弹性五谱值布尔函数的构造与分析

王维琼，李越，罗舒予，朱蒙蕊
（长安大学理学院，陕西 西安 710064）

摘　要：五谱值布尔函数在码分多址（CDMA）通信、编码与密码、真随机数生成器（TRNG）与组合设计等领域中有重要应用。基于Walsh谱中和技术，提出了一类n元弹性五谱值布尔函数的直接构造法。证明了所构造的函数非线性度最高可达$2^{n-1}-2^{\lceil \frac{n}{2} \rceil}$，达到该上界的函数代数次数为$\left\lfloor \frac{n}{2} \right\rfloor+1$，弹性阶约为$\left\lfloor \frac{n+1}{4} \right\rfloor$，且校正阶为$\left\lceil \frac{n}{2} \right\rceil$。结果表明，所构造的函数达到了密码学指标的良好折中。

关键词：布尔函数；五谱值函数；非线性度；弹性阶；校正阶
中图分类号：TN918.8
文献标志码：A
DOI：10.11959/j.issn.1000−436x.2025116

Construction and analysis of resilient five-valued spectra Boolean functions

WANG Weiqiong, LI Yue, LUO Shuyu, ZHU Mengrui
School of Science, Chang'an University, Xi'an 710064, China

Abstract: Boolean functions with five-valued spectra have important applications in code division multiple access (CDMA) communication, coding and cryptography, true random number generators (TRNG), and combinatorial design. An approach based on the Walsh spectral neutralization technique for directly constructing a class of n-variable resilient five-valued spectra Boolean functions was proposed. The nonlinearity of the resulting functions could reach up to $2^{n-1}-2^{\lceil \frac{n}{2} \rceil}$, and it was proved that functions achieving this upper bound had the algebraic degree of $\left\lfloor \frac{n}{2} \right\rfloor+1$,the resiliency order of approximately $\left\lfloor \frac{n+1}{4} \right\rfloor$, and the correction order of $\left\lceil \frac{n}{2} \right\rceil$. The results demonstrate that the constructed functions achieve a favorable balance among multiple cryptographic properties.

Keywords: Boolean function, five-valued spectra function, nonlinearity, resiliency order, correction order

0　引言

布尔函数在对称密码系统中扮演着核心角色，其密码学性质的优劣直接关系到对称密码系统的安全性。用于对称密码系统中的布尔函数需要满足一系列密码学安全指标，包括但不限于平衡性、高非线性度、高代数次数和高弹性阶。但这些安全指标之间存在着复杂的相互制约关系，使同时满足多种安全指标的布尔函数设计变得异常困难。

在布尔函数的众多密码学安全指标中，非线性度和弹性是非常重要的2个安全指标。Rothaus[1]提出的n元Bent函数的Walsh谱值有2个取值，即

收稿日期：2025−04−17；**修回日期：**2025−06−17
基金项目：国家自然科学基金资助项目（No.12271059）
Foundation Item：The National Natural Science Foundation of China (No.12271059)

$\left\{\pm 2^{\frac{n}{2}}\right\}$。这类函数达到了最优的非线性度，但缺乏平衡性和弹性，且变元个数只能为偶数。为克服这些缺陷，学者通过代数和组合的方式构造了一系列综合性质更为优良的三谱值布尔函数，如Chee等[2]提出的Semi-bent函数、Zheng等[3]提出的Plateaued函数等。这些函数可以同时具备高非线性度和弹性等密码学性质，且Walsh谱值个数较少，在密码、编码与组合设计等领域有重要应用，近年来受到了广泛关注[4-6]，且Walsh谱值个数较少的布尔函数在真随机数生成器（TRNG, true random number generator）的校正器设计中也发挥着重要应用[7-8]。例如，Lacharme[9]详细分析了线性校正器的构造，指出了布尔函数的弹性阶和校正阶之间的关系。Zhang[10]构造出一类密码学性质优良的三谱值校正器，得到了校正阶比弹性阶高1的非线性函数。Luo等[11]提出了Walsh谱中和技术，并构造了校正阶比弹性阶至少高2的三谱值非线性函数。

近年来，学者发现了具有良好密码学性质的五谱值布尔函数，这类函数在码分多址（CDMA, code division multiple access）通信系统、对称密码系统、编码理论及组合设计等领域均有重要应用[12-14]。例如，在$\mathbb{F}_2^6$上唯一几乎完全非线性（APN, almost perfect nonlinear）置换[15]的所有分量函数均为五谱值函数，且该类函数也可用作TRNG的后处理校正器。在构造方法方面，文献[16-17]通过修改MM（Maiorana-McFarland）类Bent函数间接构造了五谱值布尔函数。文献[18-19]通过修改Bent函数的真值表来构造五谱值布尔函数。文献[20-21]基于有限域上迹函数构造了几类五谱值布尔函数。文献[22-25]从Walsh谱域的角度对五谱值布尔函数进行了系统性构造。

不同于上述已知的构造方法，本文基于文献[11]中提出的Walsh谱中和技术，分段构造出一类$n(n\geqslant 10)$元弹性五谱值布尔函数，旨在使所得函数的校正阶比弹性阶至少高2，且能够在非线性度、代数次数、弹性阶和校正阶之间实现较好的折中。

1 预备知识

设$\mathbb{F}_2$是二元有限域，n为正整数，$\mathbb{F}_2^n$表示$\mathbb{F}_2$上的n维向量空间。从$\mathbb{F}_2^n$到$\mathbb{F}_2$的映射$f:\mathbb{F}_2^n\to\mathbb{F}_2$称为$n$元布尔函数，并记全体$n$元布尔函数的集合为$\mathcal{B}_n$。对于向量$X=(x_1,x_2,\cdots,x_n)\in\mathbb{F}_2^n$，其支撑集定义为$\mathrm{supp}(X)=\{1\leqslant i\leqslant n\,|\,x_i=1\}$，汉明重量为$\mathrm{wt}(X)=|\mathrm{supp}(X)|$，其中$|\cdot|$表示集合的大小。为避免歧义，用+和$\sum$表示实数域上的加法，$\oplus$和$\bigoplus$表示$\mathbb{F}_2$中的加法。为方便起见，记$\mathbf{0}_n=(0,0,\cdots,0)\in\mathbb{F}_2^n$，$\mathbf{1}_n=(1,1,\cdots,1)\in\mathbb{F}_2^n$，$\bar{X}=\mathbf{1}_n\oplus X$。

记布尔函数$f\in\mathcal{B}_n$的支撑集为$\mathrm{supp}(f)=\{X\in\mathbb{F}_2^n\,|\,f(X)=1\}$，汉明重量为$\mathrm{wt}(f)=|\mathrm{supp}(f)|$。若$\mathrm{wt}(f)=2^{n-1}$，则称$f$为平衡函数。任意$n$元布尔函数$f$可用代数正规型（ANF, algebraic normal form）表示为

$$f(x_1,x_2,\cdots,x_n)=\bigoplus_{a\in\mathbb{F}_2^n}\lambda_a\left(\prod_{i=1}^{n}x_i^{a_i}\right)\tag{1}$$

其中，$x_i,\lambda_a\in\mathbb{F}_2$，$a=(a_1,a_2,\cdots,a_n)\in\mathbb{F}_2^n$，且$x_i^{a_i}=x_i\oplus a_i\oplus 1$。式(1)中非零项的最高次数称为$f$的代数次数，记为$\deg(f)$。

定义1[26] 设$X=(x_1,x_2,\cdots,x_n)\in\mathbb{F}_2^n$，$\omega=(\omega_1,\omega_2,\cdots,\omega_n)\in\mathbb{F}_2^n$，布尔函数$f\in\mathcal{B}_n$在$\omega$处的Walsh变换定义为

$$W_f(\omega)=\sum_{X\in\mathbb{F}_2^n}(-1)^{f(X)\oplus X\cdot\omega}\tag{2}$$

其中，$X\cdot\omega=\bigoplus_{1\leqslant i\leqslant n}x_i\omega_i$表示$X$与$\omega$的内积。

Walsh变换是分析布尔函数密码学性质的重要工具，可用于刻画布尔函数的平衡性、非线性度、弹性和校正阶等密码学性质。

引理1[27] 布尔函数$f\in\mathcal{B}_n$是平衡函数当且仅当$W_f(\mathbf{0}_n)=0$。

引理2[28] 布尔函数$f\in\mathcal{B}_n$的非线性度$\mathcal{N}_f$可用Walsh变换刻画为

$$\mathcal{N}_f=2^{n-1}-\frac{1}{2}\max_{\omega\in\mathbb{F}_2^n}|W_f(\omega)|\tag{3}$$

引理3[29] 布尔函数$f\in\mathcal{B}_n$是t阶相关免疫函数当且仅当对任意$\omega\in\mathbb{F}_2^n$，$1\leqslant\mathrm{wt}(\omega)\leqslant t$，有$W_f(\omega)=0$。

若t阶相关免疫函数f是平衡的，则称f为t阶弹性函数。结合引理1与引理3可知，布尔函数f是t阶弹性函数当且仅当其Walsh变换满足：对任意$\omega\in\mathbb{F}_2^n$，$0\leqslant\mathrm{wt}(\omega)\leqslant t$，有$W_f(\omega)=0$。

引理4[9] 布尔函数$f\in\mathcal{B}_n$的校正阶为$c(c\geqslant 1)$

当且仅当对任意c'，$0 \leqslant c' \leqslant c$，都有

$$\sum_{\omega \in \mathbb{F}_2^n, \mathrm{wt}(\omega)=c'} W_f(\omega) = 0 \tag{4}$$

结合引理3与引理4可知，t阶弹性布尔函数的校正阶至少为t，但反之不一定成立。例如，布尔函数$f(x_1,x_2,x_3)=x_1 \oplus x_3 \oplus x_1x_2 \oplus x_1x_3$的校正阶为1，但其弹性阶为0。

引理5[30]　设l、m、s为正整数且m与s的二进制展开分别为$m=\sum_{i=0}^{l-1} m_i 2^i$，$s=\sum_{i=0}^{l-1} s_i 2^i$，则组合数

$$\binom{m}{s} \equiv \prod_{i=0}^{l-1} \binom{m_i}{s_i} (\mathrm{mod}\ 2) \tag{5}$$

其中，当$m<s$时，规定组合数$\binom{m}{s}$为0。

记$I=\{i \mid m_i=1, 0 \leqslant i \leqslant l-1\}$，则由引理5可知，$\binom{m}{s} \equiv 1(\mathrm{mod}\ 2) \Leftrightarrow$对$\forall 0 \leqslant i \leqslant l-1$，有$\binom{m_i}{s_i} \equiv 1(\mathrm{mod}\ 2)$。故$\binom{m}{s}$为奇数$\Leftrightarrow s_i=\begin{cases} 0\text{或}1, i \in I \\ 0, i \in \{0,1,\cdots,l-1\} \backslash I \end{cases}$，从而集合$\left\{\binom{m}{s} \mid 0 \leqslant s \leqslant m\right\}$中奇数的个数为$2^{|I|}$。

2　五谱值布尔函数

本节提出了一类弹性五谱值布尔函数的直接构造方法，并分析所得函数的非线性度、代数次数、弹性阶及校正阶等密码学性质。

2.1　构造方法

设n、m、r和s为正整数，且满足$n \geqslant 10$，$5 \leqslant m \leqslant \left\lfloor \frac{n}{2} \right\rfloor$，$0 \leqslant r \leqslant m$，$0 \leqslant s \leqslant n-m$。设$Y=(y_1,y_2,\cdots,y_m) \in \mathbb{F}_2^m$，$X=(x_1,x_2,\cdots,x_{n-m}) \in \mathbb{F}_2^{n-m}$。

1) 定义参数a_r和t_m。对$\forall r \in \{0,1,\cdots,m\}$，有

$$a_r=\begin{cases} \binom{m}{r}, & \binom{m}{r}\text{为偶数} \\ \binom{m}{r}-1, & \binom{m}{r}\text{为奇数} \end{cases} \tag{6}$$

并记$t_m=\max\left\{z \in \mathbb{Z} \middle| \sum_{s=z}^{n-m-2} \binom{n-m}{s} \geqslant \frac{1}{2}\sum_{r=0}^{m} a_r\right\}$。

2) 构造图1中映射ϕ的像集T，$T=T_1 \cup T_2 \cup T_3 \subseteq \mathbb{F}_2^{n-m}$满足以下条件。

① $T_1,T_2 \subseteq \{v \in \mathbb{F}_2^{n-m} \mid t_m \leqslant \mathrm{wt}(v) \leqslant n-m-2\}$，且$|T_1|=|T_2|=\frac{1}{2}\sum_{r=0}^{m} a_r$，$T_1 \cap T_2 \neq \varnothing$但$T_1 \neq T_2$。

② 对$\forall v \in T_1 \backslash T_2$或$v \in T_2 \backslash T_1$，有$\mathrm{wt}(v)=n-m-2$，且$\bigoplus_{v \in T_1 \backslash T_2} v \oplus \bigoplus_{v \in T_2 \backslash T_1} v \neq \mathbf{0}_{n-m}$。

③ $T_3 \subseteq \{v \in \mathbb{F}_2^{n-m} \mid \mathrm{wt}(v)=n-m-1\}$，且$|T_3|=\frac{1}{2}\left(2^m-\sum_{r=0}^{m} a_r\right)$。

3) 构造映射ϕ（如图1所示）。将$\mathbb{F}_2^m$划分为互不相交的子集U_1、U_2和U_3，即$\mathbb{F}_2^m=U_1 \cup U_2 \cup U_3$。

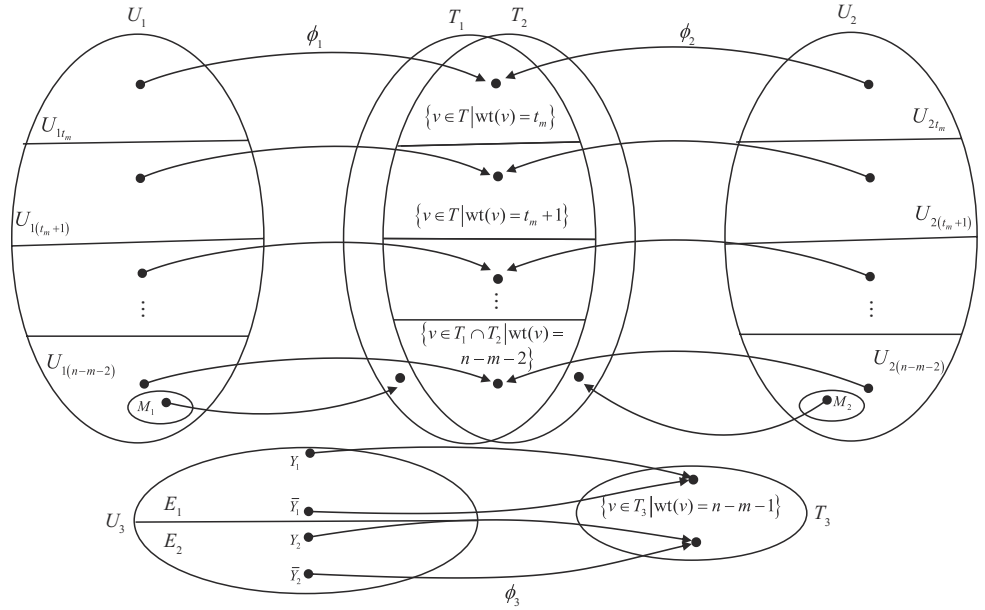

图1　映射$\phi: \mathbb{F}_2^m \to T$

并分段定义一一映射$\phi_1:U_1 \to T_1$，$\phi_2:U_2 \to T_2$，及二对一映射$\phi_3:U_3 \to T_3$，满足以下条件。

① $U_i = U_{it_m} \cup U_{i(t_m+1)} \cup \cdots \cup U_{i(n-m-2)} (i=1,2)$，其中$U_{is} = \{Y \in U_i \mid \mathrm{wt}(\phi_i(Y)) = s\}$ $(t_m \leqslant s \leqslant n-m-2)$，$|U_{is}| = |\{v \in T_i \mid \mathrm{wt}(v) = s\}|$，且$|\{Y \in U_{1s} \mid \mathrm{wt}(Y) = r\}| = |\{Y \in U_{2s} \mid \mathrm{wt}(Y) = r\}| (0 < r < m)$。

② 记$M_1 = \{Y \in U_{1(n-m-2)} \mid \phi_1(Y) \in T_1 \backslash T_2\}$，$M_2 = \{Y \in U_{2(n-m-2)} \mid \phi_2(Y) \in T_2 \backslash T_1\}$，且$|M_1| = |T_1 \backslash T_2| = |T_2 \backslash T_1| = |M_2|$。

③ $U_3 = E_1 \cup E_2$，其中$|E_1| = |E_2|$，$E_1 \cap E_2 = \varnothing$，对$\forall Y \in E_i$，都有$\overline{Y} \in E_i (i=1,2)$，且$\forall Y \in U_3$，有$\phi_3(Y) = \phi_3(\overline{Y})$。

4) 构造函数f。定义布尔函数$g(Y) \in \mathcal{B}_m$为

$$g(Y) = \begin{cases} 0, & Y \in U_1 \cup E_1 \\ 1, & Y \in U_2 \cup E_2 \end{cases} \tag{7}$$

构造n元布尔函数$f \in \mathcal{B}_n$为

$$f(Y,X) = \begin{cases} \phi_1(Y) \cdot X \oplus g(Y), & (Y,X) \in U_1 \times \mathbb{F}_2^{n-m} \\ \phi_2(Y) \cdot X \oplus g(Y), & (Y,X) \in U_2 \times \mathbb{F}_2^{n-m} \\ \phi_3(Y) \cdot X \oplus g(Y), & (Y,X) \in U_3 \times \mathbb{F}_2^{n-m} \end{cases} \tag{8}$$

注1 关于参数a_r及t_m的说明。

① 依据3)中条件①可知，$U_1 \cup U_2$中重量相同的向量个数为偶数，因此定义参数a_r以便刻画集合U_i与$T_i (i=1,2,3)$的大小。

② 为保证映射成立及刻画弹性阶，定义参数t_m。

注2 关于像集T的选取说明。

① 为使本文所构造的函数弹性尽可能高，要求T_1与T_2中向量尽可能重合多。同时，采用MM构造法构造五谱值函数时，需要一对一与二对一的映射组合，而映射ϕ_3为二对一映射，因此要求映射ϕ_1与ϕ_2的像不能完全重合，对此在2)中作了条件①与条件②的约束。

② 为了保证本文所构造的函数代数次数能够达到$m+1$，要求T_1与T_2中非重合的向量相加不为零向量，即满足2)中条件②。

注3 关于映射ϕ的构造说明。

① 为方便校正阶计算，将U_1与U_2依据像集中向量的重量进行划分，同时为满足Walsh谱中和技术的条件，要求U_{1s}与U_{2s}中重量一致的向量个数相同。对此在3)中作了条件①的约束。

② 关于U_3有以下2种情形。

情形1。若$|U_3| = 2$，则可知m必为偶数，且根据U_1与U_2的选择，此时U_3中只剩下$\mathbf{0}_m$与$\mathbf{1}_m$，$\mathbb{F}_2^m$中其他向量按同一重量的向量在U_1与U_2中对半分配。为使U_3满足3)中条件③，则一定可以选择一对向量$Y_1 \in U_1$和$Y_2 \in U_2$放入U_3中，其中$\mathrm{wt}(Y_1) = \mathrm{wt}(Y_2) = \dfrac{m}{2}$，$\phi_1(Y_1) = \phi_2(Y_2)$，且$Y_1 = \bar{Y}_2$，并分别从$U_1$与$U_2$中去掉向量$Y_1$与$Y_2$，从$T_1 \cap T_2$中去掉向量$\phi_1(Y_1)$。

情形2。若$|U_3| \geqslant 4$，则由引理5知$|U_3| = 2^k$，其中k为m的二进制展开中1的个数，即$|U_3|$为4的倍数，满足构造中的条件。

2.2 Walsh谱

定理1 由2.1节构造法生成的函数f为平衡五谱值布尔函数，$W_f(\omega) \in \{0, \pm 2^{n-m}, \pm 2^{n-m+1}\}$。

证明 设$\omega = (\beta,\alpha) \in \mathbb{F}_2^n$，其中$\beta \in \mathbb{F}_2^m$，$\alpha \in \mathbb{F}_2^{n-m}$，由式(8)中$f$的分段定义及构造方法可知

$$W_f(\omega) = W_f(\beta,\alpha) = \sum_{(Y,X) \in \mathbb{F}_2^n} (-1)^{f(Y,X) \oplus (\beta,\alpha) \cdot (Y,X)} = \underbrace{\sum_{(Y,X) \in U_1 \times \mathbb{F}_2^{n-m}} (-1)^{f(Y,X) \oplus \beta \cdot Y \oplus \alpha \cdot X}}_{S_1(\omega)} + \underbrace{\sum_{(Y,X) \in U_2 \times \mathbb{F}_2^{n-m}} (-1)^{f(Y,X) \oplus \beta \cdot Y \oplus \alpha \cdot X}}_{S_2(\omega)} + \underbrace{\sum_{(Y,X) \in U_3 \times \mathbb{F}_2^{n-m}} (-1)^{f(Y,X) \oplus \beta \cdot Y \oplus \alpha \cdot X}}_{S_3(\omega)} \tag{9}$$

其中，

$$S_1(\omega) = \sum_{Y \in U_1} (-1)^{g(Y) \oplus \beta \cdot Y} \sum_{X \in \mathbb{F}_2^{n-m}} (-1)^{(\phi_1(Y) \oplus \alpha) \cdot X} = \begin{cases} (-1)^{g(\phi_1^{-1}(\alpha)) \oplus \beta \cdot \phi_1^{-1}(\alpha)} 2^{n-m}, & \alpha \in T_1 \\ 0, & \text{其他} \end{cases} \tag{10}$$

$$S_2(\omega) = \sum_{Y \in U_2} (-1)^{g(Y) \oplus \beta \cdot Y} \sum_{X \in \mathbb{F}_2^{n-m}} (-1)^{(\phi_2(Y) \oplus \alpha) \cdot X} = \begin{cases} (-1)^{g(\phi_2^{-1}(\alpha)) \oplus \beta \cdot \phi_2^{-1}(\alpha)} 2^{n-m}, & \alpha \in T_2 \\ 0, & \text{其他} \end{cases} \tag{11}$$

$$S_3(\omega)=\sum_{Y\in U_3}(-1)^{g(Y)\oplus\beta\cdot Y}\sum_{X\in\mathbb{F}_2^{n-m}}(-1)^{(\phi_3(Y)\oplus\alpha)\cdot X}=$$

$$\begin{cases}\left[1+(-1)^{\mathrm{wt}(\beta)}\right](-1)^{g(Y_0)\oplus\beta\cdot Y_0}2^{n-m}, & \alpha=\phi_3(Y_0)\in T_3\\ 0, & \text{其他}\end{cases}\tag{12}$$

结合 T_1、T_2 和 T_3 的构造及 ϕ_1、ϕ_2 和 ϕ_3 的定义，可知 $W_f(\omega)\in\{0,\pm2^{n-m},\pm2^{n-m+1}\}$。进一步，由 $|U_1|=|U_2|$ 及 U_3 的互补划分可得 $W_f(\mathbf{0}_n)=0$，即 f 为平衡五谱值布尔函数。证毕。

2.3　非线性度及代数次数

定理 2　由 2.1 节构造法生成的函数 f 的非线性度 $\mathcal{N}_f=2^{n-1}-2^{n-m}$，代数次数 $\deg(f)=m+1$。

证明　由 f 的 Walsh 谱可知 $|W_f(\omega)|\leqslant 2^{n-m+1}$，代入式(2)得 f 的非线性度 $\mathcal{N}_f=2^{n-1}-2^{n-m}$。由式(1)知 f 的 ANF 为

$$\begin{aligned}f(Y,X)=&\bigoplus_{b\in U_1}y_1^{b_1}y_2^{b_2}\cdots y_m^{b_m}(\phi_1(b)\cdot X\oplus g(b))\oplus\\&\bigoplus_{b\in U_2}y_1^{b_1}y_2^{b_2}\cdots y_m^{b_m}(\phi_2(b)\cdot X\oplus g(b))\oplus\\&\bigoplus_{b\in U_3}y_1^{b_1}y_2^{b_2}\cdots y_m^{b_m}(\phi_3(b)\cdot X\oplus g(b))\end{aligned}\tag{13}$$

其中，$y_i^{b_i}=y_i\oplus b_i\oplus1$，$1\leqslant i\leqslant m$。

由式(13)可知，f 的 ANF 中必有项 $y_1y_2\cdots y_m\left[\left(\bigoplus_{b\in U_1}\phi_1(b)\oplus\bigoplus_{b\in U_2}\phi_2(b)\oplus\bigoplus_{b\in U_3}\phi_3(b)\right)\cdot X\right]$。一方面，因 U_3 中向量互补成对出现，且 ϕ_3 为二对一映射，可知 $\bigoplus_{b\in U_3}\phi_3(b)=\mathbf{0}_{n-m}$。另一方面，$\bigoplus_{b\in U_1}\phi_1(b)\oplus\bigoplus_{b\in U_2}\phi_2(b)=2\bigoplus_{v\in T_1\cap T_2}v\oplus\bigoplus_{v\in T_1\setminus T_2}v\oplus\bigoplus_{v\in T_2\setminus T_1}v\neq\mathbf{0}_{n-m}$，故 $\bigoplus_{b\in U_1}\phi_1(b)\oplus\bigoplus_{b\in U_2}\phi_2(b)\oplus\bigoplus_{b\in U_3}\phi_3(b)\neq\mathbf{0}_{n-m}$，从而 f 的代数次数为 $m+1$。证毕。

2.4　弹性阶

定理 3　由 2.1 节构造法生成的函数 f 的弹性阶为

$$t=\begin{cases}t_m, & t_m<n-m-2\\ n-m-3, & t_m=n-m-2\end{cases}\tag{14}$$

证明　由引理 3 可知，f 为 t 阶弹性函数当且仅当对任意 $\omega=(\beta,\alpha)\in\mathbb{F}_2^n$，$0\leqslant\mathrm{wt}(\omega)\leqslant t$，有 $W_f(\omega)=0$。

1) 当 $t_m<n-m-2$ 时

① 若 $0\leqslant\mathrm{wt}(\omega)\leqslant t_m-1$，则 $0\leqslant\mathrm{wt}(\alpha)\leqslant\mathrm{wt}(\omega)\leqslant t_m-1$，这意味着 $\alpha\notin T$，从而有 $W_f(\omega)=0$。

② 若 $\mathrm{wt}(\omega)=t_m$ 且 $\mathrm{wt}(\alpha)\leqslant t_m-1$，则 $\alpha\notin T$，从而有 $W_f(\omega)=0$。

③ 若 $\mathrm{wt}(\omega)=t_m$ 且 $\mathrm{wt}(\alpha)=t_m$，此时 $\alpha\in\{c\in\mathbb{F}_2^{n-m}\,|\,\mathrm{wt}(c)<n-m-2\}$，$\beta=\mathbf{0}_m$。则当 $\alpha\notin T_1\cap T_2$ 时，这意味着 $\alpha\notin T$，从而有 $W_f(\omega)=0$；当 $\alpha\in T_1\cap T_2$ 时，有 $W_f(\omega)=S_1(\omega)+S_2(\omega)=(-1)^{g(\phi_1^{-1}(\alpha))}\cdot2^{n-m}+(-1)^{g(\phi_2^{-1}(\alpha))}2^{n-m}=2^{n-m}-2^{n-m}=0$。

2) 当 $t_m=n-m-2$ 时

对任意 $\omega\in\mathbb{F}_2^n$，$0\leqslant\mathrm{wt}(\omega)\leqslant n-m-3$，有 $W_f(\omega)=0$。

综上所述及引理 3 可知，f 的弹性阶为 $t=\begin{cases}t_m, & t_m<n-m-2\\ n-m-3, & t_m=n-m-2\end{cases}$。证毕。

2.5　校正阶

定理 4　由 2.1 节构造法生成的函数 f 的校正阶 $c=n-m$。

证明　由引理 4 可知，弹性阶与校正阶的关系，及 2.4 节弹性阶的结论，只需验证对任意 c'，$t_m\leqslant c'\leqslant n-m$，都有 $\sum_{\omega\in\mathbb{F}_2^n,\mathrm{wt}(\omega)=c'}W_f(\omega)=0$。

$$\sum_{\substack{\omega=(\beta,\alpha)\in\mathbb{F}_2^n\\ \mathrm{wt}(\omega)=c'}}W_f(\omega)=\sum_{\substack{\omega=(\beta,\alpha)\in\mathbb{F}_2^n\\ \mathrm{wt}(\omega)=c'}}\left[S_1(\omega)+S_2(\omega)+S_3(\omega)\right]=$$

$$\sum_{\substack{\omega=(\beta,\alpha)\in\mathbb{F}_2^n\\ \mathrm{wt}(\omega)=c'}}\left[\sum_{s=t_m}^{n-m-2}\left(\sum_{Y\in U_{1s}}(-1)^{g(Y)\oplus\beta\cdot Y}\sum_{X\in\mathbb{F}_2^{n-m}}(-1)^{(\phi_1(Y)\oplus\alpha)\cdot X}+\sum_{Y\in U_{2s}}(-1)^{g(Y)\oplus\beta\cdot Y}\sum_{X\in\mathbb{F}_2^{n-m}}(-1)^{(\phi_2(Y)\oplus\alpha)\cdot X}\right)+S_3(\omega)\right]=$$

$$\sum_{s=t_m}^{n-m-2}J(s)+\sum_{\substack{\omega=(\beta,\alpha)\in\mathbb{F}_2^n\\ \mathrm{wt}(\omega)=c'}}S_3(\omega)\tag{15}$$

其中，$J(s)=\sum_{\omega=(\beta,\alpha)\in\mathbb{F}_2^n,\mathrm{wt}(\beta,\alpha)=c'}\left[S_{1s}(\omega)+S_{2s}(\omega)\right]$，$S_{is}(\omega)=\sum_{Y\in U_{is}}(-1)^{g(Y)\oplus\beta\cdot Y}\sum_{X\in\mathbb{F}_2^{n-m}}(-1)^{(\phi_i(Y)\oplus\alpha)\cdot X}$ $(i=1,2;t_m\leqslant s\leqslant n-m-2)$。

对于$J(s)(t_m \leqslant s \leqslant n-m-2)$，有以下2种情况。

情况1。当$c'<s\leqslant n-m-2$时，$\mathrm{wt}(\alpha)\leqslant c'<s$，但$\left\{\phi_i(Y)\middle|Y\in U_{is}\right\}(i=1,2)$中向量的重量均为$s$，故对任意$Y\in U_{is}$，都有$\sum\limits_{X\in\mathbb{F}_2^{n-m}}(-1)^{(\phi_i(Y)\oplus\alpha)\cdot X}=0$，从而有$J(s)=0$。

情况2。当$t_m\leqslant s\leqslant c'$时，有

$$J(s)=\sum_{\substack{\alpha\in\mathbb{F}_2^{n-m}\setminus\left\{\alpha\middle|\alpha\in T_1\cup T_2,\mathrm{wt}(\alpha)=s\right\}\\ \beta\in\mathbb{F}_2^m,\mathrm{wt}(\beta)=c'-\mathrm{wt}(\alpha)}}\left[S_{1s}(\omega)+S_{2s}(\omega)\right]+\sum_{\substack{\alpha\in T_1\cap T_2,\mathrm{wt}(\alpha)=s\\ \beta\in\mathbb{F}_2^m,\mathrm{wt}(\beta)=c'-s}}\left[S_{1s}(\omega)+S_{2s}(\omega)\right]+\sum_{\substack{\alpha\in T_1\setminus T_2,\ \mathrm{wt}(\alpha)=s\\ \beta\in\mathbb{F}_2^m,\ \mathrm{wt}(\beta)=c'-s}}S_{1s}(\omega)+$$

$$\sum_{\substack{\alpha\in T_2\setminus T_1,\ \mathrm{wt}(\alpha)=s\\ \beta\in\mathbb{F}_2^m,\ \mathrm{wt}(\beta)=c'-s}}S_{2s}(\omega)=0+\left[\sum_{\substack{\alpha\in T_1\cap T_2,\mathrm{wt}(\alpha)=s\\ \beta\in\mathbb{F}_2^m,\mathrm{wt}(\beta)=c'-s}}2^{n-m}(-1)^{\beta\cdot\phi_1^{-1}(\alpha)}-\sum_{\substack{\alpha\in T_1\cap T_2,\mathrm{wt}(\alpha)=s\\ \beta\in\mathbb{F}_2^m,\mathrm{wt}(\beta)=c'-s}}2^{n-m}(-1)^{\beta\cdot\phi_2^{-1}(\alpha)}\right]+$$

$$\sum_{\substack{\alpha\in T_1\setminus T_2,\mathrm{wt}(\alpha)=s\\ \beta\in\mathbb{F}_2^m,\mathrm{wt}(\beta)=c'-s}}2^{n-m}(-1)^{\beta\cdot\phi_1^{-1}(\alpha)}-\sum_{\substack{\alpha\in T_2\setminus T_1,\mathrm{wt}(\alpha)=s\\ \beta\in\mathbb{F}_2^m,\mathrm{wt}(\beta)=c'-s}}2^{n-m}(-1)^{\beta\cdot\phi_2^{-1}(\alpha)}=\sum_{\substack{\alpha\in T_1,\mathrm{wt}(\alpha)=s\\ \beta\in\mathbb{F}_2^m,\mathrm{wt}(\beta)=c'-s}}2^{n-m}(-1)^{\beta\cdot\phi_1^{-1}(\alpha)}-$$

$$\sum_{\substack{\alpha\in T_2,\mathrm{wt}(\alpha)=s\\ \beta\in\mathbb{F}_2^m,\mathrm{wt}(\beta)=c'-s}}2^{n-m}(-1)^{\beta\cdot\phi_2^{-1}(\alpha)}=2^{n-m}\sum_{\substack{\beta\in\mathbb{F}_2^m\\ \mathrm{wt}(\beta)=c'-s}}\sum_{Y\in U_{1s}}(-1)^{\beta\cdot Y}-2^{n-m}\sum_{\substack{\beta\in\mathbb{F}_2^m\\ \mathrm{wt}(\beta)=c'-s}}\sum_{Y\in U_{2s}}(-1)^{\beta\cdot Y}=$$

$$2^{n-m}\sum_{\substack{\beta\in\mathbb{F}_2^m\\ \mathrm{wt}(\beta)=c'-s}}\left(\sum_{Y\in U_{1s}}(-1)^{\beta\cdot Y}-\sum_{Y\in U_{2s}}(-1)^{\beta\cdot Y}\right)=0 \tag{16}$$

其中，最后一个等式成立是因为对于任意s，$t_m\leqslant s\leqslant c'$，可定义双射$\psi_s:U_{1s}\to U_{2s}$，使$\psi_s(Y)=Y'$，且满足$\mathrm{wt}(Y)=\mathrm{wt}(Y')$，从而对于任意$Y\in U_{1s}$，有

$$\sum_{\substack{\beta\in\mathbb{F}_2^m\\ \mathrm{wt}(\beta)=c'-s}}\left(\sum_{Y\in U_{1s}}(-1)^{\beta\cdot Y}-\sum_{Y\in U_{2s}}(-1)^{\beta\cdot Y}\right)=$$

$$\sum_{\substack{\beta\in\mathbb{F}_2^m\\ \mathrm{wt}(\beta)=c'-s}}\left(\sum_{Y\in U_{1s}}(-1)^{\beta\cdot Y}-\sum_{Y\in U_{1s}}(-1)^{\beta\cdot\psi_s(Y)}\right)=$$

$$\sum_{Y\in U_{1s}}\left(\sum_{\substack{\beta\in\mathbb{F}_2^m\\ \mathrm{wt}(\beta)=c'-s}}(-1)^{\beta\cdot Y}-\sum_{\substack{\beta\in\mathbb{F}_2^m\\ \mathrm{wt}(\beta)=c'-s}}(-1)^{\beta\cdot\psi_s(Y)}\right)=0 \tag{17}$$

综上，当$t_m\leqslant s\leqslant n-m-2$时，恒有$J(s)=0$。对任意$c'$，$t_m\leqslant c'\leqslant n-m$，都有$\sum\limits_{\omega\in\mathbb{F}_2^n,\mathrm{wt}(\omega)=c'}\left[S_1(\omega)+S_2(\omega)\right]=0$，即$\sum\limits_{\omega\in\mathbb{F}_2^n,\mathrm{wt}(\omega)=c'}W_f(\omega)=\sum\limits_{\omega\in\mathbb{F}_2^n,\mathrm{wt}(\omega)=c'}S_3(\omega)$。进一步地，有如下结论。

1) 若$t_m\leqslant c'\leqslant n-m-2$，则$\mathrm{wt}(\alpha)\leqslant n-m-2$，即$\alpha\notin T_3$，从而$\sum\limits_{\omega=(\beta,\alpha)\in\mathbb{F}_2^n,\mathrm{wt}(\omega)=c'}S_3(\omega)=0$。

2) 若$c'=n-m-1$且$\mathrm{wt}(\alpha)\leqslant n-m-2$，则$\alpha\notin T_3$，$\sum\limits_{\omega=(\beta,\alpha)\in\mathbb{F}_2^n,\mathrm{wt}(\omega)=c'}S_3(\omega)=0$。

3) 若$c'=n-m-1$且$\mathrm{wt}(\alpha)=n-m-1$，则$\beta=\mathbf{0}_m$，有

$$\sum_{\substack{\omega=(\beta,\alpha)\in\mathbb{F}_2^n\\ \mathrm{wt}(\omega)=c'}}S_3(\omega)=\sum_{\substack{\alpha\in\mathbb{F}_2^{n-m}\\ \mathrm{wt}(\alpha)=n-m-1}}S_3(\mathbf{0}_m,\alpha)=$$

$$\sum_{\alpha\in T_3}S_3(\mathbf{0}_m,\alpha)+\sum_{\substack{\alpha\notin T_3\\ \mathrm{wt}(\alpha)=n-m-1}}S_3(\mathbf{0}_m,\alpha)=$$

$$\frac{1}{2}\sum_{Y\in U_3}2^{n-m}\left((-1)^{g(Y)\oplus\mathbf{0}_m\cdot Y}+(-1)^{g(\bar{Y})\oplus\mathbf{0}_m\cdot\bar{Y}}\right)=$$

$$\frac{1}{2}\sum_{Y\in E_1}2^{n-m}(1+1)+\frac{1}{2}\sum_{Y\in E_2}2^{n-m}\left[(-1)+(-1)\right]=0 \tag{18}$$

4) 若$c'=n-m$，且$\mathrm{wt}(\alpha)\leqslant n-m-2$或$\mathrm{wt}(\alpha)=n-m$，则$\alpha\notin T_3$，有$\sum\limits_{\omega=(\beta,\alpha)\in\mathbb{F}_2^n,\mathrm{wt}(\omega)=c'}S_3(\omega)=0$。

5) 若$c'=n-m$，且$\mathrm{wt}(\alpha)=n-m-1$，则$\mathrm{wt}(\beta)=1$，有

$$\sum_{\substack{\omega=(\beta,\alpha)\in\mathbb{F}_2^n\\ \mathrm{wt}(\omega)=c'}} S_3(\omega)=\sum_{\substack{\alpha\in\mathbb{F}_2^{n-m},\mathrm{wt}(\alpha)=n-m-1\\ \beta\in\mathbb{F}_2^m,\mathrm{wt}(\beta)=1}} S_3(\omega)=$$

$$\sum_{\substack{\alpha\in T_3\\ \beta\in\mathbb{F}_2^m,\mathrm{wt}(\beta)=1}} S_3(\omega)+\sum_{\substack{\alpha\notin T_3\\ \beta\in\mathbb{F}_2^m,\mathrm{wt}(\beta)=1}} S_3(\omega)=$$

$$2^{n-m}\sum_{\substack{\beta\in\mathbb{F}_2^m\\ \mathrm{wt}(\beta)=1}}\left[\frac{1}{2}\sum_{Y\in U_3}\left((-1)^{g(Y)\oplus\beta\cdot Y}+(-1)^{g(\bar{Y})\oplus\beta\cdot\bar{Y}}\right)\right]=$$

$$2^{n-m-1}\sum_{\substack{\beta\in\mathbb{F}_2^m\\ \mathrm{wt}(\beta)=1}}\left[\sum_{Y\in E_1}\left((-1)^{\beta\cdot Y}+(-1)^{\beta\cdot Y\oplus 1}\right)+\right.$$

$$\left.\sum_{Y\in E_2}\left((-1)^{\beta\cdot Y\oplus 1}+(-1)^{\beta\cdot Y}\right)\right]=0 \tag{19}$$

综上可知，对于任意c'，$t_m\leqslant c'\leqslant n-m$，恒有$\sum_{\omega\in\mathbb{F}_2^n,\mathrm{wt}(\omega)=c'} W_f(\omega)=\sum_{\omega\in\mathbb{F}_2^n,\mathrm{wt}(\omega)=c'} S_3(\omega)=0$。由引理4可知，$f$的校正阶$c=n-m$。证毕。

3　推论及实例

由于参数m能取5到$\left\lfloor\frac{n}{2}\right\rfloor$之间的任意整数，本文所提构造方法能够生成一类参数灵活的五谱值布尔函数。用户可根据实际需求灵活选择和调整参数m，以获得所需函数。例如，若要求非线性度尽可能高，则可选定参数m为最大值$\left\lfloor\frac{n}{2}\right\rfloor$来获得非线性度为$2^{n-1}-2^{\left\lceil\frac{n}{2}\right\rceil}$的函数。下面给出此类函数的相关结果。

推论 1　设$m(m\geqslant 5)$为正整数，$n=2m$，则由2.1节构造法所得五谱值函数$f\in\mathcal{B}_n$的非线性度为$2^{n-1}-2^{\frac{n}{2}}$，代数次数为$\frac{n}{2}+1$，弹性阶为$\left\lfloor\frac{n}{4}\right\rfloor$，校正阶为$\frac{n}{2}$。

证明　由本文定理2与定理4可知，显然有$\mathcal{N}_f=2^{n-1}-2^{\frac{n}{2}}$，$\deg(f)=\frac{n}{2}+1$，校正阶为$\frac{n}{2}$。

1) 当m为偶数时，有$\frac{1}{2}\binom{m}{\frac{m}{2}}>m+1$，从而有

$$\sum_{s=\frac{m}{2}}^{m-2}\binom{m}{s}\geqslant\frac{1}{2}\binom{m}{\frac{m}{2}}+\sum_{r=\frac{m}{2}+1}^{m}\binom{m}{r}=\frac{1}{2}\sum_{r=0}^{m}\binom{m}{r}\geqslant\frac{1}{2}\sum_{r=0}^{m}a_r。$$

2) 当m为奇数时，有$\binom{m}{\frac{m+1}{2}}>m+1$，从而有$\sum_{s=\frac{m-1}{2}}^{m-2}\binom{m}{s}\geqslant\sum_{r=\frac{m+1}{2}}^{m}\binom{m}{r}=\frac{1}{2}\sum_{r=0}^{m}\binom{m}{r}\geqslant\frac{1}{2}\sum_{r=0}^{m}a_r$。

因此，$t_m=\left\lfloor\frac{m}{2}\right\rfloor$，由定理3可知$f$的弹性阶$t=\left\lfloor\frac{m}{2}\right\rfloor=\left\lfloor\frac{n}{4}\right\rfloor$。证毕。

推论 2　设m为正整数，$n=2m+1$，若$m=5$，则由2.1节构造法所得五谱值函数$f\in\mathcal{B}_{11}$的弹性阶为3，校正阶为6。若$m>5$，则由2.1节构造法所得五谱值函数f的非线性度为$2^{n-1}-2^{\frac{n+1}{2}}$，代数次数为$\frac{n+1}{2}$，弹性阶为$\left\lfloor\frac{n+5}{4}\right\rfloor$，校正阶为$\frac{n+1}{2}$。

证明与推论1类似。

例 1　设$n=10$，$m=5$，$Y=(y_1,y_2,\cdots,y_5)\in\mathbb{F}_2^5$，$X=(x_1,x_2,\cdots,x_5)\in\mathbb{F}_2^5$，$T=T_1\cup T_2\cup T_3\subseteq\mathbb{F}_2^5$和$\mathbb{F}_2^5=U_1\cup U_2\cup U_3$，其中，$T_1=\{00011,00101,01001,10001,00110,01010,10010,01100,10100,11000,01110,10110,11010,11100\}$，$T_2=\{00011,00101,01001,10001,00110,01010,10010,01100,10100,11000,01011,10011,01101,10101\}$，$T_3=\{01111,10111\}$，$U_1=\{10000,00010,00011,00101,00110,01001,01010,01101,00111,01011,01110,10011,01111,10111\}$，$U_2=\{00100,01000,01100,10001,10010,10100,11000,10101,10110,11001,11010,11100,11011,11101\}$，$U_3=\{00000,11111,00001,11110\}$。可定义如图2所示的映射$\phi_1$、$\phi_2$和$\phi_3$，从而由2.1节构造法得到函数$f\in\mathcal{B}_{10}$，用ANF表示为

$$\begin{aligned}f(Y,X)=&\,y_1y_2y_3y_4y_5(x_1\oplus x_2\oplus x_3\oplus x_4)\oplus\\ &y_1y_2y_3y_4(x_1\oplus x_3\oplus x_5)\oplus y_1y_2y_3y_5(x_1\oplus x_2\oplus 1)\oplus\\ &y_1y_2y_3x_3\oplus y_1y_2y_4y_5(x_1\oplus x_4\oplus x_5)\oplus\\ &y_1y_2y_4(x_2\oplus x_3\oplus x_5)\oplus y_1y_2y_5(x_4\oplus x_5\oplus 1)\oplus\\ &y_1y_3y_4y_5(x_1\oplus x_3\oplus 1)\oplus y_1y_3y_4(x_1\oplus x_2)\oplus\\ &y_2y_3y_4(x_1\oplus x_4\oplus x_5\oplus 1)\oplus y_1y_5(x_3\oplus x_4)\oplus\\ &y_3y_4y_5(x_1\oplus x_2)\oplus y_2y_5(x_1\oplus x_2\oplus x_4\oplus x_5)\oplus\\ &y_2y_4(x_1\oplus x_5\oplus 1)\oplus y_2y_3(x_2\oplus x_3\oplus 1)\oplus\\ &y_1y_4(x_4\oplus x_5\oplus 1)\oplus y_2y_4y_5(x_1\oplus x_2\oplus x_3\oplus x_5)\oplus\\ &y_3y_4(x_4\oplus x_5\oplus 1)\oplus y_3y_5(x_3\oplus x_4)\oplus\\ &y_4y_5(x_1\oplus x_2\oplus 1)\oplus y_1y_3(x_2\oplus x_5)\oplus\\ &y_1y_2(x_1\oplus x_3\oplus x_4\oplus x_5)\oplus y_2(x_3\oplus x_4\oplus 1)\oplus\\ &y_4(x_3\oplus x_4)\oplus y_5(x_1\oplus x_3\oplus 1)\oplus y_3\oplus x_4\oplus x_5\end{aligned}\tag{20}$$

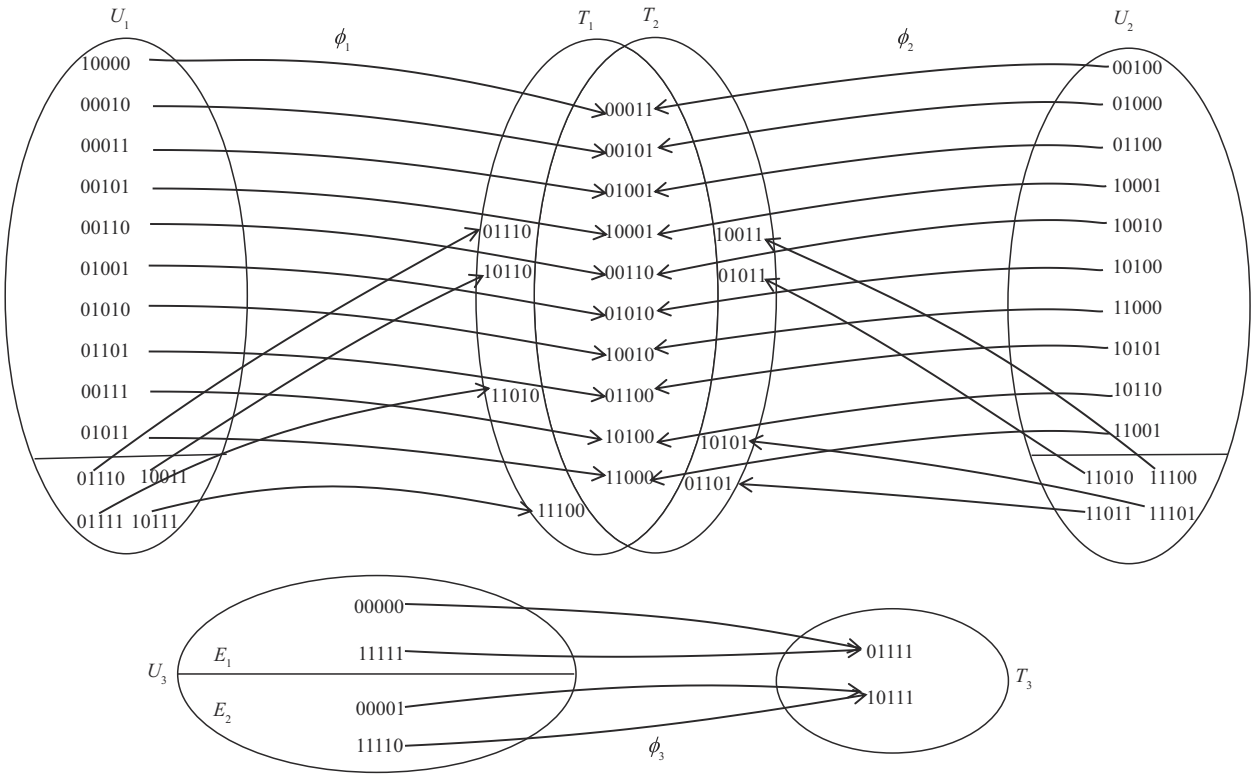

图2　映射$\phi:\mathbb{F}_2^5 \to T$

可用MATLAB程序验证f的Walsh变换取值为$\{0,\pm32,\pm64\}$，其非线性度$\mathcal{N}_f=480$，代数次数$\deg(f)=6$，弹性阶$t=2$，校正阶$c=5$。

本文结果与现有文献结果对比如表1所示。从表1中可以看出，当n为偶数时，在非线性度一致的情况下，本文所构造函数的弹性阶、校正阶及代数次数均高于文献[11]和文献[19]中的结果；对于n为奇数的情况，文献[17]与文献[19]均未考虑，本文所构造函数的非线性度略低于文献[11]中的结果，但弹性阶与校正阶均高2。

相较于文献[11]中将Semi-bent用于校正器，本文用五谱值函数作为TRNG的后处理校正器，通过

表1　　**本文结果与现有文献结果对比**

文献	t	c	N_f	$\deg(f)$
文献[19]（n为偶数）	$\leqslant\left\lfloor\frac{n-2}{4}\right\rfloor$	—	$2^{n-1}-2^{\frac{n}{2}}$	$\frac{n}{2}$
文献[11]（n为偶数）	$\left\lfloor\frac{n}{4}\right\rfloor$	$\frac{n}{2}-1$	$2^{n-1}-2^{\frac{n}{2}}$	$\frac{n}{2}$
文献[11]（n为奇数）	$\left\lfloor\frac{n-3}{4}\right\rfloor$	$\frac{n-3}{2}$	$2^{n-1}-2^{\frac{n-1}{2}}$	$\frac{n+1}{2}$
文献[17]（n为偶数）	—	—	$2^{n-1}-2^{\frac{n}{2}}$	$\leqslant\frac{n}{2}+1$
本文结果（n为偶数）	$\left\lfloor\frac{n}{4}\right\rfloor$	$\frac{n}{2}$	$2^{n-1}-2^{\frac{n}{2}}$	$\frac{n}{2}+1$
本文结果（n为奇数）	$\left\lfloor\frac{n+5}{4}\right\rfloor(m>5)$	$\frac{n+1}{2}$	$2^{n-1}-2^{\frac{n+1}{2}}$	$\frac{n+1}{2}$

对物理熵源输出的原始序列进行非线性变换，能更有效减少或消除物理随机数生成器的统计缺陷，从而提升TRNG输出序列的随机性质量。

4　结束语

本文聚焦于五谱值布尔函数的构造方法及相关密码学性质的分析，通过Luo等[11]提出的Walsh谱中和技术，给出了一类$n(n \geqslant 10)$元弹性五谱值布尔函数的分段构造方法，分析了其Walsh谱、非线性度、代数次数、弹性阶和校正阶。结果表明，本文函数校正阶比弹性阶至少高3，实现了这些密码学性质之间的良好折中。

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]//International Conference on the Theory and Application of Cryptology. Berlin: Springer, 1995: 105-118.

[3] ZHENG Y L, ZHANG X M. On plateaued functions[J]. IEEE Transactions on Information Theory, 2001, 47(3): 1215-1223.

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

[5] LI Y J, KAN H B, MESNAGER S, et al. Direct approaches for generic constructions of plateaued functions and bent functions outside M#[J]. IEEE Transactions on Information Theory, 2025, 71(2): 1400-1418.

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

[7] CHOR B, GOLDREICH O, HASTED J, et al. The bit extraction problem or t-resilient functions[C]//Proceedings of the 26th Annual Symposium on Foundations of Computer Science (SFCS 1985). Piscataway: IEEE Press, 1985: 396-407.

[8] BENNETT C H, BRASSARD G, ROBERT J M. Privacy amplification by public discussion[J]. SIAM Journal on Computing, 1988, 17(2): 210-229.

[9] LACHARME P. Analysis and construction of correctors[J]. IEEE Transactions on Information Theory, 2009, 55(10): 4742-4748.

[10] ZHANG W G. Analysis and construction of nonlinear correctors used in true random number generators[J]. IEEE Transactions on Information Theory, 2023, 69(10): 6671-6681.

[11] LUO S Y, WANG W Q, ZHANG Q, et al. Constructions of plateaued correctors with high correction order and good nonlinearity via Walsh spectral neutralization technique[J]. Designs, Codes and Cryptography, 2024, 92(12): 4531-4548.

[12] KATZ D J. Sequences with low correlation[C]//International Workshop on the Arithmetic of Finite Fields. Berlin: Springer, 2018: 149-172.

[13] DING C S. Linear codes from some 2-designs[J]. IEEE Transactions on Information Theory, 2015, 61(6): 3265-3275.

[14] 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, E107.A(7): 997-1002.

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

[16] MAITRA S, SARKAR P. Cryptographically significant Boolean functions with five valued Walsh spectra[J]. Theoretical Computer Science, 2002, 276(1/2): 133-146.

[17] 郭飞, 王子龙, 段明. 高非线性四谱值和五谱值布尔函数的构造[J]. 通信学报, 2025, 46(3): 144-150.
GUO F, WANG Z L, DUAN M. Construction of highly nonlinear Boolean functions with four-valued and five-valued spectra[J]. Journal on Communications, 2025, 46(3): 144-150.

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

[19] 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.

[20] 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.

[21] KE P H, CHEN Z X. Boolean functions with few Walsh transform values[C]//Proceedings of the 2022 10th International Workshop on Signal Design and Its Applications in Communications (IWSDA). Piscataway: IEEE Press, 2022: 1-5.

[22] 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.

[23] 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.

[24] 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.

[25] HU X W, YANG B, ZHANG J, et al. Constructing totally disjoint spectra plateaued functions and searching five-value spectrum functions in odd variables[J]. Discrete Applied Mathematics, 2022, 311: 110-128.

[26] 李超, 屈龙江, 周悦. 密码函数的安全性指标分析[M]. 北京: 科学出版社, 2011.
LI C, QU L J, ZHOU Y. Security indicators analysis of cryptographic functions[M]. Beijing: Science Press, 2011.

[27] 张卫国. 密码函数[M]. 北京: 科学出版社, 2024.
ZHANG W G. Cryptographic functions[M]. Beijing: Science Press, 2024.
[28] MEIER W, STAFFELBACH O. Nonlinearity criteria for cryptographic functions[C]//Workshop on the Theory and Application of Cryptographic Techniques. Berlin: Springer, 2001: 549-562.
[29] XIAO G Z, MASSEY J L. A spectral characterization of correlation-immune combining functions[J]. IEEE Transactions on Information Theory, 1988, 34(3): 569-571.
[30] LUCAS E. Sur les congruences des nombres eulériens et des coefficients différentiels des fonctions trigonométriques suivant un module premier[J]. Bulletin de la Société Mathématique de France, 1878, 6: 49-54.

[作者简介]

王维琼（1979– ），女，重庆人，博士，长安大学教授，主要研究方向为编码理论、密码学。

李越（2000– ），女，山西运城人，长安大学硕士生，主要研究方向为密码学。

罗舒予（2001– ），女，四川广安人，长安大学硕士生，主要研究方向为密码学。

朱蒙蕊（2001– ），女，河南南阳人，长安大学硕士生，主要研究方向为密码学。