The Differential Spectrum of A Ternary Power Mapping

Yongbo Xia

School of Mathematics and Statistics
South-Central University for Nationalities
Wuhan, China

This is a joint work with X. Zhang and C. Li

June 17, 2019, Florence, Italy

Outline

Notation

- $\mathbb{F}_{p^n}$: the finite field with p^n elements.
- α: a primitive element of $\mathbb{F}_{p^n}$.
- $f(x)$: a mapping from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^n}$.
- $\mathcal{C}_0$: the set of squares in $\mathbb{F}_{p^n}^*$.
- $\mathcal{C}_1$: the set of non-squares in $\mathbb{F}_{p^n}^*$.

The differential uniformity of $f(x)$

- $N_f(a,b)$: the number of solutions $x \in \mathrm{GF}(p^n)$ of

$$f(x+a) - f(x) = b \tag{1}$$

  where $a, b \in \mathrm{GF}(p^n)$.

- The differential uniformity Δ_f of $f(x)$:

$$\Delta_f = \max \left\{ N_f(a,b) \mid a \in \mathrm{GF}(p^n)^*, b \in \mathrm{GF}(p^n) \right\}. \tag{2}$$

  $f(x)$ is said to be differentially Δ_f-uniform.

- Perfect nonlinear function and almost perfect nonlinear function.

Differential spectrum of a power mapping

When $f(x) = x^d$ is a power mapping,

$$(x+a)^d - x^d = b \Leftrightarrow a^d \left(\left(\frac{x}{a} + 1 \right)^d - \left(\frac{x}{a} \right)^d \right) = b$$

implying that $N_f(a, b) = N_f(1, \frac{b}{a^d})$ for all $a \neq 0$.

Differential spectrum of x^d

- Assume that $f(x) = x^d$ is differentially k-uniform.
- $\omega_i = |\{b \in \mathrm{GF}(p^n) \mid N_f(1, b) = i\}| \ \left((x+1)^d - x^d = b\right)$.
- The differential spectrum of $f(x)$ is defined as the set

$$\mathbb{S} = \{\omega_0, \omega_1, \cdots, \omega_k\}.$$

Properties of differential spectrum

Basic identities

$$\sum_{i=0}^{k} \omega_i = p^n \text{ and } \sum_{i=0}^{k} i\omega_i = p^n. \quad (3)$$

Equivalence

The differential spectra of x^d and x^e are the same if

- d and e are in the same p-cyclotomic coset modulo $p^n - 1$, or
- d is the multiplicative inverse of e modulo $p^n - 1$.

The differential spectra of APN and PN power mappings

- $\mathbb{S} = \{\omega_0 = 0, \omega_1 = p^n\}$ if p is odd and $f(x) = x^d$ is PN;
- $\mathbb{S} = \left\{\omega_0 = 2^{n-1}, \omega_2 = 2^{n-1}\right\}$ if $p = 2$ and $f(x) = x^d$ is APN.

Power functions with known differential spectra (I)

Known results over $\mathbb{F}_{2^n}$

d	Condition	Δ_f	Ref.
2^s+1	$\gcd(n,s)=2$	4	Blondeau, 2010
$2^{2s}-2^s-1$	$\gcd(n,s)=2$	4	Blondeau, 2010
2^n-2	n even	4	Blondeau, 2010
$2^{2k}+2^k+1$	$n=4k$, k odd	4	Blondeau, 2010
$2^{2k}+2^k+1$	$n=4k$	4	Xiong and Yan, 2017
2^t-1	$t=3$, $n-2$	6	P. Charpin, 2011IT
2^t-1	$t=\frac{n-1}{2}, \frac{n+3}{2}$	6 or 8	Blondeau, 2014DCC
$2^m+2^{(m+1)/2}+1$	$n=2m$,$m\geq 5$ odd	8	Xiong, 2018DCC
$2^{m+1}+3$	$n=2m$,$m\geq 5$ odd	8	Xiong, 2018DCC

C. Blondeau, A. Canteaut and P. Charpin, "Differential properties of power functions," *Int. J. Information and Coding Theory*, vol. 1, no. 2, pp. 149-170, 2010.

Power functions with known differential spectra (II)

Known over $\mathbb{F}_{p^n}$, p odd

d	Condition	Δ_f	Ref.
$\frac{p^k+1}{2}$	$\gcd(n,k)=e$	$\frac{p^e-1}{2}$ or p^e+1	Choi et al, 2013
$\frac{p^n+1}{p^m+1}+\frac{p^n-1}{2}$	$p\equiv 3 \pmod 4$ $m\|n$, n odd ,	$\frac{p^m+1}{2}$	Choi et al, 2013
$d(p^k+1)\equiv 2$ $\pmod{p^n-1}$	$e=\gcd(n,k)$ n/e odd ,	$\frac{p^e+1}{2}$	Tian et al, 2017
Kasami $p^{2k}-p^k+1$	$\gcd(n,k)=1$ n odd ,	$p+1$	Yan et al, 2019TIT

S. T. Choi, S. Hong, J. S. No and H. Chung, "Differential spectrum of some power functions in odd prime characteristic," *Finite Fields Appl.*, vol. 21, pp. 11-29, 2013.

H. Yan, et al, "Differential spectrum of Kasami power permutations over odd characteristic finite fields," *IEEE Trans. Inf. Theory*, DOI 10.1109/TIT.2019.2910070, 2019.

An odd problem

Theorem (Helleseth, Rong, Sandberg, TIT, 1999)

Let $d = p^n - 3$ and $f(x) = x^d$ be a mapping over $\mathrm{GF}(p^n)$.

- if $p = 2$, then $\Delta_f = 2$ if n is odd and $\Delta_f = 4$ if n is even.
- if p is an odd prime, then $1 \leq \Delta_f \leq 5$.
- Special case: if $p = 3$ and n is odd, then $\Delta_f = 2$.

Differential spectrum for the special case $p = 2$ (Charpin 2010)

- $p^n - 3$ is equivalent to the inverse power mapping over $\mathrm{GF}(2^n)$.
- $\mathbb{S} = \{\omega_0 = 2^{n-1} + 1, \omega_2 = 2^{n-1} - 2, \omega_4 = 1\}$ for even n.
- $\mathbb{S} = \left\{\omega_0 = 2^{n-1}, \omega_2 = 2^{n-1}\right\}$ for odd n.

Main results: the case $p = 3$

Theorem (Differential uniformity)

Let $d = 3^n - 3$ and $f(x) = x^d$ be a power mapping from $\mathrm{GF}(3^n)$ to $\mathrm{GF}(3^n)$, where $n \geq 2$. Then the differential uniformity Δ_f of $f(x)$ is given by

$$\Delta_f = \begin{cases} 2, & \text{if } n \text{ is odd,} \\ 4, & \text{if } n \equiv 2 \pmod{4}, \\ 5, & \text{if } n \equiv 0 \pmod{4}. \end{cases}$$

Theorem (Differential spectra)

- Odd n: $\mathbb{S} = \{\omega_0 = \frac{3^n-3}{2}, \omega_1 = 3, \omega_2 = \frac{3^n-3}{2}\}$.
- $n \equiv 2 \pmod{4}$: $\mathbb{S} = \{\omega_0 = \frac{3^n-9}{4}, \omega_1 = 2 \cdot 3^{n-1} + 3, \omega_4 = \frac{3^{n-1}-3}{4}\}$.
- $n \equiv 0 \pmod{4}$:
  $\mathbb{S} = \{\omega_0 = \frac{3^n-1}{4}, \omega_1 = 2 \cdot 3^{n-1} + 1, \omega_4 = \frac{3^{n-1}-11}{4}, \omega_5 = 2\}$.

The sketch

Determining the value $N(b)$ and its frequency: the number of solutions of $(x+1)^d - x^d = b$.

Key equation

$$(x+1)^d - x^d = b \Rightarrow (x+1)^{-2} - x^{-2} = b \ , b \in \mathrm{GF}(3^n) \setminus \mathrm{GF}(3)$$

$$\Rightarrow x^4 + 2x^3 + x^2 + \frac{2}{b}x + \frac{1}{b} = 0, \ x \longrightarrow x - \frac{1}{2}$$

$$\Rightarrow x^4 + x^2 - ux + 1 = 0, \ u = \frac{1}{b}. \tag{4}$$

Some useful lemmas

Quadratic equation

The polynomial $Q(x) = x^2 + ax + b \in \mathrm{GF}(q)[x]$, q odd, is irreducible in $\mathrm{GF}(q)[x]$ if and only if $a^2 - 4b$ is a nonsquare in $\mathrm{GF}(q)$. In particular, if $a^2 - 4b$ is a nonzero square in $\mathrm{GF}(q)$, $Q(x)$ has two distinct roots in $\mathrm{GF}(q)$.

Cubic equation

Let $a, b \in \mathrm{GF}(3^n)$ and $a \neq 0$. The factorizations of $g(x) = x^3 + ax + b$ over $\mathrm{GF}(3^n)$ are characterized as follows:
(i) $g(x) = (1, 1, 1) \Leftrightarrow -a$ *is a square in* $\mathrm{GF}(3^n)$ and $\mathrm{Tr}_1^n(b/c^3) = 0$;
(ii) $g(x) = (1, 2) \Leftrightarrow -a$ *is not a square in* $\mathrm{GF}(3^n)$;
(iii) $g(x) = (3) \Leftrightarrow -a$ *is a square in* $\mathrm{GF}(3^n)$ and $\mathrm{Tr}_1^n(b/c^3) \neq 0$.

Some useful lemmas (continue)

The cyclotomic number (i,j): the number of solutions $(x_i, x_j) \in \mathcal{C}_i \times \mathcal{C}_j$ such that $x_i + 1 = x_j$ for $i, j \in \{0, 1\}$.

Cyclotomic numbers

- if $p^n \equiv 1 \pmod 4$, then

$$(0,0) = \frac{p^n - 5}{4},\ (0,1) = (1,0) = (1,1) = \frac{p^n - 1}{4};$$

- if $p^n \equiv 3 \pmod 4$, then

$$(0,0) = (1,0) = (1,1) = \frac{p^n - 3}{4},\ (0,1) = \frac{p^n + 1}{4}.$$

Some useful lemmas (continue)

$\mathcal{E}_{00}$: the set of $x \in \mathrm{GF}(p^n)^*$ such that x and $x+1$ both are nonzero squares, where p is odd.

Representation of $\mathcal{E}_{00}$ (Choi et al, FFA, 2013):

Each $x \in \mathcal{E}_{00}$ has the following representation

$$x = \left(\frac{\alpha^k - \alpha^{-k}}{2}\right)^2,$$

where $k \in \{1, \cdots, \frac{p^n-5}{4}\}$ if $p^n \equiv 1 \pmod 4$ and $k \in \{1, \cdots, \frac{p^n-3}{4}\}$ if $p^n \equiv 3 \pmod 4$.

Some results about the key equation

Main idea

Let $h_u(x) = x^4 + x^2 - ux + 1$. If $h_u(x)$ has two or more roots in $\mathrm{GF}(3^n)$, then

$$h_u(x) = \left(x^2 + ax + b\right)\left(x^2 - ax + b^{-1}\right),$$

where $a, b \in \mathrm{GF}(3^n)^*$ satisfy

$$\begin{cases} b + b^{-1} = a^2 + 1, \\ u = a(b - b^{-1}), \end{cases} \tag{5}$$

and at least one of $a^2 - b$ and $a^2 - b^{-1}$ is a square in $\mathrm{GF}(3^n)^*$.

- $b + b^{-1} = a^2 + 1$ holds $\Leftrightarrow$ $a^2 - 1$ is a nonzero square.
- $\left(a^2 - b\right)\left(a^2 - b^{-1}\right) = -(a^2 - 1)$.
- $u = \pm a^2\sqrt{a^2 - 1}$.

The properties about the roots of $h_u(x)$

Proposition

- for each $u \in \mathrm{GF}(3^n) \setminus \mathrm{GF}(3)$, the possible number of roots of $h_u(x)$ in $\mathrm{GF}(3^n)$ are 0, 1, 2 and 4;.
- if η is a root of $h_u(x)$ in $\mathrm{GF}(3^n)$, then it has multiplicity 1 and belongs to $\mathrm{GF}(3^n) \setminus \mathrm{GF}(3)$;

The properties about the roots of $h_u(x)$

Proposition (continue)

- when $n > 1$ is odd, $h_u(x)$ cannot have four roots in $\mathrm{GF}(3^n)$ and in this case the number of $u \in \mathrm{GF}(3^n) \setminus \mathrm{GF}(3)$ such that $h_u(x)$ has two roots in $\mathrm{GF}(3^n)$ is equal to $\frac{3^n-3}{2}$;

- when n is even, $h_u(x)$ cannot have two roots in $\mathrm{GF}(3^n)$ and in this case the number of $u \in \mathrm{GF}(3^n) \setminus \mathrm{GF}(3)$ such that $h_u(x)$ has four roots in $\mathrm{GF}(3^n)$ is equal to $\frac{3^{n-1}-3}{4}$ if $n \equiv 2 \pmod 4$ and $\frac{3^{n-1}-11}{4}$ if $n \equiv 0 \pmod 4$.

The sketch of the proof

Determining the value $N(b)$ and its frequency: the number of solutions of $(x+1)^d - x^d = b$.

Key equation

$$(x+1)^d - x^d = b \Rightarrow (x+1)^{-2} - x^{-2} = b \;, b \in \mathrm{GF}(3^n) \setminus \mathrm{GF}(3)$$

$$\Rightarrow x^4 + 2x^3 + x^2 + \frac{2}{b}x + \frac{1}{b} = 0,\; x \longrightarrow x - \frac{1}{2}$$

$$\Rightarrow x^4 + x^2 - ux + 1 = 0,\; u = \frac{1}{b}. \tag{6}$$

- Find $N(0),\; N(-1),\; N(1)$.
- Find $N(b)$: the number of solutions of $x^4 + x^2 - ux + 1 = 0,\; u = \frac{1}{b}$ with $b \in \mathrm{GF}(3^n) \setminus \mathrm{GF}(3)$.

Some problems

- The differential spectrum of x^{p^n-3} when $p > 3$
- Find the differential spectra of other power mappings.
- Find the differential spectra of other mappings, which are not power mappings.
- Find the relationship between the differential spectrum and the nonlinearity of a function over finite fields.

Thank You for Your Attention!

[1] T. Helleseth, C. Rong, and D. Sandberg, "New Families of Almost Perfect Nonlinear Power Mappings," *IEEE Trans. Inf. Theory*, vol. 45, no. 2, pp. 475-485, Mar. 1999.

[2] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," *J. Cryptol.*, vol. 4, no. 1, pp. 3-72, 1991.

[3] K. Nyberg, "Differentially uniform mappings for cryptography," In: T. Helleseth (ed.) Advances in cryptology - EUROCRYPT'93. *Lecture Notes in Computer Science*, vol. 765, pp. 55-64. Berlin Heidelberg New York: Springer 1994.

[4] T. Storer, *Cyclotomy and difference sets.* Markham, Chicago, 1967.

[5] Kenneth S. Williams, "Note on cubics over $\mathrm{GF}(2^n)$ and $\mathrm{GF}(3^n)$," *Journal of Number Theory*, vol. 7, no. 4, pp. 361-365, Nov. 1975.

[6] R. Lidl and H. Niederreiter, "Finite Fields," in *Encyclopedia of Mathematics and Its Applications*, vol. 20. Amsterdam, The Netherlands: Addison-Wesley, 1983.

[7] C. Blondeau and L. Perrin, “More differentially 6-uniform power functions”, *Des. Codes Cryptogr.*, vol .73, pp. 487-505, 2014.

[8] M. Xiong and H. Yan, “A note on the differential specturm of a differentially 4-uniform power function,” *Finite Fields Appl.*, vol. 48, pp. 117-125, 2017.

[9] P. Charpin, G. Kyureghyan and V. Sunder, “Sparse permutations with low differential uniformity,” *Finite Fields Appl.*, vol. 28, pp. 214-243, 2014.

[10] P. Charpin, “Permutations with small differential uniformity,” *Finite Fields Appl.*, vol. 28, no. 1, pp. 79-92, 2015.

[11] S. T. Choi, S. Hong, J. S. No and H. Chung, “Differential spectrum of some power functions in odd prime characteristic,” *Finite Fields Appl.*, vol. 21, pp. 11-29, 2013.

[12] M. Xiong, H. Yan and P. Yuan,“On a conjecture of differenially 8-uniform power functions,” *Des. Codes Cryptogr.*, vol. 86, pp. 1601-1621, 2018.

[13] T. Helleseth and D. Sandberg,"Some Power Mapping with Low Differential Uniformity," *Applicable Algebra in Engineering, Communication and Computing.*, vol. 8, pp. 363-370, 1997.

[14] C. Blondeau, A. Canteaut and P. Charpin, "Differential Properties of $x \mapsto x^{2^t-1}$," *IEEE Trans. Inf. Theory*, vol. 57, no. 12, pp. 8127-8137, Dec. 2011.

[15] C. Blondeau, A. Canteaut and P. Charpin, "Differential properties of power functions," *Int. J. Information and Coding Theory*, vol. 1, no. 2, pp. 149-170, 2010.

[16] C. Bracken and G. Leander, "A highly nonlinear differentially 4-uniform power mapping that permutes fields of even degree," *Finite Fields Appl.*, vol. 16, no. 4, pp. 231-242, 2010.

[17] H. Yan, et al, "Differential spectrum of Kasami power permutations over odd characteristic finite fields," *IEEE Trans. Inf. Theory*, DOI 10.1109/TIT.2019.2910070, 2019.