Advances in Applied Mathematics 应用数学进展, **2024, 13(8), 3592-3599**
Published Online August 2024 in Hans. https://www.hanspub.org/journal/aam
https://doi.org/10.12677/aam.2024.138342

Hans汉斯

一类三元幂函数的差分均匀度

袁文萍

西北师范大学数学与统计学院，甘肃 兰州

收稿日期：2024年7月1日；录用日期：2024年7月24日；发布日期：2024年7月30日

摘 要

S盒(S-boxes)作为分组密码算法中唯一的非线性组件，其性质的好坏对密码算法的安全性至关重要。为衡量S盒抵抗差分密码攻击性质的好坏，Nyberg在欧洲密码年会上提出了差分均匀度的概念。差分均匀度越小，则S盒的差分密码性质越好。因此，找寻具有较低差分均匀度的函数来构造S盒成为了如今密码学研究领域的一个热点。具有低差分的幂函数因为其特殊的代数结构和对硬件消耗低等特点，所以往往作为设计S盒的备选函数。本文，我们研究了$\mathbb{F}_{3^n}$上的一类幂函数$F(x)=x^{\frac{3^n-7}{2}}$，其中n是偶数。然后通过对奇特征有限域上二次方程的解的个数进行分析，我们确定了三元幂函数F差分均匀度的上界。结果表明F是一个差分均匀度不超过9的函数。

关键词

幂函数，差分均匀度，二次方程，有限域

The Differential Uniformity of a Class of Ternary Power Function

Wenping Yuan

College of Mathematics and Statistics, Northwest Normal University, Lanzhou Gansu

Received: Jul. 1^{st}, 2024; accepted: Jul. 24^{th}, 2024; published: Jul. 30^{th}, 2024

文章引用: 袁文萍. 一类三元幂函数的差分均匀度[J]. 应用数学进展, 2024, 13(8): 3592-3599.
DOI: 10.12677/aam.2024.138342

Abstract

Substitution boxes (S-boxes) as the only nonlinear component in block ciphers algorithm, the quality of its properties is crucial to the security of cryptographic algorithms. In order to measure the properties of S-boxes to resist differential cryptography attacks, Nyberg proposed the concept of differential uniformity at the European Cryptography Annual Conference. The lower the differential uniformity of F is, the better the differential cryptographic properties of S-boxes have. Therefore, finding a function with low differential uniformity to construct S-boxes has become a hot topic in the field of cryptography research today. Power functions with low differential uniformity are often used as alternative functions for S-boxes design because of their special algebraic structure and low hardware consumption. In this paper, we study a class of power functions $F(x) = x^{\frac{3^n-7}{2}}$ over $\mathbb{F}_{3^n}$, where n is an even. Then, by considering the number of solutions on the quadratic equation over finite field with odd characteristic, the upper bound of the differential uniformity is determined. The results show that F is a function with differential uniformity no more than 9.

Keywords

Power Function, Differential Uniformity, Quadratic Equation, Finite Field

1. 引言

差分密码分析 [1, 2], 是由 Biham 和 Shamir 在 1990 年国际密码年会中提出的攻击分组密码最有效的方法之一. 差分密码分析的主要目的是寻找一条高概率的差分或者差分特征, 而高概率的差分或者差分特征的寻找依赖于分组密码算法中唯一的非线性部件—S 盒. 为衡量 S 盒抵抗差分攻击的能力, 1993 年 Nybery 提出了差分均匀度 [3] 的概念. 其定义如下.

定义1. 设 $\mathbb{F}_q$ 是含有 q 个元素的有限域, $\mathbb{F}_q^* = \mathbb{F}_q \backslash \{0\}$, 其中 $q = p^n$ 是素数幂且 n 为正整数. 令

F 是从 $\mathbb{F}_q$ 到其自身的映射, 则 F 关于 $a \in \mathbb{F}_q$ 处的差分定义为

$$D_aF(x) = F(x+a) - F(x), \text{ 对任意 } x \in \mathbb{F}_q.$$

对任意 $a, b \in \mathbb{F}_q$, 令

$$\delta_F(a,b) = |\{x \in \mathbb{F}_q : F(x+a) - F(x) = b\}|,$$

其中 $|S|$ 是集合 S 的基数, 即集合 S 中元素的个数. 定义

$$\Delta_F = \max\left\{\delta_F(a,b) : a \in \mathbb{F}_q^*, b \in \mathbb{F}_q\right\}$$

为 F 的差分均匀度.

特别地, 若 $\Delta_F = 1$, 则称该函数为完全非线性函数 (PN 函数) [4]; 若 $\Delta_F = 2$, 则称该函数为几乎完全非线性函数 (APN 函数) [5]. 差分均匀度 Δ_F 的值与差分密码分析紧密相关, Δ_F 的值越小, 则利用其设计的密码系统抵抗差分密码攻击的能力就越强. 所以在实际应用中, 用于设计 S 盒的密码函数应具有较低的差分均匀度. 差分均匀度在密码学, 组合设计, 编码理论, 序列设计等方面也有着广泛应用. 幂函数由于其对硬件消耗低, 所以具有较低差分均匀度的幂函数常常被用来构造 S 盒. 这也使得低差分幂函数的研究成为了如今的一个热点, 读者可参考文献 [6–16] 等. 对 $\mathbb{F}_q$ 上的幂函数 $F(x) = x^d$, 其中 d 是正整数, 对任意 $a \in \mathbb{F}_q^*$ 且 $b \in \mathbb{F}_q$, 容易验证 $\delta_F(a,b) = \delta_F(1, b/a^d)$.

在全文中, 令 $F(x) = x^{\frac{3^n-7}{2}}$ 为有限域 $\mathbb{F}_{3^n}$ 上的幂函数, 其中 n 为偶数. 因为 n 为偶数, 所以 $3^n \equiv 1 \pmod 4$, 即 $3^n = 4k+1$ 对某些正整数 k 成立. 进一步, 若 k 还满足条件 $k \equiv 0 \pmod 3$, 则 F 是一个 3 对 1 函数, 否则 F 是 $\mathbb{F}_{3^n}$ 上的置换.

全文组织结构如下, 第二部分介绍了一些预备知识; 第三部分给出了函数 $F = x^{\frac{3^n-7}{2}}$ 的差分均匀度; 第四部分总结全文.

2. 基础知识

这一部分, 我们介绍有限域上的二次特征及奇特征有限域上二次方程解的个数, 这对主要结果的证明是十分重要的.

令 η 为 $\mathbb{F}_{p^n}$ 上的二次特征, 即, 对任意 $x \in \mathbb{F}_{p^n}$, 有

$$\eta(x) = x^{\frac{p^n-1}{2}} = \begin{cases} 1, & \text{若 } x \text{ 是平方元,} \\ 0, & \text{若 } x = 0, \\ -1, & \text{若 } x \text{ 是非平方元.} \end{cases}$$

下面我们介绍分圆数的概念, 设 $\mathcal{C}_1$ 和 $\mathcal{C}_{-1}$ 分别定义为 $\mathbb{F}_{p^n}^*$ 上平方元和非平方元的集合. 则分圆数 (i,j) 定义为集合 $\mathcal{C}_{i,j} = \{x \in \mathbb{F}_{p^n} \backslash \{1,-1\} : x \in \mathcal{C}_i, x+1 \in \mathcal{C}_j\}$ 的基数, 其中 $i, j \in \{1,-1\}$.

以下引理在确定 F 的差分均匀度中有着极其重要的作用.

引理1. [17] 设 $f(x)=a_2x^2+a_1x+a_0\in\mathbb{F}_{p^n}[x]$, 其中 p 是奇素数且 $a_2\neq 0$. 令 $\Delta=a_1^2-4a_0a_2$ 是二次方程 $f(x)=0$ 的判别式. 则

$$|\{x\in\mathbb{F}_{p^n}:f(x)=0\}|=\begin{cases}0, & \text{若 } \Delta \text{ 是非平方元},\\ 1, & \text{若 } \Delta=0,\\ 2, & \text{若 } \Delta \text{ 是平方元}.\end{cases}$$

3. $F(x)=x^{\frac{3^n-7}{2}}$ 在 $\mathbb{F}_{3^n}$ 上的差分均匀度, 其中 n 是偶数

本节, 我们计算 F 的差分均匀度. 为此, 我们需要考虑下面差分方程的解的个数.

$$(x+1)^{\frac{3^n-7}{2}}-x^{\frac{3^n-7}{2}}=b, \tag{1}$$

其中 $b\in\mathbb{F}_{3^n}$. 显然 因为 n 是偶数, 所以 $d=\frac{3^n-7}{2}$ 是奇数.

当 $x=0,-1$ 时, 由 (1) 式可得 $b=1$. 下面假设 $x(x+1)\neq 0$ 且 $x\in\mathbb{F}_{3^n}$. 然后在 (1) 式两边同时乘 $x^3(x+1)^3$ 可得

$$b(x^6+x^3)-\eta(x+1)x^3+\eta(x)(x+1)^3=0.$$

在上述方程中令 $t=x^3$, 则由 $x(x+1)\neq 0$ 可知 $t(t+1)\neq 0$, 故

$$bt^2+(b-\eta(t+1)+\eta(t))t+\eta(t)=0. \tag{2}$$

为给出 F 的差分均匀度, 我们首先考虑当 $b\in\mathbb{F}_3$ 时 (2) 式解的个数.

引理2. 设 $F(x)=x^{\frac{3^n-7}{2}}$ 且 n 是偶数. 则对任意的 $b\in\mathbb{F}_3$, 有

$$\delta_F(1,0)=0,\ \delta_F(1,1)\leq 9 \text{ 且 } \delta_F(1,-1)\leq 6.$$

证明 下面我们根据 $\eta(-1)=1$ (因为 n 是偶数) 及 b 的取值来证明该引理.

(1) 如果 $b=0$, 那么可根据 i,j 是否相等将 (2) 式分成以下两种情况, 其中 $t\in\mathcal{C}_{i,j}$ 且 $i,j\in\{-1,1\}$.

(1.1) $t\in\mathcal{C}_{1,1}\cup\mathcal{C}_{-1,-1}$. 由 (2) 式有

$$\eta(t)=0,$$

这与 $t(t+1)\neq 0$ 矛盾, 即 Eq.(2) 在 $\mathcal{C}_{1,1}\cup\mathcal{C}_{-1,-1}$ 中无解.

(1.2) $t\in\mathcal{C}_{-1,1}\cup\mathcal{C}_{1,-1}$. 由 (2) 式有

$$\eta(t)(1-t)=0. \tag{3}$$

显然, 因为 $t(t+1)\neq 0$, 所以 $\eta(t)\neq 0$. 故 (3) 式有解当且仅当 $1-t=0$, 即 $t=1$. 又因为

$\eta(-1)=1$, 所以 $\eta(t+1)=\eta(2)=\eta(-1)=1$, 即 $t=1\in\mathcal{C}_{1,1}$. 这与 $t\in\mathcal{C}_{-1,1}\cup\mathcal{C}_{1,-1}$ 矛盾, 因此 (3) 式在 $t\in\mathcal{C}_{-1,1}\cup\mathcal{C}_{1,-1}$ 中没有解.

综上所述,我们有 $\delta_F(1,0)=0$.

(2) 如果 $b=1$, 那么我们将 (2) 式分成以下四种情况进行讨论.

(2.1) $t\in\mathcal{C}_{1,1}$. 则根据 (2) 式, 有

$$(t-1)^2=0.$$

容易验证 $t=1$ 是多项式 $g(t)=(t-1)^2$ 的一个二重根. 再由 $\eta(-1)=1$, 所以 $\eta(t+1)=\eta(2)=\eta(-1)=1$, 即 $t=1\in\mathcal{C}_{1,1}$. 因此该方程在 $t\in\mathcal{C}_{1,1}$ 中有唯一解.

(2.2) $t\in\mathcal{C}_{-1,-1}$. 则根据 (2) 式, 有

$$t^2+t-1=0,$$

其判别式 $\Delta=-1$. 则根据引理 1 知 $\eta(\Delta)=\eta(-1)=1$, 所以 (2) 式在 $\mathcal{C}_{-1,-1}$ 至多有两个解.

(2.3) $t\in\mathcal{C}_{-1,1}$. 则根据 (2)式, 有

$$t^2-t-1=0,$$

其判别式 $\Delta=-1$. 则根据引理 1 知 $\eta(\Delta)=\eta(-1)=1$, 所以 (2) 式在 $\mathcal{C}_{-1,1}$ 至多有两个解.

(2.4) $t\in\mathcal{C}_{1,-1}$. 则根据 (2)式, 有

$$t^2+1=0,$$

其判别式 $\Delta=-1$. 则根据引理 1 知 $\eta(\Delta)=\eta(-1)=1$, 所以 (2) 式在 $\mathcal{C}_{1,-1}$ 至多有两个解.

根据上述分析, 我们可得 $\delta_F(1,1)\leq 7+2=9$.

(3) 如果 $b=-1$, 那么其证明与 $b=1$ 类似. 下面我们仍然将 (2) 式分成以下四种情况讨论.

(3.1) $t\in\mathcal{C}_{1,1}$. 则 (2) 式可写为

$$t^2+t-1=0,$$

其判别式 $\Delta=-1$. 则根据引理 1 知 $\eta(\Delta)=\eta(-1)=1$, 所以 (2) 式在 $\mathcal{C}_{1,1}$ 至多有两个解.

(3.2) $t\in\mathcal{C}_{-1,-1}$. 则由 (2) 式可得

$$(t-1)^2=0,$$

容易验证 $t=1$ 是多项式 $g(t)=(t-1)^2$ 的一个根, 又因为 $\eta(t)=\eta(1)=1,\eta(t+1)=\eta(2)=1$, 即 $t\in\mathcal{C}_{1,1}$. 这与 $t\in\mathcal{C}_{-1,-1}$ 矛盾. 因此该方程无解.

(3.3) $t\in\mathcal{C}_{-1,1}$. 则根据 (2) 式有

$$t^2+1=0,$$

该方程的判别式为$\Delta=-1$. 则根据引理 1 知 $\eta(\Delta)=\eta(-1)=1$, 所以 (2) 式在 $\mathcal{C}_{-1,1}$ 至多有两个解.

(3.4) $t\in\mathcal{C}_{1,-1}$. 则由 (2) 式可得

$$t^2-t-1=0,$$

该方程的判别式为$\Delta=-1$. 则根据引理 1 知 $\eta(\Delta)=\eta(-1)=1$, 所以 (2) 式在 $\mathcal{C}_{1,-1}$ 至多有两个解. 根据上述分析, 我们可得 $\delta_F(1,-1)\leq 6$. □

对任意的平方元 $\alpha\in\mathbb{F}_{3^n}^*$, 定义 $\sqrt{\alpha}$ 是方程 $x^2=\alpha$ 在 $\mathbb{F}_{3^n}$ 上的任意解. 接下来, 考虑 $b\in\mathbb{F}_{3^n}\backslash\mathbb{F}_3$ 时, $\delta_F(1,b)$ 的值.

引理3. 设 $F(x)=x^{\frac{3^n-7}{2}}$, 其中 n 是偶数. 则对任意 $b\in\mathbb{F}_{3^n}\backslash\mathbb{F}_3$, 有 $\delta_F(1,b)\leq 8$.

证明 类似地, 我们将 (2) 式分成以下四种情况讨论 : $t\in\mathcal{C}_{i,j}$ 对 $i,j\in\{-1,1\}$.

(1) $t\in\mathcal{C}_{1,1}$, 即, $\eta(t)=\eta(t+1)=1$. 则 (2)式等价于方程

$$t^2+t+b^{-1}=0 \tag{4}$$

其判别式为 $\Delta=(b-1)b^{-1}$.

设 $t_i=1\pm\sqrt{(b-1)b^{-1}}\in\mathcal{C}_{1,1}$ 是 (4) 式的两个解, 其中 $i=1,2$. 则可得 $\eta(t_i(t_i+1))=\eta(-b)=1,\eta(t_1t_2)=\eta((t_1+1)(t_2+1))=\eta(b)=1$.

因为 n 是偶数, 所以 $\eta(-1)=1$, 当 $\eta(\Delta)=\eta((b-1)b^{-1})=1$, 且 b 是平方元时, 可得 (4) 式在 $\mathcal{C}_{1,1}$ 中至多有两个解.

(2) $t\in\mathcal{C}_{-1,-1}$, 即, $\eta(t)=\eta(t+1)=-1$. 则 (2) 式可写为

$$t^2+t-b^{-1}=0 \tag{5}$$

其判别式为 $\Delta=(b+1)b^{-1}$.

设 $t_i=1\pm\sqrt{(b+1)b^{-1}}\in\mathcal{C}_{-1,-1}$ 是 (5) 式的两个解, 其中 $i=1,2$. 则可得 $\eta(t_i(t_i+1))=\eta(b)=1,\eta(t_1t_2)=\eta((t_1+1)(t_2+1))=\eta(-b)=1$.

因为 n 是偶数, 所以 $\eta(-1)=1$, 当 $\eta(\Delta)=\eta((b+1)b^{-1})=1$, 且 b 是平方元时, 可得 (5) 式在 $\mathcal{C}_{-1,-1}$ 中至多有两个解.

(3) $t\in\mathcal{C}_{-1,1}$, 即, $\eta(t)=-1,\eta(t+1)=1$. 则根据 (2) 式有

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

其判别式为 $\Delta=(1+b^2)b^{-2}$.

设 $t_i=(b+1)b^{-1}\pm\sqrt{(b^2+1)}b^{-1}\in\mathcal{C}_{-1,1}$ 是 (6) 式的两个解, 其中 $i=1,2$. 则可得 $\eta(t_1t_2)=\eta(-\frac{1}{b}),\eta((t_1+1)(t_2+1))=\eta(\frac{1}{b})$

因为 n 是偶数, 所以 $\eta(-1)=1$, 当 $\eta(\Delta)=\eta((1+b^2)b^{-2})=1$, 且 b 是平方元时, 可得 (6) 式在 $\mathcal{C}_{-1,1}$ 中至多有两个解.

(4) $t\in\mathcal{C}_{1,-1}$, 即, $\eta(t)=1,\eta(t+1)=-1$. 则根据 (2) 式可得

$$t^2+(b-1)b^{-1}t+b^{-1}=0 \tag{7}$$

其判别式为 $\Delta=(1+b^2)b^{-2}$.

设 $t_i=(b-1)b^{-1}\pm\sqrt{(b^2+1)}b^{-1}\in\mathcal{C}_{1,-1}$ 是 (7) 式的两个解, 其中 $i=1,2$. 则可得 $\eta(t_1t_2)=\eta(b)=1,\eta((t_1+1)(t_2+1))=\eta(-b)=1$.

因为 n 是偶数, 所以 $\eta(-1)=1$, 当 $\eta(\Delta)=\eta((1+b^2)b^{-2})=1$, 且 b 是平方元时, 可得 (7) 式在 $\mathcal{C}_{1,-1}$ 中至多有两个解.

综上所述, 可得当 $b\in\mathbb{F}_{3^n}\backslash\mathbb{F}_3$ 时 $\delta_F(1,b)\leq 8$.

至此, 引理得证.

□

为了更好的阐述 F 的差分均匀度, 我们将所证明的上述两个引理进行总结, 得到定理如下.

定理1. 设 $F(x)=x^{\frac{3^n-7}{2}}$ 是 $\mathbb{F}_{3^n}$上的幂函数, 其中 n 是偶数. 则 $\Delta_F\leq 9$.

证明 根据引理 2, 对 $b\in\mathbb{F}_3$, 有 $\delta_F(1,b)\leq 9$. 再根据引理 3, 对 $b\in\mathbb{F}_{3^n}\backslash\mathbb{F}_3$ 时 $\delta_F(1,b)\leq 8$. 因此, 由差分均匀度的定义可得 $\Delta_F\leq 9$. □

4. 总结

本文研究了 $\mathbb{F}_{3^n}$上一类幂函数 $F(x)=x^{\frac{3^n-7}{2}}$ 的差分均匀度. 当 n 是奇数时, 此函数的差分均匀度等价于幂函数 $x^{\frac{3^n-3}{2}}$ 的差分均匀度, 其中 $p^n\equiv 3\pmod 4$. 所以为了结论的完整性, 我们考虑了 n 是偶数时, F 的差分均匀度, 并给出了 F 的差分均匀度的上界, 丰富了已有结果. 未来, 我们将致力于找到更多具有低差分均匀度的幂函数并进一步分析其差分谱.

参考文献

[1] Biham, E. and Shamir, A. (1991) Differential Cryptanalysis of DES-Like Cryptosystems. *Journal of Cryptology*, **4**, 3-72. https://doi.org/10.1007/bf00630563

[2] 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.

[3] Nyberg, K. (1993) Differentially Uniform Mappings for Cryptography. In: Helleseth T., Ed., *Advances in Cryptology—EUROCRYPT'93, Lecture Notes in Computation Science*, Vol. 765, Springer, 55-64.

[4] Blondeau, C. and Nyberg, K. (2015) Perfect Nonlinear Functions and Cryptography. *Finite Fields and Their Applications*, **32**, 120-147. https://doi.org/10.1016/j.ffa.2014.10.007

[5] Pott, A. (2015) Almost Perfect and Planar Functions. *Designs, Codes and Cryptography*, **78**, 141-195. https://doi.org/10.1007/s10623-015-0151-x

[6] Helleseth, T., Rong, C. and Sandberg, D. (1999) New Families of Almost Perfect Nonlinear Power Mappings. *IEEE Transactions on Information Theory*, **45**, 475-485. https://doi.org/10.1109/18.748997

[7] Helleseth, T. and Sandberg, D. (1997) Some Power Mappings with Low Differential Uniformity. *Applicable Algebra in Engineering, Communication and Computing*, **8**, 363-370. https://doi.org/10.1007/s002000050073

[8] Jiang, S., Li, K., Li, Y., *et al.* (2022) Differential Spectrum of a Class of Power Functions. *Journal of Cryptologic Research*, **9**, 484-495.

[9] Pang, T., Li, N. and Zeng, X. (2023) On the Differential Spectrum of a Differentially 3-Uniform Power Function. *Finite Fields and Their Applications*, **87**, Article 102168. https://doi.org/10.1016/j.ffa.2023.102168

[10] Sun, G. and Wu, C. (2010) Some Functions with Low Differential Uniformity. *Wuhan University Journal of Natural Sciences*, **15**, 479-487. https://doi.org/10.1007/s11859-010-0688-5

[11] Xiang, C., Tang, C. and Ding, C. (2022) Shortened Linear Codes from APN and PN Functions. *IEEE Transactions on Information Theory*, **68**, 3780-3795. https://doi.org/10.1109/tit.2022.3145519

[12] Xia, Y., Zhang, X., Li, C. and Helleseth, T. (2020) The Differential Spectrum of a Ternary Power Mapping. *Finite Fields and Their Applications*, **64**, Article 101660. https://doi.org/10.1016/j.ffa.2020.101660

[13] Yan, H., Xia, Y., Li, C., Helleseth, T., Xiong, M. and Luo, J. (2022) The Differential Spectrum of the Power Mapping x^{p^n-3}. *IEEE Transactions on Information Theory*, **68**, 5535-5547. https://doi.org/10.1109/tit.2022.3162334

[14] Bergman, E. and Coulter, R.S. (2022) Constructing Functions with Low Differential Uniformity. *Mediterranean Journal of Mathematics*, **19**, Article 94. https://doi.org/10.1007/s00009-022-01980-0

[15] Yan, H., Mesnager, S. and Tan, X. (2023) The Complete Differential Spectrum of a Class of Power Permutations over Odd Characteristic Finite Fields. *IEEE Transactions on Information Theory*, **69**, 7426-7438. https://doi.org/10.1109/tit.2023.3293842

[16] Yan, H., Mesnager, S. and Tan, X. (2024) On a Class of APN Power Functions over Odd Characteristic Finite Fields: Their Differential Spectrum and C-Differential Properties. *Discrete Mathematics*, **347**, Article 113881. https://doi.org/10.1016/j.disc.2024.113881

[17] Lidl, R. and Niederreiter, H. (1997) Finite Fields. Cambridge University Press.