文章编号: 1001- 2486(2009) 03- 0132- 04

完全非线性函数的原像分布特征*

李 强[1], 李 超[1,2], 冯克勤[3]
(1. 国防科技大学 理学院, 湖南 长沙 410073; 2. 东南大学 移动通信国家重点实验室, 江苏 南京 210096;
3. 清华大学 数学科学系, 北京 100084)

摘 要: 完全非线性函数在密码设计与分析中具有十分重要的作用。利用代数数论的方法, 研究一般有限 Abel 群上完全非线性函数的原像分布特征, 给出了一般有限 Abel 群上完全非线性函数存在的一个必要条件, 证明了某些群上不存在完全非线性函数, 得到了素数域上完全非线性函数的原像分布。

关键词: 完全非线性函数; 原像分布; 理想分解; 素域
中图分类号: TN918.1 文献标识码: A

Properties of Preimage Distributions of Perfect Nonlinear Functions

LI Qiang[1], LI Chao[1,2], FENG Ke-qin[3]
(1. College of Science, National Univ. of Defense Technology, Changsha 410073, China;
2. State Key Lab of Mobile Communication, Southeast Univ., Nanjing 210096, China;
3. Department of Mathematical Science, Tsinghua Univ., Beijing 100084, China)

Abstract: Perfect nonlinear functions are widely used in the design and analyses of cryptosystem. Based on the method of algebraic number theory, the properties of preimage distributions of perfect nonlinear functions over finite abelian group are studied. Necessary conditions for the existence of perfect nonlinear functions over finite abelian group are presented, which proves that there are no perfect nonlinear functions for some abelian groups. Finally, the preimage distributions of perfect nonlinear functions over some prime fields are presented.

Key words: perfect nonlinear functions; preimage distributions; idea factorization; prime field

高度非线性函数在序列密码、分组密码、纠错编码和 Hash 函数的设计与分析中具有重要应用[1-3]。完全非线性函数是一类重要的高度非线性函数, 近年来, 其研究内容集中在新函数的构造和等价分类、完全非线性函数在编码密码学中应用等问题[3-4]。2004 年, C. Carlet 和 C. Ding 讨论了一般 Abel 群上完全非线性函数的原像分布问题[3], 给出了完全非线性函数原像分布的不定方程组。2007 年, 李超等利用初等数论的技巧, 研究了从 n 阶 Abel 群到 3 阶、4 阶 Abel 群的完全非线性函数的原像分布[5]。本文利用代数数论中素理想分解理论, 给出完全非线性函数存在的一个必要条件, 证明了某些特殊群上不存在完全非线性函数, 得到了素数域上完全非线性函数的原像分布。

1 完全非线性函数的原像分布特征

设$(A,\cdot)$和$(B,\cdot)$分别是 n 和m 阶有限 Abel 群, 为讨论方便, 群中的运算用乘法表示。

定义 1 设f 是从n 阶 Abel 群 A 到m 阶 Abel 群 B 的函数, 令

$$P_f = \max_{0\neq a\in A}\max_{b\in B}\frac{|\{x\in A: f(ax)f^{-1}(x)=b\}|}{n}$$

则称 P_f 为函数f 的非线性度。

差分密码攻击表明, P_f 的值越小, 则函数f 的非线性度就越高, 由 P_f 定义可知$P_f \geqslant \frac{1}{m}$。

* 收稿日期: 2008- 11- 30
基金项目: 国家自然科学基金资助项目(60803156); 东南大学移动通信国家重点实验室开放基金资助项目(W200805)
作者简介: 李强(1979—), 男, 博士生。

定义 2　设f是从n阶 Abel 群A到m阶 Abel 群B的函数, 如果$P_f=\frac{1}{m}$, 则称f是完全非线性函数。

引理 1[2]　设f是从n阶 Abel 群A到m阶 Abel 群B的完全非线性函数, 则有$m\mid n$。

引理 2[6]　设$K=Q(\xi_n)$, 其中m为正整数, $m\geqslant 3$, $m\neq 2(\mathrm{mod}\ 4)$, 则对每个素数p, 记$m=p^l m'$, 其中$l\geqslant 0, p\nmid m'$。则p在代数整数环$O_K=Z[\xi_m]$中素理想分解式为

$$pO_K=(P_1\cdots P_g)^e$$

其中, $e=\varphi(p^l)$, $g=\varphi(m')/f$, f是p模m'的阶, 满足$p^f\equiv 1(\mathrm{mod}\ m')$的最小正整数$f$。

引理 3　设f是从n阶 Abel 群A到m阶 Abel 群B的完全非线性函数, $m\mid n$, 令$k_b=\left|\left\{x\in A: f(x)=b\right\}\right|(\forall b\in B)$, 则对任意$1\neq d\in B$, f的原像分布$(k_b\mid b\in B)$满足:

$$\begin{cases}\sum\limits_{b\in B}k_b^2=n+\dfrac{n(n-1)}{m}\\ \sum\limits_{b\in B}k_bk_{bd}=\dfrac{n(n-1)}{m}\\ \sum\limits_{b\in B}k_b=n\end{cases}\tag{1}$$

证明　令$F=\sum\limits_{a\in A}f(a)=\sum\limits_{b\in B}k_b\cdot b$, $F^{(-1)}=\sum\limits_{a'\in A}f(a')^{-1}=\sum\limits_{b\in B}k_b\cdot b^{-1}$, 则$F$和$F^{(-1)}$均为群代数$Z(B)$中的元素。由于$f$是从$A$到$B$的完全非线性函数, 故

$$\begin{aligned}F\cdot F^{(-1)}&=\sum_{a,\,a'\in A}f(a)f(a')^{-1}=\sum_{a,\,c\in A}f(a)f(ac)^{-1}\\&=\sum_{a}f(a)f(a)^{-1}+\sum_{a,\,c\in A,\,c\neq 1_A}f(a)f(ac)^{-1}\\&=n\cdot 1_B+(n-1)\frac{n}{m}\boldsymbol{B}=\left[n+\frac{n(n-1)}{m}\right]\cdot 1_B+(\boldsymbol{B}-1_B)\frac{n(n-1)}{m}\end{aligned}\tag{2}$$

其中, 1_A和1_B分别为A和B中的单位元, $\boldsymbol{B}=\sum\limits_{b\in B}b\in Z(B)$。另一方面,

$$\begin{aligned}F\cdot F^{(-1)}&=\sum_{b,\,b'\in B}k_bk_{b'}bb'^{-1}=\sum_{b\in B}k_b^2\cdot 1_B+\sum_{b,\,d\in B,\,d\neq 1_B}k_bk_{bd}\cdot d\\&=\sum_{b\in B}k_b^2\cdot 1_B+\sum_{1\neq d\in B}\left(\sum_{b\in B}k_bk_{bd}\right)\cdot d\end{aligned}\tag{3}$$

比较式(2)和式(3), 有

$$\begin{cases}\sum\limits_{b\in B}k_b^2=n+\dfrac{n(n-1)}{m}\\ \sum\limits_{b\in B}k_bk_{bd}=\dfrac{n(n-1)}{m}\end{cases}$$

又显然有$\sum\limits_{b\in B}k_b=n$, 因此引理得证。

定理 1　记$v_p(n)$为素因子p在正整数n的分解式中的阶数, 即$p^{v_p(n)}\mid n$, 但$p^{v_p(n)+1}\nmid n$。f是从n阶 Abel 群A到m阶 Abel 群B的完全非线性函数, 这里$m\mid n$, 若p为n的素因子, 并且$v_p(n)$为奇数, 则pO_K在整环$Z[\xi_n]$中具有如下分解形式:

$$pO_K=(VV)^l$$

证明　用$\hat{B}$表示群B的特征群, 由于B是m阶 Abel 群, 故对每一个$\chi\in\hat{B}$和每一个$b\in B$, $\chi(b)$为m次单位根, 即$\chi(b)=\xi_m^r$。于是对每一个$\chi\in\hat{B}$和每一个$F=\sum\limits_{b\in B}k_b\cdot b\in Z(B)$, 记$\alpha_\chi=\chi(F)$, 则

$$\alpha_\chi=\chi(F)=\chi\left(\sum_{a\in A}f(a)\right)=\sum_{a\in A}\chi(f(a))=\sum_{b\in B}k_b\chi(b)\in Z[\xi_m]$$

并且 $\alpha_\chi\overline{\alpha_\chi}=\chi(F)\overline{\chi}(F)=\chi(F)\chi(F^{-1})=\chi(F\cdot F^{-1})$，由式(2)和式(3)可知

$$\alpha_\chi\overline{\alpha_\chi}=\begin{cases}n^2, & \chi=1\\ n, & \chi\neq 1\end{cases} \tag{4}$$

当 $\chi\neq 1$，则由式(4)有 $n=\alpha_\chi\overline{\alpha_\chi}$，这表示理想 nO_K 在 $Z[\xi_n]$ 中具有共轭的分解形式 $nO_K=UU$，其中 $U=\alpha_\chi O_K$，$\overline{U}=\alpha_{\overline{\chi}}O_K$，从而若 p 为 n 的素因子，并且 $v_p(n)$ 为奇数，则 pO_K 在整环 $Z[\xi_n]$ 中具有如下分解形式 $pO_K=(VW)^l$。定理得证。

由引理2，得到 pO_K 在 $Z[\xi_n]$ 中的分解式为 $pO_K=(P_1\cdots P_g)^e$，而由定理1，当 f 是从 n 阶 Abel 群 A 到 m 阶 Abel 群 B 上的完全非线性函数时，如果 $p\mid n$，并且 $v_p(n)$ 为奇数，则有 $pO_K=(VW)^l$。比较这两种分解，不难发现，$pO_K=(P_1\cdots P_g)^e$ 中素理想及其共轭总是成对出现的。根据这一点，我们讨论了 $m=3,4,5$ 时，不同 n 值条件下完全非线性函数的存在性问题。表1列出了当 $n\leqslant 200$ 时，不存在从 n 阶 Abel 群到3，4或5阶 Abel 群完全非线性函数的部分 n 值。

表1 $m=3,4,5$，$n\leqslant 200$ 时，不存在完全非线性函数的 n 的部分取值

Tab. 1 Values of n that when m equals 3, 4, 5, there does not exit any perfect nonlinear functions form abelian group of order n to abelian group of order m

m	n														
3	6	15	24	30	33	51	66	87	102	123	141	159	165	174	177
4	12	24	28	56	76	84	92	96	108	124	152	168	172	184	188
5	10	15	30	35	40	65	70	85	105	115	130	135	160	170	185

2 素数域上完全非线性函数的原像分布

下面考虑当 p 为奇素数，$n=p^l$ 时，设 f 是从 n 阶 Abel 群 A 到 p 阶 Abel 群 B 的完全非线性函数，则对任意的 $\chi\in\hat{B}$，$\chi\neq 1$，由式(4)可知 $\alpha_\chi\overline{\alpha_\chi}=n=p^l$，其中 $\alpha_\chi,\overline{\alpha_\chi}\in Z[\xi_p]$，$O_k=Z[\xi_p]$，$K=Q[\xi_p]$。由引理2可知，$pO_K$ 在 $Z[\xi_p]$ 中分解为 $pO_K=\mathfrak{P}^{p-1}$。

当 l 为偶数时，有 $(\alpha_\chi)O_K=P^{(p-1)\frac{l}{2}}$，于是可知 $(\frac{\alpha_\chi}{p^{l/2}})O_K=(1)$，即 $\frac{\alpha_\chi}{p^{l/2}}$ 为 $Z[\xi_p]$ 中的代数整数，且其所有共轭元的绝对值为1，于是 $\frac{\alpha_\chi}{p^{l/2}}$ 为 ξ_p 的共轭，即 $\frac{\alpha_\chi}{p^{l/2}}=\pm\xi_p^\lambda(0\leqslant\lambda\leqslant p-1)$，所以当 l 为偶数时，有

$$\alpha_\chi=\pm p^{l/2}\xi_p^\lambda,\quad 0\leqslant\lambda\leqslant p-1 \tag{5}$$

当 l 为奇数时，令 $l=2s+1$，则 $(\alpha_\chi)O_K=P^{(p-1)\frac{l}{2}}=(p^s\sqrt{p^*})O_K$，其中

$$\sqrt{p^*}=\begin{cases}\sqrt{p}, & p\equiv 1 \bmod 4\\ i\sqrt{p}, & p\equiv 3 \bmod 4\end{cases}$$

又

$$\sum_{x=1}^{p-1}(\frac{x}{p})\xi_p^x=\begin{cases}\sqrt{p}, & p\equiv 1 \bmod 4\\ i\sqrt{p}, & p\equiv 3 \bmod 4\end{cases}$$

因此 $\sqrt{p^*}=\sum_{x=1}^{p-1}(\frac{x}{p})\xi_p^x$，于是

$$\alpha_\chi=\pm p^{\frac{l-1}{2}}\Big[\sum_{x=1}^{p-1}(\frac{x}{p})\xi_p^x\Big]\xi_p^\lambda,\quad 0\leqslant\lambda\leqslant p-1 \tag{6}$$

现在讨论素数域上的情形。假设 g 是从 F_q 到其自身的完全非线性函数，p 为奇素数，$q=p^l$，$Tr(x)=Tr_{F_q/F_p}(x)=x+x^p+\cdots+x^{p^{l-1}}$ 为 F_q 到 F_p 上的迹函数。对任意 $a\in F_q^*$，$f(x)=Tr(ag(x))$ 是从 F_q 到 F_p 的完全非线性函数。我们确定函数 f 的原像分布。

定理 2　设 g 是从 F_q 到其自身的完全非线性函数, $q=p^l$, 则完全非线性函数 $f(x)=Tr(ag(x))$ 的原像分布 $(k_0, k_1, k_2, \cdots, k_{p-1})$ 由下式确定:

$$k_b=\begin{cases} p^{l-1}+p^{\frac{l}{2}-1}\pm p^{\frac{l}{2}}\delta_{\lambda b}, & \text{当 } 2\mid l \text{ 时}, 0\leqslant b\leqslant p-1 \\ p^{l-1}\pm p^{\frac{l-1}{2}}k'_{b-\lambda}, & \text{当 } 2\nmid l \text{ 时}, 0\leqslant b\leqslant p-1 \end{cases}$$

其中, $\delta_{\lambda b}=\begin{cases}0, & \text{当 } b\neq\lambda \\ 1, & \text{当 } b=\lambda\end{cases}$, $k'_b=\left(\frac{b}{p}\right)$, 为二次特征。

证明　由式(4)可知, $\alpha_x\overline{\alpha_x}=\begin{cases}p^{2l}, & x=1\\ p^l, & x\neq 1\end{cases}$, 且 $\alpha_x=\sum_{b=0}^{p-1}k_b\chi(b)=\sum_{b=0}^{p-1}k_b\xi_p^b$, $\sum_{b=0}^{p-1}k_b=q=p^l$, 再由式(5)和式(6)可知, 当 $x\neq 1$ 时, 得

$$\alpha_x=\begin{cases}\pm p^{l/2}\xi_p^{\lambda}, & 0\leqslant\lambda\leqslant p-1, 2\mid l \\ \pm p^{\frac{l-1}{2}}\left[\sum_{x=1}^{p-1}\left(\frac{x}{p}\right)\xi_p^x\right]\xi_p^{\lambda}, & 0\leqslant\lambda\leqslant p-1, 2\nmid l\end{cases}$$

由于 k_b 总是正整数, 且 $\sum_{b=0}^{p-1}\xi_p^b=0$, 因此, 对任意 $x\in\hat{B}$, $x\neq 1$, 我们可以选取一个足够大的正整数 N, 使得

$$\alpha_x=\begin{cases}\pm p^{l/2}\xi_p^{\lambda}+N(1+\xi_p+\xi_p^2+\xi_p^{p-1}), & 0\leqslant\lambda\leqslant p-1, 2\mid l \\ \pm p^{\frac{l-1}{2}}\left[\sum_{x=1}^{p-1}\left(\frac{x}{p}\right)\xi_p^x\right]\xi_p^{\lambda}+N(1+\xi_p+\xi_p^2+\xi_p^{p-1}), & 0\leqslant\lambda\leqslant p-1, 2\nmid l\end{cases} \tag{7}$$

现在来确定 N 的值, 当 $x=1$, $2\mid l$ 时由式(7)知, $\alpha_1=\pm\xi_p^{\lambda}p^{l/2}+N(1+\xi_p+\cdots+\xi_p^{p-1})$, 又 $\alpha_1=\sum_{b=0}^{p-1}k_b\cdot 1(b)=\sum_{b=0}^{p-1}k_b\xi_p^b$, 所以有 $k_i=\begin{cases}N\pm p^{\frac{l}{2}}, & i=\lambda\\ N, & i\neq\lambda\end{cases}$, 于是有 $\sum_{i=0}^{p-1}k_i=(p-1)N+N\pm p^{l/2}=p^l$, 即 $N=p^{l-1}\mp p^{\frac{l}{2}-1}$, 同样当 $2\nmid l$, 可知 $N=p^{l-1}$, 于是

$$\alpha_x=\begin{cases}\pm p^{l/2}\xi_p^{\lambda}+(p^{l-1}\mp p^{\frac{l}{2}-1})(1+\xi_p+\xi_p^2+\xi_p^{p-1}), & 0\leqslant\lambda\leqslant p-1, 2\mid l \\ \pm p^{\frac{l-1}{2}}\left(\sum_{x=1}^{p-1}\left(\frac{x}{p}\right)\xi_p^x\right)\xi_p^{\lambda}+p^{l-1}(1+\xi_p+\xi_p^2+\xi_p^{p-1}), & 0\leqslant\lambda\leqslant p-1, 2\nmid l\end{cases} \tag{8}$$

即当 $2\mid l$ 时, 有 $k_b=p^{l-1}\mp p^{\frac{l}{2}-1}\pm p^{\frac{l}{2}}\delta_{\lambda b}$ $(0\leqslant b\leqslant p-1)$; 当 $2\nmid l$ 时, 有 $k_b=p^{l-1}\pm p^{\frac{l-1}{2}}k'_{b-\lambda}$ $(0\leqslant b\leqslant p-1)$, 其中, $k'_i=\left(\frac{i}{p}\right)$, 定理得证。

参 考 文 献:

[1] Biham E, Shair A. Differential Cryptanalysis of DES-like Cryptosystems[J]. J. Cryptology, 1991, 4(1): 3-721.

[2] Matsui M. Linear Cryptanalysis Method for DES Cipher [C]// Advances in Cryptology-EUROCRYT' 93 Proceedings, Berlin: Springer-verlag, 1994: 386-397.

[3] Carlet C, Ding C. Highly Nonlinear Mappings[J]. Journal of Complexity, 2004, 20: 205-244.

[4] Carlet C, Ding C, Yuan J. Linear Codes form Perfect Nonlinear Mappings and Their Secret Sharing Schemes[J]. IEEE Trans. Inform. Theory, 2005, 51(6): 2089-2102.

[5] Li C, Li Q, Ling S. Properties and Applications of Preimage Distributions of Perfect Nonlinear Functions[J]. IEEE Trans on. Inform. Theory, 2009, 55(1): 64-69.

[6] 冯克勤. 代数数论[M]. 北京: 科学出版社, 2000.