高非线性四谱值和五谱值布尔函数的构造

郭飞[1]，王子龙[2]，段明[1]
（1.信息工程大学数学工程与先进计算国家重点实验室，河南 郑州 450001；
2.西安电子科技大学空天地一体化综合业务网全国重点实验室，陕西 西安 710071）

摘　要：四谱值和五谱值布尔函数对于密码学应用具有特殊的意义，通过修改Maiorana-McFarland类bent函数，给出了一种偶数元四谱值和五谱值布尔函数的构造，确定了所构造函数的Walsh谱分布，证明其非线性度和半bent函数一样高，为$2^{n-1}-2^{\frac{n}{2}}$（n为变元数），代数次数能取到3和理论上界$\frac{n}{2}+1$之间的任意值。并深入研究了该构造的一个子类，包含的函数具有五谱值和最高的代数次数$\frac{n}{2}+1$，且不存在非零线性结构。

关键词：布尔函数；四谱值函数；五谱值函数；非线性度；代数次数
中图分类号：TN918.8
文献标志码：A
DOI：10.11959/j.issn.1000–436x.2025048

Construction of highly nonlinear Boolean functions with four-valued and five-valued spectra

GUO Fei[1], WANG Zilong[2], DUAN Ming[1]
1. State Key Laboratory of Mathematical Engineering and Advanced Computing, Information Engineering University, Zhengzhou 450001, China
2. State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710071, China

Abstract: Boolean functions with four-valued and five-valued spectra are of special interest for cryptography applications. By modifying bent functions in the Maiorana-McFarland class, a construction of Boolean functions on even numbers of variables with four-valued and five-valued spectra was presented, and their spectral distributions were determined. The nonlinearity of these functions was proved to be as good as that of semi-bent functions, i.e., $2^{n-1}-2^{\frac{n}{2}}$ (n was the number of variables), and the algebraic degree could reach any value ranging from 3 to the theoretical upper bound $\frac{n}{2}+1$. Furthermore, a subclass of the construction was studied, which consisted of Boolean functions with five-valued spectra, the highest algebraic degree $\frac{n}{2}+1$, and without non-zero linear structures.

Keywords: Boolean function, four-valued spectra function, five-valued spectra function, nonlinearity, algebraic degree

0　引言

布尔函数是对称密码系统的重要组件，其密码学性质直接影响密码系统的安全性。bent函数[1]是一类具有均匀绝对值Walsh谱的布尔函数，即对于任意的n元bent函数（n为偶数），其Walsh谱只包含2个值（即$\pm 2^{\frac{n}{2}}$）。在所有布尔函数中，bent函数具有最高的非线性度，这意味着它能为密码系统提供最优的混淆效果。然而，bent函数存在不平衡

收稿日期：2024–12–26；修回日期：2025–03–03
通信作者：段明，mdscience@sina.com
基金项目：国家自然科学基金资助项目（No.62472438, No.62172319）
Foundation Items：The National Natural Science Foundation of China (No.62472438, No.62172319)

性、代数次不超过$\frac{n}{2}$、抗相关攻击性能差等缺点，限制了其在密码系统中的应用。

为了克服这些缺点，研究者提出了半 bent 函数[2]的概念，半 bent 函数具有三谱值和高非线性度，并且能同时满足其他的密码学指标，包括平衡性和优良的相关免疫度等。因此，半 bent 函数是 bent 函数很好的折中。更多关于半 bent 函数的结论，请参考文献[3-5]。近年来，四谱值和五谱值布尔函数越来越受到关注。首先，这两类函数可能具有良好的密码学性质而被应用于序列密码和分组密码。其次，这两类函数在码分多址（CDMA, code division multiple access）通信系统的设计中也发挥了重要作用[6]。另外，目前$\mathbb{F}_2^6$上唯一已知的 APN（almost perfect nonlinear）置换[7]的所有分量函数都是五谱值的，因此研究五谱值函数对于解决偶数元 APN 置换问题起到一定的促进作用。文献[8-10]研究有限域上迹函数表示的五谱值布尔函数构造。文献[11]通过修改 2 个 bent 函数的级联函数来构造高非线性度平衡和弹性五谱值布尔函数。文献[12]通过修改 bent 函数间接构造的条件来构造五谱值布尔函数。文献[13-15]通过修改已知 bent 函数的真值表来构造四谱值和五谱值布尔函数。文献[16-18]从 Walsh 谱域的角度研究五谱值布尔函数的特征和构造。

不同于上述已知的构造方法，本文通过修改 MM（Maiorana-McFarland）类 bent 函数的表达式，给出了一种构造四谱值和五谱值布尔函数的方法，并确定了所构造函数的 Walsh 谱分布，进而证明了这些函数具有四值或五值的 Walsh 谱，非线性度与半 bent 函数一致，为$2^{n-1}-2^{\frac{n}{2}}$。另外，这些函数的代数次数能取到 3 和$\frac{n}{2}+1$之间的任意值，而$\frac{n}{2}+1$是具有这些谱值的布尔函数的代数次数上界。最后，研究了该构造的一种特殊情形，包含具有最高的代数次数$\frac{n}{2}+1$的五谱值布尔函数，且不存在非零线性结构。

1　预备知识

令$\mathbb{F}_2$表示二元域，$\mathbb{F}_2^n$表示$\mathbb{F}_2$上的 n 维向量空间。整数和$\mathbb{F}_2$上的加法都用+表示，具体含义由上下文确定。任意 n 元布尔函数$f:\mathbb{F}_2^n \to \mathbb{F}_2$都能表示为

$$f(x_1,\cdots,x_n)=\sum_{\boldsymbol{u}=(u_1,\cdots,u_n)\in\mathbb{F}_2^n}\lambda_{\boldsymbol{u}}\prod_{i=1}^{n}x_i^{u_i}$$

其中，$\lambda_{\boldsymbol{u}}\in\mathbb{F}_2$。$f$ 的汉明重量定义为$w(f)=|\{\boldsymbol{x}\in\mathbb{F}_2^n|f(\boldsymbol{x})=1\}|$，代数次数定义为$\deg(f)=\max\{w(\boldsymbol{u})|\lambda_{\boldsymbol{u}}=1\}$，其中$w(\boldsymbol{u})=|\{i|u_i=1\}|$表示$\boldsymbol{u}$的汉明重量。

n 元布尔函数f在$\boldsymbol{a}\in\mathbb{F}_2^n$处的 Walsh 变换为

$$W_f(\boldsymbol{a})=\sum_{\boldsymbol{x}\in\mathbb{F}_2^n}(-1)^{f(x)+\boldsymbol{ax}} \tag{1}$$

其中，$\boldsymbol{ax}=a_1x_1+\cdots+a_nx_n\in\mathbb{F}_2$表示$\boldsymbol{a}=(a_1,\cdots,a_n)$和$\boldsymbol{x}=(x_1,\cdots,x_n)$的点积。包含所有 Walsh 变换的序列称为 Walsh 谱，即

$$[W_f(0,\cdots,0),W_f(0,\cdots,0,1),\cdots,W_f(1,\cdots,1)]$$

n 元布尔函数f的非线性度（记为$N(f)$）衡量其与所有仿射函数（次数不超过 1 的函数）之间的最小汉明距离，可以用 Walsh 变换刻画为

$$N(f)=2^{n-1}-\max_{\boldsymbol{a}\in\mathbb{F}_2^n}\frac{|W_f(\boldsymbol{a})|}{2} \tag{2}$$

定义 1　设 n 是偶数，f 是 n 元布尔函数，如果对于任意的$\boldsymbol{a}\in\mathbb{F}_2^n$都有$|W_f(\boldsymbol{a})|=2^{\frac{n}{2}}$，称 f 为 bent 函数[1]。

对于 n 元 bent 函数 f，其对偶函数（记为$\tilde{f}$）定义为$2^{\frac{n}{2}}(-1)^{\tilde{f}(x)}=W_f(\boldsymbol{x})$。任何 bent 函数的对偶函数都是 bent 函数。

MM 类 bent 函数[19]是具有如下形式的函数

$$f(\boldsymbol{x},\boldsymbol{y})=\boldsymbol{x}\pi(\boldsymbol{y})+g(\boldsymbol{y}) \tag{3}$$

其中，$\boldsymbol{x},\boldsymbol{y}\in\mathbb{F}_2^m$，$\pi$ 是$\mathbb{F}_2^m$上的任意置换，g 是任意 m 元函数。式(3)中f的对偶函数为

$$\tilde{f}(\boldsymbol{x},\boldsymbol{y})=\boldsymbol{y}\pi^{-1}(\boldsymbol{x})+g(\pi^{-1}(\boldsymbol{x})) \tag{4}$$

定义 2　设 n 是偶数，若 n 元布尔函数 f 的 Walsh 谱取值为$\{0,\pm2^{\frac{n}{2}+1}\}$，称$f$为半 bent 函数[2]。

n 元布尔函数f在$\boldsymbol{\beta}\in\mathbb{F}_2^n$处的自相关函数定义为

$$\Delta_f(\boldsymbol{\beta})=\sum_{\boldsymbol{x}\in\mathbb{F}_2^n}(-1)^{f(x)+f(x+\boldsymbol{\beta})}$$

它能用 Walsh 变换等价表示为

$$\Delta_f(\boldsymbol{\beta}) = \frac{1}{2^n}\sum_{\boldsymbol{x}\in\mathbb{F}_2^n}(W_f(\boldsymbol{x}))^2(-1)^{\boldsymbol{\beta}\boldsymbol{x}} \tag{5}$$

如果$\Delta_f(\boldsymbol{\beta}) = \pm 2^n$，称$\boldsymbol{\beta}$为$f$的线性结构。将$\mathbb{F}_2^n$中的全0向量和全1向量分别简记为$\mathbf{0}_n$和$\mathbf{1}_n$。显然，$\mathbf{0}_n$是所有$n$元布尔函数的线性结构。存在非零线性结构的布尔函数在密码系统中容易遭受攻击[20-21]。

2 四谱值和五谱值布尔函数

2.1 构造方法

令$n = 2m \geqslant 4$，$\boldsymbol{x}' = (x_1,\cdots,x_{m-1}) \in \mathbb{F}_2^{m-1}$，$\boldsymbol{y}' = (y_1,\cdots,y_{m-1}) \in \mathbb{F}_2^{m-1}$，$\boldsymbol{x} = (\boldsymbol{x}',x_m) \in \mathbb{F}_2^m$，$\boldsymbol{y} = (\boldsymbol{y}',y_m) \in \mathbb{F}_2^m$。设$\pi$是$\mathbb{F}_2^{m-1}$上的任意置换，$t$和$g$是任意$m-1$元布尔函数，定义$n$元布尔函数为

$$f(\boldsymbol{x},\boldsymbol{y}) = \boldsymbol{x}(\pi(\boldsymbol{y}'),y_m t(\boldsymbol{y}')) + g(\boldsymbol{y}') \tag{6}$$

显然，当$t = 0$（常量0函数）时，$(\pi(\boldsymbol{y}'),0)$是$\mathbb{F}_2^m$上2对1映射，f是半bent函数[22]；当$t = 1$（常量1函数）时，$(\pi(\boldsymbol{y}'),y_m)$是$\mathbb{F}_2^m$上的置换，$f$是MM类bent函数。下面研究$\deg(t) \geqslant 1$时$f$的性质。

2.2 Walsh谱特征和分布

令$\boldsymbol{u}' = (u_1,\cdots,u_{m-1}) \in \mathbb{F}_2^{m-1}$，$\boldsymbol{v}' = (v_1,\cdots,v_{m-1}) \in \mathbb{F}_2^{m-1}$，$\boldsymbol{u} = (\boldsymbol{u}',u_m) \in \mathbb{F}_2^m$，$\boldsymbol{v} = (\boldsymbol{v}',v_m) \in \mathbb{F}_2^m$。定理1给出了式(6)中$f$的Walsh谱取值情况。

定理1 式(6)中f的Walsh谱至多包含5个值$\{0,\pm 2^m,\pm 2^{m+1}\}$。

证明 由式(1)知，f在$(\boldsymbol{u},\boldsymbol{v}) \in \mathbb{F}_2^n$处的Walsh变换为

$$\begin{aligned}W_f(\boldsymbol{u},\boldsymbol{v}) &= \sum_{(\boldsymbol{x},\boldsymbol{y})\in\mathbb{F}_2^n}(-1)^{f(\boldsymbol{x},\boldsymbol{y})+(\boldsymbol{u},\boldsymbol{v})(\boldsymbol{x},\boldsymbol{y})} = \\ &\sum_{(\boldsymbol{x}',\boldsymbol{y}')\in\mathbb{F}_2^{n-2}}[(-1)^{\boldsymbol{x}'\pi(\boldsymbol{y}')+g(\boldsymbol{y}')+(\boldsymbol{u}',\boldsymbol{v}')(\boldsymbol{x}',\boldsymbol{y}')} + \\ &(-1)^{\boldsymbol{x}'\pi(\boldsymbol{y}')+g(\boldsymbol{y}')+(\boldsymbol{u}',\boldsymbol{v}')(\boldsymbol{x}',\boldsymbol{y}')+u_m} + \\ &(-1)^{\boldsymbol{x}'\pi(\boldsymbol{y}')+g(\boldsymbol{y}')+(\boldsymbol{u}',\boldsymbol{v}')(\boldsymbol{x}',\boldsymbol{y}')+v_m} + \\ &(-1)^{\boldsymbol{x}'\pi(\boldsymbol{y}')+t(\boldsymbol{y}')+g(\boldsymbol{y}')+(\boldsymbol{u}',\boldsymbol{v}')(\boldsymbol{x}',\boldsymbol{y}')+u_m+v_m}]\end{aligned}$$

令h_1和h_2表示如式(7)形式的$n-2$元bent函数。

$$\begin{cases}h_1(\boldsymbol{x}',\boldsymbol{y}') = \boldsymbol{x}'\pi(\boldsymbol{y}') + g(\boldsymbol{y}') \\ h_2(\boldsymbol{x}',\boldsymbol{y}') = \boldsymbol{x}'\pi(\boldsymbol{y}') + t(\boldsymbol{y}') + g(\boldsymbol{y}')\end{cases} \tag{7}$$

进而，有

$$\begin{aligned}W_f(\boldsymbol{u},\boldsymbol{v}) &= W_{h_1}(\boldsymbol{u}',\boldsymbol{v}') + (-1)^{u_m}W_{h_1}(\boldsymbol{u}',\boldsymbol{v}') + \\ &(-1)^{v_m}W_{h_1}(\boldsymbol{u}',\boldsymbol{v}') + (-1)^{u_m+v_m}W_{h_2}(\boldsymbol{u}',\boldsymbol{v}') = \\ &2^{m-1}[(-1)^{\tilde{h}_1(\boldsymbol{u}',\boldsymbol{v}')} + (-1)^{\tilde{h}_1(\boldsymbol{u}',\boldsymbol{v}')+u_m} + \\ &(-1)^{\tilde{h}_1(\boldsymbol{u}',\boldsymbol{v}')+v_m} + (-1)^{\tilde{h}_2(\boldsymbol{u}',\boldsymbol{v}')+u_m+v_m}]\end{aligned} \tag{8}$$

显然，$(-1)^{\tilde{h}_1(\boldsymbol{u}',\boldsymbol{v}')}+(-1)^{\tilde{h}_1(\boldsymbol{u}',\boldsymbol{v}')+u_m}+(-1)^{\tilde{h}_1(\boldsymbol{u}',\boldsymbol{v}')+v_m}+(-1)^{\tilde{h}_2(\boldsymbol{u}',\boldsymbol{v}')+u_m+v_m}$有5个可能的取值$\{0,\pm 2,\pm 4\}$。因此，$W_f(\boldsymbol{u},\boldsymbol{v})$有5个可能的取值$\{0,\pm 2^m,\pm 2^{m+1}\}$。证毕。

为了分析式(6)中f的Walsh谱分布，令

$$\begin{cases}S_1 = \{(\boldsymbol{u}',\boldsymbol{v}') \in \mathbb{F}_2^{n-2} | t(\boldsymbol{u}') = 0, \boldsymbol{u}'\boldsymbol{v}' + g(\boldsymbol{u}') = 1\} \\ S_2 = \{(\boldsymbol{u}',\boldsymbol{v}') \in \mathbb{F}_2^{n-2} | t(\boldsymbol{u}') = 0, \boldsymbol{u}'\boldsymbol{v}' + g(\boldsymbol{u}') = 0\} \\ S_3 = \{(\boldsymbol{u}',\boldsymbol{v}') \in \mathbb{F}_2^{n-2} | \boldsymbol{u}'\boldsymbol{v}' + g(\boldsymbol{u}') = 1\}\end{cases}$$

令Λ_i表示i在f的Walsh谱中出现的次数，其中$i \in \{0,\pm 2^m,\pm 2^{m+1}\}$。定理2给出了式(6)中$f$的Walsh谱分布。

定理2 设$\deg(t) \geqslant 1$，式(6)中f的Walsh谱分布为

$$\begin{cases}\Lambda_0 = 3|S_1| + 3|S_2| \\ \Lambda_{2^m} = 3\times 2^{n-2} - |S_1| - 3|S_2| - 2|S_3| \\ \Lambda_{-2^m} = 2^{n-2} - 3|S_1| - |S_2| + 2|S_3| \\ \Lambda_{2^{m+1}} = |S_2| \\ \Lambda_{-2^{m+1}} = |S_1|\end{cases} \tag{9}$$

证明 对于式(7)中的h_1和h_2，由式(4)可知

$$\begin{cases}\tilde{h}_1(\boldsymbol{u}',\boldsymbol{v}') = \boldsymbol{v}'\tau(\boldsymbol{u}') + g(\tau(\boldsymbol{u}')) \\ \tilde{h}_2(\boldsymbol{u}',\boldsymbol{v}') = \boldsymbol{v}'\tau(\boldsymbol{u}') + t(\tau(\boldsymbol{u}')) + g(\tau(\boldsymbol{u}'))\end{cases}$$

且$\tilde{h}_1(\boldsymbol{u}',\boldsymbol{v}') + \tilde{h}_2(\boldsymbol{u}',\boldsymbol{v}') = t(\tau(\boldsymbol{u}'))$，其中$\tau = \pi^{-1}$。因为$\deg(t) \geqslant 1$，所以$\tilde{h}_1(\boldsymbol{u}',\boldsymbol{v}') + \tilde{h}_2(\boldsymbol{u}',\boldsymbol{v}') = 0$和$\tilde{h}_1(\boldsymbol{u}',\boldsymbol{v}') + \tilde{h}_2(\boldsymbol{u}',\boldsymbol{v}') = 1$都会发生。结合式(8)，考虑c-1和c-2这2种情形。

c-1 对于$\tilde{h}_1(\boldsymbol{u}',\boldsymbol{v}') + \tilde{h}_2(\boldsymbol{u}',\boldsymbol{v}') = 0$，如果$(u_m,v_m) = (0,0)$，则$W_f(\boldsymbol{u},\boldsymbol{v}) = 2^{m+1}(-1)^{\tilde{h}_1(\boldsymbol{u}',\boldsymbol{v}')}$；如果$(u_m,v_m) \neq (0,0)$，则$W_f(\boldsymbol{u},\boldsymbol{v}) = 0$。

c-2 对于$\tilde{h}_1(\boldsymbol{u}',\boldsymbol{v}') + \tilde{h}_2(\boldsymbol{u}',\boldsymbol{v}') = 1$，如果$(u_m,v_m) = (1,1)$，则$W_f(\boldsymbol{u},\boldsymbol{v}) = -2^m(-1)^{\tilde{h}_1(\boldsymbol{u}',\boldsymbol{v}')}$；如果$(u_m,v_m) \neq (1,1)$，则$W_f(\boldsymbol{u},\boldsymbol{v}) = 2^m(-1)^{\tilde{h}_1(\boldsymbol{u}',\boldsymbol{v}')}$。

下面分析当π是恒等映射（即$\pi(\boldsymbol{y}') = \boldsymbol{y}'$）时$f$的Walsh谱分布，考虑以下2种情形。

1) 对于所有的$(\boldsymbol{u}',\boldsymbol{v}') \in S_3$（即$\tilde{h}_1(\boldsymbol{u}',\boldsymbol{v}') = 1$），

至少存在 $|S_1|$ 个使 $t(\boldsymbol{u}')=0$（即 $\tilde{h}_2(\boldsymbol{u}',\boldsymbol{v}')=1$），$|S_3|-|S_1|$ 个使 $t(\boldsymbol{u}')=1$（即 $\tilde{h}_2(\boldsymbol{u}',\boldsymbol{v}')=0$）。因此，在 f 的 Walsh 谱中，-2^{m+1} 出现 $|S_1|$ 次，0 出现 $3|S_1|$ 次（根据 c-1）；2^m 出现 $|S_3|-|S_1|$ 次，-2^m 出现 $3(|S_3|-|S_1|)$ 次（根据 c-2）。

2) 对于所有的 $(\boldsymbol{u}',\boldsymbol{v}')\in\mathbb{F}_2^{n-2}\backslash S_3$（即 $\tilde{h}_1(\boldsymbol{u}',\boldsymbol{v}')=0$），至少存在 $|S_2|$ 个使 $t(\boldsymbol{u}')=0$（即 $\tilde{h}_2(\boldsymbol{u}',\boldsymbol{v}')=0$），$2^{n-2}-|S_2|-|S_3|$ 个使 $t(\boldsymbol{u}')=1$（即 $\tilde{h}_2(\boldsymbol{u}',\boldsymbol{v}')=1$）。因此，在 f 的 Walsh 谱中，2^{m+1} 出现 $|S_2|$ 次，0 出现 $3|S_2|$ 次（根据 c-1）；-2^m 出现 $2^{n-2}-|S_2|-|S_3|$ 次，2^m 出现 $3(2^{n-2}-|S_2|-|S_3|)$ 次（根据 c-2）。

结合上述讨论的 2 种情形可知，当 π 是恒等映射时式(9)成立。

下面说明 π 不影响 f 的 Walsh 谱分布。令

$$\begin{cases} S_1'=\{(\boldsymbol{u}',\boldsymbol{v}')\in\mathbb{F}_2^{n-2}|t(\tau(\boldsymbol{u}'))=0,\tilde{h}_1(\boldsymbol{u}',\boldsymbol{v}')=1\} \\ S_2'=\{(\boldsymbol{u}',\boldsymbol{v}')\in\mathbb{F}_2^{n-2}|t(\tau(\boldsymbol{u}'))=0,\tilde{h}_1(\boldsymbol{u}',\boldsymbol{v}')=0\} \\ S_3'=\{(\boldsymbol{u}',\boldsymbol{v}')\in\mathbb{F}_2^{n-2}|\tilde{h}_1(\boldsymbol{u}',\boldsymbol{v}')=1\} \end{cases}$$

类似于上述分析，f 的 Walsh 谱分布为式(9)中用 $|S_i'|$ 替换 $|S_i|$ 后的结果，其中 $i=1,2,3$。因为 $\tau=\pi^{-1}$ 是 $\mathbb{F}_2^{m-1}$ 的置换，所以对于 $i=1,2,3$ 都有 $|S_i'|=|S_i|$。因此，π 不影响 f 的 Walsh 谱分布。证毕。

下面给出定理 2 的推论，说明式(6)中 f 是四谱值和五谱值布尔函数。

推论 1　设 $\deg(t)\geqslant 1$，f 为式(6)中的函数，下面的结论成立。

1) 如果 $|S_1|=0$，f 的 Walsh 谱包含 4 个值 $\{0,\pm 2^m,2^{m+1}\}$，且 $\Lambda_{2^m}=\Lambda_{-2^m}$。

2) 如果 $|S_2|=0$，f 的 Walsh 谱包含 4 个值 $\{0,\pm 2^m,-2^{m+1}\}$，且 $\Lambda_{2^m}=\Lambda_{-2^m}$。

3) 如果 $|S_1|\neq 0$ 且 $|S_2|\neq 0$，f 的 Walsh 谱包含 5 个值 $\{0,\pm 2^m,\pm 2^{m+1}\}$，且 $\Lambda_{2^m}=\Lambda_{-2^m}$ 或者 $\Lambda_{2^{m+1}}=\Lambda_{-2^{m+1}}$，但二者不会同时成立。

证明　根据定理 2 的证明中 c-1 情形可知，$\Lambda_0>0$，$\Lambda_{2^{m+1}}$ 和 $\Lambda_{-2^{m+1}}$ 不会同时等于 0。在 c-2 情形中，因为 $(u_m,v_m)=(0,1)$ 和 $(1,1)$ 时 f 的 Walsh 变换是互为相反数的，所以 $\Lambda_{2^m}>0$ 且 $\Lambda_{-2^m}>0$。也就是说，f 的 Walsh 谱中包含四值或五值。

另外，$\tilde{h}_1$ 和 $\tilde{h}_2$ 都是 bent 函数，考虑下面 2 种情形。

1) 如果 $w(\tilde{h}_1)=w(\tilde{h}_2)$，则存在相同数量的 $(\boldsymbol{u}',\boldsymbol{v}')\in\mathbb{F}_2^{n-2}$ 使 $\tilde{h}_1=0$，$\tilde{h}_2=1$ 和 $\tilde{h}_1=1$，$\tilde{h}_2=0$。由 c-2 知，$\Lambda_{2^m}=\Lambda_{-2^m}$。1)

2) 如果 $w(\tilde{h}_1)+w(\tilde{h}_2)=2^{n-2}$，则存在相同数量的 $(\boldsymbol{u}',\boldsymbol{v}')\in\mathbb{F}_2^{n-2}$ 使 $\tilde{h}_1=0$，$\tilde{h}_2=0$ 和 $\tilde{h}_1=1$，$\tilde{h}_2=1$。由 c-1 知，$\Lambda_{2^{m+1}}=\Lambda_{-2^{m+1}}$。

根据上述讨论知，如果 f 是五谱值函数，则 $\Lambda_{2^m}=\Lambda_{-2^m}$ 或者 $\Lambda_{2^{m+1}}=\Lambda_{-2^{m+1}}$；如果 f 是四谱值函数（$\Lambda_{2^{m+1}}\neq\Lambda_{-2^{m+1}}$），则 $\Lambda_{2^m}=\Lambda_{-2^m}$。证毕。

2.3　非线性度和代数次数

由推论 1 可知，$\max\limits_{\boldsymbol{\alpha}\in\mathbb{F}_2^n}|W_f(\boldsymbol{\alpha})|=2^{m+1}$，根据式(2)可得式(6)中 f 的非线性度为

$$N(f)=2^{n-1}-2^m$$

显然，f 的非线性度与半 bent 函数的非线性度是一致的，与文献[9,12,14-18]中构造的（平衡）四谱值和五谱值函数的非线性度也是一致的，这也是目前已知的同类型函数非线性度最大值。

为了分析式(6)中 f 的代数次数上界，引入引理 1。

引理 1　设整数 n,p 满足 $n\geqslant 2$，$2\leqslant p\leqslant n$，g 是 n 元布尔函数。如果对于任意的 $\boldsymbol{\alpha}\in\mathbb{F}_2^n$ 都有 $W_g(\boldsymbol{\alpha})\equiv 0(\bmod 2^{n-p+2})$，则 g 的代数次数满足 $\deg(g)\leqslant p-1$[23]。

由引理 1 可以得到命题 1。

命题 1　设 $n=2m\geqslant 4$，g 是 n 元布尔函数。如果 g 的 Walsh 谱值集合为 $\{0,\pm 2^m,2^{m+1}\}$ 或 $\{0,\pm 2^m,-2^{m+1}\}$ 或 $\{0,\pm 2^m,\pm 2^{m+1}\}$，则 g 的代数次数满足 $3\leqslant\deg(g)\leqslant m+1$。

定理 3 给出了式(6)中 f 的代数次数。

定理 3　设 $\deg(t)\geqslant 1$，f 为式(6)中的函数，$\pi=(\pi_1,\cdots,\pi_{m-1})$，其中 π_i（$1\leqslant i\leqslant m-1$）是 $n-1$ 元布尔函数。f 的代数次数为

$$\deg(f)=\max\{\max_{1\leqslant i\leqslant m-1}\deg(\pi_i)+1,\deg(t)+2,\deg(g)\}$$

显然，使用不同的 (π,t,g)，f 的代数次数能取到 3 和最大值 $m+1$（由命题 1 得到）之间的任意值。

由集合 S_i（$i=1,2$）的表达式知

$$\begin{cases}|S_1|\neq 0 \Leftrightarrow (t(\boldsymbol{x}')+1)(\boldsymbol{x}'\boldsymbol{y}'+g(\boldsymbol{x}'))\neq 0\\ |S_2|\neq 0 \Leftrightarrow (t(\boldsymbol{x}')+1)(\boldsymbol{x}'\boldsymbol{y}'+g(\boldsymbol{x}')+1)\neq 0\end{cases}$$

由文献[24]知，n元布尔函数f的代数免疫度定义为$\min\{\deg(h)|h\neq 0, fh=0 \text{ 或 } (f+1)h=0\}$，其中$h$是$n$元布尔函数。显然，$f$和$f+1$有相同的代数免疫度。如果$\deg(t)$严格大于函数$\boldsymbol{x}'\boldsymbol{y}'+g(\boldsymbol{x}')$的代数免疫度，则$|S_1|\neq 0$且$|S_2|\neq 0$。也就是说，使用这样的$t$函数，式(6)中$f$是五谱值函数。

8元四谱值和五谱值布尔函数的例子分别如例1和例2所示。

例1 令$m=4$，$\pi(y_1,y_2,y_3)=(y_1,y_1+y_2,y_1+y_2+y_3)$，$t(y_1,y_2,y_3)=y_1y_2y_3+y_1y_2+y_2y_3+y_1y_3+y_1+y_2+y_3$，$g(y_1,y_2,y_3)=1$。容易验证$|S_1|=8$，$|S_2|=0$，$|S_3|=36$。式(6)中布尔函数$f(x_1,\cdots,x_4,y_1,\cdots,y_4)$是5次函数，其频谱分布为$\Lambda_0=24$，$\Lambda_{2^4}=\Lambda_{-2^4}=112$，$\Lambda_{-2^5}=8$，$\Lambda_{2^5}=0$。

例2 令$m=4$，$\pi(y_1,y_2,y_3)=(y_1y_2+y_3,y_1,y_2)$，$t(y_1,y_2,y_3)=y_1y_2y_3+1$，$g(y_1,y_2,y_3)=y_1$。容易验证，$|S_1|=4$，$|S_2|=4$，$|S_3|=28$。式(6)中布尔函数$f(x_1,\cdots,x_4,y_1,\cdots,y_4)$是5次函数，其频谱分布为$\Lambda_0=24$，$\Lambda_{2^4}=120$，$\Lambda_{-2^4}=104$，$\Lambda_{2^5}=\Lambda_{-2^5}=4$。

3 不存在非零线性结构的五谱值布尔函数

设$m\geqslant 3$，在式(6)中，令π表示$\mathbb{F}_2^{m-1}$上的恒等映射，$t(\boldsymbol{y}')=y_1y_2\cdots y_{m-1}$，$g(\boldsymbol{y}')=0$，那么，$f$就变为

$$f(x_1,\cdots,x_m,y_1,\cdots,y_m)=\sum_{i=1}^{m-1}x_iy_i+x_m\prod_{i=1}^{m}y_i \quad (10)$$

显然，f具有最高的代数次数$m+1$（由命题1得到），并且有定理4。

定理4 式(10)中的f是五谱值布尔函数，不存在非零线性结构，其Walsh谱分布为

$$\begin{cases}\Lambda_0=3(2^{n-2}-2^{m-1})\\ \Lambda_{2^m}=\Lambda_{-2^m}=2^m\\ \Lambda_{2^{m+1}}=2^{n-3}\\ \Lambda_{-2^{m+1}}=2^{n-3}-2^{m-1}\end{cases} \quad (11)$$

目前所有已知的四谱值和五谱值布尔函数的构造都没有考虑线性结构的性质，式(10)首次给出了一类不存在非零线性结构的五谱值布尔函数。

定理4的证明将会在本节最后给出。容易验证，式(10)中的f是不平衡的。下面通过加上线性多项式，将f改成平衡函数，如推论2所示。

推论2 设f为式(10)中的函数，定义另外2个函数f_1和f_2为

$$\begin{cases}f_1(\boldsymbol{x},\boldsymbol{y})=f(\boldsymbol{x},\boldsymbol{y})+y_m\\ f_2(\boldsymbol{x},\boldsymbol{y})=f(\boldsymbol{x},\boldsymbol{y})+y_1+\sum_{i=2}^{m}(x_i+y_i)\end{cases}$$

则f_1和f_2是平衡的五谱值函数，且不存在非零线性结构，其Walsh谱分布由式(11)给出。

为了证明定理4，需要引入引理2。

引理2 定义$\mathbb{F}_2^n$的一个子集Ω为

$$\Omega=\bigcup_{i=1}^{m-1}\{\boldsymbol{e}_n^i\}\cup\{(\mathbf{1}_m,\mathbf{0}_m)\}\cup\bigcup_{i=m+1}^{n-1}\{\boldsymbol{e}_n^i\}\cup\{\mathbf{1}_n\}$$

其中，$\boldsymbol{e}_n^i$是$\mathbb{F}_2^n$中第i位为1、其余位全为0的向量。对于式(10)中的f和任意$(\boldsymbol{u},\boldsymbol{v})\in\Omega$，都有$W_f(\boldsymbol{u},\boldsymbol{v})\neq 0$。

证明 根据定理1的证明知

$$W_f(\boldsymbol{u},\boldsymbol{v})=\sum_{(\boldsymbol{x}',\boldsymbol{y}')\in\mathbb{F}_2^{n-2}}(-1)^{\boldsymbol{x}'\boldsymbol{y}'+(\boldsymbol{u}',\boldsymbol{v}')(\boldsymbol{x}'\boldsymbol{y}')}\cdot$$

$$[1+(-1)^{u_m}+(-1)^{v_m}+(-1)^{t(\boldsymbol{y}')+u_m+v_m}]$$

下面对$(\boldsymbol{u},\boldsymbol{v})\in\Omega$的不同情形展开讨论。

1) $(\boldsymbol{u},\boldsymbol{v})=\boldsymbol{e}_n^i$，$1\leqslant i\leqslant m-1$，有$u_m=v_m=0$且$(\boldsymbol{u}',\boldsymbol{v}')(\boldsymbol{x}',\boldsymbol{y}')=x_i$，进而有

$$W_f(\boldsymbol{u},\boldsymbol{v})=\sum_{(\boldsymbol{x}',\boldsymbol{y}')\in\mathbb{F}_2^{n-2}}[3+(-1)^{t(\boldsymbol{y}')}](-1)^{\boldsymbol{x}'\boldsymbol{y}'+x_i}$$

因为$t(\boldsymbol{y}')=1$当且仅当$\boldsymbol{y}'=\mathbf{1}_{m-1}$，并且$\mathbf{1}_{m-1}\boldsymbol{x}'+x_i$是$\mathbb{F}_2^{m-1}$上的平衡函数，所以可得

$$W_f(\boldsymbol{u},\boldsymbol{v})=4\sum_{\mathbf{1}_{m-1}\neq\boldsymbol{y}'\in\mathbb{F}_2^{m-1}}\sum_{\boldsymbol{x}'\in\mathbb{F}_2^{m-1}}(-1)^{\boldsymbol{x}'\boldsymbol{y}'+x_i}$$

另外，$\sum_{\boldsymbol{x}'\in\mathbb{F}_2^{m-1}}(-1)^{\boldsymbol{x}'\boldsymbol{y}'+x_i}$等于$2^{m-1}$当且仅当$\boldsymbol{y}'=\boldsymbol{e}_{m-1}^i$，其他情况都等于0。因此，有$W_f(\boldsymbol{u},\boldsymbol{v})=2^{m+1}$。

2) $(\boldsymbol{u},\boldsymbol{v})=(\mathbf{1}_m,\mathbf{0}_m)$，有$u_m=1$，$v_m=0$，且$(\boldsymbol{u}',\boldsymbol{v}')(\boldsymbol{x}',\boldsymbol{y}')=\mathbf{1}_{m-1}\boldsymbol{x}'$，进而有

$$W_f(\boldsymbol{u},\boldsymbol{v})=\sum_{(\boldsymbol{x}',\boldsymbol{y}')\in\mathbb{F}_2^{n-2}}[1-(-1)^{t(\boldsymbol{y}')}](-1)^{\boldsymbol{x}'\boldsymbol{y}'+\mathbf{1}_{m-1}\boldsymbol{x}'}=$$

$$2\sum_{\boldsymbol{x}'\in\mathbb{F}_2^{m-1}}(-1)^{\mathbf{1}_{m-1}\boldsymbol{x}'+\mathbf{1}_{m-1}\boldsymbol{x}'}=2^m$$

3) $(\boldsymbol{u},\boldsymbol{v})=\boldsymbol{e}_n^i$，$m+1\leqslant i\leqslant n-1$，有$u_m=v_m=0$且$(\boldsymbol{u}',\boldsymbol{v}')(\boldsymbol{x}',\boldsymbol{y}')=y_{i-m}$。类似于情形1)，可以得到$W_f(\boldsymbol{u},\boldsymbol{v})=2^{m+1}$。

4) $(\boldsymbol{u},\boldsymbol{v})=\mathbf{1}_n$，有$u_m=v_m=1$且$(\boldsymbol{u}',\boldsymbol{v}')(\boldsymbol{x}',\boldsymbol{y}')=$

$\mathbf{1}_{m-1}(\boldsymbol{x}'+\boldsymbol{y}')$，进而有

$$W_f(\boldsymbol{u},\boldsymbol{v})=\sum_{(\boldsymbol{x}',\boldsymbol{y}')\in\mathbb{F}_2^{n-2}}[-1+(-1)^{t(\boldsymbol{y}')}](-1)^{\boldsymbol{x}'\boldsymbol{y}'+\mathbf{1}_{m-1}(\boldsymbol{x}'+\boldsymbol{y}')}=$$
$$-2\sum_{\boldsymbol{x}'\in\mathbb{F}_2^{m-1}}(-1)^{\mathbf{1}_{m-1}\boldsymbol{x}'+\mathbf{1}_{m-1}(\boldsymbol{x}'+\mathbf{1}_{m-1})}=$$
$$-2\sum_{\boldsymbol{x}'\in\mathbb{F}_2^{m-1}}(-1)^{m-1}=(-2)^m$$

综上可知，结论成立。证毕。

下面给出定理4的证明。

证明　通过分析$|S_i|$（$i=1,2,3$）来确定f的Walsh谱分布。首先，有

$$|S_3|=|\{(\boldsymbol{u}',\boldsymbol{v}')\in\mathbb{F}_2^{n-2}|\,\boldsymbol{u}'\boldsymbol{v}'=1\}|=2^{n-3}-2^{m-2}\quad(12)$$

考虑$(\boldsymbol{u}',\boldsymbol{v}')\in S_2$，如果$\boldsymbol{u}'$中至少有一个0，则$t(\boldsymbol{u}')=0$。如果$\boldsymbol{u}'$和$\boldsymbol{v}'$有偶数个对应位都为1，则$\boldsymbol{u}'\boldsymbol{v}'=0$。设$\boldsymbol{u}'$中0的数量为$i$，如果$1\leqslant i\leqslant m-2$，$S_2$中$(\boldsymbol{u}',\boldsymbol{v}')$的数量为$2^{m-2}\binom{m-1}{i}$；如果$i=m-1$，$S_2$中$(\boldsymbol{u}',\boldsymbol{v}')$的数量为$2^{m-1}$。因此可得

$$|S_2|=\sum_{i=1}^{m-2}2^{m-2}\binom{m-1}{i}+2^{m-1}=2^{n-3}\quad(13)$$

类似地，考虑$(\boldsymbol{u}',\boldsymbol{v}')\in S_1$，如果$\boldsymbol{u}'$和$\boldsymbol{v}'$有奇数个对应位都为1，则$\boldsymbol{u}'\boldsymbol{v}'=1$。设$\boldsymbol{u}'$中0的数量为$i$，如果$1\leqslant i\leqslant m-2$，$S_1$中$(\boldsymbol{u}',\boldsymbol{v}')$的数量为$2^{m-2}\binom{m-1}{i}$；如果$i=m-1$，$S_1$中$(\boldsymbol{u}',\boldsymbol{v}')$的数量为0。因此可得

$$|S_1|=\sum_{i=1}^{m-2}2^{m-2}\binom{m-1}{i}=2^{n-3}-2^{m-1}\quad(14)$$

结合式(9)、式(12)～式(14)可知，f的Walsh谱分布满足式(11)。

下面证明f不存在非零线性结构。令

$$\begin{cases}G_1=\{(\boldsymbol{u},\boldsymbol{v})\in\mathbb{F}_2^n|W_f(\boldsymbol{u},\boldsymbol{v})=\pm2^m\}\\G_2=\{(\boldsymbol{u},\boldsymbol{v})\in\mathbb{F}_2^n|W_f(\boldsymbol{u},\boldsymbol{v})=\pm2^{m+1}\}\end{cases}$$

由式(11)可知

$$\begin{cases}|G_1|=\Lambda_{2^m}+\Lambda_{-2^m}=2^{m+1}\\|G_2|=\Lambda_{2^{m+1}}+\Lambda_{-2^{m+1}}=2^{n-2}-2^{m-1}\end{cases}$$

假设$\boldsymbol{\alpha}\in\mathbb{F}_2^n$是$f$的线性结构，根据式(5)可得

$$\Delta_f(\boldsymbol{\alpha})=\sum_{\boldsymbol{x}\in G_1}(-1)^{\boldsymbol{\alpha x}}+4\sum_{\boldsymbol{x}\in G_2}(-1)^{\boldsymbol{\alpha x}}=\pm2^n$$

另一方面，有$|G_1|+4|G_2|=2^n$。并且，容易验证$\mathbf{0}_n\in G_2$。因此，$\boldsymbol{\alpha}$是f的线性结构当且仅当对于任意的$\boldsymbol{x}\in G_1\cup G_2$都有$\boldsymbol{\alpha x}=0$。由引理2知$\Omega\subseteq G_1\cup G_2$，进而，对于任意的$\boldsymbol{x}\in\Omega$都有$\boldsymbol{\alpha x}=0$。注意到$\Omega$中的向量构成$\mathbb{F}_2^n$的一组基，所以$\boldsymbol{\alpha}=\mathbf{0}_n$。因此，$f$不存在非零线性结构。证毕。

4　结束语

本文聚焦四谱值和五谱值布尔函数的构造和密码学性质，通过修改Maiorana-McFarland类bent函数的表达式，给出了四谱值和五谱值布尔函数的构造，分析了其Walsh谱分布，证明了非线性度和半bent函数一样高，代数次数能取到3和理论上界$\frac{n}{2}+1$之间的任意值，并给出了一类不存在非零线性结构的五谱值函数。

参考文献：

[1] ROTHAUS O S. On bent functions[J]. Journal of Combinatorial Theory, Series A, 1976, 20(3): 300-305.

[2] CHEE S, LEE S J, KIM K. Semi-bent functions[C]//Proceedings of Advances in Cryptology. Berlin: Springer, 1995: 105-118.

[3] CARLET C, MESNAGER S. On semibent Boolean functions[J]. IEEE Transactions on Information Theory, 2012, 58(5): 3287-3292.

[4] SUN T F, HU B, YANG Y. Research on highly non-linear plateaued functions[J]. IET Information Security, 2019, 13(5): 515-518.

[5] 郭梦飞, 孙玉娟, 李路阳. 半Bent函数和多输出布尔函数的构造[J]. 密码学报, 2020, 7(1): 26-36.
GUO M F, SUN Y J, LI L Y. Constructions of semi-bent functions and multi-output Boolean functions[J]. Journal of Cryptologic Research, 2020, 7(1): 26-36.

[6] HELLESETH T, KUMAR P V. Sequences with low correlation[C]//Proceedings of 7th International Workshop. Berlin: Springer, 1998: 149-172.

[7] DILLON J F. APN polynomials: an update. invited talk at finite fields: theory and applications—FQ9[D]. Dublin: University College Dublin, 2009.

[8] CAO X W, HU L. Two Boolean functions with five-valued Walsh spectra and high nonlinearity[J]. International Journal of Foundations of Computer Science, 2015, 26(5): 537-556.

[9] XU G K, CAO X W, XU S D. Several classes of Boolean functions with few Walsh transform values[J]. Applicable Algebra in Engineering, Communication and Computing, 2017, 28(2): 155-176.

[10] ZHANG Y Z, DU X N, JIN W G, et al. Constructions of Boolean functions with five-valued Walsh spectra and their applications[J]. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2024, 107(7): 997-1002.

[11] MAITRA S, SARKAR P. Cryptographically significant Boolean functions with five valued Walsh spectra[J]. Theoretical Computer Science,

2002, 276(1/2): 133-146.

[12] MESNAGER S, ZHANG F R. On constructions of bent, semi-bent and five valued spectrum functions from old bent functions[J]. Advances in Mathematics of Communications, 2017, 11(2): 339-345.

[13] SUN Z Q, HU L. Boolean functions with four-valued Walsh spectra[J]. Journal of Systems Science and Complexity, 2015, 28(3): 743-754.

[14] SUN T F, HU B. Boolean functions with multiple-valued Walsh spectra[J]. Chinese Journal of Electronics, 2019, 28(6): 1165-1169.

[15] SU S H, WANG B X, LI J J. On the constructions of resilient Boolean functions with five-valued Walsh spectra and resilient semi-bent functions[J]. Discrete Applied Mathematics, 2022, 309: 1-12.

[16] HODŽIĆ S, PASALIC E, ZHANG W G. Generic constructions of five-valued spectra Boolean functions[J]. IEEE Transactions on Information Theory, 2019, 65(11): 7554-7565.

[17] HODŽIĆ S, HORAK P, PASALIC E. Characterization of basic 5-value spectrum functions through Walsh-Hadamard transform[J]. IEEE Transactions on Information Theory, 2021, 67(2): 1038-1053.

[18] WANG J X, FU F W. Three new constructions of 5-valued spectrum functions with totally disjoint spectra duals[C]//Proceedings of the 2022 IEEE International Symposium on Information Theory (ISIT). Piscataway: IEEE Press, 2022: 1743-1748.

[19] MCFARLAND R L. A family of difference sets in non-cyclic groups[J]. Journal of Combinatorial Theory, Series A, 1973, 15(1): 1-10.

[20] DUBUC S. Linear structures of Boolean functions[C]//Proceedings of IEEE International Symposium on Information Theory. Piscataway: IEEE Press, 2002: 440.

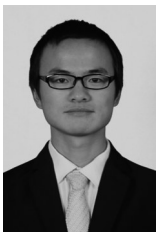
[21] EVERTSE J H. Linear structures in blockciphers[C]//Proceedings of Advances in Cryptology. Berlin: Springer, 2010: 249-266.

[22] CARLET C, GAO G P, LIU W F. Results on constructions of rotation symmetric bent and semi-bent functions[C]//Proceedings of Sequences and Their Applications. Berlin: Springer, 2014: 21-33.

[23] ZHANG X M, ZHENG Y L, IMAI H. Duality of Boolean functions and its cryptographic significance[C]//Proceedings of Information and Communications Security. Berlin: Springer, 1997: 159-169.

[24] MEIER W, PASALIC E, CARLET C. Algebraic attacks and decomposition of Boolean functions[C]//Proceedings of Advances in Cryptology. Berlin: Springer, 2004: 474-491.

[作者简介]



郭飞（1993– ），男，安徽阜阳人，博士，信息工程大学讲师，主要研究方向为信息安全、密码学等。

王子龙（1982– ），男，河南郑州人，博士，西安电子科技大学教授、博士生导师，主要研究方向为信息安全、密码学等。

段明（1980– ），男，江西萍乡人，博士，信息工程大学副教授、硕士生导师，主要研究方向为信息安全、密码学等。