Pure Mathematics 理论数学, 2021, 11(9), 1623-1629
Published Online September 2021 in Hans. http://www.hanspub.org/journal/pm
https://doi.org/10.12677/pm.2021.119179

Hans汉斯

一类基于布尔函数的极小线性码的构造

杜佳玮

西北师范大学数学与统计学院，甘肃 兰州
Email: 3230096738@qq.com

收稿日期：2021年7月28日；录用日期：2021年8月31日；发布日期：2021年9月7日

摘　要

具有较低重量的线性码在数据存储系统、设计具有良好访问结构的秘密共享方案等领域有着重要的应用。基于布尔函数的Walsh谱值分布，该文利用一类具有五值Walsh谱的布尔函数构造了一类具有六重的线性码，确定了码的参数及其重量分布，并编制Magma程序验证了结论的正确性。结果表明，所构造的码为不满足A~B条件的极小线性码，且可用来设计具有良好访问结构的秘密共享方案。

关键词

布尔函数，Bent函数，Walsh变换，二元线性码

Construction of a Class of Minimal Binary Linear Code Based on Boolean Function

Jiawei Du

College of Mathematics and Statistics, Northwest Normal University, Lanzhou Gansu
Email: 3230096738@qq.com

Received: Jul. 28th, 2021; accepted: Aug. 31st, 2021; published: Sep. 7th, 2021

Abstract

Linear codes with few-weight have important applications in data storage system and designing the secret sharing scheme with good access structures. Based on the Walsh spectrum distribution of Boolean function, this paper constructs a class of Boolean functions with five-valued Walsh spectra. The type of six-weight linear code is derived from this new function, and parameters of the code such as length and dimension are determined. And magma program is used to verify the correctness of the conclusion. The results show that the new code is minimal linear code which does not satisfy the A-B condition, and it can be used to design the secret sharing scheme with

文章引用: 杜佳玮. 一类基于布尔函数的极小线性码的构造[J]. 理论数学, 2021, 11(9): 1623-1629.
DOI: 10.12677/pm.2021.119179

good access structures.

Keywords

Boolean Function, Bent Function, Walsh Transform, Binary Linear Code

1. 引言

布尔函数在密码学、纠错码理论[1]以及信号序列设计[2]等领域有着广泛的应用，其本质是从有限域 $\mathbb{F}_{2^n}$ 到 $\mathbb{F}_2$ 上的一个映射。布尔函数密码学性质的好坏直接关系到密码体制的安全性。一般地，可以通过布尔函数的平衡性、非线性度以及代数免疫度等相关指标来衡量其密码学性质。而布尔函数的 Walsh 变换，也称 Walsh 谱，它不仅是研究布尔函数非常有力的工具[3] [4] [5]，而且也能反映函数的密码学性质。特别地，具有低值 Walsh 谱值的布尔函数在密码学、序列设计、组合设计、编码理论、强正则图等领域有着重要的应用。

具有较低重量的线性码可被应用于强正则图、鉴别代码[6]、数据存储系统、构造具有良好访问结构的秘密共享方案[7]等领域，因此构造较低重量的线性码一直是编码理论中的一个重要课题。线性码的重量分布是反应其性能的一个重要参数，不仅表明了码的纠错能力还可以用来计算信息在传输过程中产生的错误概率。然而，确定线性码的长度、维数和最小距离是比较困难的，能确定重量分布的码字则更占很小的一部分。设计具有较低重量的线性码的主要方法之一是基于定义集的构造，该方法最早是由 Baumert 等人[8]提出。近年来，国内外众多学者利用该方法研究了大量线性码的重量分布，并利用 A-B 条件判定了码的极小性。2018 年，Ding 等人[9]给出了另一种判断极小二元码的充要条件，并构造了三类极小二元码，同时确定了这些码的重量分布。本论文利用布尔函数 Walsh 谱值构造了一类不满足 A-B 条件的极小二元线性码。具体为，首先构造了一类新的布尔函数，然后通过确定该函数的 Walsh 谱值分布，研究了其在极小码中的应用。

该文的组织结构如下，第二部分主要介绍了一些基础知识。第三部分首先，构造了一类新的布尔函数并确定了函数的 Walsh 谱值分布；然后，利用新函数构造了一类极小二元线性码。第四部分总结了全文。

2. 基础知识

在下文中，设 n 是一个正整数。$\mathbb{F}_{2^n}$ 是含有 2^n 个元素的有限域，$\mathbb{F}_{2^n}^* = \mathbb{F}_{2^n} \setminus \{0\}$。$\mathbb{B}_n$ 表示从 $\mathbb{F}_{2^n}$ 到 $\mathbb{F}_2$ 上的布尔函数集。

首先介绍一些关于线性码的基础知识。

有限域 $\mathbb{F}_2$ 上的一个 $[n,k,d]$ 线性码 $\mathcal{C}$ 是 $\mathbb{F}_2$ 上 n 维空间 $\mathbb{F}_2^n$ 的一个 k 维子空间，其最小 Hamming 距离为 d，$\mathcal{C}$ 中的每一个向量称为码字。设 A_i 表示码 $\mathcal{C}$ 中重量为 i 的码字的个数。$1+A_1z+A_2z^2+\cdots+A_nz^n$ 为码 $\mathcal{C}$ 的重量计数器。序列 $(1,A_1,A_2,\cdots,A_n)$ 称为码 $\mathcal{C}$ 的重量分布。若在 $A_1,A_2,\cdots,A_n$ 中，使得 $A_i \neq 0\ (1 \le i \le n)$ 的个数为 t，称码 $\mathcal{C}$ 为 t 重码。$\mathcal{C}$ 中码字 $\boldsymbol{c}=(c_0,c_1,\cdots,c_{n-1})$ 的支撑集，定义为

$$Suppt(\boldsymbol{c})=\{0\le i\le n-1: c_i\ne 0\}.$$

若对向量$\boldsymbol{u},\boldsymbol{v}$，有$Suppt(\boldsymbol{v})\subseteq Suppt(\boldsymbol{u})$，则称$\boldsymbol{u}$覆盖$\boldsymbol{v}$。若码$\mathcal{C}$的一个非零码字$\boldsymbol{c}$只覆盖它的纯量倍数，则称$\boldsymbol{c}$是一个极小向量。若$\mathcal{C}$中的任意码字均是极小向量，则称线性码$\mathcal{C}$是极小线性码。

下面介绍有关有限域及布尔函数的相关知识。

设整数k和n满足$k\mid n$，迹函数$\mathrm{Tr}_k^n(\cdot)$表示从$\mathbb{F}_{2^n}$到$\mathbb{F}_{2^k}$上的映射，定义为[10]

$$\mathrm{Tr}_k^n(x)=x+x^{2^k}+\cdots+x^{2^{n-k}}，\text{其中 } x\in\mathbb{F}_{2^n}。$$

特别地，当$k=1$时，$\mathrm{Tr}_1^n(\cdot)=\sum_{i=0}^{n-1}x^{2^i}$称为绝对迹函数。

设$f\in\mathbb{B}_n$，f的 Walsh 变换是一个实值函数$\hat{f}:\mathbb{F}_{2^n}\to\mathbb{Z}$，对任意的$a\in\mathbb{F}_{2^n}$，其定义为

$$\hat{f}(a)=\sum_{x\in\mathbb{F}_{2^n}}(-1)^{f(x)+\mathrm{Tr}_1^n(ax)}. \tag{1}$$

若函数f的 Walsh 谱值仅有t个不同的取值，则称函数f具有t-值 Walsh 谱。显然，若令$N_i=\left|\left\{\alpha\in\mathbb{F}_{2^n}:\hat{f}(a)=v_i\right\}\right|$，其中$\alpha\in\mathbb{F}_{2^n}$，$1\le i\le t$。由 Walsh 变换的性质，有如下方程组：

$$\begin{cases}\sum_{i=1}^{t}N_i=2^n,\\ \sum_{i=1}^{t}N_iv_i=2^n(-1)^{f(0)},\\ \sum_{i=1}^{t}N_iv_i^2=2^{2n}.\end{cases} \tag{2}$$

定义 1 [3] 设$f\in\mathbb{B}_n$，$n=2m$，若对任意的$\alpha\in\mathbb{F}_{2^m}$，都有$\hat{f}(\alpha)=\pm 2^m$，则称$f(x)$为 Bent 函数。

$f(x)$是 Bent 函数，则f的对偶函数$\tilde{f}$也是 Bent 函数且与f的 Walsh 变换有如下关系

$$\hat{f}(\alpha)=2^m(-1)^{\tilde{f}(\alpha)}.$$

引理 1 [11] 设$n=2m$且$\lambda\in\mathbb{F}_{2^m}$，则$f(x)=\mathrm{Tr}_1^m\left(\lambda x^{2^m+1}\right)$是一个 Bent 函数。显然，对任意的$a\in\mathbb{F}_{2^n}$，$f(x)$在$a$点处的 Walsh 变换为

$$\hat{f}(a)=2^m(-1)^{\mathrm{Tr}_1^m\left(\lambda^{-1}a^{2^m+1}\right)+1}.$$

3. 主要结论及证明

下文中总假设$n=2m>4$。

3.1. 新布尔函数的构造及其谱值分析

首先构造布尔函数如下：

$$f_{\lambda,\gamma}(x)=\mathrm{Tr}_1^m\left(\lambda x^{2^m+1}\right)\mathrm{Tr}_1^m\left(\gamma(x+1)^{2^m+1}\right)\in\mathbb{B}_n, \tag{3}$$

其中$\lambda,\gamma\in F_{2^m}^*$，且$\lambda\ne\gamma$。

下面我们计算该函数的 Walsh 谱值及其分布。先给出一个重要引理。

引理 2 设函数f如式(3)定义，则对于任意的$a\in\mathbb{F}_{2^n}$，$f(x)$的 Walsh 变换为

$$\hat{f}(a)=\begin{cases}2^{n-1}-2^{m-1}(-1)^{\mathrm{Tr}_1^m\left((\gamma+\lambda)^{-1}\gamma^{2^m+1}\right)+\mathrm{Tr}_1^m(\gamma)}, & a=0,\\ -2^{m-1}\left(2(-1)^{\mathrm{Tr}_1^m(\gamma)}-(-1)^{\mathrm{Tr}_1^m\left(\lambda^{-1}\gamma^{2^m+1}\right)}\right), & a=\gamma,\\ -2^{m-1}\left((-1)^{\mathrm{Tr}_1^m\left(\gamma^{-1}a^{2^m+1}\right)+\mathrm{Tr}_1^n(a)}-(-1)^{\mathrm{Tr}_1^m\left(\lambda^{-1}a^{2^m+1}\right)}+(-1)^{\mathrm{Tr}_1^m\left((\gamma+\lambda)^{-1}\gamma^{2^m+1}\right)+\mathrm{Tr}_1^m\left((\gamma+\lambda)^{-1}a^{2^m+1}\right)+\mathrm{Tr}_1^m(\gamma)}\right), & \text{其它.}\end{cases}\tag{4}$$

证明 对任意的 $a\in\mathbb{F}_{2^n}$，由式(1)可得，$f(x)$ 的 Walsh 变换为

$$\begin{aligned}\hat{f}(a)&=\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}_1^m\left(\lambda x^{2^m+1}\right)\mathrm{Tr}_1^m\left(\gamma(x+1)^{2^m+1}\right)+\mathrm{Tr}_1^n(ax)}\\&=\sum_{\mathrm{Tr}_1^m\left(\mathrm{Tr}_1^m\left(\gamma(x+1)^{2^m+1}\right)\right)=0}(-1)^{\mathrm{Tr}_1^n(ax)}+\sum_{\mathrm{Tr}_1^m\left(\mathrm{Tr}_1^m\left(\gamma(x+1)^{2^m+1}\right)\right)=1}(-1)^{\mathrm{Tr}_1^m\left(\lambda x^{2^m+1}\right)\mathrm{Tr}_1^m\left(\gamma(x+1)^{2^m+1}\right)+\mathrm{Tr}_1^n(ax)}\\&=\frac{1}{2}\left(\sum_{x\in\mathbb{F}_{2^n}}\left((-1)^{\mathrm{Tr}_1^n(ax)}+(-1)^{\mathrm{Tr}_1^m\left(\gamma(x+1)^{2^m+1}\right)+\mathrm{Tr}_1^n(ax)}\right)\right.\\&\quad\left.-\sum_{x\in\mathbb{F}_{2^n}}\left((-1)^{\mathrm{Tr}_1^m\left(\lambda x^{2^m+1}\right)}\cdot(-1)^{\mathrm{Tr}_1^n(ax)}-(-1)^{\mathrm{Tr}_1^m\left(\gamma\left(x^{2^m+1}+x^{2^m}+x+1\right)\right)+\mathrm{Tr}_1^m\left(\lambda x^{2^m+1}\right)+\mathrm{Tr}_1^n(ax)}\right)\right)\\&=\frac{1}{2}\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}_1^n(ax)}+\frac{1}{2}\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}_1^m\left(\gamma x^{2^m+1}\right)+\mathrm{Tr}_1^n(ax)+\mathrm{Tr}_1^n(a)}\\&\quad-\frac{1}{2}\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}_1^m\left(\lambda x^{2^m+1}\right)+\mathrm{Tr}_1^n(ax)}+\frac{1}{2}\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}_1^m\left((\gamma+\lambda)x^{2^m+1}\right)+\mathrm{Tr}_1^n((\gamma+a)x)+\mathrm{Tr}_1^m(\gamma)}\end{aligned}$$

则由引理 1 和函数 $\mathrm{Tr}_1^m\left(\lambda x^{2^m+1}\right)$ 的 Bent 性，对 a 的取值进行分类，经简单计算可得结果。

证毕。 □

下文中：令 $A=\mathrm{Tr}_1^m\left((\gamma+\lambda)^{-1}\gamma^{2^m+1}\right)$，$B=\mathrm{Tr}_1^m(\gamma)$，$C=\mathrm{Tr}_1^m\left(\lambda^{-1}\gamma^{2^m+1}\right)$，$D=\mathrm{Tr}_1^m\left(\left(\lambda+\gamma^{-1}\right)a^{2^m+1}\right)$，$E=\mathrm{Tr}_1^m\left(\gamma^{-1}a^{2^m+1}\right)$，$F=\mathrm{Tr}_1^n(a)$，$G=\mathrm{Tr}_1^m\left(\lambda^{-1}a^{2^m+1}\right)$。则有

$$\hat{f}(0)=2^{n-1}-2^{m-1}(-1)^{A+B}.$$

下面假设 $A=B$。所以，

$$\hat{f}(0)=2^{n-1}-2^{m-1}.$$

$$\hat{f}(\gamma)=-2^{m-1}\left(2(-1)^B-(-1)^C\right)=\begin{cases}-2^{m-1}, & (B,C)=(0,0),\\ -3\cdot2^{m-1}, & (B,C)=(0,1),\\ 3\cdot2^{m-1}, & (B,C)=(1,0),\\ 2^{m-1}, & (B,C)=(1,1).\end{cases}$$

当 $a\in\mathbb{F}_{2^n}\setminus\{0,\gamma\}$ 时，因为 $(\lambda+\gamma)^{-1}=\lambda^{-1}+\gamma^{-1}$，所以有 $E+G=D$，因而仅存在以下八种情形。

$$\hat{f}(a)=-2^{m-1}\left((-1)^{E+F}-(-1)^{G}+(-1)^{D}\right)$$

$$=\begin{cases}-2^{m-1}, & \text{若}(E+F,G,D)\in\{(0,0,0),(0,1,1),(1,1,0)\},\\ 2^{m-1}, & \text{若}(E+F,G,D)\in\{(1,0,0),(0,0,1),(1,1,1)\},\\ 3\cdot 2^{m-1}, & \text{若}(E+F,G,D)\in\{(1,0,1)\},\\ -3\cdot 2^{m-1}, & \text{若}(E+F,G,D)\in\{(0,1,0)\}.\end{cases}$$

定理 1 符号含义与引理 2 相同。则当$(\lambda+\gamma)^{-1}=\lambda^{-1}+\gamma^{-1}$且$A=B=C=0$时，式(3)定义的函数$f(x)$的 Walsh 谱值分布为

$$\hat{f}(a)=\begin{cases}2^{n-1}-2^{m-1}, & \text{出现 1 次},\\ -2^{m-1}, & \text{出现 } 3\cdot 2^{n-3}-2^{m-2} \text{ 次},\\ 3\cdot 2^{m-1}, & \text{出现 } 2^{n-3}+2^{m-2} \text{ 次},\\ 2^{m-1}, & \text{出现 } 3\cdot 2^{n-3} \text{ 次},\\ -3\cdot 2^{m-1}, & \text{出现 } 2^{n-3} \text{ 次}.\end{cases}$$

证明 显然，由定理 1 之前的讨论可知，当$A=B=C=0$时，对$a\in\mathbb{F}_{2^n}$，$f(x)$的 Walsh 变换为

$$\hat{f}(a)\in\left\{2^{n-1}-2^{m-1},-2^{m-1},3\cdot 2^{m-1},2^{m-1},-3\cdot 2^{m-1}\right\}.$$

当$\hat{f}(a)=3\cdot 2^{m-1}$时，此时有$(E,F,G,D)=(1,0,0,1)$，又因为$(\lambda+\gamma)^{-1}=\lambda^{-1}+\gamma^{-1}$，则$\mathbb{F}_{2^n}$中满足此条件的元素$a$的个数$S_a$为

$$\begin{aligned}S_a&=\frac{1}{2^4}\sum_{a\in\mathbb{F}_{2^n}}\left(\left(1-(-1)^{E}\right)\left(1+(-1)^{F}\right)\left(1+(-1)^{G}\right)\left(1-(-1)^{D}\right)\right)\\&=\frac{1}{2^4}\Bigg(2^n+2^m-2^m+2^m(-1)^{\mathrm{Tr}_1^m\left(\left(\lambda^{-1}+\gamma^{-1}\right)^{-1}\right)}+2^m-2^m(-1)^{\mathrm{Tr}_1^m(\lambda)}+2^m\\&\quad+2^m(-1)^{\mathrm{Tr}_1^m(\gamma)}+2^m+2^n-2^m(-1)^{\mathrm{Tr}_1^m(\lambda)}+2^m(-1)^{\mathrm{Tr}_1^m\left(\left(\lambda^{-1}+\gamma^{-1}\right)^{-1}\right)}\Bigg)\\&=2^{n-3}+3\cdot 2^{m-4}+2^{m-3}(-1)^{\mathrm{Tr}_1^m\left(\left(\lambda^{-1}+\gamma^{-1}\right)^{-1}\right)}-2^{m-3}(-1)^{\mathrm{Tr}_1^m(\lambda)}+2^{m-4}(-1)^{\mathrm{Tr}_1^m(\gamma)}\\&=2^{n-3}+3\cdot 2^{m-4}+2^{m-3}(-1)^{\mathrm{Tr}_1^m(\gamma)+\mathrm{Tr}_1^m(\lambda)}-2^{m-3}(-1)^{\mathrm{Tr}_1^m(\lambda)}+2^{m-4}(-1)^{\mathrm{Tr}_1^m(\gamma)}\\&=2^{n-3}+2^{m-2}\end{aligned}\tag{6}$$

下面记

$$N_1=\left|\left\{a\in\mathbb{F}_{2^n}:\hat{f}(a)=-2^{m-1}\right\}\right|,$$

$$N_2=\left|\left\{a\in\mathbb{F}_{2^n}:\hat{f}(a)=2^{m-1}\right\}\right|,$$

$$N_3=\left|\left\{a\in\mathbb{F}_{2^n}:\hat{f}(a)=-3\cdot 2^{m-1}\right\}\right|.$$

因为$f(0)=0$，所以由式(2)和式(6)可得

$$\begin{cases}1+2^{n-3}+2^{m-2}+N_1+N_2+N_3=2^n,\\ 2^{n-1}-2^{m-1}+3\cdot 2^{m-1}\left(2^{n-3}+2^{m-2}\right)-2^{m-1}N_1+2^{m-1}N_2-3\cdot 2^{m-1}N_3=2^n,\\ \left(2^{n-1}-2^{m-1}\right)^2+\left(3\cdot 2^{m-1}\right)^2\left(2^{n-3}+2^{m-2}\right)+\left(2^{m-1}\right)^2\left(N_1+N_2\right)+\left(-3\cdot 2^{m-1}\right)^2N_3=2^{2n}.\end{cases}$$

解上述方程组可得

$$N_1 = 3\cdot 2^{n-3} - 2^{m-2} - 1,\ N_2 = 3\cdot 2^{n-3},\ N_3 = 2^{n-3}.$$

证毕。 □

3.2. 构造一类极小线性码

在这一小节中，我们利用新函数的 Walsh 谱值构造极小线性码。

设 $g(x)\in\mathbb{B}_n$ 满足 $g(0)=0$，且对所有的 $v\in\mathbb{F}_{2^n}$，有 $g(x)\neq v\cdot x$，则定义 $\mathbb{F}_2$ 上的线性码 $\mathcal{C}_g$ 如下：

$$\mathcal{C}_g = \left\{\left(ug(x)+\mathrm{Tr}(v\cdot x)\right)_{x\in\mathbb{F}_{2^n}^*} : u\in\mathbb{F}_2, v\in\mathbb{F}_{2^n}\right\} \tag{7}$$

引理 3 [9] 设码 $\mathcal{C}_g$ 由式(8)定义，则 $\mathcal{C}_g$ 的长度为 2^n-1，维数为 $n+1$，且其重量分布可由下述多重集给出

$$\left\{\left\{\frac{2^n-\hat{g}(w)}{2} : w\in\mathbb{F}_{2^n}\right\}\cup\left\{2^{n-1} : w\in\mathbb{F}_{2^n}^*\right\}\cup\{0\}\right\}.$$

更进一步地，$\mathcal{C}_g$ 是极小码当且仅当

$$\hat{f}(h)\pm\hat{f}(l)\neq 2^n，\text{其中 } h,l\in\mathbb{F}_{2^n}，\ h\neq l。$$

引理 4 [12] (A-B 条件)令 $w_{\min}$ 与 $w_{\max}$ 分别表示码 $\mathcal{C}$ 的极小与极大 Hamming 重量，若 $w_{\min}/w_{\max}>1/2$，则 $\mathcal{C}$ 为 $\mathbb{F}_2$ 上的极小码。该条件为判断线性码为极小码的充分条件。

定理 2 设符号含义如上，当 $(\lambda+r)^{-1}=\lambda^{-1}+r^{-1}$ 且 $A=B=C=0$ 时，则由式(3)定义的函数 f 构造的线性码 $\mathcal{C}_f$ 为 $\left[2^n-1, n+1, 2^{n-2}+2^{m-2}\right]$ 极小码，且其重量分布如表 1 所示。

Table 1. Weight distribution of $\mathcal{C}_f$

表 1. $\mathcal{C}_f$ 的重量分布

重量	频数
0	1
$2^{n-2}+2^{m-2}$	1
$2^{n-1}-3\cdot 2^{m-2}$	$2^{n-3}+2^{m-2}$
$2^{n-1}-2^{m-2}$	$3\cdot 2^{n-3}$
$2^{n-1}+2^{m-2}$	$3\cdot 2^{n-3}-2^{m-2}$
$2^{n-1}+3\cdot 2^{m-2}$	2^{n-3}
2^{n-1}	2^n-1

证明 当 $(\lambda+r)^{-1}=\lambda^{-1}+r^{-1}$ 且 $A=B=C=0$ 时，由定理 1 中函数 f 的 Walsh 谱值分布和引理 3 中的结论可得，$\mathcal{C}_f$ 的重量分布如表 1 所示。

显然，由表 1 可知，$w_{\min}/w_{\max}<1/2$，不满足 A-B 条件。而又由函数 f 的 Walsh 谱值分布可知，对任意的 $h\neq l\in\mathbb{F}_{2^n}$，有 $\hat{f}(h)\pm\hat{f}(l)\neq 2^n$ 成立，即满足引理 3 中关于极小码的判定条件，所以 $\mathcal{C}_f$ 为最小码。

证毕。 □

例： 记 $n=8$，$m=4$，α 是 $\mathbb{F}_{2^8}$ 的本原元，且满足 $\alpha^8+\alpha^4+\alpha^3+\alpha^2+1=0$。设 $\lambda=\alpha^{170}$，$\gamma=\alpha^{85}$，则我们有 $(\lambda+\gamma)^{-1}=\lambda^{-1}+\gamma^{-1}$，且

$$\mathrm{Tr}_1^m\left(\left(\gamma+\lambda\right)^{-1}\gamma^{2^m+1}\right)=\mathrm{Tr}_1^m\left(\gamma\right)=\mathrm{Tr}_1^m\left(\lambda^{-1}\gamma^{2^m+1}\right)=0,$$

则由 Magma 程序可知，码 $\mathcal{C}_f$ 的参数为 $[255,9,68]$，其重量计数器为

$$1+z^{68}+36z^{116}+96z^{124}+255z^{128}+92z^{132}+32z^{140},$$

与定理 2 的结论一致。

注记：当 A,B,C 取其他值时，所构造函数 f 的 Walsh 变换的值与 $A=B=C=0$ 时的相同，只是出现的频数不同，因此对所构造线性码的重量与定理 2 的一致，但出现的频数不同。

4. 结束语

该文首先构造了一类至多具有五值 Walsh 谱的布尔函数，并且确定了其谱值分布。其次，利用函数的谱值分布，研究了其在线性码中的应用。并设计 Magma 程序举例验证了结论的正确性。结论表明，该函数所构造的一类码为不满足 A-B 条件的六重极小线性码，且可用来设计具有良好访问结构的秘密共享方案。

参考文献

[1] Carlet, C. (2010) Boolean Function for Cryptography and Error Correcting Codes. In: Crama, Y. and Hammer, P., Eds., *Chapter of the Monography Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, Cambridge University Press, Cambridge, 257-397. https://doi.org/10.1017/CBO9780511780448.011

[2] Khoo, K. (2004) Sequence Design and Construction of Cryptographic Boolean Functions. Ph.D. Thesis, University of Waterloo (Canda), Waterloo.

[3] Carlet, C., Charpin, P. and Zinoviev, V. (1998) Codes, Bent Functions and Permutations Suitable for DES-Like Cryptosystems. *Designs, Codes and Cryptography*, **15**, 125-156. https://doi.org/10.1023/A:1008344232130

[4] Pang, T., Zeng, X., Li, N. and Xu, Y. (2020) A Class of New Quadratic Vectorial Bent Functions. *Chinese Journal of Electronics*, **29**, 85-91. https://doi.org/10.1049/cje.2020.08.002

[5] Kumar, P.V., Scholtz, R.A. and Welch, L.R. (1985) Generalized Bent Functions and Their Properties. *Journal of Combinatorial Theory*, *Series A*, **40**, 90-107. https://doi.org/10.1016/0097-3165(85)90049-4

[6] 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

[7] Yuan, J. and Ding, C. (2006) Secret Sharing Schemes from Three Classes of Linear Codes. *IEEE Transactions on Information Theory*, **52**, 206-212. https://doi.org/10.1109/TIT.2005.860412

[8] Baumert, L.D. and Mceliece, R.J. (1972) Weights of Irreducible Cyclic Codes. *Information and Control*, **20**, 158-175. https://doi.org/10.1016/S0019-9958(72)90354-3

[9] 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

[10] Lidl, R. and Niederreiter, H. (1997) Finite Fields. 2nd Edition, Cambridge University Press, Cambridge. https://doi.org/10.1017/CBO9780511525926

[11] Helleseth, T. and Kholosha, A. (2006) Monomial and Quadratic Bent Functions over the Finite Fields of Odd Characteristic. *IEEE Transactions on Information Theory*, **52**, 2018-2032. https://doi.org/10.1109/TIT.2006.872854

[12] 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