Generalized APN Functions Of The Lowest Algebraic Degree

Noureddine El-Asri
(Joint work with Valentin Suder)

Rouen Normandie University, France
noureddine.el-asri1@univ-rouen.fr
valentin-suder@univ-rouen.fr

Discrete derivatives and APN funtions

- $F(x) = \sum_{i=0}^{2^n-1} c_i x^i$ a function over $\mathbb{F}_{2^n}$.
- $\alpha \in \mathbb{F}_{2^n}^*$.
- $\Delta_\alpha F(x) := F(x+\alpha) - F(x)$ (Discrete derivative of F in direction α).

Discrete derivatives and APN funtions

- $F(x) = \sum_{i=0}^{2^n-1} c_i x^i$ a function over $\mathbb{F}_{2^n}$.
- $\alpha \in \mathbb{F}_{2^n}^*$.
- $\Delta_\alpha F(x) := F(x+\alpha) - F(x)$ (Discrete derivative of F in direction α).

Almost Perfect Nonlinear (APN) functions

F is APN over $\mathbb{F}_{2^n}$ if the equation

$$\Delta_\alpha F(x) = \beta$$

has at most 2 solutions in $\mathbb{F}_{2^n}$ for all $\alpha, \beta \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}$.

Generalization to odd characteristic

- p a prime number.
- $n \geq 1$ an integer.
- $F(x) = \sum_{i=0}^{p^n-1} c_i x^i$ is a function over $\mathbb{F}_{p^n}$.

Generalization to odd characteristic

- p a prime number.
- $n \geq 1$ an integer.
- $F(x) = \sum_{i=0}^{p^n-1} c_i x^i$ is a function over $\mathbb{F}_{p^n}$.

Generalized APN (GAPN) (Kuroda and Tsujie 2016)

F is said to be generalized APN (GAPN) if the equation

$$\sum_{i \in \mathbb{F}_p} F(x + i\alpha) = \beta$$

has at most p solutions in $\mathbb{F}_{p^n}$ for all $\alpha, \beta \in \mathbb{F}_{p^n}^* \times \mathbb{F}_{p^n}$.

Generalization to odd characteristic

- p a prime number.
- $n \geq 1$ an integer.
- $F(x) = \sum_{i=0}^{p^n-1} c_i x^i$ is a function over $\mathbb{F}_{p^n}$.

Generalized APN (GAPN) (Kuroda and Tsujie 2016)

F is said to be generalized APN (GAPN) if the equation

$$\sum_{i \in \mathbb{F}_p} F(x + i\alpha) = \beta$$

has at most p solutions in $\mathbb{F}_{p^n}$ for all $\alpha, \beta \in \mathbb{F}_{p^n}^* \times \mathbb{F}_{p^n}$.

$p = 2$

- $\sum_{i \in \mathbb{F}_p} F(x + i\alpha) = F(x + \alpha) + f(x) = F(x + \alpha) - f(x) = \Delta_\alpha F(x)$.
- GAPN = APN.

Generalized derivative

Generalized derivative (Ozbudak and Salagean 2021)

For $\alpha \in \mathbb{F}_{p^n}^*$,

$$\sum_{i \in \mathbb{F}_p} F(x + i\alpha) = (\Delta_\alpha)^{(p-1)} F(x).$$

Generalized derivative

Generalized derivative (Ozbudak and Salagean 2021)

For $\alpha \in \mathbb{F}_{p^n}^*$,

$$\sum_{i \in \mathbb{F}_p} F(x + i\alpha) = (\Delta_\alpha)^{(p-1)} F(x).$$

$$\nabla_\alpha F(x) := \sum_{i \in \mathbb{F}_p} F(x + i\alpha)$$

is the generalized derivative of F in the direction α.

Algebraic degree and GAPN-ness

Algebraic degree

The algebraic degree of $F(x) = \sum_{i=0}^{p^n-1} c_i x^i$ is defined by:

$$\deg_A(F) := \max \left\{ \sum_{u=0}^{n-1} a_u \mid 0 \le a_u < p, \quad c_{\sum_{u=0}^{n-1} a_u p^u} \neq 0 \right\}.$$

Algebraic degree and GAPN-ness

Algebraic degree

The algebraic degree of $F(x) = \sum_{i=0}^{p^n-1} c_i x^i$ is defined by:

$$\deg_A(F) := \max \left\{ \sum_{u=0}^{n-1} a_u \mid 0 \leq a_u < p, \quad c_{\sum_{u=0}^{n-1} a_u p^u} \neq 0 \right\}.$$

Proposition

$\forall \alpha \in \mathbb{F}_{p^n}^*$,

$$deg_A(\nabla_\alpha F) \leq deg_A(F) - (p-1).$$

In particular, if $deg_A(F) = p$ then, $\forall \alpha \in \mathbb{F}_{p^n}^*, \quad deg_A(\nabla_\alpha F) \leq 1$.

Algebraic degree and GAPN-ness

Algebraic degree

The algebraic degree of $F(x) = \sum_{i=0}^{p^n-1} c_i x^i$ is defined by:

$$\deg_A(F) := \max \left\{ \sum_{u=0}^{n-1} a_u \mid 0 \leq a_u < p, \quad c_{\sum_{u=0}^{n-1} a_u p^u} \neq 0 \right\}.$$

Proposition

$\forall \alpha \in \mathbb{F}_{p^n}^*$,

$$deg_A(\nabla_\alpha F) \leq deg_A(F) - (p-1).$$

In particular, if $deg_A(F) = p$ then, $\forall \alpha \in \mathbb{F}_{p^n}^*, \quad deg_A(\nabla_\alpha F) \leq 1$.

Proposition (Kuroda and Tsujie 2016)

If F is GAPN over $\mathbb{F}_{p^n}$, then $deg_A(F) \geq p$.

Generalized Dembowski Ostrom polynomials (GDO)

Definition

We call Generalized Dembowski-Ostrom (GDO) polynomials, homogeneous polynomials of algebraic degree p:

$$F(x) = \sum_i f_i x^i \in \mathbb{F}_{p^n}[x]$$

.

Contents

$F(x) = x^e$ over $\mathbb{F}_{p^n}$ where

$F(x) = x^e$ over $\mathbb{F}_{p^n}$ where

$$e = \sum_{i=0}^{\ell} k_i p^i, \quad 0 \le k_i \le p-1, \qquad \sum_{i=0}^{\ell} k_i = p, \quad \forall 0 \le i \le \ell$$

$F(x) = x^e$ over $\mathbb{F}_{p^n}$ where

$$e = \sum_{i=0}^{\ell} k_i p^i, \quad 0 \le k_i \le p-1, \qquad\qquad \sum_{i=0}^{\ell} k_i = p, \quad \forall 0 \le i \le \ell$$

Example ($p = 5$)

- $$F(x) = x^{3 \times 5^2 + 1 \times 5^1 + 1 \times 5^0}$$

$F(x) = x^e$ over $\mathbb{F}_{p^n}$ where

$$e = \sum_{i=0}^{\ell} k_i p^i, \quad 0 \le k_i \le p-1, \qquad \sum_{i=0}^{\ell} k_i = p, \quad \forall 0 \le i \le \ell$$

Example ($p = 5$)

- $$F(x) = x^{3\times 5^2 + 1\times 5^1 + 1\times 5^0}$$
- $\forall \alpha \in \mathbb{F}_{5^n}^*$ $(n \ge 3)$

$$\begin{aligned}\nabla_\alpha F(x) &= -3\alpha^{3\times 5^2+1\times 5^1+1\times 5^0-5^2} x^{5^2} - 1\alpha^{3\times 5^2+1\times 5+1\times 5^0-5^1} x^{5^1} - 1\alpha^{3\times 5^2+1\times 5+1\times 5^0-5^0} x^{5^0}\\ &= -3\alpha^{56} x^{5^2} - 1\alpha^{76} x^5 - 1\alpha^{80} x\end{aligned}$$

Theorem (Ozbudak and Salagean 2021)

A monomial GDO $F(x) = x^e$ where $e = \sum_{i=0}^{\ell} k_i p^i$ is GAPN over $\mathbb{F}_{p^n}$ if and only if

$$gcd(\sum_{i=0}^{\ell} k_i z^i, z^n - 1) = x - 1 \quad \text{in} \quad \mathbb{F}_p[z].$$

Facts

- We know that $z^n - 1 = (z-1)^{p^m} \prod_{d>1,\ d|n} Q_d(z)^{p^m}$ in $\mathbb{F}_p[z]$

Facts

- We know that $z^n - 1 = (z-1)^{p^m} \prod_{d>1,\ d|n} Q_d(z)^{p^m}$ in $\mathbb{F}_p[z]$ where

$$Q_d(z) := \prod_{\substack{s=1,\ldots,d \\ gcd(s,d)=1}} (z - \zeta^s)$$

and $\zeta \in \mathbb{F}_{p^n}$ is a root of unity of order d (d-th cyclotomic polynomial).

Facts

- We know that $z^n - 1 = (z-1)^{p^m} \prod_{d>1,\ d|n} Q_d(z)^{p^m}$ in $\mathbb{F}_p[z]$ where

$$Q_d(z) := \prod_{\substack{s=1,\dots,d \\ gcd(s,d)=1}} (z - \zeta^s)$$

  and $\zeta \in \mathbb{F}_{p^n}$ is a root of unity of order d (d-th cyclotomic polynomial).
- Irreducible factors of every $Q_d(z)$ in $\mathbb{F}_p[z]$ are of the same degree $\mathbb{O}_d(p)$ (Niederreiter Theorem 2.47) where

$$\mathbb{O}_d(p) := \min(\{m \in \mathbb{N}^* \mid p^m = 1 \pmod{d}\}).$$

Facts

- We know that $z^n - 1 = (z-1)^{p^m} \prod_{d>1,\ d|n} Q_d(z)^{p^m}$ in $\mathbb{F}_p[z]$ where

$$Q_d(z) := \prod_{\substack{s=1,\dots,d \\ gcd(s,d)=1}} (z - \zeta^s)$$

  and $\zeta \in \mathbb{F}_{p^n}$ is a root of unity of order d (d-th cyclotomic polynomial).
- Irreducible factors of every $Q_d(z)$ in $\mathbb{F}_p[z]$ are of the same degree $\mathbb{O}_d(p)$ (Niederreiter Theorem 2.47) where

$$\mathbb{O}_d(p) := \min(\{m \in \mathbb{N}^* \mid p^m = 1 \pmod{d}\}).$$

- $\sum_{i=0}^{\ell} k_i z^i = (z-1)^u V(z)$ where $V(1) \neq 0$ and $u \geq 1$

Facts

- We know that $z^n - 1 = (z-1)^{p^m} \prod_{d>1,\ d|n} Q_d(z)^{p^m}$ in $\mathbb{F}_p[z]$ where

$$Q_d(z) := \prod_{\substack{s=1,\dots,d \\ gcd(s,d)=1}} (z - \zeta^s)$$

  and $\zeta \in \mathbb{F}_{p^n}$ is a root of unity of order d (d-th cyclotomoic polynomial).
- Irreducible factors of every $Q_d(z)$ in $\mathbb{F}_p[z]$ are of the same degree $\mathbb{O}_d(p)$ (Niederreiter Theorem 2.47) where

$$\mathbb{O}_d(p) := \min(\{m \in \mathbb{N}^* \mid p^m = 1 \pmod{d}\}).$$

- $\sum_{i=0}^{\ell} k_i z^i = (z-1)^u V(z)$ where $V(1) \neq 0$ and $u \geq 1$: $\sum_{i=0}^{\ell} k_i 1^i = \sum_{i=0}^{\ell} k_i = p = 0$.

- If $deg(V(z)) < \mathbb{O}_d(p)$ for all $d > 1$ such that d divides n, then

$$gcd(\sum_{i=0}^{\ell} k_i z^i, z^n - 1) = gcd((z-1)^u, (z-1)^{p^m}).$$

- If $deg(V(z)) < \mathbb{O}_d(p)$ for all $d > 1$ such that d divides n, then

$$gcd(\sum_{i=0}^{\ell} k_i z^i, z^n - 1) = gcd((z-1)^u, (z-1)^{p^m}).$$

If $u = 1$ or $m = 0$, then

$$gcd(\sum_{i=0}^{\ell} k_i x^i, x^n - 1) = x - 1.$$

Extensions of odd degree

$$F(x) = x^e, \quad e = \sum_{i=0}^{\ell} k_i p^i \quad \text{and} \quad \sum_{i=0}^{\ell} k_i = p \quad \text{GDO type over } \mathbb{F}_{p^n}$$

Extensions of odd degree

$$F(x) = x^e, \quad e = \sum_{i=0}^{\ell} k_i p^i \quad \text{and} \quad \sum_{i=0}^{\ell} k_i = p \quad \text{GDO type over } \mathbb{F}_{p^n}$$

Theorem 1 [ES25]

If $n = q_1^{i_1}..q_s^{i_s}$ (q_i are prime numbers).

1. $n \not\equiv 0 \pmod{p}$: If $\ell \leq \min\limits_{1\leq i\leq s} \mathbb{O}_{q_i}(p)$, then F is a GAPN function.
2. $n \equiv 0 \pmod{p}$: If $\ell \leq \min\limits_{1\leq i\leq s,\ q_i\neq p} \mathbb{O}_{q_i}(p)$ or $n = p^\alpha$, and if the multiplicity of 1 as a root in $\sum_{i=0}^{\ell} k_i x^i \in \mathbb{F}_p[x]$ is equal to 1, then F is a GAPN function.

Extensions of even degree

$$F(x) = x^e, \quad e = \sum_{i=0}^{\ell} k_i p^i \quad \text{and} \quad \sum_{i=0}^{\ell} k_i = p \quad \text{GDO type over } \mathbb{F}_{p^n}$$

Extensions of even degree

$$F(x) = x^e, \quad e = \sum_{i=0}^{\ell} k_i p^i \quad \text{and} \quad \sum_{i=0}^{\ell} k_i = p \quad \text{GDO type over } \mathbb{F}_{p^n}$$

Condition : there exist $0 \leq i, j \leq \ell$ such that $k_{2i} \neq 0$ and $k_{2j+1} \neq 0$.

Extensions of even degree

$$F(x) = x^e, \quad e = \sum_{i=0}^{\ell} k_i p^i \quad \text{and} \quad \sum_{i=0}^{\ell} k_i = p \quad \text{GDO type over } \mathbb{F}_{p^n}$$

Condition : there exist $0 \leq i, j \leq \ell$ such that $k_{2i} \neq 0$ and $k_{2j+1} \neq 0$.

Theorem 2 [ES25]

If $n = 2N \not\equiv 0 \pmod{p}$ where $N \geq 3$ is an odd integer s.t

$$N = q_2^{i_2}..q_m^{i_m} \text{ and } \ell \leq \min_{2 \leq i \leq m} \mathbb{O}_{q_i}(p),$$

then $F(x) = x^e$ is a GAPN function over $\mathbb{F}_{p^n}$.

A full characterisation

- $F(x) = x^{a_2 p^2 + a_1 p + a_0}$, $a_2 + a_1 + a_0 = p$, and $0 \leq a_2, a_1, a_0 \leq p - 1$ function over $\mathbb{F}_{p^n}$.
- $n = p^\alpha \times N$ where $\alpha \geq 0$ and $gcd(N, p) = 1$

A full characterisation

- $F(x) = x^{a_2p^2+a_1p+a_0}$, $\quad a_2 + a_1 + a_0 = p$, $\quad$ and $\quad 0 \leq a_2, a_1, a_0 \leq p-1$ function over $\mathbb{F}_{p^n}$.
- $n = p^{\alpha} \times N$ where $\alpha \geq 0$ and $gcd(N, p) = 1$

Theorem 3 [ES25]

F is GAPN over $\mathbb{F}_{p^n}$ if and only if $a_0^N \neq a_2^N$ or $(a_0 = a_2$ and $\alpha = 0)$.

A full characterisation

- $F(x) = x^{a_2 p^2 + a_1 p + a_0}$, $\quad a_2 + a_1 + a_0 = p$, $\quad$ and $\quad 0 \leq a_2, a_1, a_0 \leq p-1$ function over $\mathbb{F}_{p^n}$.
- $n = p^\alpha \times N$ where $\alpha \geq 0$ and $gcd(N, p) = 1$

Theorem 3 [ES25]

F is GAPN over $\mathbb{F}_{p^n}$ if and only if $a_0^N \neq a_2^N$ or ($a_0 = a_2$ and $\alpha = 0$).

The functions $F(x) = x^{ip^2 + (p-2i)p + i}$ where $i \in \{1, .., \frac{p-1}{2}\}$ are GAPN over $\mathbb{F}_{p^n}$ for every $n \geq 3$ such that $n \not\equiv 0 \pmod{p}$.

Contents

Generalized derivative of GDO functions

$$F(x) = \sum_{i=1}^{N} f_i . x^{d_i}, \quad d_i = \sum_{j=0}^{\ell} d_{i,j} p^j \quad \textbf{GDO} \text{ over } \mathbb{F}_{p^n}.$$

Generalized derivative of GDO functions

$$F(x) = \sum_{i=1}^{N} f_i . x^{d_i}, \quad d_i = \sum_{j=0}^{\ell} d_{i,j} p^j \quad \textbf{GDO} \text{ over } \mathbb{F}_{p^n}.$$

Lemma [ES25]

$\forall \alpha \in \mathbb{F}_{p^n}$,

$$\nabla_\alpha F(x) = \sum_{j=0}^{\ell} g_j^{(F)}(\alpha) x^{p^j}$$

where

$$g_j^{(F)}(\alpha) = \sum_{i=1}^{N} -d_{i,j} f_i \alpha^{d_i - p^j}, \quad j \in [0, \ell].$$

Theorem (McGuire and Sheekey 2019)

Let $F(x) = \sum_{i=0}^{\ell} f_i.x^{p^i}$ a $\mathbb{F}_p$-function over $\mathbb{F}_{p^n}$ where $f_\ell \neq 0$ and $f_0 \neq 0$. F has p^ℓ roots in $\mathbb{F}_{p^n}$ if and only if $C^{(1)}(F).C^{(p)}(F)..C^{(p^{n-1})}(F) = I_\ell$ where :

$$C^{(p^i)}(F) := \begin{bmatrix} 0 & 0 & \dots & 0 & -\left(\frac{f_0}{f_\ell}\right)^{p^i} \\ 1 & 0 & \dots & 0 & -\left(\frac{f_1}{f_\ell}\right)^{p^i} \\ \vdots & \vdots & \ddots & 0 & \vdots \\ 0 & 0 & \dots & 1 & -\left(\frac{f_{\ell-1}}{f_\ell}\right)^{p^i} \end{bmatrix} \in \mathbb{F}_{p^n}^{\ell \times \ell}$$

Theorem (McGuire and Sheekey 2019)

Let $F(x) = \sum_{i=0}^{\ell} f_i.x^{p^i}$ a $\mathbb{F}_p$-function over $\mathbb{F}_{p^n}$ where $f_\ell \neq 0$ and $f_0 \neq 0$. F has p^ℓ roots in $\mathbb{F}_{p^n}$ if and only if $C^{(1)}(F).C^{(p)}(F)..C^{(p^{n-1})}(F) = I_\ell$ where :

$$C^{(p^i)}(F) := \begin{bmatrix} 0 & 0 & \dots & 0 & -\left(\frac{f_0}{f_\ell}\right)^{p^i} \\ 1 & 0 & \dots & 0 & -\left(\frac{f_1}{f_\ell}\right)^{p^i} \\ \vdots & \vdots & \ddots & 0 & \vdots \\ 0 & 0 & \dots & 1 & -\left(\frac{f_{\ell-1}}{f_\ell}\right)^{p^i} \end{bmatrix} \in \mathbb{F}_{p^n}^{\ell \times \ell}$$

Remark :

- $det(C^{(1)}(F).C^{(p)}(F)..C^{(p^{n-1})}(F)) = (-1)^\ell N_{p^n/p}(\frac{f_0}{f_\ell})$

Theorem (McGuire and Sheekey 2019)

Let $F(x) = \sum_{i=0}^{\ell} f_i . x^{p^i}$ a $\mathbb{F}_p$-function over $\mathbb{F}_{p^n}$ where $f_\ell \neq 0$ and $f_0 \neq 0$. F has p^ℓ roots in $\mathbb{F}_{p^n}$ if and only if $C^{(1)}(F).C^{(p)}(F)..C^{(p^{n-1})}(F) = I_\ell$ where :

$$C^{(p^i)}(F) := \begin{bmatrix} 0 & 0 & \dots & 0 & -\left(\frac{f_0}{f_\ell}\right)^{p^i} \\ 1 & 0 & \dots & 0 & -\left(\frac{f_1}{f_\ell}\right)^{p^i} \\ \vdots & \vdots & \ddots & 0 & \vdots \\ 0 & 0 & \dots & 1 & -\left(\frac{f_{\ell-1}}{f_\ell}\right)^{p^i} \end{bmatrix} \in \mathbb{F}_{p^n}^{\ell \times \ell}$$

Remark :

- $det(C^{(1)}(F).C^{(p)}(F)..C^{(p^{n-1})}(F)) = (-1)^\ell N_{p^n/p}(\frac{f_0}{f_\ell})$
- $det(C^{(1)}(F).C^{(p)}(F)..C^{(p^{n-1})}(F))) \neq 1 \implies C^{(1)}(F).C^{(p)}(F)..C^{(p^{n-1})}(F)) \neq I_\ell$

When the linearized polynomial is of degree p^2

$$F(x) = x^{(p-d)p^2+dp} + \lambda x^{kp+p-k}, \quad 1 \le k, d \le p, \ \lambda \in \mathbb{F}_{p^n}^*$$

When the linearized polynomial is of degree p^2

$$F(x) = x^{(p-d)p^2+dp} + \lambda x^{kp+p-k}, \quad 1 \leq k, d \leq p, \ \lambda \in \mathbb{F}_{p^n}^*$$

Theorem 4 [ES25]

If $N_n(\lambda \frac{k}{d}) \neq 1$, then f is a GAPN function over $\mathbb{F}_{p^n}$.

When the linearized polynomial is of degree p^2

$$F(x) = x^{(p-d)p^2+dp} + \lambda x^{kp+p-k}, \quad 1 \leq k, d \leq p, \;\; \lambda \in \mathbb{F}_{p^n}^*$$

Theorem 4 [ES25]

If $N_n(\lambda \frac{k}{d}) \neq 1$, then f is a GAPN function over $\mathbb{F}_{p^n}$.

Example

$F(x) = x^{(p-i)p^2+ip} - x^{ip+p-i}$ where $i \in \{1, .., p-1\}$ is GAPN over $\mathbb{F}_{p^n}$ for every odd positive integer $n \geq 3$.

Summary and future direction of research

$\rightarrow$ What we've done :

- New classes of monomial GAPN functions, (Up to Generalized Extended affine equivalence : Kuroda and Tsujie 2016)
- New classes of multinomial GAPN functions, (Up to Generalized Extended affine equivalence : Kuroda and Tsujie 2016)

Summary and future direction of research

$\rightarrow$ What we've done :

- New classes of monomial GAPN functions, (Up to Generalized Extended affine equivalence : Kuroda and Tsujie 2016)
- New classes of multinomial GAPN functions, (Up to Generalized Extended affine equivalence : Kuroda and Tsujie 2016)

$\rightarrow$ Future work :

- Find other new GAPN functions.
- Find possible applications in cryptography and coding theory.