On inversion in $Z\_2^n - 1$

Gohar Kyureghyan, Valentin Suder

On Inversion in $\mathbb{Z}_{2^n-1}$

Gohar M. Kyureghyan

Department of Mathematics, Otto-von-Guericke University, Universitätsplatz 2, 39106 Magdeburg, Germany

Email: gohar.kyureghyan@ovgu.de

Valentin Suder

INRIA Paris-Rocquencourt, Project-Team SECRET Domaine de Voluceau, 78153 Le Chesnay, France

Email: valentin.suder@inria.fr

Abstract

In this paper we determined explicitly the multiplicative inverses of the Dobbertin and Welch APN exponents in $\mathbb{Z}_{2^n-1}$, and we described the binary weights of the inverses of the Gold and Kasami exponents. We studied the function $\mathtt{Inv}_d(n)$, which for a fixed positive integer d maps integers $n \geq 1$ to the least positive residue of the inverse of d modulo 2^n-1, if it exists. In particular, we showed that the function $\mathtt{Inv}_d$ is completely determined by its values for $1 \leq n \leq \theta_d$, where θ_d is the order of 2 modulo the largest odd divisor of d.[1]

Keywords: modular inversion – APN/AB exponents – power functions on finite fields – algebraic degree – binary representation of integers.

1. Introduction

A mapping $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is called *almost perfect nonlinear* (APN) if for every non-zero $a \in \mathbb{F}_{2^n}$ the sets

$$\{f(x+a)+f(x) \ : \ x \in \mathbb{F}_{2^n}\}$$

contain exactly 2^{n-1} elements. When n is odd, a mapping f is called *almost bent* (AB) if for every $\alpha \neq 0,\ \beta \in \mathbb{F}_{2^n}$

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

where Tr is the absolute trace on $\mathbb{F}_{2^n}$. Every AB mapping is APN, but not vice versa. APN and AB mappings have various applications in cryptology, coding theory and combinatorics [2, 3, 7, 10].

Every mapping f of $\mathbb{F}_{2^n}$ has a unique univariate polynomial representation over $\mathbb{F}_{2^n}$ of degree not exceeding 2^n-1. With respect to a fixed $\mathbb{F}_2$-basis of $\mathbb{F}_{2^n}$, the mapping f has a unique multivariate representation over $\mathbb{F}_{2^n}$ such that its degree in every single variable is

[1] The first part of this work is an extended version of the results presented in ISIT12 [9].

less than 2. This multivariate polynomial representation is basis dependent. However its total degree does not depend on the basis choice, and it is called the algebraic degree of the mapping f. The algebraic degree of a mapping can be computed from its univariate polynomial representation: Recall that the binary weight of a nonnegative integer d is the sum of the digits in its binary representation, i.e. if $d = \sum_{i=0}^{l} d_i 2^i$ with $0 \leq d_i \leq 1$, then the binary weight of d is $\mathrm{wt}(d) = \sum_{i=0}^{l} d_i \in \mathbb{Z}$. The algebraic degree of the mapping $f(x) = \sum_{k=0}^{2^n-1} \alpha_k x^k$ on $\mathbb{F}_{2^n}$ is equal to $\max_{k,\alpha_k \neq 0}\{\mathrm{wt}(k)\}$. In particular, a monomial mapping given by $x \mapsto x^d$ with $1 \leq x \leq 2^n - 2$ has algebraic degree equal to $\mathrm{wt}(d)$.

When studying a special class of mappings of finite fields, one of the main questions to be answered is: What are the properties of polynomials describing this class of mappings? This question is widely open for AB/APN mappings. Even a much weaker question, what are the possible degrees for univariate or multivariate representations of APN mappings, is one of the open challenges in this research area. It is known that the algebraic degree of AB mappings does not exceed $\frac{n+1}{2}$ [3].

The two best understood classes of APN mappings are the so-called quadratic and monomial ones. The univariate representation of a quadratic mapping contains only terms with exponents of binary weight less or equal to 2, i.e. it is of the shape $\sum_{i,j} b_{i,j} x^{2^i+2^j} \in \mathbb{F}_{2^n}[x]$. The monomial mappings are those of shape $x \mapsto x^d$ with a fixed integer $1 \leq d \leq 2^n - 2$. An integer $1 \leq d \leq 2^n - 2$ is called APN exponent on $\mathbb{F}_{2^n}$ if the corresponding monomial mapping $x \mapsto x^d$ is APN on $\mathbb{F}_{2^n}$. All currently known APN exponents can be obtained from the ones listed below:

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

Table 1: Exponents defining APN/AB monomial mappings on $\mathbb{F}_{2^n}$

It is easy to prove that if d is an APN exponent then also $2 \cdot d \pmod{2^n - 1}$ is so, as well as the inverse d^{-1} of d modulo $2^n - 1$ if it exists. While the multiplication of an APN exponent d by 2 is a fairly easy operation, a better understanding of the inverse of d will yield more insights on APN mappings. It is well known that an APN exponent on $\mathbb{F}_{2^n}$ is invertible in $\mathbb{Z}_{2^n-1}$ if and only if n is odd. In [10, 11] the inverses of Gold's and Niho's exponents were considered. In this paper we continue this study. In particular, we find explicit formulas for the inverses of Welch's and Dobbertin's exponents (see Theorem 2.4 and 2.1 respectively) and obtain some partial results on the inverses of Gold's and Kasami's exponents (see Theorem 3.7 and 3.10 respectively for the main results). Further we study also the inverses of some other interesting classes of exponents.

When studying inverses of APN exponents d on $\mathbb{F}_{2^n}$, two cases must be distinguished:

- d depends on n (Dobbertin's, Niho's, Welch's exponents and the field inverse)
- a fixed d is an APN exponent on $\mathbb{F}_{2^n}$ for infinitely many n (Gold's and Kasami's exponents).

It appears that the study of the latter exponents is more difficult than the study of the exponents of the first type. The exponents d defining APN mappings on $\mathbb{F}_{2^n}$ for infinitely many n are called *exceptional APN exponents* [4]. In [6], it is shown that Gold's and Kasami's exponents are the only exceptional APN ones. Finding the inverses of exceptional APN exponents is an instance of the following general problem: Let $d \geq 1$ be a fixed integer and define $\mathbb{N}_d = \{n \in \mathbb{N} \ : \ \gcd(d, 2^n - 1) = 1\}$. How explicit can we describe the function $\mathtt{Inv}_d : \mathbb{N}_d \to \mathbb{N}$, which maps n to the least positive integer describing the inverse of d modulo $2^n - 1$? We show that the function $\mathtt{Inv}_d$ is completely determined by its values for $1 \leq n \leq \theta_d{}'$, where $\theta_d{}'$ is the order of 2 modulo the largest odd divisor of d. This dependence is given in Theorem 3.2. Based on properties of $\mathtt{Inv}_d$ we propose Algorithm 1 for inversion in $\mathbb{Z}_{2^n-1}$, which may be of interest for some special applications.

2. Inverses of APN exponents d on $\mathbb{F}_{2^n}$, when d depends on n

After having the conjectural modular inverse for a given integer, usually the correctness of it follows from easy calculations. Hence the main difficulty in finding inverses is to guess them. For a generic integer d we cannot of course expect to be able to guess its inverse modulo $2^n - 1$. However, if the binary representation of the integer d has a nice combinatorial pattern, then the binary representation of its modulo $2^n - 1$ inverse does not look random either, and therefore the problem could be solvable. Since the binary representations of the APN exponents listed in Table 1 are far from being random, finding their inverses explicitly is probably possible. Having this idea in mind we performed numerical experiments, which led to the formulas for Dobbertin's and Welch's exponents described below.

2.1. Dobbertin's exponent

Theorem 2.1. *Let $k \geq 1$ be an odd integer. The least positive residue of the inverse of $d = 2^{4k} + 2^{3k} + 2^{2k} + 2^k - 1$ modulo $2^{5k} - 1$ is*

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

Furthermore,

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

showing that $wt(t) = \frac{5k+3}{2}$.

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

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

Observe that $d = \frac{2^{5k}-1}{2^k-1} - 2$. Hence

$$\begin{aligned} d \cdot t &\equiv \frac{1}{2}(3A - d) = \frac{1}{2}\left(\frac{2^{5k}-1}{2^k-1} \cdot (2^{k+1}-1) - \frac{2^{5k}-1}{2^k-1} + 2\right) \\ &= \frac{1}{2}\left(\frac{2^{5k}-1}{2^k-1} \cdot (2^{k+1}-2) + 2\right) \\ &\equiv 1 \pmod{2^{5k}-1}. \end{aligned}$$

Clearly, $t < 2^{5k}-1$ and thus t is indeed the least positive residue of the inverse of d modulo $2^{5k}-1$. □

By Theorem 2.1 the inverse of Dobbertin exponent defines an APN mapping on $\mathbb{F}_{2^n}$ with algebraic degree exceeding $(n+1)/2$. The only previously known such example was the inverse mapping, with algebraic degree $n-1$. This observation shows also that the monomial mappings defined by Dobbertin's exponents and their inverses are not AB, which was originally proved in [2] by exploiting the divisibility properties of corresponding codes.

Corollary 1. *The monomial mappings with Dobbertin's exponents and their inverses are not AB.*

2.2. Niho's exponents

For the sake of the completeness, we give here the explicit inverses of Niho's exponents which were found in [11]. For $n = 2m+1$, Niho's exponent d has the shape

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

or equivalently, with $k \geq 1$,

$$d = \begin{cases} 2^{2k} + 2^k - 1 & \text{if } m = 2k \\ 2^{3k+2} + 2^{2k+1} - 1 & \text{if } m = 2k+1. \end{cases}$$

The inverses for Niho exponents depend on $n \pmod 8$ as the next theorem shows.

Theorem 2.2. (a) *Let $n = 4k+1$ and $d = 2^{2k} + 2^k - 1$ be the Niho exponent. Set t to denote the least positive residue of the inverse of d modulo $2^n - 1$. Then*

- *if k is even, i.e. if $n \equiv 1 \pmod 8$,*

$$t = \frac{2^k - 1}{3}\left(2^{3k+1} + 2^{k+1} + 1\right) + 2^k + 2^{3k+1}. \tag{1}$$

- *if k is odd, i.e. if $n \equiv 5 \pmod 8$,*

$$t = \frac{2^{k-1} - 1}{3}\left(2^{3k+2} + 2^{2k+2} + 1\right) + 2^{3k+1} + 2^{2k+1} + 2^{k-1}. \tag{2}$$

In particular,

$$wt(t) = \begin{cases} \frac{3n+5}{8} & \text{if } n \equiv 1 \pmod 8 \\ \frac{3n+9}{8} & \text{if } n \equiv 5 \pmod 8. \end{cases}$$

(b) *Let $n = 4k+3$ and $d = 2^{3k+2} + 2^{2+1} - 1$ be the Niho exponent. Set t to denote the least positive residue of the inverse of d modulo $2^n - 1$. Then*

- *if k is even, i.e. if $n \equiv 3 \pmod 8$,*

$$t = \frac{2^k - 1}{3}\left(2^{3k+4} + 2^{k+2} + 2\right) + 2^{3k+3} + 2^{k+1}. \tag{3}$$

- *if k is odd, i.e. if $n \equiv 7 \pmod 8$,*

$$t = \frac{2^{k+1} - 1}{3}\left(2^{3k+3} + 2^{2k+3} + 2\right) + 2^{2k+2}. \tag{4}$$

In particular,

$$wt(t) = \begin{cases} \frac{3n+7}{8} & \text{if } n \equiv 3 \pmod 8 \\ \frac{3n+11}{8} & \text{if } n \equiv 7 \pmod 8. \end{cases}$$

Proof. We prove only the first statement of part **(a)**, since the remaining cases follow by similar arguments.

- Let $n = 4k+1$ and k be even. Then

$$\begin{aligned} d \cdot t &= (2^{2k} + 2^k - 1)\left(\frac{2^k - 1}{3}\left(2^{3k+1} + 2^{k+1} + 1\right) + 2^k + 2^{3k+1}\right) \\ &\equiv \frac{2^k - 1}{3}\left(2^{5k+1} + 2^{4k+1} - 2^{3k+1} + 2^{3k+1} + 2^{2k+1} - 2^{k+1} + 2^{2k} + 2^k - 1\right) \\ &\quad + 2^{3k} + 2^{2k} - 2^k + 2^{5k+1} + 2^{4k+1} - 2^{3k+1} \\ &\equiv \frac{2^k - 1}{3}\left(2^{2k+1} + 2^{2k}\right) - 2^{3k} + 2^{2k} + 1 \\ &\equiv (2^k - 1)2^{2k} - 2^{3k} + 2^{2k} + 1 \\ &\equiv 1 \pmod{2^{4k+1} - 1}. \end{aligned}$$

  It remains to note that $\mathrm{wt}(t) = 2 + 3 \cdot \mathrm{wt}\left(\frac{2^k-1}{3}\right) - 1 = 1 + 3 \cdot \frac{n-1}{8} = \frac{3n+5}{8}$, since

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

  and

$$\frac{2^k - 1}{3} = \sum_{i=0}^{\frac{k}{2}-1} 2^{2i}.$$

□

2.3. Welch's exponent

Let v be a nonnegative integer with binary representation $v = \sum_{i=0}^{r-1} v_i 2^i$ where $v_{r-1} \neq 0$. If $r' \geq r$, we say that

$$\underbrace{0\,0\ldots0}_{r'-r}\; v_{r-1}\ldots v_1\, v_0$$

is the sequence of length r' representing the integer v. Two sequences $a_{r-1}\ldots a_0$ and $b_{r-1}\ldots b_0$ are called complementary if $a_i = b_i + 1 \pmod 2$ for all $0 \leq i \leq r-1$. For a sequence $\boldsymbol{a}$, we denote by $\bar{\boldsymbol{a}}$ its complementary sequence. Note that if a sequence $\boldsymbol{a} = a_{r-1}\ldots a_0$ represents the integer a, then its complementary sequence $\bar{\boldsymbol{a}}$ represents the integer $2^r - 1 - a$. This follows from the fact that the sequence $\underbrace{1\,1\ldots1}_{r}$ represents the integer $2^r - 1$. For two sequences $\boldsymbol{a}$ and $\boldsymbol{b}$, we denote by $\boldsymbol{a}|\boldsymbol{b}$ their concatenation.

Lemma 2.3. *Let $s \geq 2$ and $0 < u < 2^s$ be integers. Then the binary representation of length $2s$ of the integer $(2^s-1)\cdot u$ is $\boldsymbol{w}|\bar{\boldsymbol{w}}$, where $\boldsymbol{w}$ is the sequence of length s representing the integer $u-1$ and $\bar{\boldsymbol{w}}$ is the complement of the binary sequence $\boldsymbol{w}$ and represents the integer $2^s - u$. In particular, the binary weight of the integer $(2^s-1)\cdot u$ is s.*

Proof. The statement of the lemma follows from the observation that $(2^s-1)\cdot u = (u-1)\cdot 2^s + (2^s - u)$. Moreover, the binary representation of the length s of $2^s - u$ is the complement of that of $u-1$, since $(2^s - u) + (u-1) = 2^s - 1$. □

Theorem 2.4. *Let $n = 2k+1$. The least positive residue t of the inverse of Welch's exponent $2^k + 3$ modulo $2^{2k+1} - 1$ is:*

- *If $k \equiv 0 \pmod 8$ then*

$$t = 2^k + \frac{2^k - 1}{17}\left(13\cdot 2^{k+1} + 7\right)$$

  with binary weight $k+1$.

- *If $k \equiv 1 \pmod 8$ then*

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

  with binary weight $k+1$.

- *If $k \equiv 2 \pmod 8$ then*

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

  with binary weight k.

- *If $k \equiv 3 \pmod 8$ then*

$$t = 2^k + 2^{k+2} + 2^{k+3} + \frac{2^{k-3} - 1}{17}\left(7\cdot 2^{k+5} + 8\right)$$

  with binary weight k.

- *If* $k \equiv 4 \pmod 8$ *then*

$$t = 2^{k-4} + 2^{k-2} + 2^{k-1} + 2^{k+4} + \frac{2^{k-4}-1}{17}\left(9 \cdot 2^{k+5} + 3\right)$$

with binary weight k.

- *If* $k \equiv 5 \pmod 8$ *then*

$$t = 1 + 2^{k-3} + 2^{k-1} + 2^k + 2^{k+1} + \frac{2^{k-5}-1}{17}\left(2^{k+6} + 12\right)$$

with binary weight k.

- *If* $k \equiv 6 \pmod 8$ *then*

$$\begin{aligned} t = {} & 2^{k-5} + 2^{k-4} + 2^{k-2} + 2^{k+3} + 2^{k+4} \\ & + 2^{k+5} + 2^{k+6} + \frac{2^{k-6}-1}{17}\left(16 \cdot 2^{k+7} + 10\right) \end{aligned}$$

with binary weight $k+1$.

- *If* $k \equiv 7 \pmod 8$ *then*

$$\begin{aligned} t = {} & 2^{k-5} + 2^{k-4} + 2^{k-3} + 2^{k-2} + 2^{k+1} + 2^{k+2} \\ & + 2^{k+4} + 2^{k+7} + \frac{2^{k-7}-1}{17}\left(10 \cdot 2^{k+8} + 4\right) \end{aligned}$$

with binary weight $k+1$.

Proof. We only need to verify that $(2^k+3) \cdot t \equiv 1 \pmod{2^{2k+1}-1}$, since obviously all listed integers t are smaller than $2^{2k+1}-1$. We do this verification for $k \equiv 4 \pmod 8$, the remaining cases are similar. Thus, let $k \equiv 4 \pmod 8$ and consider

$$(2^k+3) \cdot \left(2^{k-4} + 2^{k-2} + 2^{k-1} + 2^{k+4} + \frac{2^{k-4}-1}{17}\left(9 \cdot 2^{k+5} + 3\right)\right) \pmod{2^{2k+1}-1}. \tag{5}$$

Observe that

$$(2^k+3) \cdot \left(9 \cdot 2^{k+5} + 3\right) \equiv 17 \cdot (9 + 3 \cdot 17 \cdot 2^k) \pmod{2^{2k+1}-1},$$

and therefore (5) reduces to

$$\begin{aligned} & (2^k+3) \cdot \left(2^{k-4} + 2^{k-2} + 2^{k-1} + 2^{k+4}\right) + (2^{k-4}-1) \cdot (9 + 3 \cdot 17 \cdot 2^k) = \\ & (2^k+2+1)\left(2^{k-4} + 2^{k-2} + 2^{k-1} + 2^{k+4}\right) + (2^{k-4}-1)(2^3 + 1 + 2^{k+5} + 2^{k+4} + 2^{k+1} + 2^k) \\ & \equiv 2^{2k-4} + 2^{2k-2} + 2^{2k-1} + 2^3 + 2^{k-3} + 2^{k-1} + 2^k + 2^{k+5} + 2^{k-4} + 2^{k-2} + 2^{k-1} + 2^{k+4} + \\ & 2^{k-1} + 2^{k-4} + 1 + 2^{2k} + 2^{2k-3} + 2^{2k-4} - 2^3 - 1 - 2^{k+5} - 2^{k+4} - 2^{k+1} - 2^k = \\ & 2^{2k-4} + 2^{2k-2} + 2^{2k-1} + 2^{k-3} + 2^{k-1} - 2^k + 2^{k-4} + 2^{k-2} + 2^{k-4} + 2^{2k} + 2^{2k-3} + 2^{2k-4} = \\ & 2^{2k} + 2^{2k-1} + 2^{2k-2} + 2^{2k-3} + 2 \cdot 2^{2k-4} - 2^k + 2^{k-1} + 2^{k-2} + 2^{k-3} + 2 \cdot 2^{k-4} \equiv \\ & 1 \pmod{2^{2k+1}-1}. \end{aligned}$$

To complete the proof it remains to show that the binary weight of $t = 2^{k-4} + 2^{k-2} + 2^{k-1} + 2^{k+4} + \frac{2^{k-4}-1}{17}\left(9 \cdot 2^{k+5} + 3\right)$ is k. We firstly compute the binary weight of

$$\begin{aligned}\frac{2^{k-4}-1}{17}\left(9 \cdot 2^{k+5} + 3\right) &= \frac{2^{k-4}-1}{2^8-1}(2^4-1)\left(9 \cdot 2^{k+5} + 3\right) \\ &= (2^4-1)\left(9 \cdot 2^{k+5} + 3\right)\sum_{j=0}^{\frac{k-4}{8}-1} 2^{8j} \\ &= 3(2^4-1)\sum_{j=0}^{\frac{k-4}{8}-1} 2^{8j} + 9(2^4-1)\sum_{l=\frac{k+4}{8}}^{\frac{k}{4}-1} 2^{8l+1}.\end{aligned}$$

Note that the integers 3 and 9 are less than 2^4, so Lemma 2.3 implies that the binary weight of both integers $3(2^4-1)\sum_{j=0}^{\frac{k-4}{8}-1} 2^{8j}$ and $9(2^4-1)\sum_{l=\frac{k+4}{8}}^{\frac{k}{4}-1} 2^{8l+1}$ is $4 \cdot \frac{k-4}{8} = \frac{k-4}{2}$. Thus the binary weight of t is $2 \cdot \frac{k-4}{2} + 4 = k$. □

Remark 1. The crucial step for guessing the inverses t of Welch's exponent was the observation that t satisfies certain recurrence relations. For instance, we take $n = 2k+1$ with $k \equiv 0 \pmod 8$. Set $k = 8r$ with $r \geq 0$. Suppose $\boldsymbol{t_r}$ is the binary sequence of length $n = 16r+1$ representing the least positive residue of the inverse of Welch's exponent $2^{8r}+3$ modulo $2^n - 1$. Then for every $r \geq 1$

$$\boldsymbol{t_r} = 1100\,0011\,|\,\boldsymbol{t_{r-1}}\,|\,0110\,1001$$

holds and $\boldsymbol{t_0} = 1$.

3. Inverses of a fixed integer d modulo all $2^n - 1$

In the previous section we described the inverses for Dobbertin's, Niho's and Welch's exponents, and herewith it remains to find the inverses for Gold's and Kasami's exponents to have all presently known APN exponents explicitly. A fixed Gold's or Kasami's exponent defines an APN mapping on infinitely many finite fields and therefore we aim finding the inverses of a fixed integer modulo infinitely many $2^n - 1$. For example, Gold's exponents 3 and Kasami's exponent 13 define bijective monomial APN mappings on $\mathbb{F}_{2^n}$ with any n odd. Hence we want to find inverses of 3 and 13 modulo all $2^n - 1$ where n is odd. Motivated by this observation, in the next subsection we study the following general problem: For a given fixed integer $d \geq 1$, let $\mathbb{N}_d = \{n \in \mathbb{N} \ : \ \gcd(d, 2^n - 1) = 1\}$. What can we say about the function $\mathtt{Inv}_d : \mathbb{N}_d \to \mathbb{N}$, whose output for n is the least positive integer describing the inverse of d modulo $2^n - 1$? Most of the results of the next subsection can be directly generalized for modulo $p^n - 1$, where p is a prime number.

3.1. General case

Definition 1. Let d be a fixed positive integer. For a positive integer n satisfying $\gcd(d, 2^n - 1) = 1$, set $\mathtt{Inv}_d(n)$ be the least positive residue of the inverse of d modulo $2^n - 1$, that is the integer $\mathtt{Inv}_d(n)$ is defined by

$$0 < \mathtt{Inv}_d(n) < 2^n - 1 \quad \text{and} \quad d \cdot \mathtt{Inv}_d(n) \equiv 1 \pmod{2^n - 1}.$$

In the rest of this section we assume, without loss of generality, that the fixed number d is **odd**. Indeed, if $d_1 = 2^u \cdot d$ with $u \geq 0$ then the study of the function $\mathtt{Inv}_{d_1}$ may be reduced to the one of $\mathtt{Inv}_d$ using

$$\mathtt{Inv}_{d_1}(n) \equiv 2^{n-u}\mathtt{Inv}_d(n) \pmod{2^n - 1}.$$

Let $d \geq 3$ and θ_d be the (multiplicative) order of 2 modulo d, that is θ_d is the least positive integer o such that $2^o \equiv 1 \pmod{d}$. We set $\theta_1 = 0$. The next results show that in the study of the function $\mathtt{Inv}_d$ the magnitude θ_d plays an important role: $\lfloor \theta_d/2 \rfloor$ many values of the function $\mathtt{Inv}_d$ completely determine it.

The following proposition shows that if $\mathtt{Inv}_d(r)$ is known for some $1 \leq r \leq \theta_d - 1$, then it yields the value of $\mathtt{Inv}_d(\theta_d - r)$.

Proposition 3.1. *Let* $1 \leq r \leq \theta_d - 1$ *and* $\gcd(d, 2^r - 1) = 1$. *Then* $\gcd(d, 2^{\theta_d - r} - 1) = 1$ *and*

$$\mathtt{Inv}_d(\theta_d - r) = \frac{\left(d + 1 - \frac{\mathtt{Inv}_d(r)\cdot d - 1}{2^r - 1}\right)(2^{\theta_d - r} - 1) + 1}{d}. \tag{6}$$

Proof. Note that $\gcd(d, 2^{\theta_d - r} - 1) = 1$, since $2^r \cdot (2^{\theta_d - r} - 1) = 2^{\theta_d} - 1 - (2^r - 1)$. Set t be the rational number at the right hand side of (6), i.e.

$$t := \frac{\left(d + 1 - \frac{\mathtt{Inv}_d(r)\cdot d - 1}{2^r - 1}\right)(2^{\theta_d - r} - 1) + 1}{d}.$$

First we show that t is an integer, or equivalently that

$$\left(d + 1 - \frac{\mathtt{Inv}_d(r) \cdot d - 1}{2^r - 1}\right)(2^{\theta_d - r} - 1) + 1$$

is divisible by d. Since $\gcd(d, 2^r - 1) = 1$, it is enough to show that

$$(2^r - 1)\left(\left(1 - \frac{\mathtt{Inv}_d(r) \cdot d - 1}{2^r - 1}\right)(2^{\theta_d - r} - 1) + 1\right) \equiv 0 \pmod{d},$$

which in its turn reduces to

$$(2^r - 1)2^{\theta_d - r} - (\mathtt{Inv}_d(r) \cdot d - 1)(2^{\theta_d - r} - 1) \equiv 0 \pmod{d}.$$

The left hand side of the latter congruence is

$$2^{\theta_d} - 1 - \mathtt{Inv}_d(r) \cdot d \cdot \left(2^{\theta_d - r} - 1\right),$$

which is divisible by d by the definition of θ_d.

Finally it is easy to see that $t \cdot d \equiv 1 \pmod{2^{\theta_d - r} - 1}$ and $1 \leq t \leq 2^{\theta_d - r} - 1$.

□

The following identity is obtained directly from (6):

Corollary 2. *Let* $1 \leq r \leq \theta_d - 1$ *with* $\gcd(d, 2^r - 1) = 1$. *Then*

$$\frac{d \cdot \mathtt{Inv}_d(\theta_d - r) - 1}{2^{\theta_d - r} - 1} + \frac{\mathtt{Inv}_d(r) \cdot d - 1}{2^r - 1} = d + 1. \tag{7}$$

The next theorem is the main result of this section. It shows that the value of $\mathtt{Inv}_d(n)$ can be computed from $\mathtt{Inv}_d(r)$ where r is the least positive residue of n modulo θ_d. We give three different expressions for this dependence, each of them appears to be more convenient for a certain situation. Observe that Theorem 3.2 implies in particular that in order to determine values of the inverses of d modulo all 2^n-1 it is enough to compute only finitely many of them.

Theorem 3.2. *Let $n \geq 1$ with $\gcd(d, 2^n - 1) = 1$ and $1 \leq r \leq \theta_d - 1$ such that $n \equiv r \pmod{\theta_d}$. Then*

(a)

$$\mathtt{Inv}_d(n) = \mathtt{Inv}_d(r) \cdot 2^{n-r} + \left(\frac{d \cdot \mathtt{Inv}_d(r) - 1}{2^r - 1} - 1\right) \cdot \frac{2^{n-r} - 1}{d}. \tag{8}$$

(b)

$$\mathtt{Inv}_d(n) = \mathtt{Inv}_d(r) \cdot \sum_{i=0}^{m} 2^{\theta_d \cdot i} + \left(2^{\theta_d - r} - 1 - \mathtt{Inv}_d(\theta_d - r)\right) 2^r \sum_{i=0}^{m-1} 2^{\theta_d \cdot i}, \tag{9}$$

where $m = \frac{n-r}{\theta_d}$. Equivalently,

$$\mathtt{Inv}_d(n) \quad = \quad \mathtt{Inv}_d(r) \cdot \frac{2^{\theta_d \cdot (m+1)} - 1}{2^{\theta_d} - 1} + \left(2^{\theta_d - r} - 1 - \mathtt{Inv}_d(\theta_d - r)\right) 2^r \cdot \frac{2^{\theta_d \cdot m} - 1}{2^{\theta_d} - 1}.$$

(c)

$$\mathtt{Inv}_d(n) \quad = \quad \frac{\mathtt{Inv}_d(r)(2^n - 1) - \frac{2^n - 2^r}{d}}{2^r - 1}.$$

Proof. **(a)** Set

$$t := \mathtt{Inv}_d(r) \cdot 2^{n-r} + \left(\frac{d \cdot \mathtt{Inv}_d(r) - 1}{2^r - 1} - 1\right) \cdot \frac{2^{n-r} - 1}{d}.$$

Clearly, t is a positive integer, since $2^r - 1$ divides $d \cdot \mathtt{Inv}_d(r) - 1$ and d divides $2^{n-r} - 1$. Next we show that $t < 2^n - 1$. Note that $\mathtt{Inv}_d(r) < 2^r - 2$, since otherwise $\mathtt{Inv}_d(r) = 2^r - 2 = d$, which contradicts the assumption that d is odd. Hence we have

$$\begin{aligned}
\mathtt{Inv}_d(r) &< 2^r - 2 \quad \Rightarrow \\
d \cdot \mathtt{Inv}_d(r) &< d \cdot (2^r - 2) \quad \Rightarrow \\
d \cdot \mathtt{Inv}_d(r) - 1 &< d \cdot (2^r - 1) - (d + 1) \quad \Rightarrow \\
\frac{(d \cdot \mathtt{Inv}_d(r) - 1)(2^n - 1)}{2^r - 1} &< (2^n - 1) \cdot d - \frac{(d + 1)(2^n - 1)}{2^r - 1} \quad \Rightarrow \\
\frac{(d \cdot \mathtt{Inv}_d(r) - 1)(2^n - 1)}{2^r - 1} + 1 &< (2^n - 1) \cdot d - (d + 1) + 1 \quad \Rightarrow \\
\frac{(d \cdot \mathtt{Inv}_d(r) - 1)(2^n - 1)}{2^r - 1} + 1 &< (2^n - 1) \cdot d \quad \Rightarrow \\
(2^n - 2^r) \cdot \frac{d \cdot \mathtt{Inv}_d(r) - 1}{2^r - 1} + (d \cdot \mathtt{Inv}_d(r) - 1) + 1 &< (2^n - 1) \cdot d.
\end{aligned}$$

It remains to observe that the left hand side of the last inequality is

$$(2^n - 2^r) \cdot \frac{d \cdot \mathtt{Inv}_d(r) - 1}{2^r - 1} + (d \cdot \mathtt{Inv}_d(r) - 1) + 1 =$$
$$2^{n-r}(d \cdot \mathtt{Inv}_d(r) - 1) + (2^{n-r} - 1)\frac{d \cdot \mathtt{Inv}_d(r) - 1}{2^r - 1} + 1 =$$
$$2^{n-r} \cdot d \cdot \mathtt{Inv}_d(r) + (2^{n-r} - 1)\left(\frac{d \cdot \mathtt{Inv}_d(r) - 1}{2^r - 1} - 1\right) = t \cdot d,$$

proving that indeed $t < 2^n - 1$.

To complete the proof we must show that t is the inverse of d modulo $2^n - 1$. From the above observation, we have

$$\begin{aligned} t \cdot d &= (2^n - 2^r) \cdot \frac{d \cdot \mathtt{Inv}_d(r) - 1}{2^r - 1} + (d \cdot \mathtt{Inv}_d(r) - 1) + 1 \\ &= (2^n - 1) \cdot \frac{d \cdot \mathtt{Inv}_d(r) - 1}{2^r - 1} - (2^r - 1) \cdot \frac{d \cdot \mathtt{Inv}_d(r) - 1}{2^r - 1} + (d \cdot \mathtt{Inv}_d(r) - 1) + 1 \\ &\equiv 1 \pmod{2^n - 1}. \end{aligned}$$

(b) Set

$$\mathtt{S}_d(n) = \frac{d \cdot \mathtt{Inv}_d(n) - 1}{2^n - 1}.$$

Then Corollary 2 shows that

$$\mathtt{S}_d(r) + \mathtt{S}_d(\theta_d - r) = d + 1. \tag{10}$$

Multiplying the right side of (9) by d, we have

$$\begin{aligned} & d \cdot \left(\mathtt{Inv}_d(r) \sum_{i=0}^{m} 2^{\theta_d \cdot i} + \left(2^{\theta_d - r} - 1 - \mathtt{Inv}_d(\theta_d - r)\right) 2^r \cdot \sum_{i=0}^{m-1} 2^{\theta_d \cdot i} \right) \\ &= (\mathtt{S}_d(r)(2^r - 1) + 1) \sum_{i=0}^{m} 2^{\theta_d \cdot i} \\ &\qquad + 2^r d(2^{\theta_d - r} - 1) \sum_{i=0}^{m-1} 2^{\theta_d \cdot i} - 2^r \left(\mathtt{S}_d(\theta_d - r)(2^{\theta_d - r} - 1) + 1\right) \sum_{i=0}^{m-1} 2^{\theta_d \cdot i} \\ &= \mathtt{S}_d(r) \left(2^r \left(2^{n-r} + \sum_{i=0}^{m-1} 2^{\theta_d \cdot i} \right) - \left(1 + 2^{\theta_d} \sum_{i=0}^{m-1} 2^{\theta_d \cdot i} \right) \right) + \sum_{i=0}^{m} 2^{\theta_d \cdot i} \\ &\qquad + \left(2^r (2^{\theta_d - r} - 1)(d - \mathtt{S}_d(\theta_d - r)) - 2^r \right) \sum_{i=0}^{m-1} 2^{\theta_d \cdot i} \\ &= \mathtt{S}_d(r) \left((2^n - 1) + (2^r - 2^{\theta_d}) \cdot \sum_{i=0}^{m-1} 2^{\theta_d \cdot i} \right) + \left(1 + 2^{\theta_d} \sum_{i=0}^{m-1} 2^{\theta_d \cdot i} \right) \\ &\qquad + \left(2^r (2^{\theta_d - r} - 1)(d - \mathtt{S}_d(\theta_d - r)) - 2^r \right) \sum_{i=0}^{m-1} 2^{\theta_d \cdot i} \end{aligned}$$

$$= \mathtt{S}_d(r)(2^n-1) + 1 + 2^{\theta_d}\sum_{i=0}^{m-1} 2^{\theta_d \cdot i}$$

$$+ \left(2^r(2^{\theta_d - r}-1)(d - \mathtt{S}_d(\theta_d - r) - \mathtt{S}_d(r)) - 2^r\right)\sum_{i=0}^{m-1} 2^{\theta_d \cdot i}$$

$$= 1 + \mathtt{S}_d(r)(2^n-1) + 2^r(2^{\theta_d - r}-1)(d - \mathtt{S}_d(\theta_d - r) - \mathtt{S}_d(r) + 1)\sum_{i=0}^{m-1} 2^{\theta_d \cdot i}$$

$$\equiv 1 \pmod{2^n-1},$$

where we apply (10) to get the congruence modulo $2^n - 1$.

(c) This identity follows from (8) of part (a) of this theorem.

$$\begin{aligned}
\mathtt{Inv}_d(n) &= \mathtt{Inv}_d(r)\cdot 2^{n-r} + \left(\frac{d\cdot \mathtt{Inv}_d(r) - 1}{2^r - 1} - 1\right)\cdot \frac{2^{n-r}-1}{d} \\
&= \frac{d\cdot \mathtt{Inv}_d(r)\cdot 2^{n-r}(2^r-1) + (d\cdot \mathtt{Inv}_d(r) - 1)(2^{n-r}-1) - (2^{n-r}-1)(2^r-1)}{d\cdot(2^r-1)} \\
&= \frac{d\cdot \mathtt{Inv}_d(r)(2^n-1) - (2^{n-r}-1) - (2^{n-r}-1)(2^r-1)}{d\cdot(2^r-1)} \\
&= \frac{\mathtt{Inv}_d(r)(2^n-1) - \frac{2^n-2^r}{d}}{2^r-1}.
\end{aligned}$$

□

Formulas (8) and (9) of Theorem 3.2 imply that the binary representation of inverses modulo $2^n - 1$ have a nice combinatorial structure:

Corollary 3. *Let $n > 1$ with $\gcd(d, 2^n-1) = 1$ and $1 \le r \le \theta_d - 1$ such that $n \equiv r \pmod{\theta_d}$. Set*

- $\boldsymbol{t_n}$ *be the binary sequence of length n representing $\mathtt{Inv}_d(n)$;*
- $\boldsymbol{u_{\theta_d}}$ *be the binary sequence of length θ_d representing $\left(\frac{d\cdot \mathtt{Inv}_d(r)-1}{2^r-1} - 1\right)\cdot \frac{2^{\theta_d}-1}{d}$;*
- $\boldsymbol{a_r}$ *be the binary sequence of length r representing $\mathtt{Inv}_d(r)$;*
- $\boldsymbol{\bar{b}_{\theta_d - r}}$ *be the complementary sequence of the binary sequence of length $\theta_d - r$ representing the $\mathtt{Inv}_d(\theta_d - r)$.*

Then $\boldsymbol{t_n}$ is obtained by concatenating sequences $\boldsymbol{a_r}$, $\boldsymbol{\bar{b}_{\theta_d - r}}$ and $\boldsymbol{u_{\theta_d}} = \boldsymbol{\bar{b}_{\theta_d - r}}\,|\,\boldsymbol{a_r}$ as follows:

$$\boldsymbol{t_n} = \boldsymbol{a_r}\,|\,\underbrace{\boldsymbol{u_{\theta_d}}\,|\,\boldsymbol{u_{\theta_d}}\,|\ldots|\,\boldsymbol{u_{\theta_d}}}_{m} = \boldsymbol{a_r}\,|\,\boldsymbol{\bar{b}_{\theta_d - r}}\,|\,\boldsymbol{a_r}\,|\ldots|\,\boldsymbol{\bar{b}_{\theta_d - r}}\,|\,\boldsymbol{a_r},\ \text{where } m = \frac{n-r}{\theta_d}.$$

Example 3.1. Let $d = 7$. Then $\theta_7 = 3$ and for every n not divisible by 3, we have $r = 1, 2 \equiv n \pmod 3$. Moreover, $\mathtt{Inv}_7(1) = \mathtt{Inv}_7(2) = 1$, thus from Theorem 3.2, we deduce

$$\mathtt{Inv}_7(n) = 2^{n-r} + \left(\frac{6}{2^r-1} - 1\right)\cdot \frac{2^{n-r}-1}{7}.$$

Suppose that $r = 1$, then the binary representation of $\mathtt{Inv}_7(n)$, say t, is as follow:

$$t = 1\,|\,u\,|\,u\,|\,\ldots\,|\,u = 1\,|\,10\,|\,1\,|\,10\,|\,1\,|\ldots\,|\,10\,|\,1,$$

where u is a binary sequence of length 3 representing the integer $\left(\frac{d\cdot \mathtt{Inv}_d(r)-1}{2^r-1} - 1\right)\cdot \frac{2^{\theta_d}-1}{d} = 5$.
Suppose that $r = 2$, then the binary representation of $\mathtt{Inv}_7(n)$, say t', is as follow:

$$t' = 01\,|\,u'\,|\,u'\,|\,\ldots\,|\,u' = 01\,|\,0\,|\,01\,|\,0\,|\,\ldots\,|\,01,$$

where u' is a binary sequence of length 3 representing the integer $\left(\frac{d\cdot \mathtt{Inv}_d(r)-1}{2^r-1} - 1\right)\cdot \frac{2^{\theta_d}-1}{d} = 1$.

Lemma 3.3. *Let θ_d be even and let d divide $2^{\theta_d/2}+1$. Further, suppose $n \geq 1$ is such that d and $2^n - 1$ are coprime, and let $1 \leq r \leq \theta_d - 1$ be the least positive residue of n (mod θ_d). Then the following properties hold:*

(a)

$$wt(\mathtt{Inv}_d(n)) = wt(\mathtt{Inv}_d(r)) + \frac{n-r}{2}.$$

(b)

$$wt(\mathtt{Inv}_d(\theta_d - r)) = wt(\mathtt{Inv}_d(r)) + \frac{\theta_d}{2} - r. \tag{11}$$

Proof. By Corollary 3 the binary weight of $\mathtt{Inv}_d(n)$ is

$$wt(\mathtt{Inv}_d(n)) = wt(\mathtt{Inv}_d(r)) + \frac{n-r}{\theta_d} wt(\boldsymbol{u}_{\theta_d}),$$

where $\boldsymbol{u}_{\theta_d}$ is the binary sequence of length θ_d representing the integer

$$\left(\frac{d\cdot \mathtt{Inv}_d(r)-1}{2^r-1} - 1\right)\cdot \frac{2^{\theta_d}-1}{d} = \left(\frac{d\cdot \mathtt{Inv}_d(r)-1}{2^r-1} - 1\right)\cdot \frac{2^{\theta_d/2}+1}{d}\cdot (2^{\theta_d/2}-1).$$

By Lemma 2.3, the weight of $\boldsymbol{u}_{\theta_d}$ is $\theta_d/2$, which completes the proof of (a). The statement of (b) follows from the fact that

$$\boldsymbol{u}_{\theta_d} = \bar{\boldsymbol{b}}_{\theta_d - r}\,|\,\boldsymbol{a}_r,$$

and therefore

$$\frac{\theta_d}{2} = wt(\boldsymbol{u}_{\theta_d}) = \theta_d - r - wt(\mathtt{Inv}_d(\theta_d - r)) + wt(\mathtt{Inv}_d(r)).$$

□

Remark 2. Let `Inverse` be an algorithm for inversion modulo $2^n - 1$. Theorem 3.2 and discussions of this subsection show that for several classes of integers finding their inverses modulo $2^n - 1$ can be reduced to computations modulo $2^{n'} - 1$ with n' much smaller than n. We summarize this observation in the following algorithm.

Data: positive integers d and n such that $\gcd(d, 2^n - 1) = 1$.
Result: $\texttt{Inv}_d(n)$, the inverse of d modulo $2^n - 1$.

if $n = 1$ or $d = 1$ **then**
  return 1
end
if d is even **then**
  return $2^{n-1}\texttt{Inv}_{\frac{d}{2}}(n) \pmod{2^n - 1}$
end
$\theta_d \leftarrow$ the order of 2 modulo d;
$r \leftarrow n \pmod{\theta_d}$;
if $r \neq n$ **then**
  $A \leftarrow \texttt{Inv}_d(r)$;
  return $A \cdot 2^{n-r} + \left(\dfrac{d \cdot A - 1}{2^r - 1} - 1\right) \cdot \dfrac{2^{n-r} - 1}{d}$;
else
  $d' \leftarrow d \pmod{2^n - 1}$;
  if $d' \neq d$ **then**
    return $\texttt{Inv}_{d'}(n)$
  else
    if $n > \theta_d/2$ **then**
      return $\dfrac{\left(d + 1 - \frac{\texttt{Inv}_d(\theta_d - n) \cdot d - 1}{2^{\theta_d - n} - 1}\right)(2^n - 1) + 1}{d} = \texttt{Inv}_d(n)$;
    else
      Compute $\texttt{Inv}_d(n)$ using `Inverse`;
    end
  end
end

Algorithm 1: Recursive inversion

Algorithm 1 reduces the computation of the inverse of d modulo $2^n - 1$ to one of modulo $2^r - 1$ with $1 \leq r \leq \theta_d$. In particular, this algorithm is effective for integers d with θ_d much smaller than n or for integers d with known small factors. Furthermore, this algorithm performs good for several special integers d, like Gold's and Kasami's exponents considered in the next subsections.

The next two examples compute inverses using Algorithm 1.

Example 3.2. Let $n = 97$ and $d = 2^{11} + 1 = 2049$. We compute the inverse of 2049 modulo $2^{97} - 1$:

1: $\theta_{2049} \leftarrow 22$

2: $r \leftarrow 9 \equiv 97 \pmod{22}$

3: $9 \neq 97$ then return $\texttt{Inv}_{2049}(9) \cdot 2^{88} + \left(\dfrac{2049 \cdot \texttt{Inv}_{2049}(9) - 1}{511} - 1\right) \cdot \dfrac{2^{88} - 1}{2049}$

  3.1: now $n = 9$ and $d = 2049$

3.2: $\theta_{2049} \leftarrow 22$

3.3: $r \leftarrow 9 \pmod{22}$ then

3.4: $d' \leftarrow 5 \equiv 2049 \pmod{2^9 - 1}$

3.5: return $\mathtt{Inv}_5(9)$

3.5.1: now $n = 9$ and $d = 5$

3.5.2: $\theta_5 \leftarrow 4$

3.5.3: $r \leftarrow 1 \equiv 9 \pmod{4}$

3.5.4: $1 \neq 9$ then return $2^8 + 3 \cdot \dfrac{2^8 - 1}{5}$

4: $\mathtt{Inv}_{2049}(97) = \left(2^8 + 3 \cdot \dfrac{2^8 - 1}{5}\right) \cdot 2^{88} + \left(\dfrac{2049 \cdot \left(2^8 + 3 \cdot \frac{2^8-1}{5}\right) - 1}{511} - 1\right) \cdot \dfrac{2^{88} - 1}{2049}$

Note that in this example, we do not need to call the algorithm `Inverse`.

Example 3.3. Let $n = 101$ and $d = 13$. We compute the inverse of 13 modulo $2^{101} - 1$:

1: $\theta_{13} \leftarrow 12$

2: $r \leftarrow 5 \equiv 101 \pmod{12}$

3: Using `Inverse` we compute that the inverse of 13 modulo $2^5 - 1$ is 12

4: $\mathtt{Inv}_{13}(101) = 12 \cdot 2^{96} + \left(\dfrac{155}{31} - 1\right) \cdot \dfrac{2^{96} - 1}{13}$

Note that the computation of the inverse of 13 modulo $2^{101} - 1$ was reduced to the one modulo $2^5 - 1$.

3.2. Gold's exponent

An integer $1 \leq d \leq 2^n - 2$ is called Gold's exponent if $d = 2^k + 1$ and $\gcd(n, k) = 1$. The assumption $\gcd(n, k) = 1$ is necessary and sufficient for the mapping $x \mapsto x^d$ to be APN on $\mathbb{F}_{2^n}$. In this section we use the term Gold's exponent to refer to the integers $d = 2^k + 1$ with $n/\gcd(n, k)$ odd. The assumption $n/\gcd(n, k)$ odd ensures that $2^k + 1$ is invertible modulo $2^n - 1$, cf. [5, Lemma 11.1]:

Lemma 3.4. *Let n and k be positive integers. Then*

$$\gcd(2^k + 1, 2^n - 1) = \begin{cases} 1 & \text{if } \frac{n}{\gcd(n,k)} \text{ is odd,} \\ 2^{\gcd(n,k)} + 1 & \text{otherwise.} \end{cases}$$

The inverses of APN Gold's exponents were considered in [10, Proposition 5]:

Proposition 3.5. *Let n be odd, and $\gcd(n, k) = 1$. Then*

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

and $wt(\mathtt{Inv}_{2^k+1}(n)) = \dfrac{n+1}{2}$.

Note that the integer $\frac{2^{k(n+1)}-1}{2^{2k}-1}$ is equal to the least positive residue of the inverse of 2^k+1 modulo 2^n-1 if and only if $k=1$. For $k=1$, the statement of Proposition 3.5 reduces to $\mathtt{Inv}_3(n)=\frac{2^{n+1}-1}{3}$ for all n odd.

Lemma 3.6. *Let $k \geq 1$ be an integer. The order of 2 modulo 2^k+1 is $\theta_{2^k+1}=2k$.*

Proof. Clearly, k is the smallest positive integer satisfying

$$2^k \equiv -1 \pmod{2^k+1},$$

implying that $\theta_{2^k+1}=2k$. □

Lemma 3.6 and Theorem 3.2 show that to invert a fixed Gold's exponent 2^k+1 modulo all 2^n-1 $(n \geq 1)$ it is enough to obtain the inverses $\mathtt{Inv}_{2^k+1}(r)$ for $1 \leq r < 2k$. In some of the arguments of this section it will be enough to consider only $1 \leq r \leq k$, because of the following easy observation:

Claim 1. *Let $0 \leq r < k$. Then $2^k+1 \equiv 2^k \cdot (2^r+1) \pmod{2^{k+r}-1}$. In particular, the least positive residues of inverses of 2^r+1 and 2^k+1 modulo $2^{k+r}-1$ have the same binary weight.*

The following theorem summarizes the main results on the inverses of Gold exponents.

Theorem 3.7. *Let $n,k \geq 1$ with $\gcd(n,k)=s$ and n/s odd. Set r be the least positive residue of n modulo $2k$. Then*

(a)

$$\mathtt{Inv}_{2^k+1}(n) = \mathtt{Inv}_{2^k+1}(r) \cdot 2^{n-r} + \left(\frac{(2^k+1)\cdot \mathtt{Inv}_{2^k+1}(r)-1}{2^r-1} - 1 \right)(2^k-1)\frac{2^{n-r}-1}{2^{2k}-1}.$$

(b) *Set*

- $\boldsymbol{g_n}$ *be the binary sequence of length n representing $\mathtt{Inv}_{2^k+1}(n)$;*
- $\boldsymbol{w_k}$ *be the binary sequence of length k representing $\frac{(2^k+1)\cdot \mathtt{Inv}_{2^k+1}(r)-1}{2^r-1} - 2$;*
- $\boldsymbol{a_r}$ *be the binary sequence of length r representing $\mathtt{Inv}_{2^k+1}(r)$.*

Then $\boldsymbol{g_n}$ is obtained by concatenating sequences $\boldsymbol{a_r}$, $\boldsymbol{w_k}$ and $\bar{\boldsymbol{w}}_{\boldsymbol{k}}$ as follows:

$$\boldsymbol{g_n} = \boldsymbol{a_r} \,|\, \boldsymbol{w_k} \,|\, \bar{\boldsymbol{w}}_{\boldsymbol{k}} \,|\, \ldots \,|\, \boldsymbol{w_k} \,|\, \bar{\boldsymbol{w}}_{\boldsymbol{k}}.$$

In particular, $wt(\boldsymbol{g_n}) = wt(\boldsymbol{a_r}) + \frac{n-r}{2}$.

(c) *The binary weight of $\mathtt{Inv}_{2^k+1}(n)$ is*

$$\frac{n-s}{2}+1 = \frac{n-s+2}{2}.$$

Proof. Statement (a) follows from Theorem 3.2 (a). To prove (b), set

$$u := \frac{(2^k+1)\cdot \mathtt{Inv}_{2^k+1}(r)-1}{2^r-1} - 1.$$

From the definition of $\mathtt{Inv}_{2^k+1}(r)$, it easily follows that $u < 2^k$. Lemma 2.3 combined with the part (a) of this theorem complete the proof of (b). We prove statement (c) by induction on k_1, where $k_1 = k/s$. If $k_1 = 1$ (or equivalently $k = s$), then $n \equiv s \pmod{2s}$, since n/s is odd. Consequently, $r = s$. Observe that $\mathtt{Inv}_{2^s+1}(s) = 2^{s-1}$. From (b), we have

$$wt(\mathtt{Inv}_{2^s+1}(n)) = wt(\mathtt{Inv}_{2^s+1}(s)) + \frac{n-s}{2} = 1 + \frac{n-s}{2}.$$

Suppose now that the statement holds for all $k_1 < \ell$ and take $k = s\ell$. Let $1 \le r < 2s\ell$ be the residue of $n \pmod{2s\ell}$. Then by (b) the problem reduces to finding the weight of the inverse of $2^{s\ell} + 1$ modulo $2^r - 1$. Note that if $r < s\ell$, then there is $\ell' < \ell$ such that

$$2^{s\ell} + 1 \equiv 2^{s\ell'} + 1 \pmod{2^r - 1}.$$

Hence the inverse of $2^{s\ell} + 1$ modulo $2^r - 1$ is equal to the one of $2^{s\ell'} + 1$, and we get

$$\begin{aligned} wt(\mathtt{Inv}_{2^{s\ell}+1}(n)) &= wt(\mathtt{Inv}_{2^{s\ell}+1}(r)) + \frac{n-r}{2} \\ &= wt(\mathtt{Inv}_{2^{s\ell'}+1}(r)) + \frac{n-r}{2} \\ &= 1 + \frac{r-s}{2} + \frac{n-r}{2} \\ &= 1 + \frac{n-s}{2}. \end{aligned}$$

To complete the proof we must prove the statement for the case $r \ge s\ell$. Let $r = s\ell + r'$. Then $r' = s\ell'$ for some $\ell' < \ell$. Using Claim 1, the binary weight of the inverses of $2^{s\ell} + 1$ and $2^{s\ell'} + 1$ modulo $2^{s\ell+s\ell'} - 1$ are equal, which completes the proof. □

Remark 3. The reason, why it was possible to determine the binary weight of the inverse of a Gold exponent in (c) of Theorem 3.7, is the fact that Algorithm 1 does not call the algorithm `Inverse`, when computing the inverse for a Gold exponent.

3.3. Kasami's exponent

We call integers $d = 2^{2k} - 2^k + 1$, where k is a positive integer, Kasami exponents. Such exponents define APN mappings on $\mathbb{F}_{2^n}$ if and only if $\gcd(k, n) = 1$. The next lemma summarize properties of Kasami exponents, which we need for later results:

Lemma 3.8. *Let k, n be positive integers. Then $\gcd(2^{2k} - 2^k + 1, 2^n - 1) = 1$ if and only if one of the following cases occurs:*

(a) $\frac{n}{\gcd(n,k)}$ is odd, that is $\gcd(n, 2k) = \gcd(n, k)$;

(b) $\frac{n}{\gcd(n,k)}$ 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 $0 \le u \le v$.*

Proof. Let $d = 2^{2k} - 2^k + 1$. In this proof, we use extensively Lemma 3.4. First we remark that

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

Clearly, for any n and k, the integer $\frac{n}{\gcd(n,k)}$ is either even or odd.

(a) Let $\dfrac{n}{\gcd(n,k)} \equiv 1 \pmod 2$.
Then $\gcd(2^{rk}+1, 2^n-1) = 1$ holds for all $r > 1$ odd. Hence in this case $\gcd(d, 2^n-1) = 1$, since $(2^k + 1) \cdot d = 2^{3k} + 1$.

(b) Let $\dfrac{n}{\gcd(n,k)} \equiv 0 \pmod 2$.
Then $\gcd(2^{rk} + 1, 2^n - 1) = 2^{\gcd(n,rk)} + 1$ holds for all $r > 1$ odd. If k is odd, then $3 = \gcd(d, 2^k + 1) \mid \gcd(d, 2^n - 1)$ because $3 \mid 2^n - 1$ for all n even.
Finally if k is even, it implies $\gcd(d, 2^k + 1) = 1$ and thus

$$\gcd(d \cdot (2^k + 1), 2^n - 1) = \gcd(d, 2^n - 1) \cdot \gcd(2^k + 1, 2^n - 1).$$

That is $2^{\gcd(n,3k)} + 1 = \gcd(d, 2^n - 1) \cdot (2^{\gcd(n,k)} + 1)$. Then $\gcd(n, k) = \gcd(n, 3k)$ becomes necessary and suficient to get $\gcd(d, 2^n - 1) = 1$.

□

Proposition 3.9. *Let $k > 1$ be an integer. Then the order of 2 modulo the Kasami exponent $2^{2k} - 2^k + 1$ is $\theta_d = 6k$.*

Proof. It is enough to show that $3k$ is the least positive integer satisfying $2^{3k} \equiv -1 \pmod{2^{2k}-2^k+1}$. The congruence $2^{3k} \equiv -1 \pmod{2^{2k}-2^k+1}$ holds, since clearly $2^{2k}-2^k+1$ divides $2^{3k} + 1$. Let an integer $0 < \sigma < 3k$ be such that $2^\sigma \equiv -1 \pmod{2^{2k} - 2^k + 1}$. Then $\sigma \geq 2k - 1$, since $1 < 2^l < 2^{2k} - 2^k$ for $0 < l \leq 2k - 1$. Hence suppose $\sigma = 2k + i$ with $0 \leq i < k$. Note that

$$2^{2k+i} \equiv 2^i(2^k - 1) \pmod{2^{2k} - 2^k + 1}.$$

To complete the proof it remains to observe that $2^i(2^k - 1) < 2^{2k} - 2^k$ if $0 \leq i < k$.

□

Theorem 3.2 implies for the Kasami exponents:

Theorem 3.10. *Let $n, k \geq 1$ with $\gcd(2^{2k} - 2^k + 1, 2^n - 1) = 1$. Let r be the least positive residue of n modulo $6k$. Then*

(a) $\mathtt{Inv}_{2^{2k}-2^k+1}(n)$ *is equal to*

$$\mathtt{Inv}_{2^{2k}-2^k+1}(r) \cdot 2^{n-r} + \left(\frac{(2^{2k} - 2^k + 1) \cdot \mathtt{Inv}_{2^{2k}-2^k+1}(r) - 1}{2^r - 1} - 1\right)\frac{2^{n-r} - 1}{2^{2k} - 2^k + 1}.$$

(b) *Let*

- $\boldsymbol{g_n}$ *be the binary sequence of length* n *representing* $\mathtt{Inv}_{2^{2k}-2^k+1}(n)$*;*
- $\boldsymbol{w_{3k}}$ *be the binary sequence of length* $3k$ *representing*

$$\left(\frac{(2^{2k}-2^k+1)\cdot \mathtt{Inv}_{2^{2k}-2^k+1}(r)-1}{2^r-1}-1\right)\cdot(2^k+1)-1;$$

- $\boldsymbol{a_r}$ *be the binary sequence of length* r *representing* $\mathtt{Inv}_{2^{2k}-2^k+1}(r)$.

Then $\boldsymbol{g_n}$ *is obtained by concatenating sequences* $\boldsymbol{a_r}$, $\boldsymbol{w_{3k}}$ *and* $\bar{\boldsymbol{w}}_{\boldsymbol{3k}}$ *as follows:*

$$\boldsymbol{g_n} = \boldsymbol{a_r}|\boldsymbol{w_{3k}}|\bar{\boldsymbol{w}}_{\boldsymbol{3k}}|\ldots|\boldsymbol{w_{3k}}|\bar{\boldsymbol{w}}_{\boldsymbol{3k}}.$$

In particular, $wt(\boldsymbol{g_n}) = wt(\boldsymbol{a_r}) + \frac{n-r}{2}$.

Proof. The statement follows from Theorem 3.2 and Lemma 2.3, similarly to the proof of Theorem 3.7. □

Example 3.4. Consider the Kasami exponent $13 = 2^4 - 2^2 + 1$. Lemma 3.8 shows that $\gcd(13, 2^n - 1) = 1$ if and only if $n \not\equiv 0 \pmod{12}$. Then using Theorem 3.10, we get:

- if $n \equiv 1 \pmod{12}$ then

$$\mathtt{Inv}_{13}(n) = 2^{n-1} + 11 \cdot \frac{2^{n-1}-1}{13},$$

since $\mathtt{Inv}_{13}(1) = 1$. The binary weight of $\mathtt{Inv}_{13}(n)$ is $(n+1)/2$.

- if $n \equiv 2 \pmod{12}$ then

$$\mathtt{Inv}_{13}(n) = 2^{n-2} + 3 \cdot \frac{2^{n-2}-1}{13}$$

since $\mathtt{Inv}_{13}(2) = 1$. The binary weight of $\mathtt{Inv}_{13}(n)$ is $n/2$.

- if $n \equiv 3 \pmod{12}$ then

$$\mathtt{Inv}_{13}(n) = 6 \cdot 2^{n-3} + 10 \cdot \frac{2^{n-3}-1}{13}$$

since $\mathtt{Inv}_{13}(3) = 6$. The binary weight of $\mathtt{Inv}_{13}(n)$ is $(n+1)/2$.

- if $n \equiv 4 \pmod{12}$ then

$$\mathtt{Inv}_{13}(n) = 7 \cdot 2^{n-4} + 5 \cdot \frac{2^{n-4}-1}{13}$$

since $\mathtt{Inv}_{13}(4) = 7$. The binary weight of $\mathtt{Inv}_{13}(n)$ is $(n+2)/2$.

- if $n \equiv 5 \pmod{12}$ then

$$\mathtt{Inv}_{13}(n) = 12 \cdot 2^{n-5} + 5 \cdot \frac{2^{n-5}-1}{13}$$

since $\mathtt{Inv}_{13}(5) = 12$. The binary weight of $\mathtt{Inv}_{13}(n)$ is $(n-1)/2$.

- if $n \equiv 6 \pmod{12}$ then

$$\mathtt{Inv}_{13}(n) = 34 \cdot 2^{n-4} + 6 \cdot \frac{2^{n-4}-1}{13}$$

since $\mathtt{Inv}_{13}(6) = 34$. The binary weight of $\mathtt{Inv}_{13}(n)$ is $(n-2)/2$.

Then using identity (3.3), we obtain that:

- if $n \equiv 7 \pmod{12}$ then the binary weight of $\mathtt{Inv}_{13}(n)$ is $(n-1)/2$, since $wt(\mathtt{Inv}_{13}(7)) = 3$.
- if $n \equiv 8 \pmod{12}$ then the binary weight of $\mathtt{Inv}_{13}(n)$ is $(n+2)/2$, since $wt(\mathtt{Inv}_{13}(8)) = 5$.
- if $n \equiv 9 \pmod{12}$ then the binary weight of $\mathtt{Inv}_{13}(n)$ is $(n+1)/2$, since $wt(\mathtt{Inv}_{13}(9)) = 5$.
- if $n \equiv 10 \pmod{12}$ then the binary weight of $\mathtt{Inv}_{13}(n)$ is $n/2$, since $wt(\mathtt{Inv}_{13}(10)) = 5$.
- if $n \equiv 11 \pmod{12}$ then the binary weight of $\mathtt{Inv}_{13}(n)$ is $(n+1)/2$, since $wt(\mathtt{Inv}_{13}(11)) = 6$.

Open question: Is it possible to express the binary weight of the inverse of Kasami's exponent $2^{2k} - 2^k + 1$ modulo $2^n - 1$ in terms of k and n?

r	1	3	5	7	9	11	13	15	17
$wt(\mathtt{Inv}_d(r))$	1	1	2	4	2	6	6	7	9

Table 2: Weights of the inverse of $d = 2^6 - 2^3 + 1$ modulo $2^r - 1$, $1 \le r \le 17$

r	1	2	3	4	5	6	7	8	9	10	11	12
$wt(\mathtt{Inv}_d(r))$	1	1	2	1	3	2	4	5	5	3	4	2
r	13	14	15	16	17	18	19	20	21	22	23	
$wt(\mathtt{Inv}_d(r))$	5	5	8	9	9	8	10	9	11	11	12	

Table 3: Weights of the inverse of $d = 2^8 - 2^4 + 1$ modulo $2^r - 1$, $1 \le r \le 23$

r	1	3	5	7	9	11	13	15	17	19	21	23	25	27	29
$wt(\mathtt{Inv}_d(r))$	1	2	1	3	5	5	7	2	9	9	11	11	11	14	15

Table 4: Weights of the inverses of $d = 2^{10} - 2^5 + 1$ modulo $2^r - 1$, $1 \le r \le 29$

Tables 2–4 contain the weights of the inverses for the Kasami exponents defined with $k = 3, 4, 5$. Some of the values in these tables follow from the results of Proposition 3.11:

Proposition 3.11. *Let $k, n \geq 1$ and $\gcd(2^{2k} - 2^k + 1, 2^n - 1) = 1$.*

(a) If $n \equiv b \pmod{6k}$ with $b \geq 1$ a divisor of k, then $\mathtt{Inv}_{2^{2k}-2^k+1}(k/b) = 1$ and

$$\mathtt{Inv}_{2^{2k}-2^k+1}(n) = 2^{n-k/b} + \left(\frac{2^k(2^k-1)}{2^{k/b}-1} - 1\right) \cdot \frac{2^{n-k/b}-1}{2^{2k}-2^k+1}.$$

(b) $\mathtt{Inv}_{2^{2k}-2^k+1}(k-1) = \frac{2^k-1}{3}$.

(c) $\mathtt{Inv}_{2^{2k}-2^k+1}(k+1) = \frac{2^{k+2}-1}{3} + 1$.

(d) $\mathtt{Inv}_{2^{2k}-2^k+1}(2k) = (2^k+2) \cdot \frac{2^k-1}{3} + 1$.

(e) If $n \equiv 3k/b \pmod{6k}$, where $b \geq 1$ is a divisor of k with $\gcd(b, 3) = 1$. Let b' be the least positive residue of b modulo 3, then $\mathtt{Inv}_{2^{2k}-2^k+1}(3k/b) = 2^{3k/b-1} + 2^{b' \cdot k/b-1}$.

(f) $\mathtt{Inv}_{2^{2k}-2^k+1}(4k) = (1 + 2^{k+1} + 2^{2k} + 2^{3k+1}) \cdot \frac{2^k-1}{3} + 2^k$.

(g) $\mathtt{Inv}_{2^{2k}-2^k+1}(5k) = 2^{5k} - 2^{4k} + 2^{2k} + 2^k - 1 \equiv 2^{2k}(2^{4k} - 2^{2k} + 1) \pmod{2^{5k} - 1}$.

(h) $\mathtt{Inv}_{2^{2k}-2^k+1}(6k-1) = (2^{3k}-1)(2^k+1)$.

Note that in cases (c)–(k) of the above proposition n depends on k, and hence we are in a similar situation discussed in Section 2.

For any b dividing k and being coprime to 5, we conjecture that $\mathtt{Inv}_{2^{2k}-2^k+1}(5k/b)$ is congruent to a Kasami exponent, that is, $\mathtt{Inv}_{2^{2k}-2^k+1}(5k/b) \equiv 2^u(2^{2v}-2^v+1) \pmod{2^{5k/b}-1}$ for some integers u and v.

Finally we want to remark that in some cases the computation of inverses for Kasami exponents can be reduced to the one for the Gold exponents.

Claim 2. *Let the positive integers k, n be such that $\frac{n}{\gcd(n,k)}$ is odd. Then both $2^k + 1$ and $2^{3k} + 1$ are coprime to $2^n - 1$, and therefore*

$$\mathtt{Inv}_d(n) \equiv (2^k+1)\mathtt{Inv}_{2^{3k}+1}(n) \pmod{2^n - 1}$$

holds.

3.4. $2^k - 1$ exponent

In [1] it is shown that the power mappings with exponents $2^k - 1$ have interesting properties for cryptological applications. It is well known that $\gcd(2^n - 1, 2^k - 1) = 2^{\gcd(n,k)} - 1$, and therefore $2^k - 1$ is invertible modulo $2^n - 1$ if and only if n and k are coprime. Moreover this indicates also that the calculation of the inverse of $2^k - 1$ modulo $2^n - 1$ reduces to the one of k modulo n.

Theorem 3.12. *Let $n, k \geq 2$ be coprime integers. Then*

$$\mathtt{Inv}_{2^k-1}(n) \equiv \frac{2^{k \cdot s} - 1}{2^k - 1} \pmod{2^n - 1},$$

where s is any positive integer satisfying $s \cdot k \equiv 1 \pmod{n}$. More precisely, if k_n^{-1} is the least positive residue of the inverse of k modulo n, then

$$\mathtt{Inv}_{2^k-1}(n) = \sum_{i=0}^{k_n^{-1}-1} 2^{ki \pmod{n}}. \tag{12}$$

Proof. Let $s \cdot k - 1 = n \cdot m$. Then

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

The second statement follows if we put $s = k_n^{-1}$. □

4. Conclusion

This paper is motivated by a problem to find explicitly the inverses of the known APN exponents. We succeed this for Welch and Dobbertin exponents. The case of the exceptional APN exponents, that is of the Gold and Kasami exponents, is more difficult as we show in Section 3. For the Gold exponents $2^k + 1$, we found the binary weights of their inverses modulo $2^n - 1$ in terms of n and k. For the Kasami exponents $2^{2k} - 2^k + 1$, we showed that the binary weight of the inverses is uniquely defined by the binary weight of its inverse modulo $2^r - 1$, where r is the least positive residue of n modulo $\theta_{2^{2k}-2^k+1} = 6k$. Presently, it is not clear to us whether we may expect more explicit results on Kasami exponents than those given in Theorem 3.10.

Generally, for a fixed positive integer we considered the function $\mathtt{Inv}_d$, which maps n to the least positive residue of the inverse of d modulo $2^n - 1$, where d is a fixed positive integer. We are not aware whether the function $\mathtt{Inv}_d$ was studied before. We think that a better understanding of $\mathtt{Inv}_d$ in general, as well as for special values of d, is a fundamental problem deserving a further development. In particular, it would be interesting to see if there are any connections with the algebraic feedback shift register sequences (see [8]) yielding new insights on the problem.

Bibliography

[1] 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

[2] 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.

[3] 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.

[4] J.F. Dillon, Geometry, codes and difference sets: exceptional connections. In *Codes and design* (Colombus, OH, 2000), volume 10 of Ohio State Univ. Math. Res. Inst. Publ., 73 – 85, de Gruyter, Berlin, 2002.

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

[6] 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.

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

[8] M. Goresky and A. Klapper, Algebraic Shift Register Sequences, Cambridge University Press, March 2012.

[9] G.M. Kyureghyan and V. Suder, On inverses of APN exponents. *in Proceedings of the 2012 IEEE International Symposium on Information Theory, ISIT 2012, Cambridge, MA, USA*, July 1-6, 2012

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

[11] M. Portmann and M. Rennhard, Almost perfect nonlinear permutations. *Semester Project – Swiss Federal Institute of Technology Zurich*, 1997.