Almost Perfect Nonlinear Functions

Samed Bajrić

UNIVERSITY OF PRIMORSKA

FAMNIT

23. January 2012.

Boolean function

- A *Boolean function* f in n variables is an $\mathbb{F}_2$–valued function on $\mathbb{F}_2^n$
- more formally $f : \mathbb{F}_2^n \mapsto \mathbb{F}_2$ maps

$$(x_1, \ldots, x_n) \in \mathbb{F}_2^n \mapsto f(x) \in \mathbb{F}_2$$

- unique representation of f as a polynomial over $\mathbb{F}_2$ in n variables of the form

$$f(x_1, \ldots, x_n) = \sum_{u \in \mathbb{F}_2^n} a_u \left(\prod_{i=1}^{n} x^{u_i}\right), \;\; a_u \in \mathbb{F}_2$$

is called the *algebraic normal form* of f

Vectorial Boolean function

- Any function F from $\mathbb{F}_2^n$ into $\mathbb{F}_2^n$ can be considered as a *vectorial Boolean function*, i.e. F can be presented in the form

  $$F(x_1, \ldots, x_n) = (f_1(x_1, \ldots, x_n), \ldots, f_n(x_1, \ldots, x_n))$$

  where the Boolean functions $f_1, \ldots, f_n$ are called the *coordinate* or *component functions* of the function F

- A function F is *affine* if $deg(F) \leq 1$

  F is called *linear* if it is affine and $F(0) = 0$

  The functions of the algebraic degree 2 are called *quadratic functions*

Vectorial Boolean function

- A function $F : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$ is called *balanced* if it takes every value on $\mathbb{F}_2^m$ the same number 2^{n-m} of times.

  The balanced functions from $\mathbb{F}_2^n$ to itself are the permutations of $\mathbb{F}_2^n$

- Let $F : \mathbb{F}_2^n \mapsto \mathbb{F}_2^n$. The function $W_F : \mathbb{F}_2^n \times \mathbb{F}_2^n \mapsto \mathbb{Z}$ defined by

$$W_F(a,b) = \sum_{x \in \mathbb{F}_2^n} (-1)^{b \cdot F(x) + a \cdot x}, \quad a \in \mathbb{F}_2^n, b \in \mathbb{F}_2^{n^*}$$

  is called the *Walsh transform* of the function F

- the set

$$\Lambda_F = \{W_F(a,b) : a \in \mathbb{F}_2^n, b \in \mathbb{F}_2^{n^*}\}$$

  is called the *Walsh spectrum* of F

Vectorial Boolean function

- the *nonlinearity* of a function $F : \mathbb{F}_2^n \mapsto \mathbb{F}_2^n$ is the value

$$\mathcal{NL}(F) = 2^{n-1} - \frac{1}{2} \max_{a,b \in \mathbb{F}_2^n, b \neq 0} |W_F(a,b)|$$

  which equals the minimum Hamming distance between all nonzero linear combinations of the coordinate functions of F and all affine Boolean functions on n variables.

- the nonlinearity of any function $F : \mathbb{F}_2^n \mapsto \mathbb{F}_2^n$ has the same upper bound

$$\mathcal{NL}(F) \leq 2^{n-1} - 2^{\frac{n}{2}-1}$$

  as a Boolean functions

  the functions for which equality holds are called *bent*

Vectorial Boolean function

Proposition

A function $F : \mathbb{F}_2^n \mapsto \mathbb{F}_2^n$ is bent if and only if one of the following conditions holds:

1. *for any nonzero $c \in \mathbb{F}_2^n$ the Boolean function $c \cdot F$ is bent*
2. $\Lambda_F = \{\pm 2^{\frac{n}{2}}\}$
3. *for any nonzero $a \in \mathbb{F}_2^n$ the function $F(x+a) + F(x)$ is balanced*

- A function $F : \mathbb{F}_2^n \mapsto \mathbb{F}_2^n$ is called *perfect nonlinear* if for any nonzero $a \in \mathbb{F}_2^n$ the function $F(x+a) + F(x)$ is balanced

  Clearly, a function F is bent if and only if it is perfect nonlinear

APN and AB functions

Definiton

Let F be a function from $\mathbb{F}_2^n$ into $\mathbb{F}_2^n$. For any $a \in \mathbb{F}_2^n$, derivative of F is the function D_aF from $\mathbb{F}_2^n$ into $\mathbb{F}_2^n$ defined by

$$D_aF(x) = F(x+a) + F(x), \ \ \forall x \in \mathbb{F}_2^n$$

If $D_aF(x)$ is constant then a is said to be a linear structure of F.

APN and AB functions

Definiton

Let F be a function from $\mathbb{F}_2^n$ into $\mathbb{F}_2^n$. For any $a, b \in \mathbb{F}_2^n$, we denote

$$\delta(a,b) = \#\{x \in \mathbb{F}_2^n : D_aF(x) = b\},$$

where $\#E$ is cardinality of any set E. Then, we have

$$\delta(F) = \max_{a \neq 0, b \in \mathbb{F}_2^n} \delta(a,b) \geq 2,$$

and the functions for which equality holds are said to be Almost Perfect Nonlinear (APN)

APN and AB functions

The APN property can be equivalently defined as follows.

Proposition

Let F be any function on $\mathbb{F}_2^n$. Then, F is Almost Perfect Nonlinear (APN) IF AND ONLY IF, for any nonzero $a \in \mathbb{F}_2^n$, the set

$$\{D_a F(x) : x \in \mathbb{F}_2^n\}$$

has cardinality 2^{n-1}.

APN and AB functions

- a better bound for the nonlinearity exists

$$\mathcal{NL}(F) \leq 2^{n-1} - 2^{\frac{n-1}{2}}$$

in case of equality the function F is called *almost bent (AB)* or *maximum nonlinear*

- AB functions exist only for n odd

- when n is even, functions with the nonlinearity

$$2^{n-1} - 2^{\frac{n}{2}}$$

are known and it is conjectured that this value is the highest possible nonlinearity for the case n even

APN and AB functions

- the correspondence between functions in the finite field and functions in the vector space
- any function F from $\mathbb{F}_2^n$ into $\mathbb{F}_2^n$ can be expressed as a polynomial in $\mathbb{F}_{2^n}[x]$

Example

$F : \mathbb{F}_{2^3} \mapsto \mathbb{F}_{2^3}, F(x) = x^3.$

Characterizations of AB functions

Proposition

A function $F : \mathbb{F}_{2^n} \mapsto \mathbb{F}_{2^n}$ is AB if and only if one of the following conditions is satisfied:

1. $\Lambda_F = \{0, \pm 2^{\frac{n+1}{2}}\}$;
2. *for every $a, b \in \mathbb{F}_{2^n}$ the system of equations*

$$\begin{cases} x + y + z & = & 0 \\ F(x) + F(y) + F(z) & = & b \end{cases}$$

   has $3 \cdot 2^n - 2$ solutions (x, y, z) if $b = F(a)$, and $2^n - 2$ solutions otherwise;

3. *the function $\gamma_F : \mathbb{F}_2^{2n} \mapsto \mathbb{F}_2$ defined by equality*

$$\gamma_F(a,b) = \begin{cases} 1 & \text{if } a \neq 0 \text{ and } \delta_F(a,b) \neq 0 \\ 0 & \text{otherwise} \end{cases} \quad \text{is bent.}$$

Characterizations of APN functions

Proposition

A function $F : \mathbb{F}_{2^n} \mapsto \mathbb{F}_{2^n}$ is APN if and only if one of the following conditions is satisfied:

1. $\Delta_F = \{\delta_F(a,b) : a, b \in \mathbb{F}_{2^n}, a \neq 0\} = \{0, 2\}$
2. *for every $(a,b) \neq 0$ the system*
$$\begin{cases} x + y & = & 0 \\ F(x) + F(y) & = & b \end{cases}$$
admits 0 or 2 solutions;
3. *for any nonzero $a \in \mathbb{F}_{2^m}$ the derivative D_aF is a two-to-one mapping;*
4. *the Boolean function γ_F has the weight $2^{2n-1} - 2^{n-1}$;*
5. *F is not affine on any 2-dimensional affine subspace $\mathbb{F}_2^n$*

Relationship between AB and APN functions

Lemma

Every AB function is APN function.

Example

$F : \mathbb{F}_{2^3} \mapsto \mathbb{F}_{2^3}, F(x) = x^3$, is AB and APN.

- the converse is not true in general, even in the n odd case *(counter-examples: inverse function, Dobbertin function)*
- if n is odd, then every quadratic APN function is AB

Relationship between AB and APN functions

- sufficient conditions for APN functions to be AB:

Proposition

An APN function $F : \mathbb{F}_{2^n} \mapsto \mathbb{F}_{2^n}$ is AB if and only if one of the following conditions is fulfilled:

1. *all the values in Λ_F are divisible by $2^{\frac{n+1}{2}}$*
2. *for any $c \in \mathbb{F}_{2^n}$ the Walsh transform of the function $c \cdot F$ takes three values $\{0, \pm 2^r\}$, $\frac{n}{2} \leq r \leq n$*

APN permutations

- the balanced functions from $\mathbb{F}_2^n$ to itself are the permutations of $\mathbb{F}_2^n$
- if F is APN power function with $F(x) = x^d$, then $gcd(d, 2^n - 1) = 1$ for odd n, and F is a permutation

APN permutations

- the balanced functions from $\mathbb{F}_2^n$ to itself are the permutations of $\mathbb{F}_2^n$
- if F is APN power function with $F(x) = x^d$, then $gcd(d, 2^n - 1) = 1$ for odd n, and F is a permutation

Example

$d = 3$, $n = 6$

APN permutations

- the balanced functions from $\mathbb{F}_2^n$ to itself are the permutations of $\mathbb{F}_2^n$
- if F is APN power function with $F(x) = x^d$, then $gcd(d, 2^n - 1) = 1$ for odd n, and F is a permutation

Example

$d = 3$, $n = 6$

$\Rightarrow gcd(3, 2^6 - 1) = gcd(3, 63) = 3 \neq 1$

APN permutations

- the balanced functions from $\mathbb{F}_2^n$ to itself are the permutations of $\mathbb{F}_2^n$
- if F is APN power function with $F(x) = x^d$, then $gcd(d, 2^n - 1) = 1$ for odd n, and F is a permutation

Example

$d = 3$, $n = 6$

$\Rightarrow gcd(3, 2^6 - 1) = gcd(3, 63) = 3 \neq 1$

$\alpha^{21} \Rightarrow (\alpha^{21})^3 = \alpha^{63} = 1$, since $\alpha^{2^n-1} = 1$ in every $\mathbb{F}_{2^n}$

APN permutations

- the balanced functions from $\mathbb{F}_2^n$ to itself are the permutations of $\mathbb{F}_2^n$
- if F is APN power function with $F(x) = x^d$, then $gcd(d, 2^n - 1) = 1$ for odd n, and F is a permutation

Example

$d = 3$, $n = 6$

$\Rightarrow gcd(3, 2^6 - 1) = gcd(3, 63) = 3 \neq 1$

$\alpha^{21} \Rightarrow (\alpha^{21})^3 = \alpha^{63} = 1$, since $\alpha^{2^n-1} = 1$ in every $\mathbb{F}_{2^n}$

$\alpha^{42} \Rightarrow (\alpha^{42})^3 = \alpha^{126} = (\alpha^{63})^2 = 1$

APN permutations

- the balanced functions from $\mathbb{F}_2^n$ to itself are the permutations of $\mathbb{F}_2^n$
- if F is APN power function with $F(x) = x^d$, then $gcd(d, 2^n - 1) = 1$ for odd n, and F is a permutation

Example

$d = 3$, $n = 6$

$\Rightarrow gcd(3, 2^6 - 1) = gcd(3, 63) = 3 \neq 1$

$\alpha^{21} \Rightarrow (\alpha^{21})^3 = \alpha^{63} = 1$, since $\alpha^{2^n - 1} = 1$ in every $\mathbb{F}_{2^n}$

$\alpha^{42} \Rightarrow (\alpha^{42})^3 = \alpha^{126} = (\alpha^{63})^2 = 1$

$1 \Rightarrow 1^3 = 1$

APN permutations

- the balanced functions from $\mathbb{F}_2^n$ to itself are the permutations of $\mathbb{F}_2^n$
- if F is APN power function with $F(x) = x^d$, then $gcd(d, 2^n - 1) = 1$ for odd n, and F is a permutation

Example

$d = 3$, $n = 6$

$\Rightarrow gcd(3, 2^6 - 1) = gcd(3, 63) = 3 \neq 1$

$\alpha^{21} \Rightarrow (\alpha^{21})^3 = \alpha^{63} = 1$, since $\alpha^{2^n-1} = 1$ in every $\mathbb{F}_{2^n}$

$\alpha^{42} \Rightarrow (\alpha^{42})^3 = \alpha^{126} = (\alpha^{63})^2 = 1$

$1 \Rightarrow 1^3 = 1$

Conclusion: F is not a permutation!

APN permutations

- if F is APN power function with $F(x) = x^d$, then $gcd(d, 2^n - 1) = 3$ for even n, and F is three-to-one

Fact

There are APN permutations on $\mathbb{F}_{2^6}$

Open Problem

Are there APN permutations on $\mathbb{F}_{2^{2n}}, n > 3$?

APN permutations

Theorem

If F is APN permutation, then F^{-1} is APN.

Proof

Prove F^{-1} is is APN where F is an APN permutation.
Since F is a permutation, F is bijective and since F is APN, if is $b \in D_a F$, then $F(x+a)+F(x)=b$ has exactly 2 solutions.
Let $y=F(x)$ and $y'=F(x+a)$, then $y'=y+b$. So, for given a and b, $F(x+a)+F(x)=b$ has exactly 0 or 2 solutions. But, $x+a=F^{-1}(y+b)$ and $x=F^{-1}(y)$, so $F^{-1}(y+b)+F^{-1}(y)=a$ which has exactly 0 or 2 solutions since $F(x+a)+F(x)=b$ has exactly 0 or 2 solutions. That means, F^{-1} is APN.

Known APN power functions x^d on $\mathbb{F}_{2^n}$ up to EA-equivalence and inverse

	Exponents d	Conditions
Gold functions	$2^i + 1$	gcd(i,n)=1
Kasami functions	$2^{2i} - 2^i + 1$	gcd(i,n)=1
Welch function	$2^t + 3$	$n = 2t + 1$
Niho function	$2^t - 2^{\frac{t}{2}} - 1$, t even $2^t - 2^{\frac{3t+1}{2}} - 1$, t odd	$n = 2t + 1$
Inverse function	$2^{2t} - 1$	$n = 2t + 1$
Dobbertin function	$2^{4t} + 2^{3t} + 2^{2t} + 2^t - 1$	$n = 5t$

Known APN power functions x^d on $\mathbb{F}_{2^n}$ up to EA-equivalence and inverse

	Exponents d	Conditions
Gold functions	$2^i + 1$	gcd(i,n)=1
Kasami functions	$2^{2i} - 2^i + 1$	gcd(i,n)=1
Welch function	$2^t + 3$	$n = 2t + 1$
Niho function	$2^t - 2^{\frac{t}{2}} - 1$, t even $2^t - 2^{\frac{3t+1}{2}} - 1$, t odd	$n = 2t + 1$
Inverse function	$2^{2t} - 1$	$n = 2t + 1$
Dobbertin function	$2^{4t} + 2^{3t} + 2^{2t} + 2^t - 1$	$n = 5t$

Conjecture

This list of APN power functions is complete. (Dobbertin)

Known APN power functions x^d on $\mathbb{F}_{2^n}$ up to EA-equivalence and inverse

	Exponents d	Conditions
Gold functions	$2^i + 1$	gcd(i,n)=1
Kasami functions	$2^{2i} - 2^i + 1$	gcd(i,n)=1
Welch function	$2^t + 3$	$n = 2t + 1$
Niho function	$2^t - 2^{\frac{t}{2}} - 1$, t even $2^t - 2^{\frac{3t+1}{2}} - 1$, t odd	$n = 2t + 1$
Inverse function	$2^{2t} - 1$	$n = 2t + 1$
Dobbertin function	$2^{4t} + 2^{3t} + 2^{2t} + 2^t - 1$	$n = 5t$

Conjecture

This list of APN power functions is complete. (Dobbertin)

proved by Dobbertin: APN power functions are permutations of $\mathbb{F}_{2^n}$ if n is odd, and are three-to-one if n is even

Thank you for your Attention!