有限域F_{2^n}上两类三项式的密码学性质

余仁杰,夏永波*
(中南民族大学 数学与统计学学院,武汉 430074)

摘 要 刻画了有限域F_{2^n}上两类三项式的差分谱,第一类是$f(x)=x+x^{2^{m+1}-1}+x^{2^m-2^{m+1}+1}$,其中$n=2m+1$;第二类是$g(x)=x^{2^{2k}+2^k}+x^{2^{2k}+1}+x^{2^k+1}$,其中$\gcd(n,k)=1$. 对于第一类三项式采用的方法是通过计算$f(x)$的Walsh谱,再根据差分谱和Walsh谱之间的关系来确定它的差分谱;对于第二类则是直接通过研究$g(x)$的差分方程有确定解数的条件,从而计算出差分谱,此外根据二次型理论,还确定了它的Walsh谱.

关键词 有限域;差分均匀度;差分谱;Walsh谱
中图分类号 O157 **文献标志码** A **文章编号** 1672-4321(2025)02-0277-06
doi:10.20056/j.cnki.ZNMDZK.20250218

Cryptographic properties of two classes of trinomials over finite field F_{2^n}

YU Renjie, XIA Yongbo*
(College of Mathematics and Statistics, South-Central Minzu University, Wuhan 430074, China)

Abstract The differential spectra of two classes of trinomials over finite field F_{2^n} are described. The first class is $f(x)=x+x^{2^{m+1}-1}+x^{2^m-2^{m+1}+1}$with $n=2m+1$, and the second one is $g(x)=x^{2^{2k}+2^k}+x^{2^{2k}+1}+x^{2^k+1}$, where $\gcd(n,k)=1$. For the first class, the differential spectrum is determined by calculating the Walsh spectrum of $f(x)$. For the second one, the differential spectrum is calculated directly by determining the conditions for which the differential equation has specific number of solutions. Moreover, the Walsh spectrum of $g(x)$ is also determined based on the theory of quadratic forms.

Keywords finite field; differential uniformity; differential spectrum; Walsh spectrum

分组密码作为密码学中的一种对称加密体制,由于其具有速度快、易于标准化和便于软硬件实现等特点,一直受到广泛的关注和使用. S-盒是分组密码中唯一的非线性部分在分组密码算法中扮演着重要的角色,为了衡量S-盒抵抗差分攻击[1]的能力,Nyberg于1993年在欧密会上提出了差分均匀度的概念[2]. 一个密码函数的差分均匀度越低,它抵抗差分攻击的能力便越强. 与密码函数的差分均匀度相关联的另外一种重要性质是该函数的差分谱,它能够更精细地刻画密码函数的差分性质,为寻找差分攻击路径提供依据,此外差分谱也在编码理论、序列和组合设计中起着重要作用.

当前对具有低差分均匀度密码函数的研究中,主要的对象是幂函数以及形式较好的二项式或三项式,美国高级加密标准AES算法S-盒的设计采用的是有限域F_{2^8}上差分均匀度为4的逆函数x^{-1},研究相关类型的函数有着重要的理论意义与现实价值. 目前对该类型函数的研究,可以在文献[3-10]中找到相关的结论.

本文研究了两类三项式的差分谱和Walsh谱,其中第一类是由丁存生、屈龙江以及王强等构造的F_{2^n}上的置换三项式$f(x)=x+x^{2^{m+1}-1}+x^{2^m-2^{m+1}+1}$,其中$m$是任意正整数,$n=2m+1$[4];第二类是由查正邦在文献[11]中提出的$F_{2^n}$上的几乎低差分一致性

收稿日期 2024-04-29
* **通信作者** 夏永波(1979-),男,教授,博士,研究方向:无线通讯中的序列设计、编码和密码学, E-mail:xia@mail.scuec.edu.cn
基金项目 国家自然科学基金资助项目(62171479);中南民族大学中央高校基本科研业务费专项资金资助项目(CZZ23004)

函数$g(x)=x^{2^{2k}+2^k}+x^{2^{2k}+1}+x^{2^k+1}$,其中$\gcd(n,k)=1$.对于第一类三项式,本文首先计算了其Walsh谱,再根据Walsh谱与差分谱的关系,间接计算出了它的差分谱;对于第二类三项式,则是直接从差分方程出发,通过分析差分方程有特定解数的条件,计算出了它的差分谱.此外,利用二次型理论,确定了第二类三项式的Walsh谱.

1 基本定义

设F_{p^n}表示元素个数为p^n的有限域,其中p是素数,n是正整数,并设$\mathrm{F}_{p^n}^*=\mathrm{F}_{p^n}\backslash\{0\}$.

定义1[2,12] 令$f(x)$是从F_{p^n}到自身的映射,$\forall(a,b)\in\mathrm{F}_{p^n}^*\times\mathrm{F}_{p^n}$,定义差分方程$D_af(x)=f(x+a)-f(x)=b$.设$\delta_f(a,b)$表示差分方程$D_af(x)=b$在$\mathrm{F}_{p^n}$中解的个数,即:

$$\delta_f(a,b)=\left|\left\{x\in\mathrm{F}_{p^n}\middle|f(x+a)-f(x)=b,(a,b)\in\mathrm{F}_{p^n}^*\times\mathrm{F}_{p^n}\right\}\right|$$

这里$|S|$表示集合S的基数.$f(x)$的差分均匀度定义为:

$$\delta_f=\max\left\{\delta_f(a,b)\middle|a\in\mathrm{F}_{p^n}^*,b\in\mathrm{F}_{p^n}\right\}.$$

若$\delta_f=k$,则称$f(x)$为k差分一致性函数.此外,若除了某一个a值外都有$\delta_f(a,b)\leqslant 4$,则称函数$f(x)$为几乎低差分一致函数,此时大于4的$\delta_f(a,b)$值称为偏差(Deviation).

当$f(x)$被用于构造分组密码的S-盒时,$f(x)$的差分均匀度越小,其抵抗差分攻击的能力越强.当$\delta_f=1$时,函数$f(x)$称为完全非线性(Perfect Nonlinear)函数,简称PN函数,此时$f(x)$抵抗差分攻击的能力最强.当$\delta_f=2$时,函数$f(x)$称为几乎完全非线性(Almost Perfect Nonlinear)函数,简称APN函数.注意到当$p=2$时,δ_f的最小值是2,这是因为$\forall a\in\mathrm{F}_{2^n}^*$,有$f(x+a)+f(x)=f((x+a)+a)+f(x+a)$,即差分方程$D_af(x)=b$的解总是成对出现,所以特征为2的有限域上不存在PN函数.

定义2[2] 设$f(x)$是从有限域F_{p^n}到自身的映射,若$\delta_f=k$,则定义多重集$\{\omega_0,\omega_1,\ldots,\omega_k\}$为$f(x)$的差分谱,其中:

$$\omega_i=\left|\left\{a\in\mathrm{F}_{p^n}^*,b\in\mathrm{F}_{p^n}:\delta_f(a,b)=i\right\}\right|,\ 0\leqslant i\leqslant k.$$

根据差分谱的定义,可以得到如下等式成立:

$$\sum_{i=0}^{k}\omega_i=\sum_{i=0}^{k}i\omega_i=p^n(p^n-1).$$

令$\mathrm{Tr}_1^n(\cdot)$表示从F_{p^n}到F_p的迹函数,即$\mathrm{Tr}_1^n(x)=x+x^p+x^{p^2}+\cdots+x^{p^{n-1}}$,下面给出Walsh变换的定义.

定义3[13] 设$f(x)$是从F_{p^n}到F_{p^n}的映射,$\forall(a,b)\in\mathrm{F}_{p^n}\times\mathrm{F}_{p^n}$,$f(x)$在$(a,b)$处的Walsh变换定义为:

$$W_f(a,b)=\sum_{x\in\mathrm{F}_{p^n}}\omega^{\mathrm{Tr}_1^n(af(x)+bx)},$$

其中$\omega=\mathrm{e}^{\frac{2\pi\sqrt{-1}}{p}}$是$p$次单位根.$f(x)$的Walsh谱定义为如下多重集:

$$\left\{W_f(a,b):a\in\mathrm{F}_{p^n}^*,b\in\mathrm{F}_{p^n}\right\}.$$

注1 当$f(x)$是从F_{2^n}到F_2的布尔函数时,其Walsh变换定义为:

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

当$f(x)=x^d$是有限域F_{p^n}上的幂函数,且$\gcd(d,p^n-1)=1$,那么$\forall(a,b)\in\mathrm{F}_{p^n}^*\times\mathrm{F}_{p^n}$,不妨设$c^d=a$,则有:

$$W_f(a,b)=\sum_{x\in\mathrm{F}_{p^n}}\omega^{\mathrm{Tr}_1^n(ax^d+bx)}\overset{y=cx}{=\!=}\sum_{y\in\mathrm{F}_{p^n}}\omega^{\mathrm{Tr}_1^n((y)^d+\frac{by}{c})}=W_f(1,\frac{b}{c}).$$

由于x^d是置换,则c和a是一一对应的.故$f(x)$的Walsh谱值完全由$W_f(1,b)$确定,其中b遍历F_{p^n},所以可以定义这类幂函数的Walsh谱为如下多重集:

$$\left\{W_f(1,b):b\in\mathrm{F}_{p^n}\right\}.$$

定义4[14] 设$p(x)$是从F_{2^n}到F_{2^n}的映射,且$p(x)=\sum_{i,j}a_{ij}x^{2^i+2^j}$,其中$a_{ij}\in\mathrm{F}_{2^n}$,$0\leqslant i<j\leqslant n-1$,则称$p(x)$是$\mathrm{F}_{2^n}$上的二次函数.$\forall\lambda\in\mathrm{F}_{2^n}^*$,称$Q_\lambda(x)=\mathrm{Tr}_1^n(\lambda p(x))$是$\mathrm{F}_{2^n}$到$\mathrm{F}_2$的二次型.

令$V(Q_\lambda)=\{x\in\mathrm{F}_{2^n}|Q_\lambda(x+z)+Q_\lambda(x)+Q_\lambda(z)=0,\forall z\in\mathrm{F}_{2^n}\}$,显然$V(Q_\lambda)$是在$\mathrm{F}_{2^n}$上的向量空间,不妨记$j=\dim_{\mathrm{F}_2}(V(Q_\lambda))$,则二次型$Q_\lambda(x)$的秩为$\mathrm{Rank}(Q_\lambda)=n-j$.

注2 根据$Q_\lambda(x)$的定义,显然有如下等式成立:

$$\left(\sum_{x\in\mathrm{F}_{2^n}}(-1)^{Q_\lambda(x)}\right)^2=\sum_{x\in\mathrm{F}_{2^n}}(-1)^{Q_\lambda(x)}\cdot\sum_{z\in\mathrm{F}_{2^n}}(-1)^{Q_\lambda(x+z)+Q_\lambda(x)+Q_\lambda(z)}=2^n\sum_{x\in V(Q_\lambda)}(-1)^{Q_\lambda(x)}.$$

因为$Q_\lambda(x)$是$V(Q_\lambda)$上的线性函数,所以有:

$$\sum_{x\in F_{2^n}}(-1)^{Q_\lambda(x)}=\begin{cases}\pm2^{n-\frac{\mathrm{Rank}(Q_\lambda)}{2}},&\text{若对于任意的}x\in V(Q_\lambda),\text{有}Q_\lambda(x)=0,\\0,&\text{其他},\end{cases}$$

故$Q_\lambda(x)$的秩总是一个偶数$2h$,且满足$2 \leqslant 2h \leqslant n$.

2　预备知识

引理 1[3-4]　设m是任意正整数,$n = 2m + 1$,那么三项式

$$f(x) = x + x^{2^{m+1}-1} + x^{2^n - 2^{m+1}+1},$$

是F_{2^n}上的置换三项式,并且$f(x)$是 4 差分一致函数.

对于定义在有限域F_{p^n}上的幂函数$f(x) = x^d$,其中d是任意正整数,文献[15]揭示了$f(x)$的 Walsh 谱和差分谱之间的关系.实际上,对于一般的函数同样有类似的结果,文献[14]在计算 Welch 置换三项式的差分谱时,便给出了如下相关的结论.

引理 2[14]　令$f(x)$是F_{p^n}到F_{p^n}的k差分一致函数,其中p是任意素数,$\{\omega_1, \omega_2, \dots, \omega_k\}$为其差分谱,$W_f(a, b)$是$f(x)$在$(a, b) \in F_{p^n} \times F_{p^n}$处的 Walsh 变换,则有如下等式成立:

$$\sum_{a,\, b \in F_{p^n}} \left| W_f(a, b) \right|^4 = p^{4n} + p^{2n} \sum_{i=0}^{k} i^2 \omega_i.$$

引理 3[16]　令$q(x) = x^{2^{m+1}+1}$是定义在有限域F_{2^n}上的一类幂函数,其中$n = 2m + 1$,那么$q(x)$的 Walsh 变换$W_q(1, b)$的取值分布如下:

$$W_q(1, b) = \begin{cases} 2^{\frac{n+1}{2}}, & 2^{n-2} + 2^{\frac{n-3}{2}} 次, \\ -2^{\frac{n+1}{2}}, & 2^{n-2} - 2^{\frac{n-3}{2}} 次, \\ 0, & 2^{n-1} 次, \end{cases}$$

特别地,$\forall b \in F_{2^n}$,$W_q(1, b) = 0$当且仅当$\mathrm{Tr}_1^n(b) = 0$.

引理 4[14]　设正整数n, t, l满足$\gcd(n, t) = 1$且$2l \leqslant n$.令$Q(x) = \sum_{i=1}^{l} \mathrm{Tr}_1^n(c_i x^{2^{it}+1})$,其中$c_i \in F_{2^n}$且至少存在一个$c_i$非零$(1 \leqslant i \leqslant l)$,则$Q(x)$的秩$2h$满足$n - 2l \leqslant 2h \leqslant n$.

引理 5[17]　设$Q(x)$是F_{2^n}到F_2的秩为$2h$的二次型,则它的 Walsh 变换有如下分布:

$$\hat{Q}(\lambda) = \begin{cases} \pm 2^{n-h}, & 2^{2h-1} \pm 2^{h-1}, \\ 0, & 2^n - 2^{2h}. \end{cases}$$

3　主要结果及证明

定理 1　设$f(x) = x + x^{2^{m+1}-1} + x^{2^n - 2^{m+1}+1}$是有限域$F_{2^n}$上的置换三项式,其中$n = 2m + 1$,那么$f(x)$的 Walsh 谱由表 1 给出.

表 1　$f(x)$的 Walsh 谱

Tab. 1　Walsh spectrum of $f(x)$

谱值	频数
2^n	1
$2^{\frac{n+1}{2}}$	$2^{2n-2} - 2^{n-1} + 2^{2n-\frac{n+3}{2}} - 2^{\frac{n-1}{2}}$
$-2^{\frac{n+1}{2}}$	$2^{2n-2} - 2^{n-1} - 2^{2n-\frac{n+3}{2}} + 2^{\frac{n-1}{2}}$
0	$2^{2n-1} - 1$

证明　设$(a, b) \in F_{2^n}^* \times F_{2^n}$,根据 Walsh 变换的定义,有:

$$W_f(a, b) = \sum_{x \in F_{2^n}} (-1)^{\mathrm{Tr}_1^n(af(x) + bx)} = \sum_{x \in F_{2^n}} (-1)^{\mathrm{Tr}_1^n(ax^{2^{m+1}-1} + ax^{2-2^{m+1}} + (a+b)x)} = \sum_{x \in F_{2^n}} (-1)^{\mathrm{Tr}_1^n((a^{2^m}+a)x^{2^{m+1}-1} + (a+b)x)}.$$

令$q(x) = x^{2^{m+1}+1}$,由于$\gcd(2^{m+1} + 1, 2^n - 1) = 1$,不妨设$x = y^{2^{m+1}+1}$,则:

$$W_f(a, b) = \sum_{y^{2^{m+1}+1} \in F_{2^n}} (-1)^{\mathrm{Tr}_1^n((a^{2^m}+a)y + (a+b)y^{2^{m+1}+1})} = \sum_{y \in F_{2^n}} (-1)^{\mathrm{Tr}_1^n((a^{2^m}+a)y + (a+b)y^{2^{m+1}+1})} = W_q(a + b, a^{2^m} + a).$$

再令$a + b = c$,则$W_q(a + b, a^{2^m} + a) = W_q(c, (b + c)^{2^m} + (b + c))$,其中$b$遍历$F_{2^n}$.给定$b$,因为$a \neq 0$,所以$c \neq b$.注意到当$c = b$,有:

$$W_q(c, (b + c)^{2^m} + (b + c)) = W_q(c, 0) = \sum_{x \in F_{2^n}} (-1)^{\mathrm{Tr}_1^n(cx^{2^{m+1}+1})} = \begin{cases} 2^n, & c = 0, \\ 0, & c \neq 0. \end{cases} \tag{1}$$

为了方便计算,下面先确定当(b, c)遍历$F_{2^n} \times F_{2^n}$时,$W_q(c, (b + c)^{2^m} + (b + c))$的取值分布情况.

当$c = 0$时,$W_q(c, (b + c)^{2^m} + (b + c)) = \sum_{x \in F_{2^n}} (-1)^{\mathrm{Tr}_1^n((b^{2^m}+b)x)}$,所以:

$$W_q(0, b^{2^m} + b) = \begin{cases} 2^n, & b \in F_2, \\ 0, & b \notin F_2. \end{cases}$$

当$c \neq 0$时,由于$q(x)$是F_{2^n}上的置换,设$c = d^{2^{m+1}+1}$,这里$d \in F_{2^n}^*$,且d与c是一一对应的关系,所以有:

$$W_q(c, (b + c)^{2^m} + (b + c)) = \sum_{x \in F_{2^n}} (-1)^{\mathrm{Tr}_1^n((dx)^{2^{m+1}+1} + \frac{(b+c)^{2^m}+b+c}{d}(dx))} = \sum_{dx \in F_{2^n}} (-1)^{\mathrm{Tr}_1^n((dx)^{2^{m+1}+1} + \frac{(b+c)^{2^m}+b+c}{d}(dx))} = \sum_{dx \in F_{2^n}} (-1)^{\mathrm{Tr}_1^n((dx)^{2^{m+1}+1} + (d^{2^m}+d^{2^{m+1}} + \frac{b^{2^m}+b}{d})(dx))} = W_q(1, d^{2^m} + d^{2^{m+1}} + \frac{b^{2^m} + b}{d}).$$

根据引理3,$W_q(1, d^{2^m}+d^{2^{m+1}}+\frac{b^{2^m}+b}{d})$的可能取值为0, $\pm 2^{\frac{n+1}{2}}$,并且$W_q(1, d^{2^m}+d^{2^{m+1}}+\frac{b^{2^m}+b}{d})=0$当且仅当$\mathrm{Tr}_1^n(d^{2^m}+d^{2^{m+1}}+\frac{b^{2^m}+b}{d})=0$,即$\mathrm{Tr}_1^n(\frac{b^{2^m}+b}{d})=0$.由于$\gcd(m, n)=1$,那么$b^{2^m}+b=0$当且仅当$b\in \mathrm{F}_2$.当$b\in \mathrm{F}_2$时,显然$\forall d\in \mathrm{F}_{2^n}^*$,$\mathrm{Tr}_1^n(\frac{b^{2^m}+b}{d})=0$,那么此时使$\mathrm{Tr}_1^n(\frac{b^{2^m}+b}{d})=0$的元素$(b, d)$的个数是$2(2^n-1)$;当$b\notin \mathrm{F}_2$,即$b^{2^m}+b\neq 0$时,由于迹函数是均匀分布的,则对于每一个给定的$b$,当$d$取遍$\mathrm{F}_{2^n}^*$,使$\mathrm{Tr}_1^n(\frac{b^{2^m}+b}{d})=0$的元素$d$的个数是$2^{n-1}-1$,故此时使$\mathrm{Tr}_1^n(\frac{b^{2^m}+b}{d})=0$的元素$(b, d)$的个数是$(2^{n-1}-1)(2^n-2)$;所以当$(b, d)$遍历$\mathrm{F}_{2^n}^*\times \mathrm{F}_{2^n}$时,使$W_q(1, d^{2^m}+d^{2^{m+1}}+\frac{b^{2^m}+b}{d})=0$的$(b, d)$的个数是$(2^{n-1}-1)(2^n-2)+2(2^n-1)=2^{2n-1}$.

由于d与c是一一对应的关系,从以上讨论可知:当(b, c)遍历$\mathrm{F}_{2^n}\times \mathrm{F}_{2^n}$时,使$W_q(c, (b+c)^{2^m}+(b+c))=0$的$(b, c)$对的个数为$2^{2n-1}+(2^n-2)$,使$W_q(c, (b+c)^{2^m}+(b+c))=2^n$的$(b, c)$对的个数为2.

再注意到当$c=b$时,由公式(1)可知,$W_q(c, 0)=2^n$当且仅当$c=0$,以及$W_q(c, 0)=0$当且仅当$c\neq 0$. 所以$\forall b, c\in \mathrm{F}_{2^n}, c\neq b$,使$W_q(c, (b+c)^{2^m}+(b+c))=0$的$(b, c)$对的个数为$2^{2n-1}+(2^n-2)-(2^n-1)=2^{2n-1}-1$,使$W_q(c, (b+c)^{2^m}+(b+c))=2^n$的$(b, c)$对个数为1,即$\forall a, b\in \mathrm{F}_{2^n}, a\neq 0$,使$W_f(a, b)=0$的$(a, b)$对的个数为$2^{2n-1}-1$,使$W_f(a, b)=2^n$的$(a, b)$对的个数为1. 下面不妨设使$W_f(a, b)=2^{\frac{n+1}{2}}$的$(a, b)$对的个数为$\lambda_1$,使$W_f(a, b)=-2^{\frac{n+1}{2}}$的$(a, b)$对的个数为$\lambda_2$. 因为$a\in \mathrm{F}_{2^n}^*$, $b\in \mathrm{F}_{2^n}$,所以有:

$$\lambda_1+\lambda_2+1+2^{2n-1}-1=2^{2n}-2^n. \tag{2}$$

另一方面,根据Walsh变换的定义:

$$\sum_{a\in \mathrm{F}_{2^n}^*}\sum_{b\in \mathrm{F}_{2^n}} W_f(a, b)=$$
$$\sum_{a\in \mathrm{F}_{2^n}^*}\sum_{b\in \mathrm{F}_{2^n}}\sum_{x\in \mathrm{F}_{2^n}}(-1)^{\mathrm{Tr}_1^n(af(x)+bx)}=$$
$$\sum_{x\in \mathrm{F}_{2^n}}\sum_{a\in \mathrm{F}_{2^n}^*}(-1)^{\mathrm{Tr}_1^n(af(x))}\cdot\sum_{b\in \mathrm{F}_{2^n}}(-1)^{\mathrm{Tr}_1^n(bx)}=$$
$$2^n\sum_{a\in \mathrm{F}_{2^n}^*}(-1)^{\mathrm{Tr}_1^n(af(0))}=$$
$$2^{2n}-2^n.$$

又因为$\sum_{a\in \mathrm{F}_{2^n}^*}\sum_{b\in \mathrm{F}_{2^n}} W_f(a, b)=2^n+2^{\frac{n+1}{2}}\lambda_1-2^{\frac{n+1}{2}}\lambda_2$.

所以:

$$2^n+2^{\frac{n+1}{2}}\lambda_1-2^{\frac{n+1}{2}}\lambda_2=2^{2n}-2^n. \tag{3}$$

联立方程(2),(3)便可解得λ_1, λ_2,即:

$$\lambda_1=2^{2n-2}-2^{n-1}+2^{2n-\frac{n+3}{2}}-2^{\frac{n-1}{2}}, \lambda_2=2^{2n-2}-2^{n-1}-2^{2n-\frac{n+3}{2}}+2^{\frac{n-1}{2}}.$$

定理2 设$f(x)=x+x^{2^{m+1}-1}+x^{2^n-2^{m+1}+1}$是有限域$\mathrm{F}_{2^n}$上的三项式,其中$n=2m+1$,那么$f(x)$的差分谱为:$\{\omega_0=5\cdot 2^{2n-3}-3\cdot 2^{n-2}, \omega_1=0, \omega_2=2^{2n-2}, \omega_3=0, \omega_4=2^{2n-3}-2^{n-2}\}$.

证明 由引理1可知$f(x)$是F_{2^n}上的4差分一致性函数,即当$i\notin\{0, 2, 4\}$时,$\omega_i=0$,再根据差分谱的两个基本等式以及引理2便能够得到如下方程组:

$$\begin{cases}\omega_0+\omega_2+\omega_4=2^{2n-1}-2^n,\\ 2\omega_2+4\omega_4=2^{2n-1}-2^n,\\ 2^{2n}(4\omega_2+16\omega_4)=2^{4n}+(2^{\frac{n+1}{2}})^4(2^{2n-2}-2^n),\end{cases}$$

解得:$\omega_0=5\cdot 2^{2n-3}-3\cdot 2^{n-2}$, $\omega_2=2^{2n-2}$, $\omega_4=2^{2n-3}-2^{n-2}$.

定理3 设$g(x)=x^{2^{2k}+2^k}+x^{2^{2k}+1}+x^{2^k+1}$是有限域$\mathrm{F}_{2^n}$上的三项式,其中$\gcd(n, k)=1$,那么$g(x)$的差分谱为:$\omega_0=3\cdot 2^{2n-2}-3\cdot 2^{n-1}-1$, $\omega_4=2^{2n-2}-2^{n-1}$, $\omega_{2^n}=1$;当$i\notin\{0, 4, 2^n\}$时,$\omega_i=0$.

证明 $\forall a, b\in \mathrm{F}_{2^n}$且$a\neq 0$,$g(x)$的差分方程为:

$$(a^{2^k}+a)x^{2^{2k}}+(a^{2^{2k}}+a)x^{2^k}+(a^{2^{2k}}+a^{2^k})x=b+g(a). \tag{4}$$

当$a=1$时,方程(4)左边恒为0,所以当$b+g(a)=0$即$b=g(1)=1$时,$\forall x\in \mathrm{F}_{2^n}$,方程(4)恒成立,故此时差分方程解的个数为$2^n$;若$b+g(1)\neq 0$即$b\neq 1$,则方程(4)无解.

当$a\neq 1$时,注意到方程(4)左边是一个线性化多项式,所以只需考虑齐次方程:

$$(a^{2^k}+a)x^{2^{2k}}+(a^{2^{2k}}+a)x^{2^k}+(a^{2^{2k}}+a^{2^k})x=0$$

解的个数即可. 令$x=\frac{y}{a}$,那么便有:

$$a^{2^{2k}}(a^{2^k}+a)y^{2^{2k}}+a^{2^k}(a^{2^{2k}}+a)y^{2^k}+a(a^{2^{2k}}+a^{2^k})y=0,$$

即:

$$(a^{2^{2k}-1}+a^{2^{2k}-2^k})y^{2^{2k}}+(a^{2^{2k}-1}+1)y^{2^k}+(a^{2^{2k}-2^k}+1)y=0. \tag{5}$$

下面不妨设$t=y^{2^k}+y$,带入方程并化简得:

$$a^{2^{2k}-2^k}(a^{2^k-1}+1)t^{2^k}+(a^{2^k-1}+1)^2t=0. \tag{6}$$

因为$\gcd(n, k)=1$,所以$\gcd(2^k-1, 2^n-1)=1$,又因为$a\neq 1$所以$a^{2^k-1}+1\neq 0$,故方程(6)有两个

解：$t_1=0$，$t_2=\dfrac{1+a^{2^k-1}}{a^{2^k}}$. 对于给定的 t，方程 $y^{2^k}+y=t$ 要么有两个解要么无解. 注意到当 $t_1=0$ 方程 $y^{2^k}+y=t_1$ 有两个解：$y=0$ 和 $y=1$；当 $t_2=\dfrac{1+a^{2^k-1}}{a^{2^k}}$ 时，方程 $y^{2^k}+y=t_2$ 也有两个解：$\dfrac{1}{a}$ 和 $\dfrac{1}{a}+1$，故方程(5)有4个解，从而当 $a\neq 1$ 时差分方程(4)可能的解数为4或0.

综上所述，$\forall a,\ b\in \mathrm{F}_{2^n}$ 且 $a\neq 0$，差分方程(4)可能的解数为0，4，2^n. 所以当 $i\notin\{0,\ 4,\ 2^n\}$ 时，$\omega_i=0$. 从上述分析还可知：当且仅当 $a=1$ 且 $b=1$ 时，差分方程(4)有 2^n 个解，所以 $\omega_{2^n}=1$. 结合差分谱的两个基本等式从而得到如下方程组：

$$\begin{cases}\omega_0+\omega_4+1=2^n(2^n-1),\\ 4\omega_4+2^n=2^n(2^n-1),\end{cases}$$

解得：$\omega_0=3\cdot 2^{2n-2}-2^{n-1}-1$，$\omega_4=2^{2n-2}-2^{n-1}$，即得 $g(x)$ 的差分谱.

定理 4　设 $g(x)=x^{2^{2k}+2^k}+x^{2^{2k}+1}+x^{2^k+1}$ 是有限域 F_{2^n} 上的三项式，其中 $\gcd(n,\ k)=1$，$n\geqslant 6$，那么 $g(x)$ 的 Walsh 谱由表2（n 是奇数）和表3（n 是偶数）给出.

表2　$g(x)$ 的 Walsh 谱（n 是奇数）

Tab. 2　Walsh spectrum of $g(x)$ (n is odd)

谱值	频数
$\pm 2^{\frac{n+3}{2}}$	$(2^{n-1}-1)(2^{n-4}\pm 2^{\frac{n-5}{2}})$
$\pm 2^{\frac{n+1}{2}}$	$2^{n-1}(2^{n-2}\pm 2^{\frac{n-3}{2}})$
0	$2^{n-1}(2^n-2^{n-1})+(2^{n-1}-1)(2^n-2^{n-3})$

表3　$g(x)$ 的 Walsh 谱（n 是偶数）

Tab. 3　Walsh spectrum of $g(x)$ (n is even)

谱值	频数
$\pm 2^{\frac{n+4}{2}}$	$\frac{1}{3}(2^{n-2}-1)(2^{n-5}\pm 2^{\frac{n-6}{2}})$
$\pm 2^{\frac{n+2}{2}}$	$\frac{1}{3}(11\cdot 2^{n-2}-2)(2^{n-3}\pm 2^{\frac{n-4}{2}})$
0	$\frac{1}{3}((2^{n-2}-1)(2^n-2^{n-4})+(11\cdot 2^{n-2}-2)(2^n-2^{n-2}))$

证明　$\forall a,\ b\in \mathrm{F}_{2^n}$，根据 Walsh 变换的定义，有：

$$W_g(a,\ b)=\sum_{x\in \mathrm{F}_{2^n}}(-1)^{\mathrm{Tr}_1^n(ag(x)+bx)}=\sum_{x\in \mathrm{F}_{2^n}}(-1)^{\mathrm{Tr}_1^n(a(x^{2^{2k}+2^k}+x^{2^{2k}+1}+x^{2^k+1})+bx)}=\sum_{x\in \mathrm{F}_{2^n}}(-1)^{\mathrm{Tr}_1^n((a^{2^{n-k}}+a)x^{2^k+1}+ax^{2^{2k}+1})+bx)}.$$

注意到当 $a=0$ 时，显然有：

$$W_g(a,\ b)=\begin{cases}2^n, & b=0,\\ 0, & b\neq 0.\end{cases}$$

当 $a\neq 0$ 时，不妨记 $Q_a(x)=\mathrm{Tr}_1^n((a^{2^{n-k}}+a)x^{2^k+1}+ax^{2^{2k}+1})$，则 $Q_a(x)$ 是 F_{2^n} 上的二次型. 由引理4可得 $n-4\leqslant \mathrm{Rank}(Q_a(x))\leqslant n$. 由于 $\mathrm{Rank}(Q_a(x))$ 是一个偶数，所以当 n 是奇数时，$\mathrm{Rank}(Q_a(x))$ 的可能取值为 $n-3$ 和 $n-1$；当 n 是偶数时，$\mathrm{Rank}(Q_a(x))$ 的可能取值为 $n-4$，$n-2$ 和 n.

另一方面，根据 $V(Q_a)$ 的定义，$\forall y\in \mathrm{F}_{2^n}$，计算

$$\begin{aligned}&Q_a(x+y)+Q_a(x)+Q_a(y)=\\&\mathrm{Tr}_1^n((a^{2^k}+a)(x+y)^{2^{2k}+2^k}+a(x+y)^{2^{2k}+1}+(a^{2^k}+a)x^{2^{2k}+2^k}+ax^{2^{2k}+1}+(a^{2^k}+a)y^{2^{2k}+2^k}+ay^{2^{2k}+1})=\\&\mathrm{Tr}_1^n((a^{2^k}x^{2^k}+ax^{2^{2k}}+a^{2^{2k}}x^{2^{3k}}+a^{2^k}x^{2^{3k}}+a^{2^{2k}}x^{2^{4k}}+ax)y^{2^{2k}})=\\&\mathrm{Tr}_1^n((a^{2^k}(x^{2^k}+x^{2^{3k}})+a(x^{2^k}+x)+a^{2^{2k}}(x^{2^{3k}}+x^{2^{4k}}))y^{2^{2k}}).\end{aligned}$$

对于给定 $a\neq 0$，根据上式知：当 $x\in \mathrm{F}_2$ 时，$\forall y\in \mathrm{F}_{2^n}$，总有 $Q_a(x+y)+Q_a(x)+Q_a(y)=0$，所以 $\mathrm{F}_2\subseteq V(Q_a)$，即 $\dim_{\mathrm{F}_2}(V(Q_a))\geqslant 1$，故 $\mathrm{Rank}(Q_\lambda)\leqslant n-1$. 因此当 n 是偶数时 $\mathrm{Rank}(Q_a(x))$ 的可能取值为 $n-4$ 和 $n-2$.

下面以 n 是奇数为例，来计算 $g(x)$ 的 Walsh 谱，n 是偶数时类似可得.

设 $a\in \mathrm{F}_{2^n}^*$，使 $\mathrm{Rank}(Q_a(x))=n-3$ 的元素 a 的个数为 n_1，使 $\mathrm{Rank}(Q_a(x))=n-1$ 的个数为 n_2，由引理5可知此时 $g(x)$ 的 Walsh 谱为：

$$W_g(a,\ b)=\begin{cases}0, & n_1(2^n-2^{n-1})+n_2(2^n-2^{n-3}),\\ \pm 2^{\frac{n+1}{2}}, & n_2(2^{n-2}\pm 2^{\frac{n-3}{2}}),\\ \pm 2^{\frac{n+3}{2}}, & n_1(2^{n-4}\pm 2^{\frac{n-5}{2}}).\end{cases}$$

再根据引理2以及 $g(x)$ 的差分谱，便能够得到关于 n_1，n_2 的方程，即：

$$2^{n-3}(2^{\frac{n+3}{2}})^4n_1+2^{n-1}(2^{\frac{n+1}{2}})^4n_2+2^{4n}=2^{4n}+2^{2n}(16(2^{2n-2}-2^{n-1})+2^{2n}).$$

又因为 $n_1+n_2=2^n-1$，联立这两个方程解得：$n_1=2^{n-1}-1$，$n_2=2^{n-1}$，从而确定了 n 为奇数时 $g(x)$ 的 Walsh 谱.

下面给出利用软件 Magma 计算差分谱和 Walsh 谱所得到的具体结果.

例 1　当 $m=3$ 时，$f(x)=x+x^{15}+x^{113}$，利用软件 Magma 可以得到此时 $f(x)$ 的差分谱为：$\{\omega_0=10144,\ \omega_2=4096,\ \omega_4=2016\}$，Walsh 谱为：

$$W_f(a,\ b)=\begin{cases}128,\ 1\text{次},\\ 16,\ 4536\text{次},\\ -16,\ 3528\text{次},\\ 0,\ 8191\text{次}.\end{cases}$$

例2 当 $k=3, n=5$ 时，$g(x)=x^{72}+x^{65}+x^{9}$，由软件 Magma 可以得到此时 $g(x)$ 的差分谱为：$\{\omega_0=12223, \omega_4=4032, \omega_{128}=1\}$，Walsh 谱为：

$$W_g(a,b)=\begin{cases}32, & 630\text{次},\\ -32, & 378\text{次},\\ 16, & 2304\text{次},\\ -16, & 1792\text{次},\\ 0, & 11152\text{次}.\end{cases}$$

4 结论

本文研究了在有限域 F_{2^n} 上两类不同三项式的差分谱和 Walsh 谱. 第一类是置换三项式 $f(x)=x+x^{2^{m+1}-1}+x^{2^n-2^{m+1}+1}$，其中 $n=2m+1$；第二类是几乎低差分一致性函数 $g(x)=x^{2^{2k}+2^k}+x^{2^{2k}+1}+x^{2^k+1}$，其中 $\gcd(n,k)=1$. 值得注意的是对于定义在特征为2的有限域上的函数，若它们的差分均匀度为4，那么可以考虑使用引理2中 Walsh 谱与差分谱之间的关系来计算差分谱. 目前国内外对差分谱的研究主要集中在幂函数和几类具有低差分均匀度的置换多项式上，采用的方法大多数都是从差分方程的定义出发，来分析方程的解出现的条件及个数. 感兴趣的读者可以尝试将本文中所使用的方法应用到目前未能解决的问题中，或许能够得到一些新的结果.

参 考 文 献

[1] BIHAM E, SHAMIR A. Differential cryptanalysis of DES-like cryptosystems[J]. Journal of Cryptology, 1991, 4(1): 3-72.

[2] NYBERG K. Differentially uniform mappings for cryptography[C]//EUROCRYPT. Workshop on the Theory and Application of Cryptographic Techniques. Lofthus: Springer, 1993, 55-64.

[3] ZHU X, ZENG X, CHEN Y. Some binomial and trinomial differentially 4-uniform permutation polynomials [J]. International Journal of Foundations of Computer Science, 2015, 26(4): 487-497.

[4] DING C, QU L, WANG Q, et al. Permutation trinomials over finite fields with even characteristic[J]. SIAM Journal on Discrete Mathematics, 2015, 29(1): 79-92.

[5] BRACKEN C, LEANDER G. A highly nonlinear differentially 4 uniform power mapping that permutes fields of even degree[J]. Finite Fields and Their Applications, 2010, 16(4): 231-242.

[6] BRACKEN C, TAN C H, TAN Y. Binomial differentially 4 uniform permutations with high nonlinearity[J]. Finite Fields and Their Applications, 2012, 18(3): 537-546.

[7] LI Y, WANG M. Constructing differentially 4-uniform permutations over GF (22m) from quadratic APN permutations over GF(22m+1)[J]. Designs, Codes and Cryptography, 2014, 72(2): 249-264.

[8] TAN Y, QU L, TAN C H, et al. New families of differentially 4-uniform permutations over $\mathbb F_{2^{2k}}$[M]//Lecture Notes in Computer Science. Berlin, Springer 2012.

[9] TANG D, CARLET C, TANG X. Differentially 4-uniform bijections by permuting the inverse function[J]. Designs, Codes and Cryptography, 2015, 77(1): 117-141.

[10] ZHA Z, HU L, SUN S. Constructing new differentially 4-uniform permutations from the inverse function [J]. Finite Fields and Their Applications, 2014, 25: 64-78.

[11] 查正邦. 低差分一致性函数的研究[D]. 长沙：湖南大学, 2008.

[12] FELKE P. Computing the uniformity of power mappings: A systematic approach with multi-variate method over fnite fields of odd characteristic[D]. Bochum: University of Bochum, 2005.

[13] CHARPIN P, PENG J. New links between nonlinearity and differential uniformity[J]. Finite Fields and Their Applications, 2019, 56: 188-208.

[14] WANG Y B, KADIR W, LI C L, et al. On cryptographic properties of the Welch permutation and a related conjecture[C]//Sequences and Their Applications. Saint Petersburg: Springer, 2020: 1-13.

[15] HELLESETH T, RONG C, SANDBERG D. New families of almost perfect nonlinear power mappings[J]. IEEE Transactions on Information Theory, 1999, 45(2): 475-485.

[16] GOLD R. Maximal recursive sequences with 3-valued recursive cross-correlation functions (Corresp.)[J]. IEEE Transactions on Information Theory, 1968, 14 (1): 154-156.

[17] HELLESETH T, KUMAR P V. Sequences with low correlation[A]. PLESS V S, HUFFMAN W C. Handbook of Coding Theory. Amsterdam: Elsevier Science, 1998: 1765-1853.

(责编 曹东，校对 雷建云)