On the Cycles Structure of Permutations Induced by the Perfect Nonlinear Functions over Finite Fields

Hassan Aly and Rasha Shaheen

Department of Mathematics,
Faculty of Science,
Cairo University,
Giza 12613, Egypt

Definitions

Throughout this talk $\mathbb{F}_q$ is the finite field of order $q = p^m$ where p is an odd prime and m is a positive integer.

Definition 1 *A function* $f : \mathbb{F}_q \longrightarrow \mathbb{F}_q$ *is said to be perfect nonlinear function, or shortly PNF, if*

$$\delta(x, a) = f(x + a) - f(x) - f(a)$$

is a permutation over $\mathbb{F}_q$ *for every* $a \in \mathbb{F}_q^*$.

Sometimes we call $\delta(x, a)$ as the difference function of f.

Definitions

Perfect Nonlinear Functions are used in different applications in

1. Cryptography
2. Coding
3. Finite Geometry, and
4. Combinatorial design

Some perfect nonlinear functions

1. $f_1(x) = x^2$ over $\mathbb{F}_{p^m}$,

Some perfect nonlinear functions

1. $f_1(x) = x^2$ over $\mathbb{F}_{p^m}$,
2. $f_2(x) = x^{p^k+1}$ over $\mathbb{F}_{p^m}$ where $m/\gcd(m,k)$ is odd and $k \leq m/2$,

Some perfect nonlinear functions

1. $f_1(x) = x^2$ over $\mathbb{F}_{p^m}$,

2. $f_2(x) = x^{p^k+1}$ over $\mathbb{F}_{p^m}$ where $m/\gcd(m,k)$ is odd and $k \leq m/2$,

3. $f_3(x) = x^{10} - x^6 - x^2$ over $\mathbb{F}_{3^m}$ where $m \geq 5$ is odd,

Some perfect nonlinear functions

1. $f_1(x) = x^2$ over $\mathbb{F}_{p^m}$,
2. $f_2(x) = x^{p^k+1}$ over $\mathbb{F}_{p^m}$ where $m/\gcd(m,k)$ is odd and $k \leq m/2$,
3. $f_3(x) = x^{10} - x^6 - x^2$ over $\mathbb{F}_{3^m}$ where $m \geq 5$ is odd,
4. $f_4(x) = x^{10} + x^6 - x^2$ over $\mathbb{F}_{3^m}$ where $m \geq 5$ is odd.

The diference functions

1. $\delta_1(x, a) = 2ax$ over $\mathbb{F}_{p^m}$,

The diference functions

1. $\delta_1(x,a) = 2ax$ over $\mathbb{F}_{p^m}$,
2. $\delta_2(x,a) = ax^{p^k} + a^{p^k}x$ over $\mathbb{F}_{p^m}$ where $m/\gcd(m,k)$ is odd and $k \leq m/2$,

The diference functions

1. $\delta_1(x,a) = 2ax$ over $\mathbb{F}_{p^m}$,

2. $\delta_2(x,a) = ax^{p^k} + a^{p^k}x$ over $\mathbb{F}_{p^m}$ where $m/\gcd(m,k)$ is odd and $k \leq m/2$,

3. $\delta_3(x,a) = ax^9 + a^3x^3 + (a^9 + a)x$ over $\mathbb{F}_{3^m}$ where $m \geq 5$ is odd,

The diference functions

1. $\delta_1(x,a) = 2ax$ over $\mathbb{F}_{p^m}$,
2. $\delta_2(x,a) = ax^{p^k} + a^{p^k}x$ over $\mathbb{F}_{p^m}$ where $m/\gcd(m,k)$ is odd and $k \leq m/2$,
3. $\delta_3(x,a) = ax^9 + a^3x^3 + (a^9 + a)x$ over $\mathbb{F}_{3^m}$ where $m \geq 5$ is odd,
4. $\delta_4(x,a) = ax^9 - a^3x^3 + (a^9 + a)x$ over $\mathbb{F}_{3^m}$ where $m \geq 5$ is odd.

Objectives

This talk is about some properties of the difference permutations δ_1, δ_2, δ_3, and δ_4. We will

1. count the number of fixed points of these permutations.

Objectives

This talk is about some properties of the difference permutations δ_1, δ_2, δ_3, and δ_4. We will

1. count the number of fixed points of these permutations.
2. count the number of cycles of each permutation and their lengthes for values of a in the prime finite field.

Objectives

This talk is about some properties of the difference permutations δ_1, δ_2, δ_3, and δ_4. We will

1. count the number of fixed points of these permutations.
2. count the number of cycles of each permutation and their lengthes for values of a in the prime finite field.
3. discuss cases have the same number of cycles of the same lengthes.

Objectives

This talk is about some properties of the difference permutations δ_1, δ_2, δ_3, and δ_4. We will

1. count the number of fixed points of these permutations.
2. count the number of cycles of each permutation and their lengthes for values of a in the prime finite field.
3. discuss cases have the same number of cycles of the same lengthes.
4. introduce some notes on other PNF and further work in this direction.

Fixed Points

A fixed point of a permutation $\pi(x)$ over $\mathbb{F}_q$ is a point c in $\mathbb{F}_q$ such that $\pi(c) = c$. It is easy to see that the permutation $\delta_1(x, a) = 2ax$ has

$$Fix(\delta_1(x,a)) = \begin{cases} q & : \quad \text{if } a = \frac{1}{2} \\ 1 & : \quad \text{otherwise} \end{cases}$$

Fixed Points

Theorem 2 *The number of fixed points of the permutations* $\delta_2(x,a) = ax^{p^k} + a^{p^k}x$ *for* $a \in \mathbb{F}_q^*$ *is given by*

$$Fix(\delta_2(x,a)) = \begin{cases} p^d & : \quad \textit{if } (p^k-1)|j \\ 1 & : \quad \textit{otherwise} \end{cases}$$

where $d = \gcd(k,m)$, *and* j *is the unique integer such that* $0 \le j \le q-2$ *and* $r = \omega^j$ *with* ω *a primitive element of* $\mathbb{F}_q$ *and* $r = \frac{1-a^{p^k}}{a}$.

Proof

The assertion is obvious for $a = 1$. For $a \neq 1$, we have

$$ax^{p^k} + (a^{p^k} - 1)x = 0.$$

It is obvious that $x = 0$ is a solution of the above equation. For $x \neq 0$ the above equation becomes $x^{p^k - 1} = r$, where $r = \frac{1 - a^{p^k}}{a} \neq 0$. If ω is a primitive element of $\mathbb{F}_q$ and $r = w^j$ for some j, $0 \leq j \leq q - 2$, then we have $w^{i(p^k - 1)} = w^j$ which implies that $i(p^k - 1) \equiv j \bmod (q - 1)$, which has exactly $\gcd(p^k - 1, p^m - 1) = p^{\gcd(k,m)} - 1$ solutions if and only if $p^k - 1$ divides j.

Fixed Points

The number of fixed points of the permutations $\delta_3(x,a) = ax^9 + a^3x^3 + (a^9+a)x$ for $a \in \mathbb{F}_q^*$ is given by

$$Fix(\delta_2(x,a)) = \begin{cases} 1 & : \\ 3 & : \\ 9 & : \end{cases}$$

depending on the number of solutions of the equation $ax^9 + a^3x^3 + (a^9 + a - 1)x = 0.$

Fixed Points

The number of fixed points of the permutations $\delta_3(x,a) = ax^9 - a^3x^3 + (a^9+a)x$ for $a \in \mathbb{F}_q^*$ is given by

$$Fix(\delta_2(x,a)) = \begin{cases} 1 & : \\ 3 & : \\ 9 & : \end{cases}$$

depending on the number of solutions of the equation $ax^9 - a^3x^3 + (a^9+a-1)x = 0$.

Remark

If $f_5(x) = x^n$, where $n = \frac{3^k+1}{2}$ the Coulter-Mattews perfect nonlinear function, where k is odd, $\gcd(k, m) = 1$. and $p = 3$. Computations show that the difference permutation function

$$\delta_5(x, 1) = (x + 1)^n - x^n$$

has exactly 1 or 3 fixed points for many values of k. But we have no proof of it up till now.

On the cycles structure of the permutation polynomials $\delta_1, \delta_2, \delta_3$, and δ_4.

Cycles of δ_1

Cycles of δ_1

- If $a = \frac{1}{2}$, all cycles of length one and the total number of cycles is p^n .

- If $a \neq \frac{1}{2}$, one cycle of length 1 and all other cycles of length $ord(2a)$ and the total number of cycles is $\frac{p^{n-1}}{ord(2a)} + 1$.

Cycles of δ_1

- If $a = \frac{1}{2}$, all cycles of length one and the total number of cycles is p^n .

- If $a \neq \frac{1}{2}$, one cycle of length 1 and all other cycles of length $ord(2a)$ and the total number of cycles is $\frac{p^{n-1}}{ord(2a)} + 1$.

Examples

a	**Cycle Length**	**# Cycles**
1	1	1
	3	274514
4	1	823543
5	1	1
	6	137257

Table 1: The cycle structure of $2ax$ over $\mathbb{F}_{7^7}$

Cycles of $\delta_2, \delta_3, \delta_4$

Let $L(x) \in \mathbb{F}_q[x]$ be a linearized polynomial on the form

$$(1) \qquad L(x) = \sum_{i=0}^{m-1} a_i x^{p^i}$$

where each $a_i \in \mathbb{F}_p$ and $m > 1$. Consider the operator $T : x \longrightarrow x^p$ defined on $\mathbb{F}_{p^m}$. Let $h(x) = \sum_{i=0}^{m-1} a_i x^i$ with $a_i \in \mathbb{F}_p$. Then $L(x)$ given in (1) can be written in the form $L(x) = h(T)(x)$, where $h(T)(x) = \left(\sum_{i=0}^{n-1} a_i T^i\right)(x) = \sum_{i=0}^{n-1} a_i T^i(x)$ and $T^i(x)$ is the composition of $T^i(x)$ with itself i times.

Cycles of $\delta_2, \delta_3, \delta_4$

It is known that a subspace W of $\mathbb{F}_{p^m}$ is said to be T-invarient subspace if $T(W) \subseteq W$. W is T-invarient subspace of $\mathbb{F}_{p^m}$ if and only if $W = \ker g(T)$ the kernal of $g(T)$, where $g(x) \in \mathbb{F}_p[x]$, $g(x)|x^m - 1$, and $\dim W$= degree $g(x)$.

Cycles of $\delta_2, \delta_3, \delta_4$

Consider the canonical factorization of $x^m - 1$ as

$$x^m - 1 = (x^{m_1} - 1)^{p^t} = \prod_{i=1}^{l} g_i(x)^{p^t},$$

where $m = p^t m_1$ with $(m_1, p) = 1$ and $g_i(x)$ is an irreducible polynomial over $\mathbb{F}_p$ of degree k_i. Set $W_i = \ker(g_i(T))$ and $W_i^{(j)} = \ker(g_i(T)^j)$, then we have

(2) $$\mathbb{F}_{p^m} = \bigoplus_{i=1}^{l} W_i^{(p^t)}$$

Cycles of $\delta_2, \delta_3, \delta_4$

Require: The linearized permutation polynomial $L(x) = \sum_{i=0}^{n-1} a_i x^{p^i}, \ a_i \in \mathbb{F}_p$.

Cycles of $\delta_2, \delta_3, \delta_4$

Require: The linearized permutation polynomial $L(x) = \sum_{i=0}^{n-1} a_i x^{p^i},\ a_i \in \mathbb{F}_p$.

Ensure: The lengths and the numbers of the cycles for each W_i, the T-invarient subspace of $\mathbb{F}_{p^m}$ with $\gcd(p, m) = 1$.

Cycles of $\delta_2, \delta_3, \delta_4$

1: Define $h(x) = \sum_{i=0}^{m-1} a_i x^i$.

2: Factorize $(x^m - 1)$ as $(x^m - 1) = \prod_{i=0}^{l} g_i(x)$, where each $g_i(x)$ is an irreducible polynomial over $\mathbb{F}_p$ with degree k_i.

3: **for** $i = 1$ to l **do**

4:    Find a root ω of $g_i(x)$ in $\mathbb{F}_{p^{k_i}}$.

5:    Calculate $h(\omega)$ in $\mathbb{F}_{p^{k_i}}$.

6:    Find j_i the multiplicative order of $h(\omega)$ in $\mathbb{F}_{p^{k_i}}$ which is the cycle length.

7:    Calculate $c_i = \frac{p^{k_i}-1}{j_i}$ which is the number of the cycles of length j_i.

8: **end for**

9: **return** all j_i's and c_i's.

Magma program

```
/* cycles structure Algorithm 1 */
algorithm1:=procedure(p,n)
g<w>:=GF(p,n);
L<x>:=PolynomialRing(GF(p));
h<x>:=PolynomialRing(GF(p));
printf"Enter the coefficient of h(x) a0.....a%o\n",n-1;
s:=[];
for i:= 0 to n-1 do
printf "a%o=",i;
readi a;
Append(~s,a);
end for;
h:=h!s;
h;
g:={@f[1]:f in Factorization(x^n-1 )@};
j:=AssociativeArray();
c:=AssociativeArray();
for i:=1 to #g do
k:=Degree(g[i]);
w:={@r[1] : r in Roots(g[i],GF(p,k))@};
hw:=Evaluate(h,w[1]);
j[i]:=Order(hw);
c[i]:=(p^k-1)/j[i];
printf "j%o=%o c%o=%o \n", i,j[i],i,c[i];
end for;
end procedure;
```

Examples for δ_2

$\mathbb{F}_p^n$	**a**	**k**	**Cycle Length**	**# Cycles**
$\mathbb{F}_{3^{10}}$	1	2	1	1
			2	4
			40	1476
$\mathbb{F}_{7^5}$	5	3	1	1
			6	1
			240	70
$\mathbb{F}_{11^3}$	10	2	1	1
			3	40
			5	2
			15	80

Table 2: The cycles structure of $ax^{p^k} + a^{p^k}x$.

Examples for δ_3 and δ_4

Dif. Function	a	Cycle Length	# Cycles
$\delta_4 = ax^9 - a^3x^3 + a(a^8+1)x$	1	1	1
		2	1
		6	4
		18	1092
	-1	1	3
		3	8
		9	2184
$\delta_3 = ax^9 + a^3x^3 + a(a^8+1)x$	1	1	9
		3	240
		9	2106
	-1	1	1
		2	4
		6	120
		18	1053

Table 3: The cycles structure of $ax^9 \mp a^3x^3 + a(a^8+1)x$.

Cycles of $\delta_2, \delta_3, \delta_4$

Now any element $\alpha \in \mathbb{F}_q$ can be uniquely represented as

$$\alpha = \alpha_1 + \alpha_2 + \ldots + \alpha_l,$$

where $\alpha_i \in W_i$ and the length of the cycle that contains α can be determined as

$$|C(\alpha)| = lcm(j_1, j_2, \ldots, j_l). \tag{3}$$

Notice that if $\alpha_i = 0$ for some element $\alpha \in \mathbb{F}_q$, then $j_i = 1$ in this case.

cases have the same number of cycles of the same length

Definition 3 *L_1 and L_2 are said to be equivalent if as permutations they have the same number of cycles of the same length over $\mathbb{F}_{p^m}$, we write $L_1 \sim L_2$.*

Definition 4 *L_1 and L_2 are said to be strongly equivalent if for every T-invarient subspace W of $\mathbb{F}_p^m$, the restrictions $L_1|W$ and $L_2|W$ induce the same number of cycles of the same length in W. This is denoted by $L_1 \approx L_2$.*

cases have the same number of cycles of the same length

In this case $\delta_1(x, a)$ have the same number of cycles of the same length for different values of a have the same $ord(2a)$.

cases have the same number of cycles of the same length

Theorem 5 *Let* $L_1(x) = x^{p^{s_1}} + x$ *and* $L_2(x) = x^{p^{s_2}} + x$*. If* $s_1 \equiv p^s s_2 \pmod{n}$*, for some* $0 \leq s \leq m-1$ *then* $L_1(x)$ *is strongly equivalent to* $L_2(x)$ *over* $\mathbb{F}_{p^m}$*.*

Example

Over $\mathbb{F}_{57}$

Example

Over $\mathbb{F}_{57}$

the permutations $x^{25} + x$ and $x^{125} + x$

Example

Over $\mathbb{F}_{5^7}$

the permutations $x^{25} + x$ and $x^{125} + x$

splits up the finite field into

Example

Over $\mathbb{F}_{5^7}$

the permutations $x^{25} + x$ and $x^{125} + x$

splits up the finite field into

1 cycle of length 1
1 cycle of length 4
72 cycles of length 217
72 cycles of length 868

Example

Over $\mathbb{F}_{5^7}$

the permutations $x^{25} + x$ and $x^{125} + x$

splits up the finite field into

1 cycle of length 1
1 cycle of length 4
72 cycles of length 217
72 cycles of length 868

cases have the same number of cycles of the same lengthes

Theorem 6 *Let* $L(x) = ax^9 \mp a^3x^3 + a(a^8+1)x$,*where* $a \in \{1, -1\}$. *If* $m = 3^k$ *then the cycles lengthes are* $2^i.3^j$ *where*

$$i = \begin{cases} 0 & L(1) = 1, \\ 1 & L(1) = -1. \end{cases}$$

and $j = 0, 1, \ldots, k$.

Further work

Study the same for the CM function:

$f(x) = x^{(3^k+1)/2}$ over $\mathbb{F}_{3^m}$ where $\gcd(n,k) = 1$ and $k \geq 3$ is odd,

Further work

Let $f(x) = x^n$ be a perfect nonlinear function over $\mathbb{F}_q$.
Let $\delta(x, a) = (x + a)^n - x^n$ be its permutation.
1. How many fixed points are there for δ?
2. What about the cycles structure of δ?