幂函数型完全非线性函数原像分布的特征*

海 昕,戴清平,李 超
(国防科技大学 理学院,湖南 长沙 410073)

摘 要:完全非线性函数是特征为奇数的有限域上抗差分密码攻击最优的函数,目前已有的六类完全非线性函数都是2-1的。当$\Pi(x)$为F_{q^m}上的Dembowski-Ostrom函数或者Coulter-Matthews函数时,从F_{q^m}到F_q的完全非线性函数$\mathrm{tr}(a\Pi(x))$的原像分布恰有两种取值,其中一种取值对应F_{q^m}所有平方剩余元,另一种取值对应F_{q^m}所有非平方剩余元。该结论在文中得到了证明。

关键词:完全非线性函数;迹函数;原像分布
中图分类号:TN918.1 **文献标志码**:A **文章编号**:1001-2486(2012)05-0142-04

Property of preimage distribution of perfect nonlinear function with the form of power functions

HAI Xin, DAI Qingping, LI Chao
(College of Science, National University of Defense Technology, Changsha 410073, China)

Abstract: Perfect nonlinear function is the optimal function on finite fields with odd character that can resist differential cryptanalysis. All the six classes of the already known perfect functions currently are 2-1. This study proved that when is Dembowski-Ostrom function or Coulter-Matthews function on , the preimage distribution of the perfect nonlinear function has just two kinds of values, one corresponds to all the elements of quadratic residual on , and the other kind corresponds to all the non quadratic residual on .

Key words: perfect nonlinear function; trace function; preimage distribution

1 引言

差分密码攻击[1]是目前攻击迭代分组密码最有效的方法之一。为了抵抗差分密码攻击,密码算法及其密码组件应当具有高度的非线性性。完全非线性函数是特征为奇数的有限域上非线性度最优的密码函数,能够为密码算法提供了良好的"混淆"作用,是抵抗差分密码攻击最优的一类函数。记F_{q^m}为q^m元有限域,这里q是素数的方幂,函数f: $\mathrm{F}_{q^m}\to\mathrm{F}_{q^m}$称为$\mathrm{F}_{q^m}$上的完全非线性函数,是指对任意的$a\in\mathrm{F}_{q^m}^*$,$f(x+a)-f(x)$是$\mathrm{F}_{q^m}$上的置换。这表明当$\mathrm{F}_{q^m}$的特征为偶素数时,$\mathrm{F}_{q^m}$上不存在完全非线性函数。当$\mathrm{F}_{q^m}$的特征为奇素数时,构造$\mathrm{F}_{q^m}$上的完全非线性函数是一个非常困难的问题,到目前为止只有如下六类:

(1) $\Pi_1(x)=x^{q^t+1}$,其中$t\geqslant 0$为整数,$\frac{m}{(m,t)}$是奇数[3];

(2) $\Pi_2(x)=x^{\frac{3k+1}{2}}$,其中$q=3$,$k$是奇数,$(m,k)=1$[4];

(3) $\Pi_3(x)=x^{10}-ux^6-u^2x^2$,其中$q=3$,$m$是奇数,$u\in\mathrm{F}_{q^m}^*$[5];

(4) $\Pi_4(x)=ux^{p^s+1}-u^{p^k}x^{p^{lk}+p^{-lk+s}}$,其中$m=3k$,$(3,k)=1$,$k/(k,s)$为奇数,$s=\pm k \bmod 3$,

$$l=\begin{cases}1, & k=s \mod 3\\ -1, & k=-s \mod 3\end{cases}$$

并且u是F_{p^m}中的本原元[6];

(5) $\Pi_5(x)=(bx)^{p^s+1}-((bx)^{p^s+1})^{p^k}+\sum_{i=0}^{k-1}c_ix^{p^i(p^k+1)}$,其中$m=2k$,$s$和$k$均为正整数,使得$(k+s,2k)=(k+s,k)$,并且$(p^s+1,p^k+1)\neq(p^s+1,(p^k+1)/2)$;同时,$b\in\mathrm{F}_{p^m}^*$,$\sum_{i=0}^{k-1}c_ix^{p^i}$是$\mathrm{F}_{p^m}$上的一个置换,并且系数$c_i\in\mathrm{F}_{p^k}(0\leqslant i<k)$[7];

(6) $\Pi_6(x)=ux^{p^k+1}+vx^{p^s+p^t}+v^{p^k}x^{p^{k+s}+p^{k+t}}+\sum_{0\leqslant i\leqslant k-1}w_ix^{p^{k+i}+p^i}$,其中$m=2k$,$s$和$k$均为正整数,使

* 收稿日期:2012-03-10
基金项目:国家自然科学基金资助项目(61070215, 61103191)
作者简介:海昕(1977—),男,河北唐山人,博士研究生,E-mail:haixin@nudt.edu.cn;
李超(通信作者),男,教授,博士,博士生导师,E-mail:lichao_nadt@sina.com

得 $2(\mathrm{E}\frac{n}{(n,t-s)}$;同时 $u \notin \mathrm{F}_{p^k}$,$\alpha$ 是 F_{p^m} 中的本原元,$(p^{s-t}+1,p^k+1)r, v=\alpha^r$,并且 $w_i \in \mathrm{F}_{p^k}(1 \leqslant i < k)$[7]。

上述六类函数中除了 Coulter-Matthews 函数外,其余五类函数的代数次数都是 2,这样的函数统称为 Dembowski-Ostrom 型函数。文献[2]证明了 Dembowski-Ostrom 型函数都是 $2-1$ 的,注意到 Coulter-Matthews 函数的幂指数具有性质 $(\frac{3^k+1}{2}, 3^m-1)=2$,从而可知该类函数也是 $2-1$ 的函数,这表明有限域上所有已知的完全非线性函数都是 $2-1$ 函数。

设 β 是 F_q 中本原元,则 $\mathrm{F}_q=\{0,\beta^1,\beta^2,\cdots,\beta^{q-1}\}$。如果 $\varphi(x)$ 是从 F_{q^m} 到 F_q 的函数,记 $k_0=|\{x \in \mathrm{F}_{q^m} | \varphi(x)=0\}|$,$k_i=|\{x \in \mathrm{F}_{q^m} | \varphi(x)=\beta^i\}|(i=1,\cdots,q-1)$,则称 $(k_0,k_1,\cdots,k_{q-1})$ 为函数 $\varphi(x)$ 的原像分布。文献[2]进一步证明了如下结论:

命题 1[2]　设 q 是奇素数的方幂,m 是大于 1 的正整数,$a \in \mathrm{F}_{q^m}^*$,$\Pi(x)$ 是从 F_{q^m} 到自身的 Dembowski-Ostrom 型的完全非线性函数,$\mathrm{tr}(\cdot)$ 表示从 F_{q^m} 到 F_q 的迹函数。那么从 F_{q^m} 到 F_q 的完全非线性函数 $\mathrm{tr}(a\Pi(x))$ 的原像分布具有如下特征:

(1) 当 m 为奇数时,分别有 $(q^m-1)/2$ 个元素 $a \in \mathrm{F}_{q^m}^*$,对应下列两种原像分布:

$$\Omega_1=(q^{m-1},q^{m-1}-q^{\frac{m-1}{2}},q^{m-1}+q^{\frac{m-1}{2}},\cdots,q^{m-1}-q^{\frac{m-1}{2}},q^{m-1}+q^{\frac{m-1}{2}}),$$

$$\Omega_2=(q^{m-1},q^{m-1}+q^{\frac{m-1}{2}},q^{m-1}-q^{\frac{m-1}{2}},\cdots,q^{m-1}+q^{\frac{m-1}{2}},q^{m-1}-q^{\frac{m-1}{2}})。$$

(2) 当 m 为偶数时,分别有 $(q^m-1)/2$ 个元素 $a \in \mathrm{F}_{q^m}^*$,对应下列两种原像分布:

$$\Omega_3=(q^{m-1}+(q-1)q^{\frac{m-2}{2}},q^{m-1}-q^{\frac{m-2}{2}},\cdots,q^{m-1}-q^{\frac{m-2}{2}}),$$

$$\Omega_4=(q^{m-1}-(q-1)q^{\frac{m-2}{2}},q^{m-1}+q^{\frac{m-2}{2}},\cdots,q^{m-1}+q^{\frac{m-2}{2}})。$$

命题 1 刻画了当 $\Pi(x)$ 是 F_{q^m} 上的 Dembowski-Ostrom 型的完全非线性函数时,从 F_{q^m} 到 F_q 的完全非线性函数 $\mathrm{tr}(a\Pi(x))$ 的原像分布特征。本文进一步证明了当 $\Pi(x)$ 为 F_{q^m} 上已知的幂函数型的完全非线性函数时,即 $\Pi(x)$ 为 Dembowski-Ostrom 函数或者 Coulter-Matthews 函数时,从 F_{q^m} 到 F_q 的完全非线性函数 $\mathrm{tr}(a\Pi(x))$ 的原像分布恰有两种取值,其中一种取值对应 F_{q^m} 所有平方剩余元,另一种取值对应 F_{q^m} 所有非平方剩余元。这一结果表明对于目前已知的六类完全非线性函数来说,命题 1 的结论均成立。

2　原像分布特征

定义 1　设 q 是奇素数的方幂,F_q 上的二次特征 η 定义为

$$\eta(x)=\begin{cases}0, & x=0\\ 1, & x=\beta^{2l}\\ -1, & x=\beta^{2l+1}\end{cases},$$

这里 β 是 F_q 中的本原元。

引理 1[9]　设 $f(x_1,x_2,\cdots,x_n)$ 是 F_q 上秩为 r 的二次型,q 是奇素数的方幂。那么 $f(x_1,x_2,\cdots,x_n)$ 等价于一个对角型的二次型 $a_1y_1^2+a_2y_2^2+\cdots+a_ry_r^2$,其中 $a_1,a_2,\cdots,a_r$ 是 F_q 中的非零元。

引理 2[9]　设 m 是正整数,q 是奇素数的方幂,η 是 F_q 上的二次特征,$b \in \mathrm{F}_q$。如果 $f(x_1,x_2,\cdots,x_m)$ 是 F_q 上非退化二次型,Δ 表示 $f(x_1,x_2,\cdots,x_m)$ 的行列式,那么方程 $f(x_1,x_2,\cdots,x_m)=b$ 在 F_q^m 中的解的个数 N_b 为

(1) 当 m 为奇数时,$N_b=q^{m-1}+q^{\frac{m-1}{2}}\eta((-1)^{\frac{m-1}{2}}b\Delta)$,

(2) 当 m 为偶数时,$N_b=q^{m-1}+v(b)q^{\frac{m-2}{2}}\eta((-1)^{\frac{m}{2}}\Delta)$,

这里 $v(b)=-1(b \in \mathrm{F}_q^*)$,且 $v(0)=q-1$。

引理 3　设 q 是奇素数的方幂,m 是大于 1 的正整数。如果 $\Pi(x)$ 为 Dembowski-Ostrom 函数或者 Coulter-Matthews 函数,则对于每一个非零 $a \in \mathrm{F}_{q^m}$,$\mathrm{tr}(a\Pi(x))$ 的原像分布与 $\mathrm{tr}(ax^2)$ 的原像分布是一致的。

证明　我们只给出 Dembowski-Ostrom 函数情形下的证明,Coulter-Matthews 函数情形下的证明类似可得。

设 b 是 F_q^m 中任意元素。如果 $b=0$,则方程 $x^{q^t+1}=b$ 与 $x^2=b$ 在 F_q^m 中只有零解。如果 $b \neq 0$,令 α 是 F_q^m 中的一个本原元,那么 $b=\alpha^j$,这里 j 为某个正整数。于是方程 $x^{q^t+1}=b$ 在 F_q^m 中有解 $\gamma=\alpha^i$ 当且仅当 $i(q^t+1) \equiv j \bmod q^m-1$,类似地,方程 $x^2=b$ 在 F_q^m 中有解 $\delta=\alpha^k$ 当且仅当 $2k \equiv j \bmod q^m-1$。注意到当 $t \geqslant 0$ 为整数,并且 $\frac{m}{(m,t)}$ 是奇数时,$(q^t+1, q^m-1)=2$,从而同余方程 $i(q^t+1) \equiv j \bmod q^m-1$ 对于 i 有解当且仅当同余方程 $2k \equiv j \bmod q^m-1$ 对于 j 有解,这时解的个数均为 2,这表明 $x^{q^t+1}=b$ 解的个数与 $x^2=b$ 解的个数相同,故对每

一个 $c \in \mathrm{F}_q$，均有 $|\{x \mid x \in \mathrm{F}_{q^m}, \mathrm{tr}(ax^{q^t+1}) = c\}| = |\{x \mid x \in \mathrm{F}_{q^m}, \mathrm{tr}(ax^2) = c\}|$，这说明当 $\Pi(x)$ 为 Dembowski-Ostrom 函数时，$\mathrm{tr}(a\Pi(x))$ 的原像分布与 $\mathrm{tr}(ax^2)$ 的原像分布一致。

由于 $\Pi(x) = x^2$ 是一类特殊的 Dembowski-Ostrom 型函数，故 $\mathrm{tr}(ax^2)$ 的原像分布具有命题 1 中所表述的特征。再根据引理 3，可以得知当 $\Pi(x)$ 为 Dembowski-Ostrom 函数或者 Coulter-Matthews 函数时，从 F_{q^m} 到 F_q 的完全非线性函数 $\mathrm{tr}(a\Pi(x))$ 的原像分布具有命题 1 中所刻画的特征，下面进一步刻画这两类函数的原像分布特征：

引理 4 设 $\{\alpha_1, \alpha_2, \cdots, \alpha_m\}$ 是 F_{q^m} 在 F_q 上的一组基，$B = [\alpha_i^{q^{j-1}}]_{m\times m}$，令 $b = \det(B)$，那么 $b^q = (-1)^{m-1}b$，进而 $b \in \mathrm{F}_q$ 当且仅当 m 是奇数。

证明 由行列式定义，设 $b_{ij} = \alpha_i^{q^{j-1}}$，

则 $b_{ij}^q = \alpha_i^{q^j} = \begin{cases} b_{i,j+1}, & j = 1,2,\cdots \\ b_{i,0}, & j = m \end{cases}$，

于是

$$\begin{aligned} b^q &= \Big(\sum_{i_1 i_2 \cdots i_m} (-1)^{\tau(i_1 i_2 \cdots i_m)} b_{1i_1} b_{2i_2} \cdots b_{mi_m}\Big)^q \\ &= \sum_{i_1 i_2 \cdots i_m} (-1)^{\tau(i_1 i_2 \cdots i_m)} b_{1i_1}^q b_{2i_2}^q \cdots b_{mi_m}^q \\ &= \sum_{i_1 i_2 \cdots i_m} (-1)^{\tau(i_1 i_2 \cdots i_m)} b_{1,i_1+1} b_{2,i_2+1} \cdots b_{m,i_m+1} \end{aligned}$$

其中 $i_t + 1 \triangleq \begin{cases} t+1, & t \leqslant m-1 \\ 1, & t = m \end{cases}$。

下面考虑 $(-1)^{\tau(i_1 i_2 \cdots i_m)}$ 和 $(-1)^{\tau(i_1+1, i_2+1, \cdots, i_m+1)}$ 之间的关系。设 $0 \leqslant t \leqslant m-1$，$i_1 i_2 \cdots i_m = u_1 \cdots u_t m u_{t+1} \cdots u_m$，$i_1 + 1, i_2 + 1, \cdots, i_m + 1 = u_1 + 1, \cdots, u_t + 1, 1, u_{t+1} + 1, \cdots, u_m + 1$。由于 $u_1 \cdots u_t u_{t+1} \cdots u_m$ 和 $u_1 + 1, \cdots, u_t + 1, u_{t+1} + 1, \cdots, u_m + 1$ 的逆序数完全相同，记为 τ_0，则

$$\tau(i_1 \cdots i_m) = \tau_0 + m - (t+1),$$

$$\tau(i_1 + 1, \cdots, i_m + 1) = \tau_0 + t$$

于是 $\tau(i_1+1, \cdots, i_m+1) = \tau(i_1 \cdots i_m) - m + (t+1) + t = \tau(i_1 \cdots i_m) + 2t - (m-1)$

从而

$$\begin{aligned} b^q &= \sum_{i_1 i_2 \cdots i_n} (-1)^{\tau(i_1 i_2 \cdots i_n)} b_{1,i_1+1} \cdots b_{m,i_m+1} \\ &= (-1)^{m-1} \sum_{i_1 i_2 \cdots i_m} (-1)^{\tau(i_1+1, \cdots, i_m+1)} b_{1,i_1+1} \cdots b_{m,i_m+1} \\ &= (-1)^{m-1} b \end{aligned}$$

注意到 $b \in \mathrm{F}_q$ 当且仅当 $b^q = b$，于是 $b \in \mathrm{F}_q$ 当且仅当 m 是奇数。

引理 5 设 $\{\alpha_1, \alpha_2, \cdots, \alpha_m\}$ 是 F_{q^m} 在 F_q 上的一组基，对每一个元素 $x \in \mathrm{F}_{q^m}$，x 在基 $\{\alpha_1, \alpha_2, \cdots, \alpha_m\}$ 下的坐标为 $\{x_1, x_2, \cdots, x_m\}$，$\mathrm{tr}(\cdot)$ 表示从 F_{q^m} 到 F_q 的迹函数，则 $\mathrm{tr}(ax^2)$ 具有如下二次型表示

$$\mathrm{tr}(ax^2) = \sum_{i,j=1}^{m} a_{ij} x_i x_j,$$

这里 $a_{ij} = \mathrm{tr}(a\alpha_i\alpha_j)$，$i, j = 1, 2, \cdots, m$

用 Δ_a 表示上述二次型的行列式，则 $\Delta_a = a^{\frac{q^m-1}{q-1}} \Delta(\alpha_1, \alpha_2, \cdots, \alpha_m)$，其中

$$\Delta(\alpha_1, \alpha_2, \cdots, \alpha_m) = \begin{vmatrix} \mathrm{tr}(\alpha_1\alpha_1) & \mathrm{tr}(\alpha_1\alpha_2) & \cdots & \mathrm{tr}(\alpha_1\alpha_m) \\ \mathrm{tr}(\alpha_2\alpha_1) & \mathrm{tr}(\alpha_2\alpha_2) & \cdots & \mathrm{tr}(\alpha_2\alpha_m) \\ \vdots & \vdots & & \vdots \\ \mathrm{tr}(\alpha_m\alpha_1) & \mathrm{tr}(\alpha_m\alpha_2) & \cdots & \mathrm{tr}(\alpha_m\alpha_m) \end{vmatrix}。$$

证明 根据迹函数的线性性质，易知

$$\mathrm{tr}(ax^2) = \sum_{i,j=1}^{m} a_{ij} x_i x_j,$$

其中

$$a_{ij} = \mathrm{tr}(a\alpha_i\alpha_j), \quad i, j = 1, 2, \cdots, m$$

于是该二次型的行列式为

$$\begin{aligned} \Delta_a &= \begin{vmatrix} \mathrm{tr}(a\alpha_1\alpha_1) & \mathrm{tr}(a\alpha_1\alpha_2) & \cdots & \mathrm{tr}(a\alpha_1\alpha_m) \\ \mathrm{tr}(a\alpha_2\alpha_1) & \mathrm{tr}(a\alpha_2\alpha_2) & \cdots & \mathrm{tr}(a\alpha_2\alpha_m) \\ \vdots & \vdots & & \vdots \\ \mathrm{tr}(a\alpha_m\alpha_1) & \mathrm{tr}(a\alpha_m\alpha_2) & \cdots & \mathrm{tr}(a\alpha_m\alpha_m) \end{vmatrix} \\ &= \begin{vmatrix} a\alpha_1 & (a\alpha_1)^q & \cdots & (a\alpha_1)^{q^{m-1}} \\ a\alpha_2 & (a\alpha_2)^q & \cdots & (a\alpha_2)^{q^{m-1}} \\ \vdots & \vdots & & \vdots \\ a\alpha_m & (a\alpha_m)^q & \cdots & (a\alpha_m)^{q^{m-1}} \end{vmatrix} \\ &\quad \begin{vmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_m \\ \alpha_1^q & \alpha_2^q & \cdots & \alpha_m^q \\ \vdots & \vdots & & \vdots \\ \alpha_1^{q^{m-1}} & \alpha_2^{q^{m-1}} & \cdots & \alpha_m^{q^{m-1}} \end{vmatrix} \\ &= a^{\frac{q^m-1}{q-1}} \begin{vmatrix} \alpha_1 & \alpha_1^q & \cdots & \alpha_1^{q^{m-1}} \\ \alpha_2 & \alpha_2^q & \cdots & \alpha_2^{q^{m-1}} \\ \vdots & \vdots & & \vdots \\ \alpha_m & \alpha_m^q & \cdots & \alpha_m^{q^{m-1}} \end{vmatrix} \\ &\quad \begin{vmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_m \\ \alpha_1^q & \alpha_2^q & \cdots & \alpha_m^q \\ \vdots & \vdots & & \vdots \\ \alpha_1^{q^{m-1}} & \alpha_2^{q^{m-1}} & \cdots & \alpha_m^{q^{m-1}} \end{vmatrix} \\ &= a^{\frac{q^m-1}{q-1}} \begin{vmatrix} \mathrm{tr}(\alpha_1\alpha_1) & \mathrm{tr}(\alpha_1\alpha_2) & \cdots & \mathrm{tr}(\alpha_1\alpha_m) \\ \mathrm{tr}(\alpha_2\alpha_1) & \mathrm{tr}(\alpha_2\alpha_2) & \cdots & \mathrm{tr}(\alpha_2\alpha_m) \\ \vdots & \vdots & & \vdots \\ \mathrm{tr}(\alpha_m\alpha_1) & \mathrm{tr}(\alpha_m\alpha_2) & \cdots & \mathrm{tr}(\alpha_m\alpha_m) \end{vmatrix} \\ &= a^{\frac{q^m-1}{q-1}} \Delta(\alpha_1, \alpha_2, \cdots, \alpha_m) \end{aligned}$$

定理 1　设 q 是奇素数的方幂,m 是大于 1 的正整数,$a \in \mathrm{F}_{q^m}^*$,η 是 F_q 上的二次特征, $\Delta_a = \det(\mathrm{tr}(ax^2))$,则对所有 $a \in \mathrm{F}_{q^m}^*$,

(1) 当 m 为奇数时,

$$\eta(\Delta_a) = \begin{cases} 1, & \text{若 } a \text{ 为平方剩余元} \\ -1, & \text{若 } a \text{ 为非平方剩余元} \end{cases}$$

(2) 当 m 为偶数时,

$$\eta(\Delta_a) = \begin{cases} -1, & \text{若 } a \text{ 为平方剩余元} \\ 1, & \text{若 } a \text{ 为非平方剩余元} \end{cases}$$

证明　根据引理 5,

$\Delta_a = a^{\frac{q^m-1}{q-1}}\Delta(\alpha_1,\alpha_2,\cdots,\alpha_m)$,注意到

$$\Delta(\alpha_1,\alpha_2,\cdots,\alpha_m) = \begin{vmatrix} \mathrm{tr}(\alpha_1\alpha_1) & \mathrm{tr}(\alpha_1\alpha_2) & \cdots & \mathrm{tr}(\alpha_1\alpha_m) \\ \mathrm{tr}(\alpha_2\alpha_1) & \mathrm{tr}(\alpha_2\alpha_2) & \cdots & \mathrm{tr}(\alpha_2\alpha_m) \\ \vdots & \vdots & & \vdots \\ \mathrm{tr}(\alpha_m\alpha_1) & \mathrm{tr}(\alpha_m\alpha_2) & \cdots & \mathrm{tr}(\alpha_m\alpha_m) \end{vmatrix} =$$

$$\begin{vmatrix} \alpha_1 & \alpha_1^q & \cdots & \alpha_1^{q^{m-1}} \\ \alpha_2 & \alpha_2^q & \cdots & \alpha_2^{q^{m-1}} \\ \vdots & \vdots & & \vdots \\ \alpha_m & \alpha_m^q & \cdots & \alpha_m^{q^{m-1}} \end{vmatrix} \begin{vmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_m \\ \alpha_1^q & \alpha_2^q & \cdots & \alpha_m^q \\ \vdots & \vdots & & \vdots \\ \alpha_1^{q^{m-1}} & \alpha_2^{q^{m-1}} & \cdots & \alpha_m^{q^{m-1}} \end{vmatrix} = b^2$$

这里 b 的定义见引理 4,于是 $\Delta_a = a^{\frac{q^m-1}{q-1}}b^2$。令 α 是 F_{q^m} 中的本原元,则 $\beta = \alpha^{\frac{q^m-1}{q-1}}$ 是 F_q 中的本原元。

当 m 为奇数时,由引理 4,b 是 F_q 中非零元素,故 $\eta(b^2) = 1$。如果 a 是 F_{q^m} 中的平方剩余元,则存在正整数 l,使得 $a = \alpha^{2l}$,故 $\Delta_a = \beta^{2l}b^2$,这时 $\eta(\Delta_a) = 1$;如果 a 是 F_{q^m} 中的平方非剩余元,则存在正整数 l,使得 $a = \alpha^{2l+1}$,故 $\Delta_a = \beta^{2l+1}b^2$,这时 $\eta(\Delta_a) = -1$。

当 m 为偶数时,由引理 4,b 不是 F_q 中非零元素,但 b^2 是 F_q 中的非零元素。这时 b^2 一定是 F_q 中的平方非剩余元,否则存在 F_q 中的非零元素 θ,使得 $b^2 = \theta^2$,从而 $b = \pm\theta$ 为 F_q 中的元素,矛盾!因此 $\eta(b^2) = -1$。如果 a 是 F_{q^m} 中的平方剩余元,则存在正整数 l,使得 $a = \alpha^{2l}$,故 $\Delta_a = \beta^{2l}b^2$,这时 $\eta(\Delta_a) = -1$;如果 a 是 F_{q^m} 中的平方非剩余元,则存在正整数 l,使得 $a = \alpha^{2l+1}$,故 $\Delta_a = \beta^{2l+1}b^2$,这时 $\eta(\Delta_a) = 1$。

根据引理 2、引理 3 和定理 1,容易得到如下结论:

定理 2　设 q 是奇素数的方幂,m 是大于 1 的正整数,$a \in \mathrm{F}_{q^m}^*$,$\Pi(x)$ 是 Dembowski-Ostrom 函数或者 Coulter-Matthews 函数,$\mathrm{tr}(\cdot)$ 表示从 F_{q^m} 到 F_q 的迹函数。那么从 F_{q^m} 到 F_q 的完全非线性函数 $\mathrm{tr}(a\Pi(x))$ 的原像分布具有如下特征:

(1) 当 m 为奇数时,F_{q^m} 中平方剩余元和非平方剩余元恰好对应下列两种原像分布之一,

$$\Omega_1 = (q^{m-1}, q^{m-1} - q^{\frac{m-1}{2}}, q^{m-1} + q^{\frac{m-1}{2}}, \cdots, q^{m-1} - q^{\frac{m-1}{2}}, q^{m-1} + q^{\frac{m-1}{2}}),$$

$$\Omega_2 = (q^{m-1}, q^{m-1} + q^{\frac{m-1}{2}}, q^{m-1} - q^{\frac{m-1}{2}}, \cdots, q^{m-1} + q^{\frac{m-1}{2}}, q^{m-1} - q^{\frac{m-1}{2}})$$

(2) 当 m 为偶数时,F_{q^m} 中平方剩余元和非平方剩余元恰好对应下列两种原像分布之一,

$$\Omega_3 = (q^{m-1} + (q-1)q^{\frac{m-2}{2}}, q^{m-1} - q^{\frac{m-2}{2}}, \cdots, q^{m-1} - q^{\frac{m-2}{2}}),$$

$$\Omega_4 = (q^{m-1} - (q-1)q^{\frac{m-2}{2}}, q^{m-1} + q^{\frac{m-2}{2}}, \cdots, q^{m-1} + q^{\frac{m-2}{2}})。$$

参考文献(References)

[1] Biham E, Shamir A. Differential cryptanalysis of DES-like cryptosystems[J]. Journal of Cryptology, 1991, 4:3 - 72.

[2] 李平,李超,周悦. 基于 Dembowski-Ostrom 型完全非线性函数的线性码的权分布[J]. 应用科学学报,2010, 28(5):441 - 446.
LI Ping, LI Chao, ZHOU Yue. Weight distributions of linear codes from perfect nonlinear functions of dembowski-ostrom type[J]. Journal of Applied Sciences, 2010, 28(5):441 - 446. (in Chinese)

[3] Dembowski P, Ostrom T G. Planes of order n with collineation groups of order n^2[J]. Math. Z., 1968, 193:239 - 258.

[4] Coulter R S, Matthews R W. Planar functions and planes of Lenz-Barlotti class II[J]. Design, Coding and Cryptography, 1997, 10:167 - 184.

[5] Ding C, Yuan J. A family of skew hadamard difference sets [J]. Comb. Theory, Series A, 2006, 113:1526 - 1535.

[6] Zha Z, Kyureghyan G M, Wang X. Perfect nonlinear binomials and their semifields[J]. Finite Fields and Their Applications, 2009, 15(2):125 - 133.

[7] Budaghyan L, Helleseth T. New Perfect Nolinear Multinomials over $\mathrm{F}_{p^{2k}}$ for Any Odd Prime p. SETA[C]//2008, LNCS 5203:403 - 414.

[8] Lidl R, Niederreiter H. Finite fields[M]. Cambridge, UK: Cambridge University Press, 1997.