On Inverses of APN Exponents

Valentin Suder
Joint work with Gohar Kyureghyan

Outline

Background on APN/AB functions

APN power functions

Finding inverses of some power functions, in particular APN

Almost Perfect Nonlinear (APN) functions

A function

$$F : \mathbb{F}_{2^n} \mapsto \mathbb{F}_{2^n}$$

is called APN (almost perfect nonlinear) if for any $a \in \mathbb{F}_{2^n}^*$ and any $b \in \mathbb{F}_{2^n}$ the equation

$$F(x+a) + F(x) = b$$

has at most 2 solutions in $\mathbb{F}_{2^n}$.

Fact

APN functions have optimal resistance against differential attacks.

Almost Bent (AB) functions

A function

$$F : \mathbb{F}_{2^n} \mapsto \mathbb{F}_{2^n}, \ n \text{ odd}$$

is called *AB* (almost bent) if

$$\sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr(\alpha F(x) + \beta x)} \in \{0, \ \pm 2^{\frac{n+1}{2}}\}$$

for any $\alpha \neq 0, \ \beta \in \mathbb{F}_{2^n}$.

Fact

1. *AB functions have optimal resistance against linear attacks.*
2. *Any AB function is also APN.*

Power functions

For an integer d, the function of $\mathbb{F}_{2^n}$ defined by

$$x \mapsto x^d$$

is called a power function with exponent d.

Interest:

- lower implementation cost in hardware.
- differential properties are related to the weight enumerators of cyclic codes.

Theorem

1. *An APN power function on $\mathbb{F}_{2^n}$ is bijective if n is odd, and it is $3-to-1$ if n is even.*
2. *An exponent d defines an APN/AB power function if and only if $2 \cdot d$ does so.*
3. *The (compositional) inverse of an APN/AB bijective function is APN/AB as well.*

Known APN/AB power functions

APN/AB power functions x^d over $\mathbb{F}_{2^n}$ with $n = 2t + 1$

	exponents d	
Gold (quadratic)	$2^k + 1$ with $\gcd(k, n) = 1$, $1 \leq k \leq t$	APN/AB
Kasami	$2^{2k} - 2^k + 1$ with $\gcd(k, n) = 1$ $2 \leq k \leq t$	APN/AB
Welch	$2^t + 3$	APN/AB
Niho	$2^t + 2^{\frac{t}{2}} - 1$ if t is even $2^t + 2^{\frac{3t+1}{2}} - 1$ if t is odd	APN/AB
inverse	$2^{2t} - 1$	APN
Dobbertin	$2^{4k} + 2^{3k} + 2^{2k} + 2^k - 1$ if $n = 5k$	APN

Question

Ideal case: Is it possible to find explicit formulas for the inverses of some exponents, in particular APN exponents?

At least, can we find some interesting informations about these inverses?

Algebraic degree

The algebraic degree of the power function $x \mapsto x^d$ on $\mathbb{F}_{2^n}$ is the Hamming weight of the binary representation of d modulo $2^n - 1$. We denote it by $wt_{2,n}(d)$.

Example ($d = 13$)

- $n = 3$, $13 \equiv 6 = (110)_2 \pmod 7$ *so* $wt_{2,3}(13) = 2$.
- $n \geq 4$, $13 \equiv 13 = (1101)_2 \pmod{2^n - 1}$ *so* $wt_{2,n}(13) = 3$.

Proposition (Carlet, Charpin, Zinoviev (1998))

The algebraic degree of an AB function on $\mathbb{F}_{2^n}$ *does not exceed* $(n+1)/2$.

Inverses of power functions

A power function $F : x \mapsto x^d$ is bijective on $\mathbb{F}_{2^n}$ if and only if $\gcd(d, 2^n - 1) = 1$.

The inverse is then the power function

$$x \mapsto x^e$$

where its exponent e is such that $ed \equiv 1 \pmod{2^n - 1}$:

$$(x^d)^e = x^{ed} \equiv x \pmod{x^{2^n} - x}$$

Quadratic exponents

$$x \mapsto x^{2^k+1}$$

- A quadratic exponent $2^k + 1$ defines a bijective power function on $\mathbb{F}_{2^n}$ if and only if $\frac{n}{\gcd(n,k)}$ is odd.
- When $\gcd(n, k) = 1$ these exponents are called Gold exponents.
- Quadratic power functions appear in many applications.

Quadratic exponents

Theorem

Let $\gcd(n,k) = s$ and $t = n/s$ be odd. Then

$$(2^k+1)^{-1} \equiv \left(\sum_{i=0}^{s-2} \sum_{j=0}^{\frac{t-3}{2}} 2^{i+(2j+1)k} \right) + \sum_{j=0}^{\frac{t-1}{2}} 2^{s-1+2jk} \pmod{2^n-1}$$

Furthermore, $wt_{2,n}((2^k+1)^{-1}) = \frac{n-s+2}{2}$.

Corollary (Nyberg (1993))

Let n be odd, and $\gcd(n,k) = 1$. *Then*

$$(2^k+1)^{-1} \equiv \frac{2^{k(n+1)}-1}{2^{2k}-1} \equiv \sum_{j=0}^{\frac{n-1}{2}} 2^{2jk} \pmod{2^n-1}$$

Some examples

$$\gcd(n,k) = s \qquad \text{and} \qquad t = n/s \text{ odd}$$

$$(2^k+1)^{-1} \equiv \left(\sum_{i=0}^{s-2} \sum_{j=0}^{\frac{t-3}{2}} 2^{i+(2j+1)k} \right) + \sum_{j=0}^{\frac{t-1}{2}} 2^{s-1+2jk} \pmod{2^n-1}$$

Example

$n = 15,\ k = 3 \qquad \Rightarrow \qquad \gcd(n,k) = 3 \text{ and } t = 5.$

$$\begin{aligned}(2^3+1)^{-1} &= (2^3(1+2) + 2^{3\cdot 3}(1+2)) + (2^2 + 2^{2\cdot 3+2} + 2^{4\cdot 3+2}) \\ &= (000011000011000)_2 + (100000100000100)_2 \\ &= (100011100011100)_2\end{aligned}$$

Some examples

$$\gcd(n,k) = s \qquad \text{and} \qquad t = n/s \text{ odd}$$

$$(2^k+1)^{-1} \equiv \left(\sum_{i=0}^{s-2} \sum_{j=0}^{\frac{t-3}{2}} 2^{i+(2j+1)k} \right) + \sum_{j=0}^{\frac{t-1}{2}} 2^{s-1+2jk} \pmod{2^n-1}$$

Example

$n = 10,\ k = 4 \qquad \Rightarrow \qquad \gcd(n,k) = 2 \text{ et } t = 5.$

$$\begin{aligned}
(2^4+1)^{-1} &= (2^4 + 2^{3\cdot 4}) + (2 + 2^{2\cdot 4+1} + 2^{4\cdot 4+1}) \\
&\equiv (2^4 + 2^2) + (2 + 2^9 + 2^7) \pmod{2^{10}-1} \\
&= (0000010100)_2 + (1010000010)_2 \\
&= (1010010110)_2
\end{aligned}$$

Welch exponents

$$n = 2t + 1, \qquad x \mapsto x^{2^t+3}$$

Theorem

- If $t \equiv 1 \pmod 8$ then

$$(2^t + 3)^{-1} = 2^{t-1} + 2^t + \frac{2^{t-1} - 1}{17}\left(7 \cdot 2^{t+2} + 1\right)$$

  with binary weight $t + 1$.
- If $t \equiv 2 \pmod 8$ then

$$(2^t + 3)^{-1} = 1 + 2^{t+1} + \frac{2^{t-2} - 1}{17}\left(5 \cdot 2^{t+3} + 16\right)$$

  with binary weight t.
- Similar expressions for $t \equiv 3, 4, 5, 6, 7, 0 \pmod 8$.

Dobbertin exponents

$$n = 5k, \qquad x \mapsto x^{2^{4k}+2^{3k}+2^{2k}+2^k-1}$$

Theorem

For an odd k, let $d = 2^{4k} + 2^{3k} + 2^{2k} + 2^k - 1$ then,

$$d^{-1} = \frac{1}{2}\left(\frac{2^{5k}-1}{2^k-1} \cdot \frac{2^{k+1}-1}{3} - 1\right).$$

Furthermore,

$$2 \cdot d^{-1} = \left(\sum_{i=0}^{4} \sum_{j=0}^{\frac{k-1}{2}} 2^{ik+2j}\right) - 1,$$

showing that $wt_{2,n}(d^{-1}) = \frac{5k+3}{2}$.

Kasami exponents

$$x \mapsto x^{2^{2k}-2^k+1}$$

Lemma

A Kasami exponent $2^{2k} - 2^k + 1$ defines a bijective power function on $\mathbb{F}_{2^n}$ if and only if one of the following cases occurs:

(A) $\frac{n}{\gcd(n,k)}$ *is odd;*

(B) $\frac{n}{\gcd(n,k)}$ *is even, k is even and* $\gcd(k, n) = \gcd(3k, n)$.

The Kasami exponents are APN if and only if $\gcd(n, k) = 1$.

Partial Results

Theorem (Case (A))

$n = t \cdot \gcd(n,k)$ with t odd and $d = 2^{2k} - 2^k + 1$.

- If $t \equiv 1 \pmod 3$, then

$$d^{-1} \equiv 1 + 2^{2k}(2^{3k}-1)(2^k+1)\sum_{j=0}^{\frac{t-7}{6}} 2^{6kj}$$

$$\equiv 1 + 2^{2k} \cdot (2^k+1) \cdot \frac{2^{n-k}-1}{2^{3k}+1} \pmod{2^n - 1}.$$

- Similar expressions for $t \equiv 2, 3 \pmod 3$.

Fact

- $t \equiv 1, 2 \pmod 3$, $gcd(n,k) = k \Rightarrow wt_{2,n}(d^{-1}) = \frac{n-k+2}{2}$.
- $t \equiv 0 \pmod 3$, $gcd(n,k) = k \Rightarrow wt_{2,n}(d^{-1}) = \frac{n-3k+4}{2}$.

$2^k - 1$ exponents

$$x \mapsto x^{2^k-1}$$

They are not APN, but still have good differential properties (Blondeau, Canteaut, Charpin (2011)).

Theorem

n and k coprime positive integers,

$$(2^k-1)^{-1} \equiv \sum_{i=0}^{k^{-1}-1 \pmod n} 2^{ki} \pmod{2^n-1}$$
$$= \frac{2^{k\cdot k^{-1}}-1}{2^k-1}.$$

Furthermore, $wt_{2,n}((2^k-1)^{-1}) = k^{-1} \pmod n$.

Conclusion

We considered the problem of finding an explicit formula for the inverses of some interesting exponents, in particular APN exponents.

Succeeded: Welch, Dobbertin, quadratic and exponents of the form $2^k - 1$ (Gold and Niho are already known).
Partial results: Kasami

We have also examined other exponents. Similar results can be deduced in an odd characteristic.