On Inverses of APN Exponents

Gohar Kyureghyan, Valentin Suder

On Inverses of APN Exponents

Gohar M. Kyureghyan[1,2]
[1]Department of Mathematics
Otto-von-Guericke University
Universitätsplatz 2
39106 Magdeburg, Germany
Email: gohar.kyureghyan@ovgu.de

Valentin Suder[2]
[2]INRIA Paris-Rocquencourt
Project-Team SECRET
Domaine de Voluceau - B.P. 105
78153 Le Chesnay Cedex, France
Email: valentin.suder@inria.fr

***Abstract*—In this extended abstract we present results on the inverses modulo $2^n - 1$ of the known APN exponents. In particular, we describe explicitly the inverses of the Welch and Dobbertin exponents and give the main ideas of their proofs. Further, we observe that the inverse of the Dobbertin exponent defines an APN function on $\mathbb{F}_{2^n}$ of algebraic degree $\frac{n+3}{2}$, which is the first example of such a function.**

I. Introduction

The classical modular inversion is the problem to invert numbers modulo a *fixed* number. We consider a dual problem, inverting a fixed number d modulo $2^n - 1$ for *all* suitable n.

Let d be a fixed positive integer and $n \geq 2$ such that $\gcd(2^n - 1, d) = 1$. Then d is invertible modulo $2^n - 1$ for all such n. We denote by d^{-1} the least positive residue of d modulo $2^n - 1$. Are there any properties shared by the inverses d^{-1} modulo any $2^n - 1$? Is it possible to find an explicit formula for d^{-1} modulo $2^n - 1$ for all n? In this paper we study these questions for several families of integers d: mainly for the exponents of the known APN power functions on $\mathbb{F}_{2^n}$. We call integers defining APN power function APN exponents. The inverses of APN exponents are APN as well. It is usually said that the known APN and AB power permutations are those listed in Table I (with their shifts and inverses modulo $2^n - 1$), cf. [7]. However, for a better understanding of APN and AB exponents, it could be helpful to have explicit representations of these inverses. An important parameter for an APN exponent is its binary weight, which defines the algebraic degree of the corresponding function and thus resistance of it to some cryptological attacks. The study of inverses of APN exponents was originated in [13] and [14], where the inverses and their binary weights for the so-called Gold and Niho exponents were found respectively. In this paper we give the inverses and their binary weights for the so-called Welch and Dobbertin exponents. Herewith the Kasami exponent remains the only known APN exponent for which the inverse is not completely understood. For the Kasami exponent we have some partial results. We generalize also the work of Nyberg [13], and give results for exponents of the shape $2^k - 1$. This paper is an extended abstract, more complete studies will appear in a forthcoming article.

II. Differential and linear properties

Let $\mathbb{F}_{2^n}$ be the finite field of order 2^n, for basic theory on finite fields we refer to [11].

Definition 1. (a) *A function $F : \mathbb{F}_{2^n} \mapsto \mathbb{F}_{2^n}$ is called APN (almost perfect nonlinear) if for any non-zero $a \in \mathbb{F}_{2^n}$ and any $b \in \mathbb{F}_{2^n}$ the equation $F(x+a) + F(x) = b$ has at most 2 solutions.*

(b) *A function $F : \mathbb{F}_{2^n} \mapsto \mathbb{F}_{2^n}$, n 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 all $\alpha \neq 0, \ \beta \in \mathbb{F}_{2^n}$.

The APN and AB functions provide the best resistance to differential and linear attacks, respectively, when used as S-boxes in cryptography. There are very few known examples of APN and AB functions. The best studied such functions are the power functions $x \mapsto x^d$, $x \in \mathbb{F}_{2^n}$, where d is a fixed integer. Power APN and AB functions play also an important role in coding theory and in the study of reversed Dickson polynomials [8], [10].

It is easy to see that a power function $F : \mathbb{F}_{2^n} \mapsto \mathbb{F}_{2^n}$ is bijective if and only if $\gcd(d, 2^n - 1) = 1$.The (compositional) inverse of a bijective power function $F(x) = x^d$ is given by $F^{-1}(x) = x^e$ where e is the inverse of d modulo $2^n - 1$, i.e. $ed \equiv 1 \pmod{2^n - 1}$.

Definition 2. *Let d and n be positive integers. We denote by $wt_2(d)$ the Hamming weight of the binary representation of d, and by $wt_{2,n}(d)$ the Hamming weight of the least positive residue of d modulo $2^n - 1$. The algebraic degree of the power function $x \mapsto x^d$ on $\mathbb{F}_{2^n}$ is $wt_{2,n}(d)$.*

Observe that if $1 \leq d \leq 2^n - 1$ then $wt_2(d) = wt_{2,n}(d)$.

The following theorem summarizes the properties of APN and AB power functions, see for example [1], [7], [8].

Theorem 1. 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 (where $3 - to - 1$ means that every non-zero image has 3 preimages).*

2) *Any AB function is APN.*

3) *The (compositional) inverse of an APN/AB function is APN/AB as well.*
4) *An exponent d defines APN/AB function if and only if $2 \cdot d$ does so.*
5) *The algebraic degree of an AB function on $\mathbb{F}_{2^n}$ does not exceed $(n+1)/2$.*

Remark 1. *We say that d and d' are in the same cyclotomic coset modulo $2^n - 1$ if*

$$d' \equiv 2^i \cdot d \pmod{2^n - 1}$$

for some $0 \leq i \leq n-1$. When working modulo $2^n - 1$, we call $2^i \cdot d$ a shift of d.

The known APN and AB power permutations are those listed in Table I (with their shifts and inverses modulo $2^n - 1$), see for example Chapter 3 of [7].

	exponents d	
Gold	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
inverse	$2^{2t}-1$	APN
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
Dobbertin	$2^{4k}+2^{3k}+2^{2k}+2^k-1$ if $n=5k$	APN

TABLE I

EXPONENTS DEFINING APN/AB POWER FUNCTIONS ON $\mathbb{F}_{2^n}$, $n = 2t+1$

III. QUADRATIC EXPONENTS

The integers of binary weight 2 define power functions of algebraic degree 2 on $\mathbb{F}_{2^n}$, therefore they are often referred to as quadratic exponents. The next result is well known, a proof of it can be found, for example, in [12, Lemma 11.1].

Lemma 1. *Let n and k be positive integers. Then $\frac{n}{\gcd(n,k)}$ is odd if and only if $\gcd(2^k+1, 2^n-1) = 1$; and $\frac{n}{\gcd(n,k)}$ is even if and only if $\gcd(2^k+1, 2^n-1) = 2^{\gcd(n,k)}+1$.*

The quadratic APN exponents are the Gold exponents in Table I.

Theorem 2. *Let n and k be positive integers such that*

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

Then

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

with convention $\sum_{i=a}^{b} 2^i = 0$ for $a > b$. Furthermore,

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

Proof: Direct calculations show

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

To complete the proof of (1), it remains to show that

$$\sum_{i=0}^{s-1}\sum_{j=0}^{t-1} 2^{i+jk} \equiv 0 \pmod{2^n-1}. \qquad (2)$$

Since $2^r \equiv 2^{r \pmod n} \pmod{2^n-1}$, we can consider the exponents in (2) as elements of the cyclic group $\mathbb{Z}_n$. Let $\langle g \rangle$ be the subgroup of $\mathbb{Z}_n$ generated by $g \in \mathbb{Z}_n$. Then

$$\langle k \rangle = \langle \gcd(k,n) \rangle = \langle s \rangle.$$

Using these observations we have

$$\sum_{j=0}^{t-1} 2^{i+jk} \equiv 2^i \sum_{j=0}^{t-1} 2^{js} \pmod{2^n-1},$$

where the exponents of the latter sum describe the coset $i + \langle s \rangle$. Since the set of cosets of $\langle s \rangle$ partition $\mathbb{Z}_n$ we get

$$\sum_{i=0}^{s-1}\sum_{j=0}^{t-1} 2^{i+jk} \equiv 2^n - 1 \equiv 0 \pmod{2^n-1}.$$

The above considerations show in particular that the different summands in (1) remain distinct modulo (2^n-1). Hence

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

completing the proof.

Remark 2. *It is easy to see by direct calculations that*

$$(2^k+1)^{-1} \equiv 2^{n-1}\left(1 + (2^k-1)(2^k + 2^{3k} + \cdots + 2^{(t-2)k})\right) \equiv 1 + \sum_{i=1}^{t}(-1)^i \cdot 2^{ki-1} \pmod{2^n-1}.$$

Further, sum (1) of Theorem 2 can be written as

$$2^k(2^{s-1}-1)\frac{2^{2k\frac{t-1}{2}}-1}{2^{2k}-1} + 2^{s-1}\frac{2^{2k\frac{t+1}{2}}-1}{2^{2k}-1}.$$

As a special case of Theorem 2, we have:

Corollary 1. *[13, Proposition 5]*
Let n be odd, and $\gcd(n,k) = 1$. Then

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

and

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

IV. Kasami exponents

We call integers $2^{2k}-2^k+1$ with $0<k<n$ Kasami exponents. In our considerations we may assume $k \le \frac{n}{2}$, since $2^{2k}-2^k+1$ and $2^{2(n-k)}-2^{n-k}+1$ lie in the same cyclotomic coset modulo 2^n-1. Indeed, $(2^{2(n-k)}-2^{n-k}+1)2^{2k} \equiv 2^{2k}-2^k+1 \pmod{2^n-1}$.

Lemma 2. 1)
$$\gcd(2^{2k}-2^k+1, 2^k+1) = \begin{cases} 1 & \textit{if } k \textit{ is even,} \\ 3 & \textit{otherwise.} \end{cases}$$

2) *Let n be even and $0<2k<n$. If $\gcd(2^{2k}-2^k+1, 2^n-1)=1$, then k is even as well.*

The following lemma describes Kasami exponents, which are invertible modulo (2^n-1).

Lemma 3. *It holds $\gcd(2^{2k}-2^k+1, 2^n-1)=1$ if and only if one of the following cases occurs:*

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

Equivalently, $\gcd(2^{2k}-2^k+1, 2^n-1)=1$ if and only if one of the following cases occurs:

- *n is odd and $k \ge 1$ is arbitrary*
- *$n=2^r a$ and $k=2^r b$, where a is odd and $1 \le r$.*
- *$n=2^r 3^u a$ and $k=2^s 3^v b$, where b is odd, $1 \le s < r$ and $0 \le u \le v$.*

Note that if $\frac{n}{\gcd(n,k)}$ is odd, then 2^k+1 and $2^{3k}+1$ are invertible modulo 2^n-1. Then the observation $2^{2k}-2^k+1=(2^{3k}+1)/(2^k+1)$ together with Theorem 2 implies:

Proposition 1. *Let n and k be positive integers such that $\frac{n}{\gcd(n,k)}$ is odd. Then*
$$(2^{2k}-2^k+1)^{-1} \equiv (2^k+1)(2^{3k}+1)^{-1} \pmod{2^n-1}.$$

Theorem 3. *Let $n=t\cdot\gcd(n,k)$ with t odd and $d=2^{2k}-2^k+1$. The least positive residue d^{-1} satisfies:*

- *If $t \equiv 1 \pmod 3$, then*
$$\begin{aligned} d^{-1} &\equiv 1+2^{2k}(2^{3k}-1)(2^k+1)\sum_{j=0}^{\frac{t-7}{6}} 2^{6kj} \\ &\equiv 1+2^{2k}\cdot(2^k+1)\cdot\frac{2^{n-k}-1}{2^{3k}+1} \pmod{2^n-1}. \end{aligned}$$
In particular, if $gcd(n,k)=k$ then $wt_{2,n}(d^{-1})=\frac{n-k+2}{2}$.
- *If $t \equiv 0 \pmod 3$, then*
$$\begin{aligned} d^{-1} \equiv 2^{k-1}&\left(1+2^{2k}(2^{3k}-1)(2^k+1)\sum_{j=0}^{\frac{t-9}{6}} 2^{6kj}\right) \\ &+2^{n-1} \pmod{2^n-1}. \end{aligned}$$
In particular, if $gcd(n,k)=k$ then $wt_{2,n}(d^{-1})=\frac{n-3k+4}{2}$.
- *If $t \equiv 2 \pmod 3$, then*
$$\begin{aligned} d^{-1} \equiv 2^{2k}&\left(1+2^{2k}(2^{3k}-1)(2^k+1)\sum_{j=0}^{\frac{t-11}{6}} 2^{6kj}\right) \\ &+2^k-2^{n-k} \pmod{2^n-1}. \end{aligned}$$
In particular, if $gcd(n,k)=k$ then $wt_{2,n}(d^{-1})=\frac{n-k+2}{2}$.

(Here we put $\sum_{i=a}^{b} 2^i = 0$ for $a>b$.)

Proof: Note that the Kasami exponent satisfies:
$$(2^{2k}-2^k+1)\left((2^{3k}-1)(2^k+1)\right)=2^{6k}-1.$$
The rest follows by direct calculations.

Remark 3. *It is interesting to observe that Kasami exponents $d=2^{2k}-2^k+1$ with small ratio $\frac{n}{k}$ fulfill:*

- *if $k=n/2$ then $c\ell(d)=c\ell(2^{n/2+1}-1)$*
- *if $k=n/3$ then $c\ell(d^{-1})=c\ell(2^k+1)$*
- *if $k=n/5$ then $c\ell(d^{-1})=c\ell(2^{4k}-2^{2k}+1)$,*

where $c\ell(a)=c\ell(b)$ denotes that the integers a and b are in the same cyclotomic coset.

V. Welch exponents

For $n=2t+1$, integers of the shape 2^t+3 are called Welch exponents when considered modulo 2^n-1. In contrast to the quadratic and Kasami exponents, the Welch exponent depends on n. In fact, it is proved in [9], that the only APN exponents which do not depend on n are Gold and Kasami exponents.

Our considerations show that the main difficulty in finding the inverses modulo 2^n-1 for a given integer is to guess it. After having the conjectural inverse for an integer, usually the correctness of it follows by easy direct calculations. The following lemma helps us to guess the inverse of the Welch exponent.

Lemma 4. *Let $n=2t+1$. Then the inverse ω of the Welch exponent 2^t+3 modulo 2^n-1 is defined by the following identity*
$$\omega\cdot(2^4+1) \equiv 2^n-2^{t+1}+5 \pmod{2^n-1}. \tag{3}$$

Proof: Note that the Welch exponent satisfies:
$$(2^t+3)\cdot 2(2^t-3)=2^n-18 \equiv -17 \pmod{2^n-1}.$$
Multiplying both sides of the above identity by $-\omega$ implies:
$$17\cdot\omega \equiv -2^{t+1}+6 \equiv 2^n-2^{t+1}+5 \pmod{2^n-1}.$$

Remark 4. *From Lemma 4 and Theorem 2 it follows that the inverse of the Welch exponent 2^t+3 modulo 2^n-1 can be calculated as*
$$(2^n-2^{t+1}+5)\cdot\left(\sum_{i=0}^{t} 2^{8i}\right) \pmod{2^n-1}. \tag{4}$$
Observe that (4) is not the least positive residue of the inverse of the Welch exponent modulo 2^n-1, since some of its summands exceed 2^n-1.

The advantage of defining identity (3) of ω is that the involved numbers 17 and $2^n - 2^{t+1} + 5 = 2^{t+1}(2^t - 1) + 5$ have binary representations with "easy" combinatorics. This allows us to find the binary representation of the least positive residue of $\omega \pmod{2^n - 1}$, which will yield the explicit form and the algebraic degree of the compositional inverse of the Welch power function.

Theorem 4. *Let ω be the least positive residue of the inverse of Welch exponent modulo $2^n - 1$ with $n = 2t + 1$.*

- *If $t \equiv 0 \pmod 8$ then*
$$\omega = 2^t + \frac{2^t - 1}{17}\left(13 \cdot 2^{t+1} + 7\right)$$
with binary weight $t + 1$.
- *If $t \equiv 1 \pmod 8$ then*
$$\omega = 2^{t-1} + 2^t + \frac{2^{t-1} - 1}{17}\left(7 \cdot 2^{t+2} + 1\right)$$
with binary weight $t + 1$.
- *If $t \equiv 2 \pmod 8$ then*
$$\omega = 1 + 2^{t+1} + \frac{2^{t-2} - 1}{17}\left(5 \cdot 2^{t+3} + 16\right)$$
with binary weight t.
- *If $t \equiv 3 \pmod 8$ then*
$$\omega = 2^t + 2^{t+2} + 2^{t+3} + \frac{2^{t-3} - 1}{17}\left(7 \cdot 2^{t+5} + 8\right)$$
with binary weight t.
- *If $t \equiv 4 \pmod 8$ then*
$$\omega = 2^{t-4} + 2^{t-2} + 2^{t-1} + 2^{t+4} + \frac{2^{t-4} - 1}{17}\left(9 \cdot 2^{t+5} + 3\right)$$
with binary weight t.
- *If $t \equiv 5 \pmod 8$ then*
$$\omega = 1 + 2^{t-3} + 2^{t-1} + 2^t + 2^{t+1} + \frac{2^{t-5} - 1}{17}\left(2^{t+6} + 12\right)$$
with binary weight t.
- *If $t \equiv 6 \pmod 8$ then*
$$\begin{aligned}\omega = {} & 2^{t-5} + 2^{t-4} + 2^{t-2} + 2^{t+3} + 2^{t+4} \\ & + 2^{t+5} + 2^{t+6} + \frac{2^{t-6} - 1}{17}\left(16 \cdot 2^{t+7} + 10\right)\end{aligned}$$
with binary weight $t + 1$.
- *If $t \equiv 7 \pmod 8$ then*
$$\begin{aligned}\omega = {} & 2^{t-5} + 2^{t-4} + 2^{t-3} + 2^{t-2} + 2^{t+1} + 2^{t+2} \\ & + 2^{t+4} + 2^{t+7} + \frac{2^{t-7} - 1}{17}\left(10 \cdot 2^{t+8} + 4\right)\end{aligned}$$
with binary weight $t + 1$.

Proof: We demonstrate the proof ideas for $t \equiv 0 \pmod 8$. Let $t = 8k$, $n = 16k + 1$ and $\omega_{k,0}$ be the least positive residue of the inverse of Welch exponent modulo $2^n - 1$. We denote by $\overline{\boldsymbol{\omega_{k,0}}}$ the binary representation of $\omega_{k,0}$ of length n. The main observation yielding the proof is that $\overline{\boldsymbol{\omega_{k,0}}}$ can be found recursively as follows:

$$\overline{\boldsymbol{\omega_{1,0}}} = 1100\,0011\ 1\ 0110\,1001$$

and for $k \geq 2$ it holds

$$\overline{\boldsymbol{\omega_{k,0}}} = 1100\,0011\ \overline{\boldsymbol{\omega_{k-1,0}}}\ 0110\,1001.$$

In particular, the binary weight of $\omega_{k,0}$ is $8k + 1 = t + 1$. By Lemma 4 it is enough to show that $\omega_{k,0}$ satisfies identity (3). Note that $\omega_{k,0}$ satisfy identity (3) if and only if the sum (with carry) of the sequence $\overline{\boldsymbol{\omega_{k,0}}}$ with its 4-shift is the sequence

$$\underbrace{11\ldots1}_{t}\underbrace{00\ldots0}_{t-2}101.$$

Observe that

$$\overline{\boldsymbol{\omega_{k,0}}} = a\,\bar{a}\,\ldots\,a\,\bar{a}\,1\,c\,\bar{c}\,c\,\bar{c}\,\ldots\,c\,\bar{c},$$

where $a = 1100$ and $c = 0110$, and $\bar{a}, \bar{c}$ are their binary complements respectively. And thus the sum corresponding to $(1 + 2^4) \cdot \omega_{k,0}$ is

$$\begin{array}{cccc} a\,\bar{a}\,\ldots\,a & \bar{a}\,1 & c\,\bar{c}\,c\,\bar{c}\,\ldots\,c & \bar{c} \\ \bar{a}\,\ldots\,a\,\bar{a} & 1\,c & \bar{c}\,c\,\bar{c}\,\ldots\,c\,\bar{c} & a \\ \hline \\ 111\ldots11 & 11110 & 000\ldots00 & 0101 \end{array}$$

proving the statement.

VI. Niho exponents

For completeness, we give here also results for Niho exponents obtained by Portmann and Rennhard [14]. For $n = 2t + 1$, integers d of the shape

$$\begin{aligned} d &= 2^t + 2^{\frac{t}{2}} - 1 \text{ if } t \text{ is even} \\ &= 2^t + 2^{\frac{3t+1}{2}} - 1 \text{ if } t \text{ is odd} \end{aligned}$$

are called Niho exponents. The inverses for Niho exponents depend on $n \pmod 8$. Observe, that in the case $n \equiv 1 \pmod 4$, that is $n = 4a + 1$, the Niho exponent is $d = 2^{2a} + 2^a - 1$. In the case $n \equiv 3 \pmod 4$, that is $n = 4a + 3$, the Niho exponent is given by $2^{3a+2} + 2^{2a+1} - 1$.

Theorem 5. **(a)** *Let $n = 4a + 1$ and $d = 2^{2a} + 2^a - 1$. Then*

- *if a is even*
$$d^{-1} = \sum_{i=0}^{\frac{a}{2}} 2^{2i} + \sum_{i=\frac{a}{2}}^{a-1} 2^{2i+1} + 2^{3a+2} + \sum_{i=\frac{3a}{2}+1}^{\frac{n-3}{2}} 2^{2i+1}$$
- *if a is odd*
$$d^{-1} = \sum_{i=0}^{\frac{a-1}{2}} 2^{2i} + 2^{2a+1} + \sum_{i=a+1}^{\frac{3a+1}{2}} 2^{2i} + \sum_{i=\frac{3a+1}{2}}^{\frac{n-3}{2}} 2^{2i+1}$$

In particular,

$$wt_{2,n}(d^{-1}) = \begin{cases} \frac{3n+5}{8} & \text{if } n \equiv 1 \pmod 8 \\ \frac{3n+9}{8} & \text{if } n \equiv 5 \pmod 8). \end{cases}$$

(b) *Let $n = 4a + 3$ and $d = 2^{3a+2} + 2^{2a+1} - 1$. Then*

- *if a is even*

$$d^{-1} = \sum_{i=0}^{\frac{a}{2}} 2^{2i+1} + \sum_{i=\frac{a}{2}+1}^{a} 2^{2i} + 2^{3a+3} + \sum_{i=\frac{3a}{2}+2}^{\frac{n-1}{2}} 2^{2i}$$

- *if a is odd*

$$d^{-1} = \sum_{i=0}^{\frac{a-1}{2}} 2^{2i+1} + 2^{2a+2} + \sum_{i=a+1}^{\frac{3a+1}{2}} 2^{2i+1} + \sum_{i=\frac{3a+3}{2}}^{\frac{n-1}{2}} 2^{2i}$$

In particular,

$$wt_{2,n}(d^{-1}) = \begin{cases} \frac{3n+7}{8} & \text{if } n \equiv 3 \pmod 8 \\ \frac{3n+11}{8} & \text{if } n \equiv 7 \pmod 8). \end{cases}$$

VII. Dobbertin exponents

We call the integer $2^{4k} + 2^{3k} + 2^{2k} + 2^k - 1 = \frac{2^{5k}-1}{2^k-1} - 2$ considered modulo $2^n - 1$ with $n = 5k$ Dobbertin's exponent.

Theorem 6. *Let $k \geq 1$ be an odd integer and $n = 5k$. Then the least positive residue of the inverse of $d = 2^{4k} + 2^{3k} + 2^{2k} + 2^k - 1$ modulo $2^n - 1$ is*

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

Furthermore,

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

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

Proof: Set $A := \frac{2^{5k}-1}{2^k-1} \cdot \frac{2^{k+1}-1}{3}$. Then

$$2^k \cdot A \equiv A \pmod{2^{5k}-1},$$

and direct calculations using the above identity show that $2d^{-1} \cdot d \equiv 2 \pmod{2^n - 1}$.

Not much is known about the possible algebraic degrees of APN functions. By Theorem 6 the inverse of Dobbertin exponent defines an APN function on $\mathbb{F}_{2^n}$ with algebraic degree exceeding $(n+1)/2$ for n odd. The only previously known such example was the inverse function, with algebraic degree $n-1$. This observation with Theorem 1 (5) shows that the functions defined by Dobbertin exponent and their inverses are not AB, which was originally shown in [5] by exploiting the divisibility properties of corresponding codes.

Corollary 2. *Power functions with Dobbertin exponents and their inverses are not AB.*

VIII. $2^k - 1$ exponents

In [3] it is shown that the exponents $2^k - 1$ have interesting properties for cryptological applications. Here we give the inverse of these exponents:

Theorem 7. *For coprime positive integers n and k it holds*

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

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

IX. Conclusions

The classical modular inversion is the problem to invert numbers modulo a *fixed* number. We consider a dual problem, inverting a fixed number d modulo $2^n - 1$ for *all* suitable n. In this paper we found explicitly the inverses for Welch and Dobbertin exponents. A future project is a systematic study of this problem for other fixed integers d.

Acknowledgment

The authors would like to thank Pascale Charpin for number of comments and suggestions, which improved this manuscript. This work was partially supported by French DGA and ANR BLOC.

References

[1] T. Berger and A. Canteaut and P. Charpin and Y. Laigle-Chapuy Almost Perfect Nonlinear functions. *IEEE Trans. Inform. Theory*, 52(9):4160–4170, September 2006.

[2] C. Blondeau and A. Canteaut and P. Charpin, Differential properties of power functions. *Information and coding theory*, 1(2), 149–170, 2010.

[3] C. Blondeau and A. Canteaut and P. Charpin, Differential properties of $x \mapsto x^{2^k-1}$ *IEEE Trans. Inform. Theory*, 57(12): 8127–8137 , December 2011

[4] C. Boura and A. Canteaut, On the influence of the algebraic degree of F^{-1} on the algebraic degree of $G \circ F$. Submitted.

[5] A. Canteaut, P. Charpin and H. Dobbertin, Weight divisibility of cyclic codes, highly nonlinear functions on $\mathbf{F}_{2^m}$, and cross-correlation of maximum-length sequences, *SIAM J. Discrete Math.* 13(1): 105–138, 2000.

[6] A. Canteaut and M. Naya-Plasencia, Structural weakness of permutations with a low differential uniformity and generalized crooked functions. *Contemporary Mathematics*, 518(2009).

[7] C. Carlet, Vectorial Boolean Functions for Cryptography, http://www.math.univ-paris13.fr/ carlet/chap-vectorial-fcts-corr.pdf.

[8] C. Carlet and P. Charpin and V. Zinoviev, Codes, Bent Functions and Permutations Suitable for DES-like Cryptosystems. *Designs, Codes and Cryptography* 15(2): 125–256, 1998.

[9] F. Hernando and G. McGuire, Proof of a Conjecture on the Sequence of Exceptional Numbers, Classifying Cyclic Codes and APN Functions. *Journal of Algebra* 343(1): 78-92, October 2011.

[10] X.-d. Hou, G. L. Mullen, J. A. Sellers and J. L. Yucas, Reversed Dickson polynomials over finite fields Original Research Article *Finite Fields and Appl.*, 15(6): 748–773, December 2009.

[11] R. Lidl and H. Niederreiter Finite Fields. *Encyclopedia of mathematics and its applications*, 20, 1983.

[12] R.J. McEliece, Finite Fields for computer Scientists and Engineers. Kluwer, Boston, 1987.

[13] K. Nyberg, Differentially uniform mappings for cryptography. *Advances in cryptology – EUROCRYPT'93*, LNCS 765, 55–64, 1993.

[14] M. Portmann and M. Rennhard, Almost Perfect Nonlinear Permutations. *Semester Project – Swiss Federal Institute of Technology Zurich*, 1997.