APN 関数の一般化とその分類について

黒田 匡迪 (日本文理大学)

joint work with 辻栄 周平 (広島国際学院大学)

2019 年 9 月 5 日

於：日本文理大学 湯布院研修所
Introduction

$p : \text{prime, } F := \mathbb{F}_{p^n}$

**Definition (almost perfect nonlinear function)**

A function $f : F \to F$ is called **almost perfect nonlinear (APN)** if

$$N_f(a, b) := \# \{x \in F \mid D_a f(x) := f(x + a) - f(x) = b\} \leq 2$$

for any $a \in F^\times$ and $b \in F$.

- $f$ is called **perfect nonlinear (PN)** if $N_f(a, b) \leq 1$ for $\forall a \in F^\times$, $\forall b \in F$.
- If $f$ is linear, $D_a f(x) = f(a)$. Hence $N_f(a, b) = \begin{cases} p^n & (f(a) = b), \\ 0 & (f(a) \neq b). \end{cases}$
- When $p = 2$, there is no PN function, since $D_a f(x + a) = D_a f(x)$.
- When $p = 2$, $f : \text{APN} \iff N_f(a, b) = 0$ or $2$ for $\forall a \in F^\times$, $\forall b \in F$.
- When $p = 2$, there are applications in cryptography, coding theory, etc.
- When $p \geq 3$, in the above definition, there is no reason why $N_f(a, b) \leq 2$.
- \sim APN with $p \geq 3$ have quite different properties from APN with $p = 2$.
- \sim We give modified definition, which is a generalization of APN with $p = 2$. 

\[\begin{align*}
\end{align*}\]
## Application to cryptography: Substitution box (S-box)

### Function $\text{AES}_K(M)$ (AES128)

\[
\begin{align*}
(K_0, \ldots, K_{10}) &\leftarrow \text{expand} \ (K)  \\
 s &\leftarrow M \oplus K_0  \\
 \text{for } r = 1 \text{ to } 10 \text{ do}  \\
 &\quad s \leftarrow S(s)  \\
 &\quad s \leftarrow \text{shift-rows}(s)  \\
 &\quad \text{if } r \leq 9 \text{ then } s \leftarrow \text{mix-cols}(s) \text{ fi}  \\
 &\quad s \leftarrow s \oplus K_r  \\
 \text{endfor}  \\
 \text{return } s
\end{align*}
\]

- $K$: public key, $M$: plaintext
- $|K| = |M| = 128$
- $K_0, \ldots, K_{10}$: keys
- $S$: S-box
- $S$ is the inverse function $S(x) = x^{-1}$.
- However, when $n = 8$, the inverse function is not APN ($N_S(a, b) \leq 4$).
- For resistance to linear and differential attacks, we need properties of S-boxes: high nonlinearity (i.e., low differential uniformity) and high algebraic degree.
- For practical use, $S$ is the inverse function $S(x) = x^{-1}$.
- No examples of bijective APN functions on $\mathbb{F}_{2^8}$ are known.
Recall that $f : F \to F$ : APN
\[\begin{align*}
def N_f(a, b) &= \# \{x \mid D_a f(x) = f(x + a) - f(x) = b\} \leq 2 \quad (a(\neq 0), b \in F) \\
\iff N_f(a, b) &= 0 \text{ or } 2 \quad (a(\neq 0), b \in F), \text{ when } p = 2 \quad (\because D_a f(x + a) = D_a f(x)).
\end{align*}\]
When $p \geq 3$, there is no reason why $N_f(a, b) \leq 2$.

$\rightsquigarrow$ We give modified definition, which is a generalization of APN with $p = 2$.

**Definition (generalized almost perfect nonlinear function)**

$f : F \to F$ is a generalized almost perfect nonlinear (GAPN) function if
\[\tilde{N}_f(a, b) := \# \left\{ x \in F \mid \tilde{D}_a f(x) := \sum_{i \in \mathbb{F}_p} f(x + ia) = b \right\} \leq p\]
for any $a \in F^\times$ and $b \in F$.

- When $p = 2$, GAPN functions coincide with APN functions.
- Note that $\tilde{D}_a f(x + ia) = \tilde{D}_a f(x)$ for $\forall i \in \mathbb{F}_p$. Hence
  \[f : \text{GAPN} \iff \tilde{N}_f(a, b) = 0 \text{ or } p \text{ for } \forall a \in F^\times, \forall b \in F.\]

**Today's topic**

The classification of monomial GAPN functions.

$\rightsquigarrow$ We obtain a partial classification of monomial GAPN functions.
A classification of monomial APN functions \((p = 2)\)

Table 1 gives a complete list (up to CCZ-equivalence) of known monomial APN functions.

<table>
<thead>
<tr>
<th>Function</th>
<th>Exponents (d)</th>
<th>Conditions</th>
<th>Year</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gold function</td>
<td>(2^i + 1)</td>
<td>(\gcd(i, n) = 1)</td>
<td>1968, 93</td>
</tr>
<tr>
<td>Kasami function</td>
<td>(2^{2i} - 2^i + 1)</td>
<td>(\gcd(i, n) = 1)</td>
<td>1971, 93</td>
</tr>
<tr>
<td>Welch function</td>
<td>(2^t + 3)</td>
<td>(n = 2t + 1)</td>
<td>1999</td>
</tr>
<tr>
<td>Niho function</td>
<td>(2^t + 2^{\frac{t}{2}} - 1, \ t: \text{even})</td>
<td>(n = 2t + 1)</td>
<td>1999</td>
</tr>
<tr>
<td></td>
<td>(2^t + 2^{\frac{3t+1}{2}} - 1, \ t: \text{odd})</td>
<td>(n = 2t + 1)</td>
<td></td>
</tr>
<tr>
<td>Inverse function</td>
<td>(2^n - 2)</td>
<td>(n \text{ is odd})</td>
<td>1993</td>
</tr>
<tr>
<td>Dobbertin function</td>
<td>(2^{4t} + 2^{3t} + 2^{2t} + 2^t - 1)</td>
<td>(n = 5t)</td>
<td>1999</td>
</tr>
</tbody>
</table>

- It is sometimes believed that this list is complete.
- We give generalizations of Gold, Welch and inverse functions.
Let $p \geq 2$, $F = \mathbb{F}_{p^n}$ and let $f_d : F \rightarrow F$, $f_d(x) = x^d$ with $d < p^n$.

**Definition (algebraic degree)**

$d^\circ(f_d) :=$ the total degree of the multivariable function $f_d$ on the $n$-dimensional vector space $F$ over $\mathbb{F}_p$

$$= w_p(d) := \sum_{s=0}^{n-1} d_s,$$

where $\sum_{s=0}^{n-1} d_sp^s$ is the $p$-adic expansion of $d$.

**Examples**

$$w_2 (2^i + 1) = 2 \text{ (Gold functions)}, \quad w_2 (2^t + 3) = 3 \text{ (Welch functions)},$$

$$w_2 (2^n - 2) = w_2 (2 + 2^2 + \cdots + 2^{n-1}) = n - 1 \text{ (Inverse function)}.$$

**Propositions (K and Tsujie)**

1. Clearly, $d^\circ(f_d) \leq n(p - 1)$ (as $p^n - 1 = (p - 1)(1 + p + \cdots + p^{n-1})$).
2. $d^\circ(f_d) < p \Rightarrow \tilde{D}_a f_d(x) : \text{constant} \Rightarrow f_d$ is not GAPN function on $F$.
3. When $p \geq 3$, if $d^\circ(f_d)$ is even, then $f_d$ is not GAPN function on $F$.

$\Rightarrow$ When $p \geq 3$, we may assume that

$$d^\circ(f_d) \text{ is odd and } p \leq d^\circ(f_d) \leq n(p - 1) - 1.$$

$\Rightarrow$ We will give monomial GAPN functions $f_d$ with $d^\circ(f_d) = p$ or $n(p - 1) - 1$. 
Definition (*$p$*-exceptional)

The exponent $d$ is *$p$*-exceptional if $f_d(x) = x^d$ is GAPN function on infinitely many extension fields of $\mathbb{F}_p$.

- 2-exceptional exponents are so-called exceptional exponents.
- The following Theorem was conjectured by Dillon and was proved by Hernando and McGuire:

**Theorem (Hernando and McGuire, 2011)**

The only 2-exceptional exponents are Gold numbers ($d = 2^i + 1$) and Kasami numbers ($d = 2^{2i} - 2^i + 1$).

⇒ The classification of all exceptional monomial APN functions for $p = 2$ has been completed.
⇒ However, the complete classification of all monomial APN functions is not obtained yet.
⇒ When $p = 2$, the complete list has been conjectured.
Monomial PN functions for odd characteristic

Recall that $f : F \rightarrow F : \text{PN}$

$\overset{\text{def}}{\leftrightarrow} N_f(a, b) = \# \{ x \mid D_a f(x) = f(x + a) - f(x) = b \} \leq 1 \ (a(\neq 0), b \in F)$

$\implies$ When $p = 2$, there are no PN functions.

When $p \geq 3$, any PN function is an APN function.

$\implies$ Hernando, McGuire, and Monserrat conjectured a characterization of PN functions similar to above Theorem [HM2011], and this conjecture was proved by Zieve:

**Theorem (Zieve, 2015)**

The monomial function $f_d(x) = x^d$ is PN function on infinitely many extension fields of $\mathbb{F}_p$ if and only if either $d = p^i + p^j$ where $p$ is odd and $i \geq j \geq 0$; or $d = \frac{3^i + 3^j}{2}$ where $p = 3$ and $i > j \geq 0$ with $i \not\equiv j \mod 2$.

$\implies$ The classification of all “exceptional” monomial PN has been completed.

$\implies$ We want to give the classification of all $p$-exceptional monomial GAPN functions similar to cases of APN (with $p = 2$) [HM2011] or PN [Z2015].

$\implies$ We will give a family of $p$-exceptional monomial GAPN functions, which is a generalization of Gold functions.

$\implies$ We will give a conjecture for 3-exceptional exponents.
Monomial GAPN functions $f_d$ on $F$ with $d^\circ(f_d) = p$

We may assume that

$$d = 1 + p^{i_2} + \cdots + p^{i_p} \text{ with } 0 \leq i_2 \leq \cdots \leq i_p, \ (i_2, \ldots, i_p) \neq (0, \ldots, 0).$$

**Theorem (K)**

Assume that $p \nmid n$. $f_d$ is a GAPN function on $F = \mathbb{F}_{p^n}$

$$\iff \{ \beta \in \mathbb{F}_p \mid 1 + \beta^{i_2} + \cdots + \beta^{i_p} = 0 \} \cap \{ \gamma \in \mathbb{F}_p \mid \gamma^n = 1 \} = \{1\}$$

**Proof**: $\tilde{D}_a f_d(x) = \sum_{i \in \mathbb{F}_p} (x + ia)^d = a^d \sum_{i \in \mathbb{F}_p} \left( \frac{x}{a} + i \right)^d = a^d \tilde{D}_1 f_d \left( \frac{x}{a} \right)$

and

$$\varphi_d(X) := -\tilde{D}_1 f_d(X) = X + X^{p^{i_2}} + \cdots + X^{p^{i_p}} = \sum_{s=0}^{n-1} \alpha_s X^{p^s}.$$

In particular, $\varphi_d : F \to F$ is an $\mathbb{F}_p$-linear.

Assume that $\exists x_0 \in F \text{ s.t. } \tilde{D}_a f_d(x_0) = b$. Then

$$\tilde{N}_{f_d}(a, b) = \# \{ x \in F \mid \tilde{D}_a f_d(x) = b \} = \# \{ x \in F \mid \varphi_d \left( \frac{x}{a} \right) = \varphi_d \left( \frac{x_0}{a} \right) \}$$

$$= \# \{ x \in F \mid \varphi_d \left( \frac{x-x_0}{a} \right) = 0 \} = \# \text{Ker} (\varphi_d : F \to F).$$
Monomial GAPN functions $f_d$ on $F$ with $d^\circ(f_d) = p$

Therefore, $f_d : \text{GAPN on } F \iff \#\ker(\varphi_d : F \to F) = p$

$\iff \dim_{F_p} \text{Im}(\varphi_d : F \to F) = n - 1$

The matrix representation of $\varphi_d(X) = \sum_{s=0}^{n-1} \alpha_s X^{p^s}$ w.r.t. $\{b, b^p, \ldots, b^{p^{n-1}}\}$ is

$$
\begin{bmatrix}
\alpha_0 & \alpha_{n-1} & \cdots & \alpha_1 \\
\alpha_1 & \alpha_0 & \cdots & \alpha_2 \\
\vdots & \vdots & \ddots & \vdots \\
\alpha_{n-1} & \alpha_{n-2} & \cdots & \alpha_0
\end{bmatrix},
$$

and its eigenvalues are $1 + \gamma^{i_2} + \cdots + \gamma^{i_p}$ with $\gamma^n = 1$

$\quad (= 0$ if $\gamma = 1$).

Therefore, $f_d : \text{GAPN on } F \quad (= \mathbb{F}_{p^n})$

$\iff \{\beta \in \overline{F_p} \mid 1 + \beta^{i_2} + \cdots + \beta^{i_p} = 0\} \cap \{\gamma \in \overline{F_p} \mid \gamma^n = 1\} = \{1\}$

**Corollary (K)**

(i) For $\forall d$ with $w_p(d) = p$, $\exists n \in \mathbb{N}$ s.t. $f_d$ is a GAPN function on $\mathbb{F}_{p^n}$.

(ii) There are infinitely many such $n$’s in (i).

In particular, any exponent $d$ with $w_p(d) = p$ is $p$-exceptional.
Monomial GAPN functions \( f_d \) on \( F \) with \( d^\circ(f_d) = p \)

In particular, when \( d = p^i + p - 1 \) (i.e., \( i_2 = \cdots = i_{p-1} = 0 \), \( i := i_p > 0 \)),
\( f_d : \) GAPN function on \( F \) \iff \( \{ \beta \in \overline{F}_p | \beta^i = 1 \text{ and } \beta^n = 1 \} = \{1\} \)
\iff \( \gcd(i, n) = 1 \)

We called them generalized Gold functions. When \( p = 2 \), they are Gold functions.

### Example (a generalization of Welch function : \( d = 2^t + 3 \), \( n = 2t + 1 \))

Assume that \( p \nmid n \). Let \( d = p^t + p + 1 \), \( t = \begin{cases} \frac{n-1}{2} & (n \text{ is odd}), \\ \frac{n}{2} & (n \text{ is even}). \end{cases} \)

Then \( f_d \) is a GAPN function on \( \overline{F}_{p^n} \iff p = 2 \) and \( n \) is odd, or \( p = 3 \).

- When \( p = 2 \) and \( n \) is odd, \( f_d \) is a Welch function.
- When \( p \geq 5 \), \( f_d \) is not GAPN, since \( d^\circ(f_d) = 3 < p \).
- When \( p = 3 \), we can check easily that

\[
\{ \beta \in \overline{F}_3 | \beta^t = -(1 + \beta) \} \cap \{ \gamma \in \overline{F}_3 | \gamma^n = 1 \} = \{1\}.
\]
Monomial GAPN functions $f_d$ on $\mathbb{F}_{p^n}$ with $d^o(f_d) = n(p - 1) - 1$

The inverse function on $F$ is defined by $f_{p^n-2}(x) = x^{p^n-2}$. Then
\begin{equation*}
p^n - 2 = p^n - 1 - 1 = (p - 1) \left(1 + p + \cdots + p^{n-1}\right) - 1.
\end{equation*}
Hence $d^o(f_d) = (n - 1)(p - 1) + p - 2 = n(p - 1) - 1$.

**Theorem (K and Tsujie)**

When $p \geq 3$, the inverse function $f_{p^n-2}$ on $F$ is a GAPN function.

Note that when $p = 2$, the inverse function is APN if $n$ is odd.

**Proof:** Assume that $\exists x_0 \in F$ s.t. $\sum_{i \in \mathbb{F}_p} (x_0 + ia)^{-1} = b$.

Then the equation has $p$ solutions $x_0 + ja$ ($j \in \mathbb{F}_p$).

\begin{equation*}
x_0 \not\in \mathbb{F}_p a \Rightarrow b \prod_{i \in \mathbb{F}_p} (x_0 + ia) = \exists g(x_0) \text{ with } \deg g < p
\end{equation*}
\begin{equation*}
\Rightarrow b \neq 0 \text{ and the number of solutions outside } \mathbb{F}_p a \text{ is exactly } p.
\end{equation*}

\begin{equation*}
x_0 \in \mathbb{F}_p a \Rightarrow b = \sum_{i \in \mathbb{F}_p} (ia)^{-1} = a^{-1} \cdot 0 = 0.
\end{equation*}

In any case, $\left\{ x \in F \left| \sum_{i \in \mathbb{F}_p} (x + ia)^{-1} = b \right. \right\} = x_0 + \mathbb{F}_p a$.  

Monomial GAPN functions $f_d$ on $\mathbb{F}_{p^n}$ with $d^\circ(f_d) = n(p - 1) - 1$

Since $w_p(d) = n(p - 1) - 1$, for some $0 \leq j \leq n - 1$, we have
\[d = (p - 1)(1 + p + \cdots + p^{n-1}) - p^j = p^n - p^j - 1.\]

Let $Fb_j(x) := x^{p^n - j}$ (a Frobenius isomorphism). Then we have
\[(f_d \circ Fb_j)(x) = \left(x^{p^n - j}\right)^{p^n - p^j - 1} = \left(x^{p^n}\right)^{p^n - j} \cdot \left(x^{p^n - j}\right)^{-p^j} \cdot \left(x^{p^n - j}\right)^{-1}
= x^{p^n - j} \cdot x^{-1} \cdot \left(x^{p^n - j}\right)^{-1}
= x^{-1} = x^{p^n - 2}.

Therefore

$f_d$ is GAPN on $\mathbb{F}$ $\iff$ the inverse function $f_{p^n - 2}$ on $\mathbb{F}$ is GAPN.

Corollary

Any monomial function $f_d$ on $\mathbb{F}$ with $d^\circ(f_d) = n(p - 1) - 1$ is GAPN.
The other monomial GAPN functions on $F$

Assume that $p = 3$.

- When $n \in \{1, 2, 3\}$, there are no monomial GAPN functions $f_d$ on $\mathbb{F}_{3^n}$ with $3 < d^\circ(f_d) < 2n - 1$, clearly.

- When $n = 5$, we have the following Table:

  Table 2. monomial GAPN functions $f_d$ on $\mathbb{F}_{3^5}$ with $d^\circ(f_d) = 5$ or $7$

<table>
<thead>
<tr>
<th>$d^\circ(f_d)$</th>
<th>Exponents $d$</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>23, 35, 49, 73, 97, 113, 137, 169, 173, 199</td>
</tr>
<tr>
<td>7</td>
<td>79, 107, 197, 227</td>
</tr>
</tbody>
</table>

- When $n \in \{4, 6, 7, 8\}$, there are no monomial GAPN functions $f_d$ on $\mathbb{F}_{3^n}$ with $3 < d^\circ(f_d) < 2n - 1$, by simple computations.

Conjecture 1

For sufficiently large $n$, there are no monomial GAPN functions $f_d$ on $\mathbb{F}_{3^n}$ with $3 < d^\circ(f_d) < 2n - 1$.

In particular, the only 3-exceptional exponents are given by

$$d = 1 + 3^i + 3^j \quad (0 \leq i \leq j, \ (i, j) \neq (0, 0)).$$