\boldsymbol{x}\in\boldsymbol{U}}(-1)^{\boldsymbol{a}_1\cdot\boldsymbol{x}}=\sum_{\boldsymbol{x}\in\boldsymbol{U}}(-1)^{0\cdot\boldsymbol{x}}=|\boldsymbol{U}|=2^s-1-\frac{s(s+1)}{2} \tag{16}$$

设$\mathrm{wt}(\boldsymbol{a}_1)=i$, $1\le i\le s$，由Krawchouk多项式的定义和引理2可得

$$\begin{aligned}\sum_{\boldsymbol{x}\in\boldsymbol{U}}(-1)^{\boldsymbol{a}_1\cdot\boldsymbol{x}}&=\sum_{\boldsymbol{x}\in\boldsymbol{F}_2^s}(-1)^{\boldsymbol{a}_1\cdot\boldsymbol{x}}-\sum_{\boldsymbol{x}\in\boldsymbol{F}_2^s,\,\mathrm{wt}(\boldsymbol{x})\le 2}(-1)^{\boldsymbol{a}_1\cdot\boldsymbol{x}}\\&=0-(P_0(i)+P_1(i)+P_2(i))\\&=-\left(1+s-2i+\frac{s^2+4i^2-4si-s-2i}{2}\right)\\&=-A(i)\end{aligned} \tag{17}$$

引理得证。

注记1　由m是奇数，且$2^s-|\boldsymbol{U}|\le 2^t-|\boldsymbol{V}|$，由$\boldsymbol{U}$和$\boldsymbol{V}$的定义，有

$$\begin{aligned}&2^s-|\boldsymbol{U}|-(2^t-|\boldsymbol{V}|)\\&=2^s-\left(2^s-1-s-\frac{s(s-1)}{2}\right)-(2^t-1)\\&=2+\frac{s(s+1)}{2}-2^t\\&=2+\frac{(m+1)(m+3)}{8}-2^{\frac{m-1}{2}}\le 0\end{aligned} \tag{18}$$

可得$m\ge 11$。

下文中，除非特别说明，总假设$k(k\ge 7)$为奇数。关于$A(i),1\le i\le s$的取值，有如下的结论：

引理7　符号如上所示，则有

(1) 当s形如$(k^2-1)/8$时，若

$$i=\begin{cases}\dfrac{2s+3+k}{4}, & k\equiv 1,3\ (\mathrm{mod}\,8)\\ \dfrac{2s+3-k}{4}, & k\equiv 5,7\ (\mathrm{mod}\,8)\end{cases} \tag{19}$$

有$A(i)=0$，且对所有的$1\le j\le s$，有$A(j)\ne\pm 1$。

(2) 当s形如$(k^2+7)/8$时，若

$$i=\begin{cases}\dfrac{2s+3-k}{4}, & k\equiv 1,3\ (\mathrm{mod}\,8)\\ \dfrac{2s+3+k}{4}, & k\equiv 5,7\ (\mathrm{mod}\,8)\end{cases} \tag{20}$$

有$A(i)=-1$，且对所有的$1\le j\le s$，有$A(j)\ne 0,1$。

(3) 当s形如$(k^2-9)/8$ (奇数$k\ge 9$) 时，若

$$i=\begin{cases}\dfrac{2s+3-k}{4}, & k\equiv 1,3\ (\mathrm{mod}\,8)\\ \dfrac{2s+3+k}{4}, & k\equiv 5,7\ (\mathrm{mod}\ 8)\end{cases} \tag{21}$$

有$A(i)=1$，且对所有的$1\le j\le s$，有$A(j)\ne 0,-1$。

(4) 对所有的$1\le i\le s$，有$-2s\le A(i)\le s(s-3)/2$。

证明　(1) 若存在正整数$1\le i\le s$，使得$A(i)=0$时，由判别式$\Delta=32s+4>0$可知，$i=(2s+3\pm\sqrt{8s+1})/4$为两个不等实根，显然此时s是形如$(k^2-1)/8$的正整数，其中$k\ge 7$，且有

$$i=\begin{cases}\dfrac{2s+3+k}{4}, & k\equiv 1,3\ (\mathrm{mod}\,8)\\ \dfrac{2s+3-k}{4}, & k\equiv 5,7\ (\mathrm{mod}\,8)\end{cases} \tag{22}$$

特别地，由s的选取，对所有的$1\le j\le s$，必有$A(j)\ne\pm 1$。

(2) 和(3)的证明与(1)类似，此处不再赘述。

(4) 由$m \ge 11$可知，$s = \dfrac{m+1}{2} \ge 6$。为讨论方便，令函数$A(x) = 2x^2 - 3x - 2sx + \dfrac{s^2+s}{2} + 1$，$1 \le x \le s$。显然$A(x)$的对称轴为$x = \dfrac{2s+3}{4}$，曲线$A(x)$上的点$P(1, \dfrac{s(s-3)}{2})$与对称轴的距离为$\dfrac{2s-1}{4}$，点$Q(s, \dfrac{s(s-5)}{2}+1)$与对称轴的距离为$\dfrac{2s-3}{4}$。显然，点$P$距离对称轴最远，从而可得

$$\max\{A(i): 1 \le i \le s\} = A(1) = \frac{s(s-3)}{2} \ge 9 \tag{23}$$

同时，可以看出曲线上的整数坐标点$B(\lfloor (s+1)/2 \rfloor, A(\lfloor (s+1)/2 \rfloor))$($\lfloor \cdot \rfloor$为下取整函数)距离对称轴较近，且有

$$\begin{aligned}\min\{A(i): 1 \le i \le s\} &= \begin{cases} A\left(\dfrac{s+1}{2}\right), & s\text{为奇数} \\ A\left(\dfrac{s}{2}+1\right), & s\text{为偶数} \end{cases} \\ &= -2s \end{aligned} \tag{24}$$

证毕

由上述引理 3～引理7，可得下述定理。

定理1 设符号定义如上，且函数$f(x,y) = \phi(x)\cdot y + 1$，$\phi$是从$\boldsymbol{F}_2^s\backslash\boldsymbol{U}$到$\boldsymbol{F}_2^t\backslash\boldsymbol{V}$的嵌入映射，且对任意的$x \in \boldsymbol{U}$，有$\phi(x) = 0$。则式 (9) 中定义的码$C_f$是一个$[2^m-1, m+1, 2^{m-1}-2^{t-2}s(s-3)]$极小2元线性码。码$C_f$的重量分布见表1。特别地，在表 1 中，当$s$形如$(k^2-1)/8$时，$(\varepsilon_1,\varepsilon_2,\varepsilon_3) = (1,0,0)$；当$s$形如$(k^2+7)/8$时，$(\varepsilon_1,\varepsilon_2,\varepsilon_3) = (0,0,1)$；当$s$形如$(k^2-9)/8$ $(k \ge 9)$时，$(\varepsilon_1,\varepsilon_2,\varepsilon_3) = (0,1,0)$；当$s$取其他形式时，$(\varepsilon_1,\varepsilon_2,\varepsilon_3) = (0,0,0)$。

证明 设$\mathrm{wt}(\boldsymbol{a}_1) = i$，$1 \le i \le s$，由引理6和式(14)可得

$$\begin{aligned}&\hat{f}(\boldsymbol{a}_1,\boldsymbol{a}_2) \\ &= \begin{cases} 2^t(-1)^{1+\boldsymbol{a}_1\cdot\phi^{-1}(\boldsymbol{a}_2)}, & \boldsymbol{a}_2 \in \mathrm{Im}\phi\backslash\{\boldsymbol{0}\} \\ 2^t\displaystyle\sum_{\boldsymbol{x}\in\phi^{-1}(0)}(-1)^{1+\boldsymbol{a}_1\cdot\boldsymbol{x}}, & \boldsymbol{a}_2 = \boldsymbol{0} \\ 0, & \boldsymbol{a}_2 \notin \mathrm{Im}\phi \end{cases} \\ &= \begin{cases} -2^t(2^s-1-\frac{s(s+1)}{2}), & \boldsymbol{a}_2 = \boldsymbol{0}, \boldsymbol{a}_1 = \boldsymbol{0} \\ 2^tA(i), & a_2 = \boldsymbol{0}, \mathrm{wt}(\boldsymbol{a}_1) = i \ne 0 \\ -2^t(-1)^{\boldsymbol{a}_1\cdot\phi^{-1}(\boldsymbol{a}_2)}, & \boldsymbol{a}_2 \in \mathrm{Im}\phi\backslash\{\boldsymbol{0}\} \\ 0, & \boldsymbol{a}_2 \notin \mathrm{Im}\phi \end{cases} \end{aligned} \tag{25}$$

观察式(25)，由$s = \dfrac{m+1}{2}$, $t = \dfrac{m-1}{2}$可知

$$\left.\begin{aligned} &-2^t\left(2^s-1-\frac{s(s+1)}{2}\right) < 2^{t+s} = 2^m, \\ &\quad \boldsymbol{a}_2 = \boldsymbol{0}, \boldsymbol{a}_1 = \boldsymbol{0} \\ &2^tA(i) \le 2^{t-1}s(s-3) < 2^{t-1}s^s = 2^{m-1}, \\ &\quad \boldsymbol{a}_2 = \boldsymbol{0}, \mathrm{wt}(\boldsymbol{a}_1) = i \ne 0 \\ &-2^t(-1)^{\boldsymbol{a}_1\cdot\phi^{-1}(\boldsymbol{a}_2)} < 2^t = 2^{\frac{m-1}{2}}, \\ &\quad \boldsymbol{a}_2 \in \mathrm{Im}\phi\backslash\{\boldsymbol{0}\} \\ &0, \ \boldsymbol{a}_2 \notin \mathrm{Im}\phi \end{aligned}\right\} \tag{26}$$

显然，当$1 \le i \le s$时，对$\boldsymbol{F}_2^s \times \boldsymbol{F}_2^t$中任意两组向量$(\boldsymbol{a}_1,\boldsymbol{a}_2) \ne (\boldsymbol{b}_1,\boldsymbol{b}_2)$，有$\hat{f}(\boldsymbol{a}_1,\boldsymbol{a}_2) \pm \hat{f}(\boldsymbol{b}_1,\boldsymbol{b}_2) \ne 2^m$，则由引理4可知，码$C_f$是极小码。

结合引理3和式(25)，可得码C_f的长度和维数参数为$[2^m-1, m+1]$。

为考虑码的重量分布，需讨论如式 (27) 的集合的基数

$$\left.\begin{aligned} &|\{\boldsymbol{a}_1 \in \boldsymbol{F}_2^s : \mathrm{wt}(\boldsymbol{a}_1) = i\}| = \binom{s}{i} \\ &\left|\left\{\boldsymbol{a}_2 \in \boldsymbol{F}_2^t : \boldsymbol{a}_2 \in \mathrm{Im}\phi\right\}\right| = \boldsymbol{F}_2^s\backslash\boldsymbol{U} + 1 = 2 + \frac{s(s+1)}{2} \\ &\left|\left\{\boldsymbol{a}_2 \in \boldsymbol{F}_2^t : \boldsymbol{a}_2 \notin \mathrm{Im}\phi\right\}\right| = 2^t - 2 - \frac{s(s+1)}{2} \end{aligned}\right\} \tag{27}$$

下面将给出码的重量分布的证明，首先给出

表 1 码C_f的重量分布

重量	频数
0	1
2^{m-1}	$2^m - 1 + 2^s\left(2^t - 2 - \dfrac{s(s+1)}{2}\right) + \varepsilon_1\binom{s}{(2s+3\pm k)/4}$
$2^{m-1} - 2^{t-1}A(i)$	$\binom{s}{i}$ $\left(1 \le i \le s, i \ne \dfrac{2s+3\pm k}{4}\right)$
$2^{m-1} - 2^{t-1}$	$2^{s-2}s(s+1) + \varepsilon_2\binom{s}{(2s+3\pm k)/4}$
$2^{m-1} + 2^{t-1}$	$2^s + 2^{s-2}s(s+1) + \varepsilon_3\binom{s}{(2s+3\pm k)/4}$
$2^{m-1} + 2^{t-1}\left(2^s - 1 - \dfrac{s(s+1)}{2}\right)$	1

表1中当s形如$(k^2-1)/8$时的证明，其他情形类似可证，不再赘述。

接下来，求$\hat{f}(\boldsymbol{a}_1,\boldsymbol{a}_2)$的频数，其中$(\boldsymbol{a}_1,\boldsymbol{a}_2)\in F_2^s\times F_2^t$。由式(25)可知，

(1) 显然，$\hat{f}(a_1,a_2)=-2^t\left(2^s-1-\dfrac{s(s+1)}{2}\right)$出现的次数为1。

(2) 由引理7 (1)和式(27)可得，$\hat{f}(\boldsymbol{a}_1,\boldsymbol{a}_2)=2^tA(i)$且$A(i)\neq 0$出现的次数为$\binom{s}{i}$，$(1\le i\le s, i\neq \dfrac{2s+3\pm k}{4})$。

(3) 当$\hat{f}(\boldsymbol{a}_1,\boldsymbol{a}_2)=-2^t$时，

(a) 当$\phi^{-1}(\boldsymbol{a}_2)=0$时，有$|\{\boldsymbol{a}_1\in\boldsymbol{F}_2^s\}|\cdot 1=2^s$对$(\boldsymbol{a}_1,\boldsymbol{a}_2)$，使得$\hat{f}(\boldsymbol{a}_1,\boldsymbol{a}_2)=-2^t$；

(b) 当$\phi^{-1}(\boldsymbol{a}_2)\neq 0$时，由式 (6) 可知，满足此条件的$\boldsymbol{a}_2$的个数为$|\boldsymbol{F}_2^s\backslash\boldsymbol{U}|-1=\dfrac{s(s+1)}{2}$，且对每个$\phi^{-1}(\boldsymbol{a}_2)\neq 0$，必有$\dfrac{1}{2}|\{\boldsymbol{a}_1\in\boldsymbol{F}_2^s\}|=2^{s-1}$个$\boldsymbol{a}_1$，使得$\boldsymbol{a}_1\phi^{-1}(\boldsymbol{a}_2)\neq 0$。因此有$2^{s-2}s(s+1)$对$(\boldsymbol{a}_1,\boldsymbol{a}_2)$，使得$\boldsymbol{a}_1\phi^{-1}(\boldsymbol{a}_2)\neq 0$。

综上，谱值$\hat{f}(\boldsymbol{a}_1,\boldsymbol{a}_2)=-2^t$出现的次数为$2^s+2^{s-2}s(s+1)$。

(4) 当$\hat{f}(\boldsymbol{a}_1,\boldsymbol{a}_2)=2^t$时，类似于(3)中的(b)的讨论，可知该谱值出现的次数为$2^{s-2}s(s+1)$。

(5) 当$\hat{f}(\boldsymbol{a}_1,\boldsymbol{a}_2)=0$时，由引理7 (1) 和式 (27)可得，此谱值出现的次数为$|\{(\boldsymbol{a}_1,\boldsymbol{a}_2):\boldsymbol{a}_2\notin \mathrm{Im}\phi\}|+\left|\left\{(\boldsymbol{a}_1,\boldsymbol{0}):\mathrm{wt}(\boldsymbol{a}_1)=\dfrac{2s+3\pm k}{4}\right\}\right|=2^s\left(2^t-2-\dfrac{s(s+1)}{2}\right)+\binom{s}{(2s+3\pm k)/4}$。

综上，可得

$$\hat{f}(\boldsymbol{a}_1,\boldsymbol{a}_2)=\begin{cases}-2^t\left(2^s-1-\dfrac{s(s+1)}{2}\right), & 1\\ 2^tA(i), & \binom{s}{i},\left(1\le i\le s, i\neq\dfrac{2s+3\pm k}{4}\right)\\ -2^t, & 2^s+2^{s-2}s(s+1)\\ 2^t, & 2^{s-2}s(s+1)\\ 0, & 2^s\left(2^t-2-\dfrac{s(s+1)}{2}\right)+\binom{s}{(2s+3\pm k)/4}\end{cases}\tag{28}$$

由式(9)即C_f的定义可知，当$u=0$时，仍有2^m-1个重量为2^{m-1}的码字。再结合引理3，整理可得表1。

下面确定码的最小和最大重量。由引理7 (4)可得

$$2^{m-1}-2^{t-2}s(s-3)<2^{m-1}-2^{t-1}\tag{29}$$

又因为$2s<2^s-1-\dfrac{s(s+1)}{2}$，进而可得

$$2^{m-1}+2^ts<2^{m-1}+2^{t-1}\left(2^s-1-\frac{s(s+1)}{2}\right)\tag{30}$$

再结合表1可知

$$\left.\begin{aligned}w_{\min}&=2^{m-1}-2^{t-2}s(s-3)\\ w_{\max}&=2^{m-1}+2^{t-1}\left(2^s-1-\frac{s(s+1)}{2}\right)\end{aligned}\right\}\tag{31}$$

从而码C_f的参数为$[2^m-1,m+1,2^{m-1}-2^{t-2}s(s-3)]$。定理得证。

推论1　(1) 码C_f是$s+3(s\ge 6)$重码，显然C_f至少是9重码。

(2) 当$m=11,13$时，易得$w_{\min}/w_{\max}>1/2$，C_f是满足Ashikhmin-Barg条件的极小码。

(3) 当$m\ge 15$时，易得$w_{\min}/w_{\max}<1/2$，C_f虽不满足Ashikhmin-Barg条件，但满足引理4，C_f仍是极小码。

3.2 第2类极小2元线性码

设非空集合$\boldsymbol{D}\subset\boldsymbol{F}_2^m\backslash\{0\}$且$\overline{\boldsymbol{D}}\subset\boldsymbol{F}_2^m\backslash\{\{\boldsymbol{0}\}\cup\boldsymbol{D}\}$，$\boldsymbol{D}$的特征函数为

$$f_{\boldsymbol{D}}(\boldsymbol{x})=\begin{cases}1, & \boldsymbol{x}\in\boldsymbol{D}\\ 0, & \boldsymbol{x}\notin\boldsymbol{D}\end{cases}\tag{32}$$

令$\overline{\boldsymbol{D}}\subset\boldsymbol{F}_2^m\backslash\{\{\boldsymbol{0}\}\cup\boldsymbol{D}\}$，则对所有的$\boldsymbol{w}\in\boldsymbol{F}_2^m$，函数$f_{\boldsymbol{D}}(\boldsymbol{x})$与$f_{\overline{\boldsymbol{D}}}(\boldsymbol{x})$的Walsh谱值满足

$$\hat{f}_{\boldsymbol{D}}(\boldsymbol{w})+\hat{f}_{\overline{\boldsymbol{D}}}(\boldsymbol{w})=2\tag{33}$$

下文中，设f为定理1中定义的函数，令$\boldsymbol{D}=\mathrm{Suppt}(f)$，显然有$f_{\boldsymbol{D}}(\boldsymbol{x},\boldsymbol{y})=f(\boldsymbol{x},\boldsymbol{y})$，其中$(\boldsymbol{x},\boldsymbol{y})\in\boldsymbol{F}_2^s\times\boldsymbol{F}_2^t$。

下面给出本节的主要结论。

定理2　设符号定义如上，则码$C_{f_{\boldsymbol{D}}}$是一个$\left[2^m-1,m+1,2^{m-1}-2^{t-1}\left(2^s-1-\dfrac{s(s+1)}{2}\right)-1\right]$极小2元线性码。码$C_{f_{\boldsymbol{D}}}$的重量分布见表2。特别地，在表2中，当$s$形如$(k^2-1)/8$时，$(\varepsilon_1,\varepsilon_2,\varepsilon_3)=(1,0,0)$；当$s$形如$(k^2+7)/8$时，$(\varepsilon_1,\varepsilon_2,\varepsilon_3)=(0,0,1)$；当$s$形如$(k^2-9)/8$ $(k\ge 9)$时，$(\varepsilon_1,\varepsilon_2,\varepsilon_3)=(0,1,0)$；当$s$取其他形式时，$(\varepsilon_1,\varepsilon_2,\varepsilon_3)=(0,0,0)$。

证明　由于本定理的证明和定理1的类似，此处仅给出主要的证明步骤。设$\mathrm{wt}(\boldsymbol{a}_1)=i$, $1\le i\le s$，由式(25)和式(33)可得

$$\hat{f}_{\bar{\boldsymbol{D}}}(\boldsymbol{a}_1,\boldsymbol{a}_2)=2-\hat{f}_{\boldsymbol{D}}(\boldsymbol{a}_1,\boldsymbol{a}_2)$$
$$=\begin{cases}2+2^t\left(2^s-1-\dfrac{s(s+1)}{2}\right), & \boldsymbol{a}_1=0,\boldsymbol{a}_2=0\\ 2-2^tA(i), & \mathrm{wt}(\boldsymbol{a}_1)=i\neq 0,\boldsymbol{a}_2=0\\ 2+2^t(-1)^{\boldsymbol{a}_1\cdot\phi^{-1}(\boldsymbol{a}_2)}, & \boldsymbol{a}_2\in \mathrm{Im}\phi\backslash\{0\}\\ 0, & \boldsymbol{a}_2\notin \mathrm{Im}\phi\end{cases} \tag{34}$$

与定理1的证明类似可得，对$\boldsymbol{F}_2^s\times\boldsymbol{F}_2^t$中任意两组向量$(\boldsymbol{a}_1,\boldsymbol{a}_2)\neq(\boldsymbol{b}_1,\boldsymbol{b}_2)$，有$\hat{f}_{\bar{\boldsymbol{D}}}(\boldsymbol{a}_1,\boldsymbol{a}_2)\pm\hat{f}_{\bar{\boldsymbol{D}}}(\boldsymbol{b}_1,\boldsymbol{b}_2)\neq 2^m$，则由引理4可知，码$C_{f_{\bar{\boldsymbol{D}}}}$是极小码。

结合引理3和式(34)，可得码$C_{f_{\bar{\boldsymbol{D}}}}$的长度和维数参数为$[2^m-1,m+1]$。

又由式(34)可得

$$\hat{f}_{\bar{\boldsymbol{D}}}(\boldsymbol{a}_1,\boldsymbol{a}_2)=\begin{cases}2+2^t\left(2^s-1-\dfrac{s(s+1)}{2}\right), & 1\\ 2-2^tA(i), & \binom{s}{i}\left(1\le i\le s,i\neq\dfrac{2s+3\pm k}{4}\right)\\ 2+2^t, & 2^s+2^{s-2}s(s+1)\\ 2-2^t, & 2^{s-2}s(s+1)\\ 2, & 2^s\left(2^t-2-\dfrac{s(s+1)}{2}\right)+\binom{s}{(2s+3\pm k)/4}\end{cases} \tag{35}$$

结合引理3，整理可得表2。

注意到$2^s-1-\dfrac{s(s+1)}{2}>2s$，因而有

$$\left.\begin{aligned}&2^{m-1}+2^{t-2}s(s-3)-1>2^{m-1}+2^{t-1}-1\\ &2^{m-1}-2^ts-1>2^{m-1}-2^{t-1}\left(2^s-1-\frac{s(s+1)}{2}\right)-1\end{aligned}\right\} \tag{36}$$

再结合表2可知

$$\left.\begin{aligned}&w_{\min}=2^{m-1}-2^{t-1}\left(2^s-1-\frac{s(s+1)}{2}\right)-1\\ &w_{\max}=2^{m-1}+2^{t-2}s(s-3)-1\end{aligned}\right\} \tag{37}$$

从而码$C_{f_{\bar{\boldsymbol{D}}}}$的参数为$\left[2^m-1,m+1,2^{m-1}-2^{t-1}\left(2^s-1-\dfrac{s(s+1)}{2}\right)-1\right]$。定理得证。

推论2 （1）码$C_{f_{\bar{\boldsymbol{D}}}}$是$s+4(s\ge 6)$重码，显然$C_{f_{\bar{\boldsymbol{D}}}}$至少是10重码。

（2）当$m\ge 11$时，易得$w_{\min}/w_{\max}<1/2$，$C_{f_{\bar{\boldsymbol{D}}}}$虽不满足Ashikhmin-Barg条件，但满足引理4，$C_{f_{\bar{\boldsymbol{D}}}}$仍是极小码。

4 结论

本文在文献[13, 14]的基础上，利用一类特殊的Maiorana-McFarland函数得到了两类不满足Ashikhmin-Barg条件的极小2元线性码，并给出了

表 2 码$C_{f_{\bar{\boldsymbol{D}}}}$的重量分布

重量	频数
0	1
2^{m-1}	2^m-1
$2^{m-1}+2^{t-1}A(i)-1$	$\binom{s}{i}\left(1\le i\le s,i\neq\dfrac{2s+3\pm k}{4}\right)$
$2^{m-1}-1$	$2^s\left(2^t-2-\dfrac{s(s+1)}{2}\right)+\varepsilon_1\binom{s}{(2s+3\pm k)/4}$
$2^{m-1}+2^{t-1}-1$	$2^{s-2}s(s+1)+\varepsilon_3\binom{s}{(2s+3\pm k)/4}$
$2^{m-1}-2^{t-1}-1$	$2^s+2^{s-2}s(s+1)+\varepsilon_2\binom{s}{(2s+3\pm k)/4}$
$2^{m-1}-2^{t-1}\left(2^s-1-\dfrac{s(s+1)}{2}\right)-1$	1

码的参数和重量分布。结果表明，构造的这两类极小2元线性码均可用作设计具有良好访问结构的秘密共享方案。

参 考 文 献

[1] ÇALKAVUR S. A study on multisecret-sharing schemes based on linear codes[J]. *Emerging Science Journal*, 2020, 4(4): 263–271. doi: 10.28991/esj-2020-01229.

[2] WANG Yaru, LI Fulin, and ZHU Shixin. Two-weight linear codes and their applications in secret sharing[J]. *Chinese Journal of Electronics*, 2019, 28(4): 706–711. doi: 10.1049/cje.2019.04.006.

[3] CHABANNE H, COHEN G, and PATEY A. Towards secure two-party computation from the wire-tap channel[C]. The 16th International Conference on Information Security and Cryptology, Seoul, Korea, 2014: 34–46. doi: 10.1007/978-3-319-12160-4_3.

[4] NIEMINEN R and JÄRVINEN K. Practical privacy-preserving indoor localization based on secure two-party computation[J]. *IEEE Transactions on Mobile Computing*, 2021, 20(9): 2877–2890. doi: 10.1109/TMC.2020.2990871.

[5] WANG Qichun and STĂNICĂ P. New bounds on the covering radius of the second order Reed-Muller code of length 128[J]. *Cryptography and Communications*, 2019, 11(2): 269–277. doi: 10.1007/s12095-018-0289-2.

[6] CARLET C. The automorphism groups of the Kerdock codes[J]. *Journal of Information and Optimization Sciences*, 1991, 12(3): 387–400. doi: 10.1080/02522667.1991.10699078.

[7] BAUMERT L D and MCELIECE R J. Weights of irreducible cyclic codes[J]. *Information and Control*, 1972, 20(2): 158–175. doi: 10.1016/S0019-9958(72)90354-3.

[8] DING Cunsheng and NIEDERREITER H. Cyclotomic linear codes of order 3[J]. *IEEE Transactions on Information Theory*, 2007, 53(6): 2274–2277. doi: 10.1109/TIT.2007.896886.

[9] XIANG Can. Linear codes from a generic construction[J]. *Cryptography and Communications*, 2016, 8(4): 525–539. doi: 10.1007/s12095-015-0158-1.

[10] DING Cunsheng. A construction of binary linear codes from Boolean functions[J]. *Discrete Mathematics*, 2016, 339(15): 2288–2303. doi: 10.1016/j.disc.2016.03.029.

[11] CHANG S and HYUN J Y. Linear codes from simplicial complexes[J]. *Designs, Codes and Cryptography*, 2018, 86(10): 2167–2181. doi: 10.1007/s10623-017-0442-5.

[12] HENG Ziling, DING Cunsheng, and ZHOU Zhengchun. Minimal linear codes over finite fields[J]. *Finite Fields and Their Applications*, 2018, 54: 176–196. doi: 10.1016/j.ffa.2018.08.010.

[13] DING Cunsheng, HENG Ziling, and ZHOU Zhengchun. Minimal binary linear codes[J]. *IEEE Transactions on Information Theory*, 2018, 64(10): 6536–6545. doi: 10.1109/TIT.2018.2819196.

[14] MESNAGER S, QI Yanfeng, RU Hongming, *et al*. Minimal linear codes from characteristic functions[J]. *IEEE Transactions on Information Theory*, 2020, 66(9): 5404–5413. doi: 10.1109/TIT.2020.2978387.

[15] ASHIKHMIN A and BARG A. Minimal vectors in linear codes[J]. *IEEE Transactions on Information Theory*, 1998, 44(5): 2010–2017. doi: 10.1109/18.705584.

[16] MACWILLIAMS F J and SLOANE N J A. The Theory of Error-Correcting Codes[M]. Amsterdam: Elsevier-North-Holland, 1997.

杜小妮：女，教授，博士生导师，研究方向为密码学与信息安全.

胡金霞：女，硕士生，研究方向为密码学与信息安全.

金文刚：男，博士生，研究方向为密码学与信息安全.

孙彦中：男，博士生，研究方向为密码学与信息安全.

责任编辑：余　蓉