On Alltop functions

Fuad Hamidli, Ferruh Özbudak

Middle East Technical University

July 7, 2017

OUTLINE

1. Introduction and basic definitions

2. Alltop Functions
   - results by Hall,Rao, Donovan-2012
   - results by Hall,Rao, Gagola-2013

3. Classification
   - Over $\mathbb{F}_{q^2}$
   - Over $\mathbb{F}_{q^3}$

4. p-ary Alltop Functions

Definition

Let p be an odd prime and $\mathbf{F} = \mathbb{F}_{p^n}$. Derivative of a function f at a point $a \in \mathbf{F}$ is defined as

$$D_a f(x) = f(x+a) - f(x)$$

$f : \mathbf{F} \to \mathbf{F}$ is called a planar function or perfectly nonlinear (PN) if for each $a \neq 0$,

$$D_a f(x)$$

is bijective.

Definition

Two functions $f, g : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ are EA-equivalent (extended affine) if there are two linearized permutation polynomials L_1 and L_2 and an affine polynomial L_3 such that

$$g = L_1 \circ f \circ L_2 + L_3$$

which defines an equivalence relation.

Definition

A Dembowski-Ostrom polynomial (quadratic polynomial) is a polynomial $f(x) \in \mathbb{F}_{p^n}[x]$ with the shape

$$f(x) = \sum_{i,j=0}^{n-1} a_{ij} x^{p^i + p^j}$$

with $a_{ij} \in \mathbb{F}_{p^n}$

Alltop Functions

Definition

Let p be an odd prime. A function $f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ is called an Alltop function if $D_a f(x) = f(x+a) - f(x)$ is planar for all $a \in \mathbb{F}_{p^n}^*$
Equivalently, $f(x)$ is an Alltop function if
$D_b D_a f(x) = f(x+a+b) - f(x+a) - f(x+b) + f(x)$ is permutation for all $a, b \in \mathbb{F}_{p^n}^*$

Example

x^3 is an Alltop function over $\mathbb{F}_{p^n}$ for an odd prime $p > 3$, $n \geq 1$.
This was the only known one up to 2013.

Theorem

There are no Alltop type polynomials over $\mathbb{F}_{3^n}$.
(Hall, Rao, Donovan, 2012)

Theorem

(New result by Hall, Rao, Gagola, 2013) Let $p \geq 5$ be an odd prime and n an integer such that 3 does not divide $p^n + 1$. Then $f(x) = x^{p^n+2}$ is an Alltop polynomial on $\mathbb{F}_{p^{2n}}$.

Over $\mathbb{F}_{q^2}$

Let $q = p^n$, for p prime, n positive integer.
All inequivalent cubic q-monomials over $\mathbb{F}_{q^2}$**:**

- x^3- Alltop in everywhere (Alltop, 1980)
- x^{q+2}- Alltop if and only if 3 does not divide $q + 1$ (2013, Hall, Rao, Gagola)

Over $\mathbb{F}_{q^2}$

All inequivalent cubic q-binomials over $\mathbb{F}_{q^2}$:

- 1) $x^3 + cx^{3q}$- Alltop if and only if c is not $q-1$ power
- 2)$x^{q+2} + cx^{2q+1}$- Alltop if and only if c is not a $q-1$ power and 3 does not divide $q+1$
- 3) $x^3 + cx^{2q+1}$:(MAGMA Calculations)
  Alltop when $q = 5$ and c=2, ω^{14}, ω^{22} (Equivalent to x^3 in all cases)
  Alltop when $q = 7$ and c = ω^2, ω^6, ω^{14}, ω^{18}, ω^{26}, ω^{30}, ω^{38}, ω^{42} (Equivalent to either x^3 or x^{7+2})
- 4) $x^3 + cx^{q+2}$:
  Not Alltop when $q = 5, 7, 11, 13$ (MAGMA calculations)

Over $\mathbb{F}_{q^2}$

Theorem: Let $f(x) = x^3 + ux^{2q+1}$ from $\mathbb{F}_{q^2}$ to itself, where $u \in \mathbb{F}^*_{q^2}$ and let ω be a cyclic generator of a field $\mathbb{F}_{q^2}$.
a) there exist maps $L_1(x) = ax + bx^q$ and $L_2(x) = cx + dx^q$ in $\mathbb{F}_{q^2}$ such that $L_1 \circ x^3 \circ L_2 = f(x)$ if and only if $u = 3\omega^{k(1-q)}$ for any odd integer $k \in [1, 2, 3, ..., q+1]$
b) there exist maps $L_1(x) = ax + bx^q$ and $L_2(x) = cx + dx^q$ in $\mathbb{F}_{q^2}$ such that $L_1 \circ x^{q+2} \circ L_2 = f(x)$ if and only if $u = \omega^{k(1-q)}$ for any odd integer $k \in [1, 2, 3, ..., q+1]$

Over $\mathbb{F}_{q^2}$

Corollary: Let $f(x) = x^3 + ux^{2q+1}$ from $\mathbb{F}_{q^2}$ to itself, where $u \in \mathbb{F}^*_{q^2}$ and let ω be a cyclic generator of a field $\mathbb{F}_{q^2}$.
a) if $u = 3\omega^{n(1-q)}$ for any odd integer $n \in [1, 2, ..., q+1]$ then f is an Alltop function, which is EA-equivalent to x^3.
b) if $u = \omega^{n(1-q)}$ for any odd integer $n \in [1, 2, ..., q+1]$ and 3 does not divide $q+1$, then f is an Alltop function, which is EA-equivalent to x^{q+2}.

Over $\mathbb{F}_{q^3}$

Theorem

Except x^3 and its EA-equivalence class, there is no Alltop cubic q-monomials in $\mathbb{F}_{q^3}$.

- x^3
- x^{q+2} *-not Alltop*
- x^{2q+1} *-not Alltop*
- x^{q^2+q+1} *-not Alltop*

Over $\mathbb{F}_{q^3}$

All inequivalent cubic q-binomials over $\mathbb{F}_{q^3}$:

- 1) $x^3 + cx^{q+2}$ - Not Alltop for $q = 5, 7$
- 2) $x^3 + cx^{q^2+2}$ - Not Alltop for $q = 5, 7$
- 3) $x^3 + cx^{2q+1}$ - Not Alltop for $q = 5, 7$
- 4) $x^3 + cx^{q^2+q+1}$ - Not Alltop for $q = 5, 7$
- 5) $x^3 + cx^{2q^2+1}$ - Not Alltop for $q = 5, 7$

Over $\mathbb{F}_{q^3}$

All inequivalent cubic q-binomials over $\mathbb{F}_{q^3}$:

- 6) $x^3 + cx^{3q}$ - Alltop if and only if c is not $q-1$ power, EA-equivalent to x^3.
- 7) $x^3 + cx^{q^2+2q}$ - Not Alltop for $q = 5, 7$
- 8) $x^3 + cx^{2q^2+q}$ - Not Alltop for $q = 5, 7$
- 9) $x^{q+2} + cx^{q^2+2}$ - Not Alltop for $q = 5, 7$
- 10) $x^{q+2} + cx^{2q+1}$ - Not Alltop for $q = 5, 7$

Over $\mathbb{F}_{q^3}$

All inequivalent cubic q-binomials over $\mathbb{F}_{q^3}$:

- 11) $x^{q+2} + cx^{q^2+q+1}$ - Not Alltop for $q = 5, 7$
- 12) $x^{q+2} + cx^{2q^2+1}$ - Not Alltop for $q = 5, 7$
- 13) $x^{q+2} + cx^{2q^2+q}$ - Not Alltop for $q = 5, 7$
- 14) $x^{q^2+2} + cx^{2q+1}$ - Not Alltop for $q = 5, 7$
- 15) $x^{q^2+2} + cx^{q^2+q+1}$ - Not Alltop for $q = 5, 7$

p-ary Alltop Functions

Definition

1)Let p be an odd prime, $n > 0$ and f be a function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$. f is called p-ary bent (perfectly nonlinear) if $D_a f(x) = f(x+a) - f(x)$ is balanced for any $a \in \mathbb{F}^*_{p^n}$.

Definition

2)(New) f is called p-ary Alltop if $D_a f(x)$ is p-ary bent for any $a \in \mathbb{F}^*_{p^n}$, that is $D_b(D_a(f(x)))$ is balanced for any $a, b \in \mathbb{F}^*_{p^n}$.

Observation: $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ is p-ary Alltop if and only if

$$\sum_{x \in \mathbb{F}_{p^n}} \epsilon_p^{D_b D_a f(x)} = 0,$$

for all $a, b \in \mathbb{F}^*_{p^n}$, where ϵ_p is a p-th root of unity in $\mathbb{F}_{p^n}$.

Characterizations of cubic p-ary Alltop functions

Let f be an arbitrary cubic function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$. Then f can be written as

$$f(x) = Tr^n(xD(x)) + Tr^n(xA(x)) + \alpha(x),$$

where $D(x)$ is Dembowski-Ostrom polynomial, $A(x)$ is a linearized polynomial given by

$$A(x) = \sum_{0 \leq i \leq n-1} a_i x^{p^i}$$

with $a_i \in \mathbb{F}_{p^n}$ and $\alpha(x)$ is an affine polynomial for $x \in \mathbb{F}_{p^n}$.

Characterizations of cubic p-ary Alltop functions

Let $B : \mathbb{F}_{p^n} \times \mathbb{F}_{p^n} \to \mathbb{F}_p$ be the quadratic map depending on D defined as

$$B(x, y) = D(x + y) - D(x) - D(y)$$

for $x, y \in \mathbb{F}_{p^n}$. For $a, b \in \mathbb{F}_{p^n}$, let

$$L_{a,b,B}f(x) = Tr^n(xB(a, b)) + Tr^n(aB(x, b)) + Tr^n(bB(x, a))$$

for every $x \in \mathbb{F}_{p^n}$.
For $a, b \in \mathbb{F}_{p^n}$ let $C_{a,b,d}$ and $C_{a,b,A}$ be the constant functions from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ defined as

$$C_{a,b,D} = Tr^n(aB(a, b)) + Tr^n(bB(a, b)) + Tr^n(aD(b)) + Tr^n(bD(a))$$

$$C_{a,b,A} = Tr^n(aA(b)) + Tr^n(bA(a))$$

Characterizations of cubic p-ary Alltop functions

Lemma (Mesnager, Özbudak, Sinak)

Let f be an arbitrary cubic function in the form $f(x) = Tr^n(xD(x)) + Tr^n(xA(x)) + \alpha(x)$. The second order derivative of f at $(a, b) \in \mathbb{F}_{p^n}^2$ is the affine function defined as

$$D_b D_a f(x) = L_{a,b,B} f(x) + C_{a,b,D} + C_{a,b,A}$$

for $x \in \mathbb{F}_{p^n}$.

Result 1: $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ is a p-ary Alltop function if and only if

$$\sum_{x \in \mathbb{F}_{p^n}} \epsilon_p^{L_{a,b,B} f(x)} = 0$$

Let $S = \{(a, b) : L_{a,b,B} f(x) = 0$, for any $x \in \mathbb{F}_{p^n}\}$
Result 2: $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ is p-ary Alltop function if and only if

$$S = \{(o, y) : y \in \mathbb{F}_{p^n}\} \cup \{(x, 0) : x \in \mathbb{F}_{p^n}\}$$

Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ so that $f(x) = Tr(F(x))$, where $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ is a cubic function.

Example

1. $F(x) = x^3, f(x) = Tr(x^3)$
Then $D(x) = x^2, B(x, y) = 2xy$ and
$L_{a,b,B}f(x) = Tr(x2ab) + Tr(a2bx) + Tr(b2ax) = 6Tr(abx)$
When $p \neq 3$, f is a p-ary Alltop function.

Example

2. $n = 2, F(x) = x^{p+2}$ and $f(x) = Tr(x^{p+2})$. Then
$D(x) = x^{p+1}, B(x, y) = xy^p + x^p y$ and

$$L_{a,b,B}f(x) = Tr(x(a^p b + ab^p)) + Tr(a(x^p b + xb^p))) + Tr(b(a^p x + ax^p))$$

After simplifications,

$$L_{a,b,B}f(x) = Tr(2x(ab^p + a^p b + a^{1/p} b^{1/p}))$$

f is p-ary Alltop if and only if $ay^p + a^p y + ay$ has no nonzero solution y in $\mathbb{F}_{p^2}$. If 3 does not divide $p + 1$, then condition is satisfied and f is p-ary Alltop. In this case F will be Alltop in $\mathbb{F}_{p^2}$.

Example

3. Let $F(x) = x^3 + cx^{2p+1}$, $f(x) = Tr(F(x))$ where $c \in \mathbb{F}_{p^n}$ and ω is a cyclic generator of a field $\mathbb{F}_{p^n}$

- If $n = 2$, $p = 5$, $c = \omega^{13}$ then $f(x)$ is p-ary Alltop but $F(x)$ is not Alltop.
- If $n = 3$, $p = 7$, $c = \omega^{49}$ then $f(x)$ is p-ary Alltop but $F(x)$ is not Alltop.

Theorem

Let $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ be any function and $f_\alpha : \mathbb{F}_{p^n} \to \mathbb{F}_p$ be defined as $f_\alpha(x) = Tr(\alpha F(x))$ for any $\alpha \in \mathbb{F}^*_{p^n}$. Then F is Alltop if and only if f_α is p-ary Alltop for any $\alpha \in \mathbb{F}^*_{p^n}$.

THANK YOU!