APN 関数の一般化について

黒田　匡迪 (Kuroda Masamichi) *　北海道大学大学院　理学研究院　数学部門

概要

有限体 $\mathbb{F}_{p^n}$ からそれ自身への関数 f で, 各方程式

$$f(x+a)-f(x)=b, \quad a(\neq 0), b \in \mathbb{F}_{p^n}$$

が高々 2 つの解を $\mathbb{F}_{p^n}$ に持つものを almost perfect nonlinear (APN) 関数という. 特に, $p=2$ の場合に, 暗号理論や有限幾何学への応用が期待され, 盛んに研究されてきた. 一方で, p が奇素数の場合では, $p=2$ の場合と同様の性質は成り立ちづらく, $p=2$ の場合に比べてあまり研究されてこなかった. 本講演では, p が奇素数の場合の APN 関数を定義しなおし, それが $p=2$ の場合の自然な一般化になっていることを紹介する. なお, この研究は北海道大学の辻栄周平氏との共同研究である.

1　はじめに

f を標数 p の有限体 $\mathbb{F}_{p^n}$ からそれ自身への関数とする. 任意の $a \in \mathbb{F}_{p^n}$ に対し, a に関する f の差分関数 D_af を次で定める:

$$D_af : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_{p^n}, \quad x \longmapsto D_af(x) := f(x+a)-f(x).$$

また, 任意の $a, b \in \mathbb{F}_{p^n}$ に対し,

$$N_f(a,b) := \#\{x \in \mathbb{F}_{p^n} \mid D_af(x)=b\}$$

と定める. ここで, f が almost perfect nonlinear (APN) 関数であるとは,

$$N_f(a,b) \leq 2 \quad \text{for any } a(\neq 0), b \in \mathbb{F}_{p^n}$$

を満たすときにいう. $p=2$ の場合には, 暗号理論への応用が知られている. 例えば, これらの関数からブロック暗号での S ボックスを構成できる. 一方, 有限幾何 (例えば, 高次元双対超卵形) との関係も知られている. しかし, $p \geq 3$ の場合では, $p=2$ の場合と同様の性質は成り立ちづらく, $p=2$ の場合に比べてあまり研究されてこなかったように思える. 本講演では, 奇素数の場合に APN 関数の定義を修正し, それが $p=2$ の場合の自然な一般化になっていることを紹介する. なお, APN 関数に関する現在までの研究は, [18] に非常に良くまとめられている. しかし, 高次元双対超卵形との関係については触れられていない. これについては, [11], [19] が詳しい.

第 2 章では, APN 関数に関係するいくつかの基本的な用語を定義する. 第 3 章では, $p=2$ の場合に APN 関数の例や性質を簡単に紹介する. 第 4 章では, APN 関数の一般化である generalized almost perfect nonlinear (GAPN) 関数の定義を与え, 例や性質を紹介し, APN 関数の自然な一般化であることを述べる.

* E-mail: m-kuroda@math.sci.hokudai.ac.jp

2　基本的な用語

APN 関数に関係するいくつかの基本的な用語を紹介する. この章では, p は任意の素数とする.

2.1　代数的次数

関数 $f : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_{p^n}$ と任意の自然数 m に対して, 関数 $[f]^m : \mathbb{F}_{p^n}^m \longrightarrow \mathbb{F}_{p^n}$ を次で定める：

$$[f]^m(x_1, \ldots, x_m) := \sum_{I \subset [m]} (-1)^{m-|I|} f\left(\sum_{i \in I} x_i\right).$$

但し, $[m] = \{1, \ldots, m\}$ であり, $I = \emptyset$ のときは, $f\left(\sum_{i \in I} x_i\right) = f(0)$ とする. また, $[f]^0 := f(0)$ と定める. 例えば,

$$\begin{aligned}
[f]^1(x) &= f(x) - f(0), \\
[f]^2(x, y) &= f(x + y) - f(x) - f(y) + f(0), \\
[f]^3(x, y, z) &= f(x + y + z) - f(x + y) - f(x + z) - f(y + z) + f(x) + f(y) + f(z) - f(0)
\end{aligned}$$

である. 簡単な計算から次の命題が成り立つ：

命題 2.1. 任意の自然数 m と任意の x, y, z_1, $\ldots$, $z_{m-1} \in \mathbb{F}_{p^n}$ に対して, 次が成り立つ：

$$[f]^{m+1}(x, y, z_1, \ldots, z_{m-1}) = [f]^m(x + y, z_1, \ldots, z_{m-1}) - [f]^m(x, z_1, \ldots, z_{m-1}) - [f]^m(y, z_1, \ldots, z_{m-1}).$$

有限体上の関数 $f : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_{p^n}$ は次数 p^n 以下の多項式

$$f(x) = \sum_{i=0}^{p^n - 1} c_i x^i \in \mathbb{F}_{p^n}[x]$$

で一意的に表わされることが知られている. 各 $0 \leq i < p^n$ の p-進展開が $i = \sum_{s=0}^{n-1} i_s p^s$ $(0 \leq i_s < p)$ とかけるとき, i の p-weight $w_p(i)$ を $w_p(i) := \sum_{s=0}^{n-1} i_s$ で定める. このとき, 簡単な計算により, $m > w_p(i)$ ならば, $\left[x^i\right]^m = 0$ となることが示せる. 従って, 次の事実が得られる：

$$m > \max\{w_p(i) \mid c_i \neq 0\} \Longrightarrow [f]^m = 0.$$

この事実から, 代数的次数を次で定める：

定義 2.2. f を零関数でないとする. $[f]^m \neq 0$ となる最大の m を f の代数的次数といい, $d^\circ(f)$ とかく.

命題 2.1 と上の事実から, 次が直ちに従う.

命題 2.3. (1) $d^\circ(f) = 0$ であるための必要十分条件は, f が零でない定数関数であること.
(2) $d^\circ(f) = m(\geq 1)$ であるための必要十分条件は, $[f]^m$ が零でない $\mathbb{F}_p$-多重線形形式であること.
(3) $d^\circ(f) \leq \max\{w_p(i) \mid c_i \neq 0\}$.

2.2 Fourier 変換と Walsh 係数

定義 2.4. 任意の関数 $g : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_p$ に対し, $\mathcal{F}(g)$ を g の *Fourier* 変換に付随する次の値として定める：

$$\mathcal{F}(g) := \sum_{x \in \mathbb{F}_{p^n}} \zeta_p^{g(x)}.$$

但し, ζ_p は 1 の原始 p 乗根である.

関数 $f : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_{p^n}$ と任意の $b \in \mathbb{F}_{p^n}$ に対して,

$$f_b : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_p,\ x \longmapsto \mathrm{Tr}(bf(x))$$

と定める. f_b を f の成分という. 各 $a(\neq 0) \in \mathbb{F}_{p^n}$ に対して, $\mathbb{F}_{p^n}$ 上の恒等写像の成分を φ_a とかく. つまり,

$$\varphi_a : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_p,\ x \longmapsto \mathrm{Tr}(ax)$$

と定める.

定義 2.5. 関数 $f : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_{p^n}$ の *Walsh* 係数を次で定める：

$$W_f(a, b) := \mathcal{F}(\varphi_a + f_b) \quad (a(\neq 0), b \in \mathbb{F}_{p^n}).$$

2.3 有限体上の関数の同値関係

2 つの関数 $f, g : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_{p^n}$ に対して, 次の同値関係を考える ([6], [16]).

定義 2.6. (1) f と g が extended affine (EA)-同値であるとは, 次の条件を満たすことをいう：

ある affine 写像 (すなわち, 線形写像 + 平行移動) A と全単射 affine 写像 A_1, A_2 が存在して,
$g = A_1 \circ f \circ A_2 + A$ となる.

このとき, $f \underset{EA}{\sim} g$ とかく.

(2) f と g が Carlet, Charpin, Zinoviev (CCZ)-同値であるとは, 次の条件を満たすことをいう：

ある全単射 affine 写像 $\mathcal{L} : \mathbb{F}_{p^n}^2 \to \mathbb{F}_{p^n}^2$ が存在して,
$\mathcal{L}(G(f)) = G(g)$ を満たす.

このとき, $f \underset{CCZ}{\sim} g$ とかく. 但し, $G(f)$ は f のグラフである. つまり, $G(f) = \{(x, f(x)) \mid x \in \mathbb{F}_{p^n}\}$.

これら 2 つの同値関係には, 次の関係が知られている ([6]).

命題 2.7. EA-同値は CCZ-同値の特別な場合である, すなわち, $f \underset{EA}{\sim} g \Longrightarrow f \underset{CCZ}{\sim} g$

注意 2.8. *EA*-同値は代数的次数を保つが, *CCZ*-同値は代数的次数を保たないことが知られている.

3 $\mathbb{F}_{2^n}$ 上の APN 関数について

この章では, $p = 2$ の場合に APN 関数の例や性質を簡単に紹介していく.

3.1 APN 関数の特徴づけ

Nyberg によって, 次の特徴づけが与えられた ([17]).

定理 3.1. 関数 $f : \mathbb{F}_{2^n} \longrightarrow \mathbb{F}_{2^n}$ に対し, f_b $(b \in \mathbb{F}_{2^n})$ を f の成分とする. このとき, 任意の $a(\neq 0) \in \mathbb{F}_{2^n}$ に対して,

$$\sum_{b \in \mathbb{F}_{2^n}} \mathcal{F}^2(D_a f_b) \geq 2^{2n+1}$$

が成り立つ. 加えて, f が APN であるための必要十分条件は, 全ての $a(\neq 0) \in \mathbb{F}_{2^n}$ に対して, 等号が成立することである.

ここで, $\mathcal{F}^2(D_a f_b) = \left(\sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(b(f(x+a)-f(x)))} \right)^2$ より, $\mathcal{F}^2(D_0 f_b) = \mathcal{F}^2(D_a f_0) = 2^{2n}$ が任意の a, $b \in \mathbb{F}_{2^n}$ に対して成り立つので, 次が得られる.

系 3.2. 関数 $f : \mathbb{F}_{2^n} \longrightarrow \mathbb{F}_{2^n}$ に対し, f_b $(b \in \mathbb{F}_{2^n})$ を f の成分とする. このとき,

$$\sum_{a \in \mathbb{F}_{2^n}} \sum_{b \in \mathbb{F}_{2^n}^\times} \mathcal{F}^2(D_a f_b) \geq (2^n - 1) 2^{2n+1}$$

が成り立つ. 加えて, f が APN であるための必要十分条件は, 等号が成立することである.

関数 $f : \mathbb{F}_{2^n} \longrightarrow \mathbb{F}_{2^n}$ が代数的に 2 次である場合, すなわち,

$$B_f(x, y) := [f]^2(x, y) = f(x + y) - f(x) - f(y) + f(0)$$

が双線形形式である場合は, APN 関数であるかどうかの判定は, 少し容易になる :

命題 3.3. $f : \mathbb{F}_{2^n} \longrightarrow \mathbb{F}_{2^n}$ を代数的に 2 次の関数とする. このとき, 任意の $a \in \mathbb{F}_{2^n}^\times$ と任意の $b \in \mathbb{F}_{2^n}$ に対して, $N_f(a, b) = 0$ あるいは, $N_f(a, b) = N_f(a, D_a f(0))$ が成り立つ. 特に, f が APN であるための必要十分条件は, $N_f(a, D_a f(0)) \leq 2$ が任意の $a \in \mathbb{F}_{2^n}^\times$ で成り立つことである.

Proof. $N_f(a, b) \neq 0$ とし, $D_a f(x) = b$ となる x を 1 つ取り固定する. $D_a f(y) = D_a f(0)$ を満たす任意の y に対し, B_f の双線形性より, $D_a f(x + y) = b$ が示せる. このことから, $\{z \mid D_a f(z) = b\} = \{x + y \mid D_a f(y) = D_a f(0)\}$ が得られるので, $N_f(a, b) = N_f(a, D_a f(0))$ が得られる. □

3.2 AB 関数と APN 関数の関係

次に, APN 関数と密接な関係にある almost bent (AB) 関数を定義する.

定義 3.4. 関数 $f : \mathbb{F}_{2^n} \longrightarrow \mathbb{F}_{2^n}$ が *almost bent (AB)* であるとは,

$$W_f(a, b) \in \left\{ 0, \pm 2^{\frac{n+1}{2}} \right\} \quad \textit{for any } a \in \mathbb{F}_{2^n},\ b \in \mathbb{F}_{2^n}^\times$$

を満たすときにいう.

ここで, 定義より, $W_f(a,b) = \mathcal{F}(\varphi_a + f_b) = \sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(ax+bf(x))}$ なので, $W_f(a,b)$ は常に整数である. 故に, AB 関数は n が奇数の時にしか存在しない. APN 関数と AB 関数の間には次の関係が知られている ((1) は [7], (2) は [1] を参照せよ).

定理 3.5. *n を奇数とする. このとき,*

(1) 任意の *AB* 関数は *APN* であり,
(2) 任意の代数的に 2 次の *APN* 関数は *AB* である.

3.3 2 つの同値関係と APN 関数

命題 3.6. 2 つの関数 $f, g : \mathbb{F}_{2^n} \longrightarrow \mathbb{F}_{2^n}$ に対し, 次が成り立つ ([3]).

(1) $f \underset{CCZ}{\sim} g$ のとき, f は APN (resp. AB) $\Longleftrightarrow$ g は APN (resp. AB).
(2) $f \underset{CCZ}{\sim} g$ のとき, f が代数的に 2 次であっても g が代数的に 2 次とは限らない.
(3) $f \underset{EA}{\sim} g$ のとき, f は代数的 2 次 $\Longleftrightarrow$ g は代数的 2 次.

命題 2.7 より,

$$f \underset{EA}{\sim} g \text{ のとき, } f \text{ は APN} \Longleftrightarrow g \text{ は APN.}$$

も従う. 一般に, CCZ-同値であっても EA-同値とは限らない, つまり, 命題 2.7 の逆は成立しないが, 代数的に 2 次の APN 関数の場合は, 逆も成り立つ. このことは, Y. Edel によって予想され, 最終的には, S. Yoshiara によって証明された ([20]) :

定理 3.7. *f と g を代数的 2 次の APN 関数とする. このとき, $f \underset{EA}{\sim} g \Longleftrightarrow f \underset{CCZ}{\sim} g$.*

3.4 APN 関数の具体例 : 特に, APN 冪関数

例 3.8. 有限体 $\mathbb{F}_{2^n}$ 上の冪関数 $f(x) = x^d$ の形の APN 関数は次の 7 種類が知られている :

表 1 知られている $\mathbb{F}_{2^n}$ 上の APN 冪関数 $f(x) = x^d$

		d	条件	$w_2(d)$	参考文献
(1)	Gold function	$2^i + 1$	$\gcd(i,n) = 1$	2	[12] [16]
(2)	Kasami function	$2^{2i} - 2^i + 1$	$\gcd(i,n) = 1$	$i+1$	[14] [15]
(3)	Welch function	$2^t + 3$	$n = 2t+1$	3	[9]
(4)	Niho function	$2^t + 2^{\frac{t}{2}} - 1$, t は偶数	$n = 2t+1$	$\frac{t+2}{2}$	[8]
(5)		$2^t + 2^{\frac{3t+1}{2}} - 1$, t は奇数	$n = 2t+1$	$t+1$	
(6)	Inverse function	$2^{2t} - 1$	$n = 2t+1$	$n-1$	[2] [16]
(7)	Dobbertin function	$2^{4t} + 2^{3t} + 2^{2t} + 2^t - 1$	$n = 5t$	$t+3$	[10]

また, (1), ..., (5) は AB であるが, (6), (7) は $n \geq 5$ のとき, AB でない ([12], [16], [15], [4], [5], [13]).

4　主結果

第 3 章で紹介したような APN 関数の性質は, $p \geq 3$ の場合では一般には成立しない. 特に, 例 3.8, (6) の Inverse function ですら APN 関数ではない. この章では, $p \geq 3$ の場合に APN 関数の定義を修正し, その性質を述べる. 特に, 系 3.2, 命題 3.3, 命題 3.6 の一般化を与える. また, $p \geq 3$ の場合に, AB の定義を一般化することで, 定理 3.5 の我々の定義における類似を述べる. 加えて, 例 3.8 の (1) Gold function と (6) Inverse function が自然に一般化されることも紹介する. そのために, まず, APN 関数の一般化である generalized almost perfect nonlinear (GAPN) 関数を定義する. 以下, p は任意の素数とする.

4.1　GAPN 関数の定義と特徴づけ

定義 4.1. 関数 $f : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_{p^n}$ と任意の $a \in \mathbb{F}_{p^n}$ に対し, $\tilde{D}_a f : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_{p^n}$ を次で定める：

$$\tilde{D}_a f(x) := \sum_{i \in \mathbb{F}_p} f(x + ia).$$

また, 任意の a, $b \in \mathbb{F}_{p^n}$ に対し,

$$\tilde{N}_f(a, b) := \left\{ x \in \mathbb{F}_{p^n} \mid \tilde{D}_a f(x) = b \right\}$$

とする. このとき, 関数 f が *generalized almost perfect nonlinear (GAPN)* であるとは,

$$\tilde{N}_f(a, b) \leq p \quad \textit{for any } a(\neq 0),\ b \in F_{p^n}$$

を満たすときにいう.

注意 4.2. $p = 2$ のとき, $\tilde{D}_a f(x) = f(x) + f(x + a)$ となり, 通常の差分関数 $D_a f$ と一致する. また, $\tilde{N}_f(a, b) = N_f(a, b)$ である. 故に, *APN* であることと *GAPN* であることは同値である.

このとき, Nyberg による APN 関数の特徴づけ (系 3.2) の一般化が得られる.

定理 4.3. 関数 $f : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_{p^n}$ に対し, f_b $(b \in \mathbb{F}_{p^n})$ を f の成分とする. このとき,

$$\sum_{a \in \mathbb{F}_{p^n}, b \in \mathbb{F}_{p^n}^{\times}} |\mathcal{F}(\tilde{D}_a f_b)|^2 \geq (p^n - 1)p^{2n+1}$$

が成り立つ. 加えて, f が *GAPN* であるための必要十分条件は, 等号が成立することである.

ここで, $\mathcal{F}(\tilde{D}_a f_b) = \sum_{x \in \mathbb{F}_{p^n}} \zeta_p^{\mathrm{Tr}(b\tilde{D}_a f(x))}$ は一般には複素数である. 従って, 絶対値を付ける必要がある.

$p = 2$ のときに, 代数的 2 次な関数が重要な役割を果たしたように, GAPN おいては, 代数的 p 次が同様の役割を果たす. 例えば, 次の命題 3.3 の一般化が得られる：

命題 4.4. $f : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_{p^n}$ を代数的に p 次の関数とする. このとき, 任意の $a \in \mathbb{F}_{p^n}^{\times}$ と任意の $b \in \mathbb{F}_{p^n}$ に対して, $\tilde{N}_f(a, b) = 0$ あるいは, $\tilde{N}_f(a, b) = \tilde{N}_f(a, \tilde{D}_a f(0))$ が成り立つ. 特に, f が *GAPN* であるための必要十分条件は, $\tilde{N}_f(a, \tilde{D}_a f(0)) \leq p$ が任意の $a \in \mathbb{F}_{p^n}^{\times}$ で成り立つことである.

EA-同値は, 代数的 p 次であることと GAPN であることを保つ. つまり, 命題 3.6 の一般化が成り立つ：

命題 4.5. 2 つの関数 $f, g : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_{p^n}$ に対して, 次が成り立つ.

(1) $f \underset{EA}{\sim} g$ のとき, f は GAPN $\Longleftrightarrow$ g は GAPN.
(2) $f \underset{EA}{\sim} g$ のとき, f は代数的 p 次 $\Longleftrightarrow$ g は代数的 p 次.

4.2 GAB の定義と GAPN との関係：特に, $p = 3$ の場合

$p \geq 3$ の場合に, 次のような AB 関数 (定義 3.4) の自然な一般化を考える.

定義 4.6. 関数 $f : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_{p^n}$ が *generalized almost bent (GAB)* であるとは,

$$W_f(a, b) \in \left\{0, \pm p^{\frac{n+1}{2}}\right\} \quad \textit{for any } a \in \mathbb{F}_{p^n},\ b \in \mathbb{F}_{p^n}^{\times}$$

を満たすときにいう.

定義 4.1 と 定義 4.6 の定義において, GAPN と GAB の関係を調べると, 定理 3.5 は完全には一般化されない. 実際, $p = 3$ の場合には, 次が成り立つ：

定理 4.7. 関数 $f : \mathbb{F}_{3^n} \longrightarrow \mathbb{F}_{3^n}$ は $f(-x) = -f(x)$ $(x \in \mathbb{F}_{3^n})$ を満たすと仮定する. f は代数的に 3 次の関数とする. このとき, f が *GAB* 関数ならば, f は *GAPN* 関数である.

注意 4.8. (1) $p = 2$ のとき, AB 関数は APN 関数であった. しかし, 定理 4.7 の仮定である "f が代数的に 3 次" は必要である. 実際, 代数的に 3 次でない関数 f で GAB だが GAPN でないものが存在する. 例えば, $f : \mathbb{F}_{3^5} \to \mathbb{F}_{3^5}$, $f(x) = x^{17}$ がそうである.
(2) $p = 2$ のとき, n が奇数であれば, 代数的に 2 次の APN 関数は AB であった. 残念ながら, 我々の定義では, この事実は一般化されない. 実際, 代数的に 3 次の GAPN 関数でも GAB でないものが存在する (つまり, 定理 4.7 の逆は成立しない). 例えば, $f : \mathbb{F}_{3^5} \to \mathbb{F}_{3^5}$, $f(x) = x^{11}$ がそうである.
(3) 定理 4.7 と同様の事実が $p \geq 5$ でも成り立つと予想している. 実際, 数値実験では反例はあらわれていない. しかしながら, いまだ証明は出来ていない.

4.3 GAPN 関数の具体例

GAPN 関数の具体例として, 例 3.8 の (1) Gold function と (6) Inverse function の一般化を紹介する.

命題 4.9. $f : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_{p^n}$ を次で定義する：

$$f(x) := x^{1+p^{i_1}+\cdots+p^{i_{p-1}}} \quad (i_1, \ldots, i_{p-1} \geq 0 \text{ and } (i_p, \ldots, i_{p-1}) \neq (0, \ldots, 0))$$

このとき,

(1) f は代数的に p 次以下であり,
(2) $\left\{x \in \mathbb{F}_{p^n} \mid x + x^{p^i} + \cdots x^{p^{i_{p-1}}} = 0\right\} = \mathbb{F}_p$ を仮定すると, f は代数的次数 p の GAPN 関数である.

この命題の系として, Gold function の一般化が得られる.

系 4.10. $f : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_{p^n}$ を次で定義する：

$$f(x) := x^{p^i+p-1} \quad (i > 0 \text{ and } \gcd(i, n) = 1)$$

このとき, f は代数的 p 次な GAPN 関数である.

Proof. $(i_1, i_2, \ldots, i_{p-1}) = (i, 0, \ldots, 0)$ とおく. このとき, 命題 4.9, (2) の仮定は, $\left\{x \in \mathbb{F}_{p^n} \mid x^{p^i-1} = 1\right\} = \mathbb{F}_p^\times$ と同値になり, これは, $\gcd(i, n) = 1$ と同値である. □

系 4.10 において, $p = 2$ とすると, Gold function が得られる. また, Inverse function も GAPN になることがわかる.

命題 4.11. $f : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_{p^n}$ を次で定義する：

$$f(x) := x^{p^n-2} = \begin{cases} x^{-1} & (x \neq 0), \\ 0 & (x = 0). \end{cases}$$

このとき, f は GAPN 関数である.

参考文献

[1] T. P. Berger, A. Canteaut, P. Charpin, Y. Laigle-Chapuy, *On almost perfect nonlinear functions over* $\mathbb{F}_2^n$, IEEE Trans. Inf. Theory **52**, pp. 4160–4170 (2006).

[2] T. Beth, C. Ding, *On almost perfect nonlinear permutations*, In: Advances in Cryptology-EUROCRYPT'93 (Lecture Notes in Computer Science). New-York: Springer-Verlag, vol. 765, pp. 65–76 (1994).

[3] L. Budaghyan, C. Carlet, A. Pott, *New classes of almost bent and almost perfect nonlinear polynomials*, IEEE Trans. Inf. Theory **52**, pp. 1141–1152 (2006).

[4] A. Canteaut, P. Charpin, H. Dobbertin, *Binary m-sequences with three-valued crosscorrelation: A proof of Welch's conjecture*, IEEE Trans. Inf. Theory **46**, pp. 4–8 (2000).

[5] A. Canteaut, P. Charpin, H. Dobbertin, *Weight divisibility of cyclic codes, highly nonlinear functions on* $\mathbb{F}_{2^m}$*, and crosscorrelation of maximum-length sequences*, SIAM J. Discr. Math., vol. 13, no. 1, pp. 105–138 (2000).

[6] C. Carlet, P. Charpin, V. Zinoviev, *Codes, bent functions and permutations suitable for DES-like cryptosystems*, Des. Codes Cryptogr. **15**, pp. 125–156 (1998).

[7] F. Chabaud, S. Vaudenay, *Links between differential and linear cryptanalysis*, In: Advances in Cryptology-EUROCRYPT'94 (Perugia). Lecture Notes in Computer Science, vol. 950, pp. 356–365 Springer, Berlin (1995).

[8] H. Dobbertin, *Almost perfect nonlinear functions on* GF(2^n)*: the Niho case*, Inf, Comput., vol. 151, no. 1-2, pp. 57–72 (1999).

[9] H. Dobbertin, *Almost perfect nonlinear functions on* GF(2^n)*: the Welch case*, IEEE Trans. Inf. Theory **45**, pp. 1271–1275 (1999).

[10] H. Dobbertin, *Almost perfect nonlinear functions on* GF(2^n)*: A new case for n divisible by* 5, in Finite Fields and Applications (Augsburg, 1999). Berlin, Germany: Springer-Verlag, pp. 113–121, (2001)

[11] Y. Edel, *On quadratic APN functions and dimensional dual hyperovals*, Des. Codes Cryptogr. **57**, pp. 35–44 (2010).

[12] R. Gold, *Maximal recursive sequences with* 3*-valued recursive crosscorrelation function*, IEEE Trans. Inf. Theory, vol. It-**45**, pp. 154–156 (1968).

[13] H. H. Hollmann, Q. Xiang, *A proof of the Welch and Niho conjectures on crosscorrelations of binary m-sequences*, Finite Fields Appl., vol. 7, no. 2, pp. 253–286, (2001)

[14] H. Janwa, R. M. Wilson, *Hyperplane sections of Fermat varieties in* $\mathbb{P}^3$ *in cher.* 2 *and some applications to cyclic codes*, in Applied Algebra, Algebraic Algorithms and Error-Correcting Codes (San Juan, PR, 1993) (Lecture Notes in Computer Science). Berlin, Germany: Springer-Verlag, vol. 673, pp. 180–194 (1993).

[15] T. Kasami, *The weight enumerators for several classes of subcodes of the* 2*nd order binary Reed-Muller codes*, Inf, Contr., vol. 18, pp. 369-394 (1971).

[16] K. Nyberg, *Differentially uniform mappings for cryptography*, in Advances in Cryptography. EUROCRYPT' 93 (Lecture Notes in Computer Science), T. Helleseth, Ed. New York: Springer-Verlag, vol. 765, pp. 55–64 (1993).

[17] K. Nyberg, *S-boxes and round functions with controllable linearity and differential uniformity*, in Fast Software Encryption - FSE'94 (Lecture Notes in Computer Science). Berlin, Germany: Springer-Verlag, vol. 1008, pp. 111-130 (1995).

[18] A. Pott, *Almost perfect and planar functions*, Des. Codes Cryptogr. **78**, pp. 141–195 (2016).

[19] S. Yoshiara, *Dimensional dual arcs-a survey*, In:Finite Geometries, Groups, and Computation, pp. 247 –266. De Gruyter, Berlin (2006).

[20] S. Yoshiara, *Equivalences of quadratic APN functions*, J. Algebr. Comb. **35**, pp. 461 –475 (2012).