Advances in Applied Mathematics 应用数学进展, **2023, 12(8), 3631-3638**
Published Online August 2023 in Hans. https://www.hanspub.org/journal/aam
https://doi.org/10.12677/aam.2023.128361

Hans汉斯

一类基于Kasami函数的极小线性码的构造

张莹中

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21日；录用日期：2023年8月13日；发布日期：2023年8月21日

摘　要

布尔函数和线性码在设计序列密码共享方案等方面有重要的应用。本文基于Kasami函数构造了一类具有五值Walsh谱的布尔函数，研究了新函数的Walsh谱值分布，利用新函数构造了一类五重极小线性码。

关键词

布尔函数，Walsh变换，极小线性码

Construction of a Class of Minimal Linear Codes Based on Kasami Functions

Yingzhong Zhang

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

Received: Jul, 21st, 2023; accepted: Aug, 13th, 2023; published: Aug, 21st, 2023

Abstract

Boolean functions and linear codes with few-weights have important applications in

文章引用: 张莹中. 一类基于Kasami函数的极小线性码的构造[J]. 应用数学进展, 2023, 12(8): 3631-3638.
DOI: 10.12677/aam.2023.128361

designing sequence ciphers and in designing shared schemes. In this paper, we construct a class Boolean functions with five-valued Walsh spectra using Kasami functions and investigate the distribution of Walsh spectral values of the new functions. Finally, a class of minimal linear codes with five-weights is constructed by using the new functions.

Keywords

Boolean Function, Walsh Transform, Minimal Linear Codes

1. 引言

布尔函数是密码函数中重要的函数之一, 在流密码和对称密码体制的设计和分析中起着主导作用. 构造同时具备多种优良密码学性质的布尔函数一直是研究的热点. Walsh 变换是研究布尔函数密码学性质最重要的工具之一, 具有较少 Walsh 谱值的密码函数在对称密码体制的算法设计、代数编码和组合设计理论研究中起着重要作用, 因而受到国内外学者的广泛关注. Bent 函数作为布尔函数中非线性度最优, 且只具有两值 Walsh 谱 [1], 在应用密码、纠错编码理论、序列设计理论等领域已被广泛研究.

线性码比非线性码更容易编码和译码且传送信息更快, 所以在通讯系统、计算机系统等领域有着广泛的应用. 特别地, 对于具有较低重量的线性码在研究认证码 [2]、结合方案 [3]、强正则图 [4]、秘密共享方案 [5]等方面至关重要. 1998 年 Ashikhmin 和 Barg [6]给出了线性码为极小线性码的充分条件; 2015 年 Ding [7,8]通过 2-设计构造给出了几类具有较低重量的线性码; 2018 年 Ding 等人 [9,10]给出了线性码是极小线性码的充要条件并构造了三簇二元极小线性码, 确定了其重量分布; 2019 年 Zhang 等人 [11]构造了四簇极小线性码, 并确定了其重量分布.

本文利用 Kasami 函数构造了一类具有五值 Walsh 谱的布尔函数, 并研究了新函数的 Walsh 谱值分布. 最后利用新函数构造了一类五重极小线性码, 确定了码的长度, 维数及重量分布.

全文组织结构如下, 第二部分介绍本文涉及到的基本概念及基础知识; 第三部分首先利用布尔函数的二阶构造, 基于 Kasami 函数构造了一类具有五值 Walsh 谱的布尔函数并确定了新函数的谱值分布, 同时利用新函数设计了一类二元极小线性码, 且给出了其重量分布; 最后, 总结全文.

2. 基础知识

设 n 为正整数, $\mathbb{F}_{2^n}$ 为有 2^n 个元素的有限域, $\mathbb{F}_{2^n}^* = \mathbb{F}_{2^n} \setminus \{0\}$. 对于任何正整数 $r|n$, 迹函数 Tr_r^n 定义如下

$$\mathrm{Tr}_r^n(x) = x + x^{2^r} + \ldots + x^{2^{n-r}},\ x \in \mathbb{F}_{2^n},$$

且有 $\mathrm{Tr}_r^n(x) = \mathrm{Tr}_r^n(x^2)$. 特别地, 当 $r = 1$ 时, $\mathrm{Tr}_1^n(x)$ 称为绝对迹函数. 设 $\mathbb{F}_2$ 是二元有限域, $\mathbb{F}_2^n$ 是 $\mathbb{F}_2$ 上的 n 维向量空间, 从 $\mathbb{F}_2^n$ 到 $\mathbb{F}_2$ 的映射 $f : \mathbb{F}_2^n \to \mathbb{F}_2$ 被称为 n 元布尔函数. 令 $\mathcal{B}_n$ 为所有 n 元布尔函数的集合. 布尔函数的 Walsh 变换, 是研究布尔函数性质最重要的数学工具之一, 其定义如下

定义1. 设 f 是从 $\mathbb{F}_{2^n}$ 到 $\mathbb{F}_2$ 的函数, 则 f 的 Walsh 变换是一个实值函数 $\widehat{f} : \mathbb{F}_{2^n} \to \mathbb{Z}$, 且对任意的 $\alpha \in \mathbb{F}_{2^n}$, 函数 f 在 α 处的 Walsh 谱值定义为

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

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. 令 $N_i = |\{\alpha \in \mathbb{F}_{2^n} : \widehat{f}(\alpha) = v_i\}|$, 其中 $1 \le i \le t$, v_i 是 f 不同的 Walsh 谱值. 由 Walsh 变换的性质, 有如下方程组

$$\begin{cases} \sum\limits_{i=1}^{t} N_i = 2^n, \\ \sum\limits_{i=1}^{t} N_i v_i = 2^n(-1)^{f(0)}, \\ \sum\limits_{i=1}^{t} N_i v_i^2 = 2^{2n}, \end{cases} \tag{1}$$

下文中将利用 (1) 式计算函数 f 的 Walsh 谱值分布.

设 $n = m + k$, m 和 k 是正整数, $\mathbb{F}_{2^n}$ 和 $\mathbb{F}_{2^m} \times \mathbb{F}_{2^k}$ 同构, $(y, z) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^k}$, 则 $\mathbb{F}_{2^n}$ 上的多变元布尔函数 $f(y, z)$ 在任意 $(a_1, a_2) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^k}$ 处的 Walsh 变换定义为

$$\widehat{f}(a_1, a_2) = \sum_{y \in \mathbb{F}_{2^m}, z \in \mathbb{F}_{2^k}} (-1)^{f(y,z)+\mathrm{Tr}_1^m(a_1 y)+\mathrm{Tr}_1^k(a_2 z)}. \tag{2}$$

定义2. 设 n 是偶数, $f \in \mathcal{B}_n$, 若对任意的 $\alpha \in \mathbb{F}_{2^n}$, 都有 $\widehat{f}(\alpha) = \pm 2^{n/2}$, 则称 $f(x)$ 为 bent 函数. 若 $f(x)$ 是 bent 函数, 则 f 的对偶函数 f^* 与其 Walsh 变换有如下关系

$$\widehat{f}(\alpha) = 2^{n/2}(-1)^{f^*(\alpha)}.$$

引理1. [12] 设 $n = 2m$ 且 $\lambda \in \mathbb{F}_{2^m}^*$, 则 $f(x) = \mathrm{Tr}_1^m(\lambda x^{2^m+1})$ 是一个 bent 函数. 对任意的

$a \in \mathbb{F}_{2^m}$, $f(x)$ 在 a 点处的 Walsh 变换为

$$\widehat{f}(a) = 2^m(-1)^{\mathrm{Tr}_1^m(\lambda^{-1}a^{2^m+1})+1}. \tag{3}$$

显然其对偶函数是 $f^*(x) = \mathrm{Tr}_1^m(\lambda^{-1}x^{2^m+1}) + 1$.

设 $f(x)$ 是 $\mathbb{F}_{2^n}$ 到 $\mathbb{F}_2$ 上满足 $f(0) = 0$ 的布尔函数, 且对于任意的 $v \in \mathbb{F}_{2^n}$, $f(x) \neq \mathrm{Tr}_1^n(vx)$, 给出 $\mathbb{F}_2$ 上一般线性码 $\mathcal{C}_f$ 如下:

$$\mathcal{C}_f = \{(\alpha f(x) + \mathrm{Tr}_1^n(\beta x))_{x\in\mathbb{F}_{2^n}^*} : \alpha \in \mathbb{F}_2,\ \beta \in \mathbb{F}_{2^n}\}. \tag{4}$$

下面给出判断一个线性码是极小线性码的充分条件.

引理2. [6] 一个线性码 $\mathcal{C}$ 如果满足 $\frac{w_{\min}}{w_{\max}} > \frac{1}{2}$, 则其在 $\mathbb{F}_2$ 上是极小的, 其中 $w_{\min}$ 与 $w_{\max}$ 分别表示码 $\mathcal{C}$ 的极小汉明重量与极大汉明重量.

3. 主要结论及证明

3.1. 新函数构造及谱值分析

首先构造布尔函数如下:

$$\mathfrak{f}(x, y) = \mathrm{Tr}_1^m(\lambda x^{2^m+1}) + \mathrm{Tr}_1^k(c_1y)\mathrm{Tr}_1^k(c_2y)\mathrm{Tr}_1^m(r(x+1)^{2^m+1}), \tag{5}$$

其中 $r, \lambda \in \mathbb{F}_{2^m}^*$, 且 $\lambda \neq r$, $c_1,\ c_2 \in \mathbb{F}_{2^k}$ 线性无关.

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3. 设 $\mathfrak{f}(x, y)$ 由 (5) 式所定义, 则对于任意的 $(u, v) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^k}$, $\mathfrak{f}(u, v)$ 的 Walsh 谱值为

$$\widehat{\mathfrak{f}}(u,v) = \begin{cases} -2^{k-2+\frac{m}{2}}(3(-1)^{\mathrm{Tr}_1^m((\lambda)^{-1}u^{2^m+1})} + (-1)^{\mathrm{Tr}_1^m((\lambda+r)^{-1}(r+u)^{2^m+1})+\mathrm{Tr}_1^m(r)}), & v = 0, \\ -2^{k-2+\frac{m}{2}}((-1)^{\mathrm{Tr}_1^m((\lambda)^{-1}u^{2^m+1})} - (-1)^{\mathrm{Tr}_1^m((\lambda+r)^{-1}(r+u)^{2^m+1})+\mathrm{Tr}_1^m(r)}), & v \in \{c_1, c_2\}, \\ -2^{k-2+\frac{m}{2}}((-1)^{\mathrm{Tr}_1^m((\lambda+r)^{-1}(r+u)^{2^m+1})+\mathrm{Tr}_1^m(r)} - (-1)^{\mathrm{Tr}_1^m((\lambda)^{-1}u^{2^m+1})}), & v = c_1 + c_2, \\ 0 & \text{其他}, \end{cases} \tag{6}$$

证明 对于任意 $(\varepsilon_1, \varepsilon_2) \in \mathbb{F}_2^2$, 定义如下集合

$$T(\varepsilon_1, \varepsilon_2) = \{y \in \mathbb{F}_{2^k} \mid \mathrm{Tr}_1^k(c_1y) = \varepsilon_1, \mathrm{Tr}_1^k(c_2y) = \varepsilon_2\},$$

则对任意的 $(u,v)\in\mathbb{F}_{2^n}\times\mathbb{F}_{2^k}$, 有

$$\begin{aligned}
&\widehat{\mathfrak{f}}(u,v)\\
&=\sum_{x\in\mathbb{F}_{2^n},y\in\mathbb{F}_{2^k}}(-1)^{\mathfrak{f}(x,y)+\mathrm{Tr}_1^n(ux)+\mathrm{Tr}_1^k(vy)}\\
&=\sum_{x\in\mathbb{F}_{2^n}}\sum_{(\varepsilon_1,\varepsilon_2)\in\mathbb{F}_2^2}\sum_{y\in T(\varepsilon_1,\varepsilon_2)}(-1)^{\mathrm{Tr}_1^m(\lambda x^{2^m+1})+\varepsilon_1\varepsilon_2\mathrm{Tr}_1^m(r(x+1)^{2^m+1})+\mathrm{Tr}_1^n(ux)+\mathrm{Tr}_1^k(vy)}\\
&=\sum_{x\in\mathbb{F}_{2^n}}\sum_{(\varepsilon_1,\varepsilon_2)\in\mathbb{F}_2^2}\sum_{y\in\mathbb{F}_{2^k}}(-1)^{\mathrm{Tr}_1^m(\lambda x^{2^m+1})+\varepsilon_1\varepsilon_2\mathrm{Tr}_1^m(r(x+1)^{2^m+1})+\mathrm{Tr}_1^n(ux)+\mathrm{Tr}_1^k(vy)}\prod_{j=1}^{2}\left(\frac{1+(-1)^{\mathrm{Tr}_1^k(c_jy)+\varepsilon_j}}{2}\right)\\
&=\begin{cases}
-2^{k-2+\frac{n}{2}}\left(3(-1)^{\mathrm{Tr}_1^m(\lambda^{-1}u^{2^m+1})}+(-1)^{\mathrm{Tr}_1^m((\lambda+r)^{-1}(r+u)^{2^m+1})+\mathrm{Tr}_1^m(\gamma)}\right), & v=0,\\
-2^{k-2+\frac{n}{2}}\left((-1)^{\mathrm{Tr}_1^m(\lambda^{-1}u^{2^m+1})}-(-1)^{\mathrm{Tr}_1^m((\lambda+r)^{-1}(r+u)^{2^m+1})+\mathrm{Tr}_1^m(r)}\right), & v\in\{c_1,c_2\},\\
-2^{k-2+\frac{n}{2}}\left((-1)^{\mathrm{Tr}_1^m((\lambda+r)^{-1}(r+u)^{2^m+1})+\mathrm{Tr}_1^m(r)}-(-1)^{\mathrm{Tr}_1^m((\lambda)^{-1}u^{2^m+1})}\right), & v=c_1+c_2,\\
0 & \text{其他},
\end{cases}
\end{aligned}\tag{7}$$

显然证明完毕. □

定理1. 符号含义与引理 3 相同, 若$C=1$, 则(5)式定义的函数$\mathfrak{f}(x,y)$的Walsh谱值分布如下

$$\widehat{\mathfrak{f}}(u,v)=\begin{cases}
0, & \text{出现 } 2^{n+k}-5\cdot2^{n-1}+3\cdot2^{\frac{n}{2}-1}\text{ 次},\\
\pm2^{\frac{n}{2}+k}, & \text{出现 } 2^{n-2}+2^{\frac{n}{2}-2}\text{ 次},\\
2^{\frac{n}{2}+k-1}, & \text{出现 } 2^n-2^{\frac{n}{2}+1}\text{ 次},\\
-2^{\frac{n}{2}+k-1}, & \text{出现 } 2^n\text{ 次}.
\end{cases}\tag{8}$$

证明 首先讨论函数 $\mathfrak{f}(x,y)$ 的 Walsh 谱值, 令 $A=\mathrm{Tr}_1^m(\lambda^{-1}u^{2^m+1})$, $B=\mathrm{Tr}_1^m((r+\lambda)^{-1}u^{2^m+1})$, $C=\mathrm{Tr}_1^m(\gamma)$, 由引理 1 可知

$$\sum_{u\in\mathbb{F}_{2^n}}(-1)^A=2^{\frac{n}{2}}(-1)^{\mathrm{Tr}_1^m(\lambda0^{2^m+1})+1}=-2^{\frac{n}{2}}.\tag{9}$$

当 $C=1$ 时, 由引理 3 对任意的 $(u,v)\in\mathbb{F}_{2^n}\times\mathbb{F}_{2^k}$, 分两种情形讨论:

(1) $A\neq B$ 时, 有

$$\widehat{\mathfrak{f}}(u,v)=\begin{cases}
(-1)^{A+1}2^{\frac{n}{2}+k}, & v=0,\\
0, & \text{其他}.
\end{cases}$$

(2) $A=B$ 时, 有

$$\widehat{\mathfrak{f}}(u,v)=\begin{cases}
(-1)^{A+1}2^{\frac{n}{2}+k-1}, & v=0,\ v=c_1\text{ 或 }v=c_2,\\
(-1)^A2^{\frac{n}{2}+k-1}, & v=c_1+c_2,\\
0, & \text{其他}.
\end{cases}$$

接下来讨论 $\mathfrak{f}(x,y)$ 的 Walsh 谱值分布. 首先考虑 $\widehat{\mathfrak{f}}(u,v)=-2^{\frac{n}{2}+k}$ 出现的次数, 注意到 $v=0$ 且

$A=0,B=1$ 时, $\widehat{\mathfrak{f}}(u,v)=-2^{\frac{n}{2}+k}$, 设 N_4 表示 $\mathbb{F}_{2^n}\times\mathbb{F}_{2^k}$ 中满足此条件的 (u,v) 的个数, 则有

$$\begin{aligned} N_4 &= \frac{1}{2^2}\sum_{u\in\mathbb{F}_{2^n}}(1+(-1)^A)(1-(-1)^B) \\ &= \frac{1}{2^2}\sum_{u\in\mathbb{F}_{2^n}}(1+(-1)^A-(-1)^B-(-1)^{A+B}), \end{aligned}$$

与 (9) 式类似, $\sum\limits_{u\in\mathbb{F}_{2^n}}(-1)^B=\sum\limits_{u\in\mathbb{F}_{2^n}}(-1)^{A+B}=-2^{\frac{n}{2}}$, 因此

$$N_4=\frac{1}{2^2}(2^n-2^{\frac{n}{2}}+2^{\frac{n}{2}}+2^{\frac{n}{2}})=2^{n-2}+2^{\frac{n}{2}-2}.$$

其次考虑 $\widehat{\mathfrak{f}}(u,v)=2^{\frac{n}{2}+k}$ 出现的次数, 注意到 $v=0$ 且 $A=1,B=0$ 时, $\widehat{\mathfrak{f}}(u,v)=2^{\frac{n}{2}+k}$, 设 N_5 表示 $\mathbb{F}_{2^n}\times\mathbb{F}_{2^k}$ 中满足此条件的 (u,v) 的个数, 则有

$$\begin{aligned} N_5 &= \frac{1}{2^2}\sum_{u\in\mathbb{F}_{2^n}}(1-(-1)^A)(1+(-1)^B) \\ &= \frac{1}{2^2}\sum_{x\in\mathbb{F}_{2^n}}(1+(-1)^B-(-1)^A-(-1)^{A+B}) \\ &= \frac{1}{2^2}(2^n+2^{\frac{n}{2}}+2^{\frac{n}{2}}-2^{\frac{n}{2}}) \\ &= 2^{n-2}+2^{\frac{n}{2}-2}. \end{aligned}$$

下面引入 N_i $(1\le i\le 3)$ 的定义,

$$N_1 = |\{(u,v)\in\mathbb{F}_{2^n}\times\mathbb{F}_{2^k}:\widehat{\mathfrak{f}}(u,v)=0\}|, \tag{10}$$

$$N_2 = |\{(u,v)\in\mathbb{F}_{2^n}\times\mathbb{F}_{2^k}:\widehat{\mathfrak{f}}(u,v)=2^{\frac{n}{2}+k-1}\}|, \tag{11}$$

$$N_3 = |\{(u,v)\in\mathbb{F}_{2^n}\times\mathbb{F}_{2^k}:\widehat{\mathfrak{f}}(u,v)=-2^{\frac{n}{2}+k-1}\}|. \tag{12}$$

因为 $\mathfrak{f}(0,0)=0$, 将 (10) 式以及 N_4,N_5 带入方程组 (1) 中, 有

$$\begin{cases} 2^{n+k} &= 2^{n-1}+2^{\frac{n}{2}-1}+N_1+N_2+N_3, \\ 2^{n+k} &= -2^{\frac{n}{2}+k}(2^{n-2}+2^{\frac{n}{2}-2})+2^{\frac{n}{2}+k}(2^{n-2}+2^{\frac{n}{2}-2}) \\ &\quad -2^{\frac{n}{2}+k-1}\cdot N_2+2^{\frac{n}{2}+k-1}\cdot N_3, \\ 2^{2(n+k)} &= 2^{n+2k}(2^{n-2}+2^{\frac{n}{2}-2})+2^{n+2k}(2^{n-2}+2^{\frac{n}{2}-2}) \\ &\quad +2^{n+2k-2}\cdot N_2+2^{n+2k-2}\cdot N_3, \end{cases}$$

解得

$$\begin{cases} N_1 = 2^{n+k} - 5 \cdot 2^{n-1} + 3 \cdot 2^{\frac{n}{2}-1}, \\ N_2 = 2^n - 2^{\frac{n}{2}+1}, \\ N_3 = 2^n. \end{cases}$$

因而得证. □

3.2. 新函数构造及谱值分析

本节的主要工作是利用构造的新布尔函数设计一类极小线性码.

引理4. [13] 设码 $\mathcal{C}_f$ 由 (4) 式定义, 则 $\mathcal{C}_f$ 的长度为 2^{n-1}, 维数为 $n+1$, 其重量分布可由下述多重集给出

$$\{\{\frac{2^n - \widehat{f}(\omega)}{2} : \omega \in \mathbb{F}_{2^n}\} \cup \{2^{n-1} : \omega \in \mathbb{F}_{2^n}^*\} \cup \{0\}\}.$$

定理2. 设符号定义如上, 则由 (5) 式定义的函数 $\mathfrak{f}(x,y)$ 基于 (4) 式构造的线性码 $\mathcal{C}_\mathfrak{f}$ 是参数为 $[2^{n+k-1}, n+k+1, 2^{n+k-1} - 2^{m+k-1}]$ 的窄极小码, 其重量分布见表1, 其中

Table 1. The weight distribution of $\mathcal{C}_{\mathfrak{f}(x,y)}$

表 1. $\mathcal{C}_{\mathfrak{f}(x,y)}$ 的重量分布

重量	频数
0	1
2^{n+k-1}	$2^{n+k} - 5 \cdot 2^{n-1} + 3 \cdot 2^{\frac{n}{2}-1}$
$2^{n+k-1} \pm 2^{m+k-1}$	$2^{n-2} + 2^{\frac{n}{2}-2}$
$2^{n+k-1} - 2^{m+k-2}$	$2^n - 2^{\frac{n}{2}+1}$
$2^{n+k-1} + 2^{m+k-2}$	2^n

证明 由定理 1 中的函数 $\mathfrak{f}(x,y)$ 的 Walsh 谱值分布和引理 4 的结论可得 $\mathcal{C}_\mathfrak{f}$ 的重量分布见表1. 由上表可知 $w_{\min} = 2^{n+k-1} - 2^{m+k-1}$, $w_{\max} = 2^{n+k-1} + 2^{m+k-1}$, 从而 $\frac{w_{\min}}{w_{\max}} > \frac{1}{2}$, 所以满足 Aschikhmin-Barg 条件, 故为窄极小码. □

例1. 假设 $n=8$, $k=2$, 且 ζ 是 $\mathbb{F}_{2^8}$ 上满足 $\zeta^8 + \zeta^6 + \zeta^5 + \zeta + 1 = 0$ 的本原元, 令 $c_1 = 1$, $c_2 = \zeta^{85}$, $\lambda = \zeta^{17}$, $r = \zeta^{85}$, $\mathrm{Tr}_1^n(r) = 0$ 通过 Magma 程序验证码 $\mathcal{C}_\mathfrak{f}$ 的参数为 $[542, 11, 510]$, 其重量计数器为

$$1 + 408z^{512} + 241z^{526} + 68z^{542} + 256z^{558} + 68z^{574}$$

这与定理 2 的结论一致.

4. 结论

本文基于 Kasami 函数构造了一类具有五值 Walsh 谱的布尔函数并确定了新函数的谱值分布. 同时, 用 Magma 程序验证了结论的正确性. 另外利用新函数设计了一类线性码, 且给出了其重量分

布. 结果表明, 所构造的线性码是满足 Ashikhmin-Barg 条件的五重极小线性码, 可用作设计具有良好访问结构的秘密共享方案.

参考文献

[1] Rothaus, O. (1976) On Bent Functions. *Journal of Combinatorial Theory, Series A*, **20**, 300-305. https://doi.org/10.1016/0097-3165(76)90024-8

[2] Ding, C., Helleseth, T., Klove, T. and Wang, X. (2007) A Generic Construction of Cartesian Authentication Codes. *IEEE Transactions on Information Theory*, **53**, 2229-2235. https://doi.org/10.1109/TIT.2007.896872

[3] Delsarte, P. (1973) Four Fundamental Parameters of a Code and Their Combinatorial Significance. *Information and Control*, **23**, 407-438. https://doi.org/10.1016/S0019-9958(73)80007-5

[4] 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

[5] 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

[6] 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

[7] 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

[8] 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

[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] Heng, Z., Ding, C. and Zhou, Z. (2018) Minimal Linear Codes over Finite Fields. *Finite Fields and Their Applications*, **54**, 176-196. https://doi.org/10.1016/j.ffa.2018.08.010

[11] Zhang, W., Yan, H. and Wei, H. (2019) Four Families of Minimal Binary Linear Codes with $w_{min}/w_{max} \leq 1/2$. *Applicable Algebra in Engineering, Communication and Computing*, **30**, 175-184. https://doi.org/10.1007/s00200-018-0367-x

[12] Mesnager, S. (2014) Several New Infinite Families of Bent Functions and Their Duals. *IEEE Transactions on Information Theory*, **60**, 4397-4407. https://doi.org/10.1109/TIT.2014.2320974

[13] 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