On the Properties of S-boxes

A Study of Differentially 6-Uniform Monomials over Finite Fields of Characteristic 2

LÉO PERRIN

Master's Thesis at the Mathematics Department
Supervisor: Dr. Céline Blondeau
Examiner: Dr. Olof Heden

Abstract

S-boxes are key components of many symmetric cryptographic primitives. Among them, some block ciphers and hash functions are vulnerable to attacks based on differential cryptanalysis, a technique introduced by Biham and Shamir in the early 90's. Resistance against attacks from this family depends on the so-called differential properties of the S-boxes used.

When we consider S-boxes as functions over finite fields of characteristic 2, monomials turn out to be good candidates. In this Master's Thesis, we study the differential properties of a particular family of monomials, namely those with exponent $2^t - 1$. In particular, conjectures from Blondeau's PhD Thesis are proved.

More specifically, we derive the differential spectrum of monomials with exponent $2^t - 1$ for several values of t using a method similar to the proof Blondeau *et al.* made of the spectrum of $x \mapsto x^7$. The first two chapters of this Thesis provide the mathematical and cryptographic background necessary while the third and fourth chapters contain the proofs of the spectra we extracted and some observations which, among other things, connect this problem with the study of particular Dickson polynomials.

Keywords: Symmetric cryptography, Differential uniformity, Differential spectrum, Kloosterman sum, Power function, Roots of trinomial, $x \mapsto x^{2^t-1}$, Dickson polynomial, Differential Cryptanalysis.

Acknowledgement

While acknowledgements may seem like the easiest part of a thesis to write due to their lack of scientific content, they actually involve a skill which is only remotely sharpened throughout scientific studies: literary talent. And it gets even worse when you happen not to be a native speaker of the language you have to write them in. However, I will do my best to express here the gratitude I have for several people.

Before anyone else, my deepest thanks go to Céline Blondeau. I wonder what she thought when she received my mail asking for informations about master's thesis's at her lab but I cannot express how happy I am she thought it might be a good idea to have me there. Enumerating all the things she taught me would would probably take an additional full chapter of this thesis. If I ever manage to become a cryptographer — and I have now good hopes I will — it will be for the largest part thanks to her.

I would also like to express my gratitude for Kaisa Nyberg, the head of the cryptography group at Aalto University, for treating me like a regular member of the group despite my somewhat odd status.

But despite my working at Aalto, I was still a KTH student and would thus like to thank some people there for their help. First, Olof Heden committed to read my thesis and judge my presentation. I am aware of the huge amount of work corresponding to this and I am really grateful he agreed to do this. Petter Brändén and Mattias Dahl were also very helpful: seeing people in charge of what essentially amounted — in my case — to paperwork being actually helpful is something which, as a Frenchman, I thought impossible. I really thank them for their patience concerning my strange project.

I thank also Kimmo, Antti, Risto and Siert, with whom I ate and had coffee every day, who helped me relax and showed me a glimpse of the Finnish culture. I hope they will forgive my ranting way too often about the food quality of the place where we ate.

On a more personal level, the mathematics would have driven me crazy if it was not for Aalto's aikido club where I could exercise and make new friends. In the same way, I truly appreciated the kindness of my friend Alexandra.

Introduction

It is a euphemism to say that protecting data from eavesdropping or tempering is a topic of crucial importance in the Internet era. Such protection is provided by cryptographic primitives such as ciphers modifying data to make it impossible to read without a key, hash functions associating an unfalsifiable fingerprint to any binary string of any length or message authentication codes (MAC) used to ensure a message was not modified.

The design of such cryptographic primitives is a complicated task and has been an active topic in research laying at the intersection of pure mathematics and computer science ever since the invention of computers. There are two main groups of cryptographic primitives: the asymmetric and the symmetric ones. Asymmetric cryptography deals (roughly) with building cryptosystems such that the key to encrypt is made public and the key to decrypt, which is different, is kept secret. However, we are interested here in symmetric cryptography which is about encryption of data such that decryption and encryption use the same (secret) key.

When building a symmetric cipher, its designers must keep many things in mind. It should be fast when being ran on a regular personal computer as well as on much less computationally powerful embedded systems. It should be possible for cryptographers to study it to assess its qualities so using a known structure is a plus. Lastly and most obviously, it must be secure. But what does "secure" mean in this context? Intuitively, a cipher with good security is a cipher such that an attacker cannot recover the plaintext corresponding to a ciphertext and, in particular, that recovering the key must be, for all practical purposes, impossible. To achieve this, ciphers usually consist of the multiple combination of linear operations and non-linear operations providing respectively diffusion and confusion (Shannon's construction). The non-linear operations are often done by small sub-functions from $\mathbb{F}_{2^m}$ to $\mathbb{F}_{2^n}$ called S-boxes, where $\mathbb{F}_{2^n}$ is the finite field of characteristic 2 and size 2^n.

A method allowing to retrieve the key used to encrypt a binary string is called an attack. Examples of families of attacks are linear attacks and algebraic attacks. Here, we study the resilience of ciphers against one of the main ones: the differential attack. Introduced by Biham and Shamir in the early 90's in [BS91], this attack can be prevented using S-boxes with particular properties such as a low differential uniformity, a quantity defined by Nyberg in [Nyb94]. A more finely grained measure of its resilience is the differential spectrum which was properly defined by Blondeau *et al.* in a recent paper [BCC10a]. The purpose of this master Thesis is to study the differential properties of a particular class of S-boxes by proving conjectures made in Blondeau's PhD Thesis ([Blo11]).

S-boxes are functions from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$ and, as such, can be seen as polynomials. Monomials, i.e. polynomial with only one non-zero coefficient are good candidates for use as S-boxes because their algebraic structure allows an easier study and because they are cheaper to implement in hardware. The class of exponents $2^t - 1$ was studied by Blondeau *et al.* in [BCC11] and, in particular, the complete differential spectrum of $x \mapsto x^7$ corresponding to the case $t = 3$ was extracted. We prove here that $x \mapsto x^{2^t-1}$ yields essentially the same differential spectrum as $x \mapsto x^7$ for $t = (n-1)/2$ and $t = (n+3)/2$ when n is odd and for $t = (kn+1)/3$ and $t = (jn+2)/3$ when 3 does not divide n and $k = 1, 2$ and $j = 3 - k$ are such that t is an integer. An article describing these results has been accepted at the International Workshop on Coding and Cryptography 2013 [BP13].

While working on this Thesis, we learnt how to do research: its process of course but also less scientific but still important things such as the rank of the different conferences in theoretical computer science, names of researchers working in the same field and thus whose lists of publications provide valuable resources, how to write a scientific paper and how to submit it for publication. Another skill acquired is the use of SAGE [SJ05], an open-source set of advanced mathematical Python library providing, among other things, tools to perform computations in finite fields of any characteristic. All the results presented here have been checked using it in fields of size 2^7 up to 2^{14}.

The structure of this Thesis is as follows. First, we shall introduce the cryptological concepts behind this work. In the second part, the notions corresponding to the differential properties of an S-box are introduced and a review of known results on this topic is made. The third part consists in the proofs of the main results of this Thesis, namely the value of the differential spectrum of the monomials with exponent $t = (kn+1)/3$ and $t = (jn+2)/3$ in a first section and then $t = (n-1)/2$ and $t = (n+3)/2$ in a second one. In the last chapter, remarks are made to link this work with properties of the so-called reversed Dickson polynomials, to discuss the general properties of these functions, to determine which are the best candidates for use as a actual S-boxes and to show a connexion between monomials with exponents $2^t - 1$ and $2^{t+1} - 1$. Conjectures regarding the differentially 6-uniform power functions are also discussed.

Contents

Chapter 1

Cryptological Background

S-boxes are part of the design of many block ciphers, hash functions and message authentication codes (MAC). Examples of block cipher are the DES (Data Encryption Standard) [Nat99] and its successor, the AES (Advanced Encryption Standard) [DR98]. They are used of course to encrypt sensitive data but also as part of the design of some cryptographic hash functions. Hash functions turn any binary string into a "digest" of fixed length and are used to provide practically unfalsifiable fingerprints for computer files. The last standard for hashing algorithms is Keccak [BDPA11], winner of the SHA-3 competition.

Having "good" block ciphers is thus a very important factor to achieve a decent security on modern computers. In this context, "good" means that the block cipher must be resilient against a large variety of attacks, the main ones being differential and linear cryptanalysis as well as their generalisations.

In the rest of this chapter, we shall give the definitions of some cryptological concepts used throughout this Thesis. They are part of the cryptological folklore but one can find them for instance in [Sti05]. Then, we shall look at what a differential cryptanalysis is.

We denote by $|s|$ the length of any binary string s and by $s_1||s_2$ the concatenation of the binary strings s_1 and s_2.

1.1 Cryptographic Primitives

The whole point of this Master's Thesis is to study some key components of many symmetric block ciphers, namely the so-called S-boxes. First, let us formally define what a symmetric block cipher is.

Definition 1 (Symmetric Cipher). *A cipher $\mathcal{C}$ is a 5-tuple of finite sets $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ yielding the following properties:*

- *$\mathcal{P}$ is the set of the plaintexts.*
- *$\mathcal{C}$ is the set of the ciphertexts.*

- *$\mathcal{K}$ is the set of the possible keys.*
- *For every k in $\mathcal{K}$, there is an encryption rule $e_k : \mathcal{P} \rightarrow \mathcal{C}$ and a decryption rule $d_k : \mathcal{C} \rightarrow \mathcal{P}$ such that for any plaintext x of $\mathcal{P}$, $(d_k \circ e_k)(x) = x$. In other words, if we encrypt a text x with a key k and decrypt the ciphertext we just obtained using the same key k, we have to obtain the plaintext x back (see Figure 1.1).*

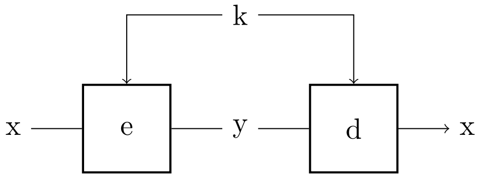

Figure 1.1. Schematic diagram of a symmetric cipher.

Note that it must of course hold that $|e_k(p_i)| = |p_i| = c$ because the transformation e_k has to be a bijection. Otherwise, decryption would be impossible.

Definition 2 (Block cipher)**.** *A block-cipher $\mathcal{C}$ of block-size b is a symmetric cipher which encrypts binary strings of size b into binary strings of size b.*

A block cipher as such does not allow the encryption of binary strings of arbitrary length. However, if we "slice" a plaintext $x_1||x_2||...||x_u$ of size $b \times u$ into u blocks of size b $(x_1, ..., x_u)$, we can run a block cipher on every block we obtained. The way in which the block cipher is used to encrypt this longer ciphertext is called the *mode of operation*. The simplest consists in encrypting each block separately (see Figure 1.2). It is called ECB (Electronic Code Book) but should not be used due to its lack of security.

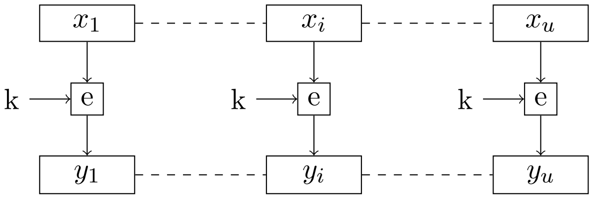

Figure 1.2. The ECB mode of encryption: a plaintext x made of u blocks x_i of size b is encrypted into a ciphertext y made of u blocks y_i.

Ciphers are usually built using multiple iterations of a so-called *round function* made of the composition of a linear operation and a non-linear one. The non-linear part is often performed by dividing the input into several blocks of small size and then applying a highly non-linear function to each of these blocks separately. The functions applied to these small blocks are called *S(ubstitution)-boxes*. Such S-boxes are at the core of the design of a broad family of symmetric block ciphers: that of the Substitution-Permutation Networks (SPN). They can also be used as part of the round function of other constructions such as Feistel Networks — it is the case of the DES for instance.

The general principle of the round function of a Substitution-Permutation Network is given Figure 1.3. Such a function is applied several times on the input (one iteration is called a *round*), the keys k^i depending on the index of the round. Actual implementations of SPN's include Rijndael [DR98], which is the Advanced Encryption Standard (AES), and the ultra-lightweight cipher PRESENT [BKL+07]. Encryption of a binary string x^0 is performed by iteratively adding[1] x^i with the round key k^i, applying the non-linear transformation S to each sub-block of the result and then use a bijection P on the whole output of the S-boxes to obtain x^{i+1}.

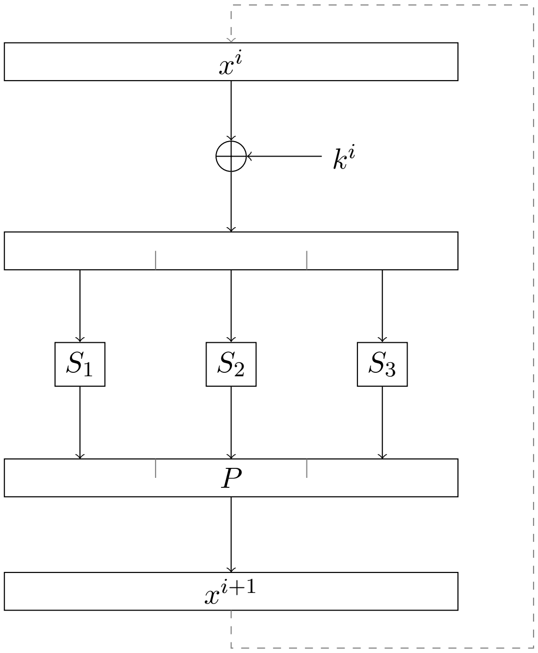

Figure 1.3. The round function of a Substitution-Permutation Network using three S-boxes. It is applied several time to the current state.

Note that S-boxes may not have to be permutations in the case where they are used in block ciphers that are not SPN's. For instance, those used in the Feistel function of the Data Encryption Standard (DES) map six bits to four, as described in the specification of this algorithm [Nat99].

1.2 Cryptanalysis

The aim of this Thesis is to study a property of the S-boxes that is crucial for the resilience of a cryptosystem against a differential cryptanalysis. First, we shall

[1] Addition is performed in $\mathbb{F}_{2^n}$ so, in particular, $1 + 1 = 0$.

define what a cryptanalysis is, then we shall look at the different attack models and, at last, we shall see what a differential cryptanalysis is.

1.2.1 Some Attack Models

Definition 3 (Cryptanalysis)**.** *The action of trying to extract useful data from a ciphertext without any previous knowledge of the key. A person trying to perform a cryptanalysis is called an attacker.*

The Kerchoff assumption is usually assumed in cryptography. It states that the attacker knows the algorithm used to encrypt some data but not the key. Hence, the task of an attacker is usually to find the said key.

The attacker can have different kind of data at their disposal. The data they have defines the attack model they are using.

Definition 4 (Known ciphertext)**.** *Such an attack is performed by an attacker having only some ciphertexts.*

Definition 5 (Known plaintext)**.** *In this cryptanalysis, the attacker has several pairs plaintext-ciphertext obtained using the same cipher and the same key.*

Definition 6 (Chosen plaintext)**.** *In this case, the attacker has the complete encryption algorithm (including its key) as a black-box. Therefore, this attack is a known plaintext attack where the attacker can choose the plaintexts.*

There are other attack models but their study is beyond the scope of this Thesis.

1.2.2 General Principle of the Differential Cryptanalysis

Differential cryptanalysis was introduced by Biham and Shamir in [BS91]. However, its principle was already known by the NSA and IBM earlier. In fact, it has been disclosed since that the DES algorithm was designed to be resilient against this attack [Cop94]. This section provides an overview of the principle of this attack.

It is a chosen plaintext attack: the attacker has a “black-box” made of the cipher and its key and he can encrypt any plaintext until the key is retrieved. This attack looks at the so-called propagation ratios which are the probabilities of differentials, objects that are defined below.

Definition 7. *Let $E : \mathbb{F}_{2^m} \to \mathbb{F}_{2^n}$ be a block cipher. We call differential a pair $(\Delta x, \Delta y)$ where*

- *$\Delta x = x \oplus x'$ where x and x' are two plaintexts.*
- *$\Delta y = y \oplus y'$ where $y = E(x)$ and $y' = E(x')$.*

Definition 8. *The propagation ratio $R_p(a,b)$ of a differential (a,b) is the probability of the differential (a,b) or, in other words, the probability that the output difference Δy equals b knowing that the input difference Δx equals a:*

$$R_p(a,b) = \mathbf{Pr}[E(x) + E(x+a) = b]. \tag{1.1}$$

If the cipher used was perfect, the probability of every differential would be the same, i.e. 2^{-n}. However, in practice, some differentials have a much higher probability. The aim of a differential cryptanalysis is to use this imperfection to retrieve the key.

Consider a block cipher made of r rounds with round function F_{k^i} $(1 \leq i \leq r)$ described Figure 1.3, k^i being the i-th round key. Let R be the composition of the S-box layer and the permutation layer such that $F_k(x) = R(x+k)$. Let (a,b) be a differential:

$$\begin{aligned} & F_k(x+a) + F_k(x) = b \\ \Longrightarrow\ & R(x+a+k) + R(x+k) = b. \end{aligned}$$

Then the difference in the input of E is $(x+a+k)+(x+k) = a$: the key does not play any role any more. The idea of differential cryptanalysis is to find a sequence of high probably differentials (a_i, b_i) of the function F_{k^i} for i in $[1, r-1]$ which can be "plugged" together in the sense that $F_{k^i}(x)+F_{k^i}(x+a_i) = b_i$. Such differentials form a so-called *differential trail*. The usual hypothesis is that of the round independence: the probability of the differential trail is the product of the propagation ratio of the differentials it is made off.

Once a differential with high[2] probability is found, many couples of ciphertexts (x, x') such that $x + x' = a$ are fed to the encryption algorithm. We know with "high" probability some of the bits of the output of the before-last round, namely those that are on the differential. Therefore, we can retrieve some information about the key k^r used in the last round.

Note that if the distribution of the propagation ratios is close to the uniform distribution, this attack will fail because it is in this case impossible to find differential trails with high probabilities.

1.3 Criteria for the Resilience Against Different Attacks

Criteria have been found to predict the influence an S-box will have over the resilience of a cipher against not only differential cryptanalysis but also related attacks such that higher order differential cryptanalysis or different ones like linear attacks. Note that they only provide information about the strength of an encryption algorithm against currently known attacks. They are thus necessary for a cipher to be "good" but may turn out not to be sufficient in the future if a new family of attack is discovered.

[2] "High" in this context means significantly higher than 2^{-rn} where n is the block size and r the number of rounds.

Nyberg [Nyb94] provides such a list. S-boxes must be:

- Highly non-linear.
- Have a high algebraic degree.
- Efficient construction and computability.
- Good resistance against differential cryptanalysis.

Non-linearity and algebraic degree are notions defined in Section 4.3. The properties implying a good resistance against differential cryptanalysis are related to the differential properties of the S-box and are the main topic of this Thesis. In what follows, we shall first introduce the concepts of differential uniformity and differential spectrum and then study extensively those of a family of monomials.

Chapter 2

Differential Properties of Monomials

2.1 Mathematical Notations

Let us first introduce the mathematical concepts and notations we are going to use throughout this Thesis.

Definition 9 (Finite field of characteristic 2)**.** *Up to isomorphism, there is only one finite field of characteristic 2 and size* 2^n*. We denote this field* $\mathbb{F}_{2^n}$*.*

Definition 10 (Boolean Function)**.** *A Boolean function with* n *variables is a function from* $\mathbb{F}_2^n$ *to* $\mathbb{F}_2$*. The set of the Boolean functions with* n *variables is* $\mathcal{B}_n$*.*

It is natural to extend this definition to function having not a single bit as their output but several.

Definition 11 (Vectorial Function)**.** *A vectorial function is a function from* $\mathbb{F}_{2^n}$ *to* $\mathbb{F}_{2^m}$*. The set of all such vectorial functions is denoted* $\mathcal{B}_n^m$*.*

A tool we shall use extensively is the *trace function*, in particular the so-called *absolute trace.*

Definition 12 (Trace)**.** *The trace of* $\alpha \in \mathbb{F}_{2^n}$ *over the sub-field* $\mathbb{F}_{2^k}$ *with* k *dividing* n *is equal to:*

$$\mathbf{Tr}_k^n(\alpha) = \sum_{i=0}^{n/k-1} \alpha^{2^{ki}}.$$

Definition 13 (Absolute trace)**.** *We call absolute trace the trace over* $\mathbb{F}_2$ *and we denote it* $\mathbf{Tr}$*:*

$$\mathbf{Tr}(\alpha) = \sum_{i=0}^{n-1} \alpha^{2^i}.$$

We shall focus on a particular type of functions: the monomials. Furthermore, we shall focus mainly on *power permutations.*

Definition 14 (Permutation)**.** *A permutation over $\mathbb{F}_{2^n}$ is a function which maps every element of $\mathbb{F}_{2^n}$ to a unique element of $\mathbb{F}_{2^n}$.*

Definition 15 (Power permutation)**.** *We call "power permutation" a bijective monomial, i.e. a monomial $x \mapsto x^d$ over $\mathbb{F}_{2^n}$ which is a permutation.*

The following lemma about power permutations is well known and will be used in this Thesis.

Lemma 1. *A monomial $x \mapsto x^d$ is a power permutation over $\mathbb{F}_{2^n}$ if and only if* $\gcd(d, 2^n - 1) = 1$.

As we shall study monomials with exponents $2^t - 1$, the inverse of $2^t - 1$ modulo $2^n - 1$ will often be used. When it exists, we shall denote it $\tau = (2^t - 1)^{-1} \mod (2^n - 1)$ and use the following theorem to compute it.

Theorem 1 (Theorem 7 from [KS12])**.** *Let t and n be co-prime and t^{-1} be the inverse of t modulo n. Then $2^t - 1$ is invertible modulo $2^n - 1$ and its inverse τ is:*

$$\tau \equiv (2^t - 1)^{-1} \equiv \sum_{i=0}^{t^{-1}-1} 2^{ti} \mod (2^n - 1).$$

At last, the size of any set S is denoted $|S|$.

2.2 Differential Spectrum: Definition and Properties

Now that the background of our study is defined, let us look at the definition of the differential spectrum itself as well as that of related concepts. The definitions of coefficients $\delta(a, b)$ and of differential uniformity were introduced in [Nyb94].

Definition 16 (Derivative)**.** *Let F be a function of $\mathcal{B}_n^m$ and let a be an element of $\mathbb{F}_{2^n}$. The derivative of F to the direction a is defined by*

$$\mathbb{D}_a F : x \mapsto F(x + a) + F(x).$$

Definition 17. *Let F be a function of $\mathcal{B}_n^m$, let a be an element of $\mathbb{F}_{2^n}$ and b be in $\mathbb{F}_{2^m}$. Then we call $\delta(a, b)$ the following quantity:*

$$\delta(a, b) \;=\; |\{x \in \mathbb{F}_{2^n}, \mathbb{D}_a F = b\}|.$$

Recall the definition of the propagation ratio (Definition 8): we have the following connexion between $R_p(a, b)$ and $\delta(a, b)$:

$$R_p(a, b) = \frac{\delta(a, b)}{2^n}. \tag{2.1}$$

Therefore, the lower the values $\delta(a, b)$, the better.

Note that if x is a solution of $\mathbb{D}_aF(x) = b$ then so does $x + a$. Indeed, in characteristic 2, $F(x+a+a)+F(x+a) = F(x)+F(x+a)$. Thus, $\delta(a, b)$ has to be even. Besides, if F is a monomial $x \mapsto x^d$, then we have the following for $a \neq 0$:[1]

$$\begin{aligned} F(x+a) + F(x) &= (x+a)^d + x^d \\ &= a^d\Big(\big(\frac{x}{a}+1\big)^d + \big(\frac{x}{a}\big)^d\Big). \end{aligned}$$

Therefore, $\delta(a, b) = \delta(1, b/a^d)$. To know the value of all the $\delta(a, b)$, it is thus enough to study all the $\delta(1, b)$. For the sake of simplicity and since this is the quantity we shall deal with, we let:

$$\delta(b) = \delta(1, b)$$

Definition 18 (Differential uniformity)**.** *Let F be a function of $\mathcal{B}_n^m$. The differential uniformity of F is the following quantity:*

$$u(F) \;=\; \max_{a\neq 0,b}\left(\delta(a,b)\right)$$

We then say that F is differentially $u(F)$-uniform. If F is a monomial, we have that

$$u(F) \;=\; \max_{a\neq 0,b}\left(\delta(b)\right).$$

As $\delta(0)$ and $\delta(1)$ often require a special treatment, we introduce the local differential uniformity.

Definition 19 (Local differential uniformity)**.** *We say that a monomial F is* locally *differentially Δ-uniform if $\delta(b) \leq \Delta$ for all $b \neq 0, 1$ and we say that the local differential uniformity of F is Δ. We denote by $U(F)$ the local uniformity of a monomial F.*

In particular, functions which are differentially 2-uniform are called Almost Perfect Non-linear (APN). Their properties were intensively studied, see Section 2.4.1. We now have all the tools at hand to give the definition of the differential spectrum, a concept introduced in [BCC10a].

Definition 20 (Differential Spectrum)**.** *Let $F(x) = x^d$ be a power function over $\mathbb{F}_{2^n}$. Then for odd i we define ω_i to be such that:*

$$\omega_i = |\ \{b \in \mathbb{F}_{2^n},\ \delta(b) = i\}\ |.$$

The differential spectrum of F is then the following:

$$\{\omega_0, \omega_2, ..., \omega_{u(F)}\}.$$

[1] The case $a = 0$ is of no importance anyway since $\mathbb{D}_0F$ is always equal to zero.

As we shall see later, the cases where $b = 0$ or $b = 1$ often require a special treatment. Therefore, it is easier to study what we call the restricted differential spectrum.

Definition 21 (Restricted differential spectrum)**.** *Let $F(x) = x^d$ be a power function over $\mathbb{F}_{2^n}$. Then for odd i we define Ω_i to be such that:*

$$\Omega_i = |\ \{b \in \mathbb{F}_{2^n} \backslash \mathbb{F}_2,\ \delta(b) = i\}\ |.$$

The restricted differential spectrum of F is then the following:

$$\{\Omega_0, \Omega_2, ..., \Omega_{U(F)}\}.$$

The sum of the elements of the spectrum of a monomial yields interesting values.

Lemma 2. *The following two equalities hold if $\{\omega_0, ..., \omega_{u(F)}\}$ is the differential spectrum of a function F*

$$\sum_{i=0}^{\delta(F)} \omega_i = 2^n \quad , \quad \sum_{i=0}^{\delta(F)} i \times \omega_i = 2^n.$$

The differential spectrum is also not modified if we replace an exponent by another from the same cyclotomic class or by its inverse modulo $2^n - 1$.

Lemma 3 (Lemma 1 in [BCC10a])**.** *Let $F_e = x^e$ and $F_d = x^d$ be two power functions. F_d and F_e have the same differential spectrum if one of the following condition holds:*

- *There exists k such that $e = 2^k d \mod (2^n - 1)$ (i.e. e and d are in the same cyclotomic class).*
- *$gcd(2^n - 1,\ d) = 1$ and $e = d^{-1} \mod (2^n - 1)$.*

2.3 On the Cryptographic Importance of the Differential Spectrum

The differential uniformity gives a first measure of the resilience of the cipher against differential attack. Indeed, the higher it is, the less uniformly distributed the values of $S(x) + S(x + a)$ will be.

However, for a given differential uniformity, different differential spectra will imply different theoretical propagation ratio. Consider the "toy" cipher[2] in Figure 2.1. It is what is called a *Generalised Feistel Network*, a structure presented by Nyberg in [Nyb96]: the input data is divided in four blocks of identical size and these then go through the network. Our toy cipher has two rounds. Note that an addition

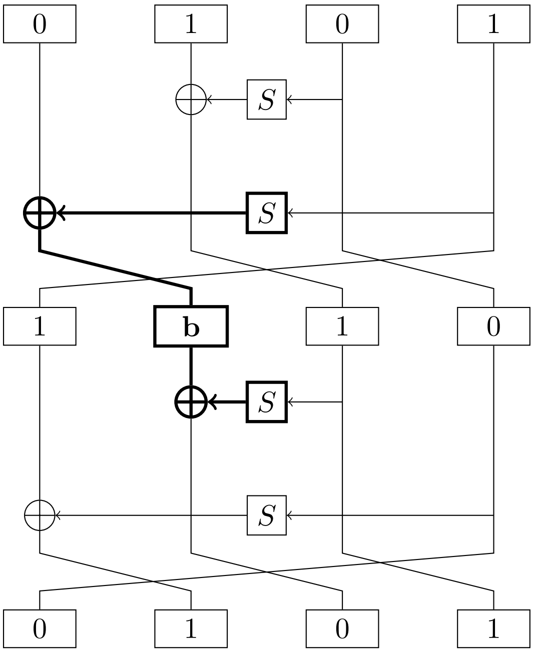

Figure 2.1. A very simple generalised Feistel network and how a differential propagates through it. Places where the difference is b are represented thicker. Illustrates the point of the study of the differential spectrum.

with the round key is part of the cipher but, since we represent the evolution of a differential, it has no effect so we do not show it.

The probability to have this output difference knowing the input difference is equal to the sum over all possible values of b of the probability that a difference of 1 is mapped by S to a difference b, and so twice (once because $0 \oplus S(1) = b$ and once because we want $S(1) \oplus b = 0$, i.e. $S(1) = b$ again). In other words, the propagation ratio of $(0, 1, 0, 1) \to (0, 1, 0, 1)$ is R with

$$R = \sum_{b \in \mathbb{F}_{2^n}} \mathbf{Pr}[S : 1 \to b] \cdot \mathbf{Pr}[S : 1 \to b],$$

where the standard hypothesis of round independence is used.

Note that having a difference of 1 mapped to a difference b by S is equivalent to having $S(x+1) + S(x) = b$ for a plaintext x. Thus, if S is a monomial, we can use its differential spectrum to compute this probability: b is such that $\delta(b)$ values x exist such that $S(x+1) + S(x) = b$, so $\mathbf{Pr}(S : 1 \to b)$ is $\delta(b)/2^n$. There is $\omega_{\delta(b)}$ such x's for every b where $\{\omega_0, ...\omega_{u(S)}\}$ is the differential spectrum of S. Thus, the

[2] It was also used by Blondeau in [Blo11] to illustrate the interest of the differential spectrum. However, our study also takes differentially 6-uniform functions into account.

propagation ratio R becomes

$$\begin{aligned} R &= \sum_{k=0}^{u(S)} \omega_k \times \left(\frac{k}{2^n}\right)^2 \\ &= \frac{1}{2^{2n}} \sum_{k=0}^{u(S)} \omega_k k^2. \end{aligned}$$

To illustrate the interest of the differential spectrum, we computed for several monomials $F_d : x \mapsto x^d$ differentially 4- or 6-uniform and having different spectra in the field $\mathbb{F}_{2^{10}}$ the value $\ell_d = \sum_{k=0}^{u(S)} k^2 \omega_k$. The monomials, their spectra and the corresponding values of ℓ_d are given Table 2.1. Recall that the more evenly distributed the propagation ratios are, the better the cipher. Therefore, is is best to have a low value for ℓ_d.

$u(F_d)$	d	Differential Spectrum of F_d	ℓ_d
4	511	$\omega_0 = 513,\ \omega_2 = 510,\ \omega_4 = 1$	2056
	84	$\omega_0 = 572,\ \omega_2 = 392,\ \omega_4 = 60$	2528
	103	$\omega_0 = 588,\ \omega_2 = 360,\ \omega_4 = 76$	2656
	87	$\omega_0 = 632,\ \omega_2 = 272,\ \omega_4 = 120$	3008
	160	$\omega_0 = 768,\ \omega_2 = 0,\ \omega_4 = 256$	4096
6	147	$\omega_0 = 597,\ \omega_2 = 347,\ \omega_4 = 75,\ \omega_6 = 5$	2768
	122	$\omega_0 = 608,\ \omega_2 = 330,\ \omega_4 = 76,\ \omega_6 = 10$	2896
	152	$\omega_0 = 628,\ \omega_2 = 300,\ \omega_4 = 76,\ \omega_6 = 20$	3136
	118	$\omega_0 = 623,\ \omega_2 = 315,\ \omega_4 = 61,\ \omega_6 = 25$	3136
	7	$\boldsymbol{\omega_0 = 583,\ \omega_2 = 405,\ \omega_4 = 1,\ \omega_6 = 35}$	2896
	54	$\omega_0 = 667,\ \omega_2 = 242,\ \omega_4 = 75,\ \omega_6 = 40$	3608
	167	$\omega_0 = 688,\ \omega_2 = 210,\ \omega_4 = 76,\ \omega_6 = 50$	3856

Table 2.1. The differential properties of several monomials in $\mathbb{F}_{2^{10}}$.

As we can see, the value of ℓ_d is not entirely determined by the differential uniformity of F_d. Indeed, it varies depending on the value of the whole spectrum. Furthermore, the value of ℓ_d (and thus the propagates ratio R) increases as the coefficient $\omega_{u(F_d)}$ increases except for F_7. In this case, $\omega_6 = 35$ so we would expect p_7 to be greater than $p_{118} = 3136$ as for F_{118}, $\omega_6 = 25$. However, since $\omega_4 = 1$ is very low for F_7, the influence of ω_6 is "compensated". We identify in Chapter 3 several functions having essentially the same spectrum as $x \mapsto x^7$.

We also notice that the lowest value of ℓ_d corresponds to the exponent 511, i.e. $2^{10-1} - 1$ which is in the cyclotomic class of the inverse function. As a matter of fact, the inverse function is widely used today, most notably by the current encryption standard AES [DR98].

2.4 Known Differential Spectra

Differential uniformity has been the topic of intensive research since its introduction in [Nyb94]. The most interesting functions from a cryptographic point of view are those with the lowest differential uniformity (see Section 2.3). It is thus natural that the first functions studied were the differentially 2-uniform (APN). Differentially 4-uniformity was studied next as well as the differentially 6-uniform functions, which are the topic of this Thesis.

2.4.1 APN and Differentially 4-Uniform Functions

APN-functions were the first studied and while their differential spectrum was not explicitly extracted, it is actually always the same. Indeed, the equations a spectrum must satisfy impose that

$$\omega_0 = 2^{n-1},\ \omega_2 = 2^{n-1}.$$

Nyberg proved in [Nyb94], the paper where the notion of differential uniformity is introduced, that the inverse function was differentially 2-uniform in $\mathbb{F}_{2^n}$ when n is odd. Other results then followed; they are summarized in Table 2.2 and 2.3[3]. Recall that exponents in the same cyclotomic class yield the same differential spectrum (and, in particular, the same differential uniformity). Thus, the exponent $2^{n-1}-1$ is the same as the inverse function (note that $2 \times (2^{n-1}-1) \equiv -1 \mod (2^n-1)$).

name	exponent	condition(s)	reference
Quadratic	2^t+1	$\gcd(t,n)=1$, $t \leq m$	[Nyb94]
Kasami	$2^{2t}-2^t+1$	$\gcd(t,n)=1$, $2 \leq t \leq m$	[Kas71]
Welsh	2^m+3	-	[Dob99b]
Niho	$2^m+2^{m/2}-1$ $2^m+2^{(3m+1)/2}-1$	m even, m odd	[Dob99a]
Inverse	$2^{n-1}-1$	-	[Nyb94]
Dobbertin	$2^{4g}+2^{3g}+2^{2g}+2^g-1$	$n=5g$	[Dob00]

Table 2.2. Known APN power functions in $\mathbb{F}_{2^n}$ with $n=2m+1$.

APN functions provide the best resilience against differential cryptanalysis. In fact, they correspond to the optimal case. What is the point in studying other classes of functions with higher differential uniformity then? Differential cryptanalysis is not the only attack against which a cipher has to be secure and the properties needed to achieve this are different — for instance, non-linearity is a crucial factor to prevent linear attacks. Furthermore, there cannot be any bijective APN monomial in a field

[3] These tables were first presented in [Can06]

name	exponent	condition(s)	reference
Quadratic	$2^t + 1$	$\gcd(t, n) = 1$, $t \leq m$	[Nyb94]
Kasami	$2^{2t} - 2^t + 1$	$\gcd(t, n) = 1$, $2 \leq t \leq m$	[Kas71]
Dobbertin	$2^{4g} + 2^{3g} + 2^{2g} + 2^g - 1$	$n = 5g$	[Dob00]

Table 2.3. Known APN power functions in $\mathbb{F}_{2^n}$ with $n = 2m$.

$\mathbb{F}_{2^n}$ if n is even [BCCLC06]. Furthermore, while an APN non-monomial polynomial was found recently in $\mathbb{F}_{2^6}$ [BDMW10], it is the only APN function for even n known today (up to equivalence). When n is even, differential 4-uniformity is the best a power permutation can achieve.

Differentially 4-uniform monomials have also been extensively studied. It has been conjectured in [Blo11] that all the differentially 4-uniform monomials are, up to equivalence, given in Table 2.4. If this conjecture is true, all differentially 4-uniform are known. While differential 4-uniformity is the best possible for a monomial for even n, differential 6-uniformity can be sufficient in the case of large S-boxes.

name	exponent condition	ω_0	ω_2	ω_4
Quadratic	$2^t + 1$ $\gcd(t, n) = 2$	$2^n - 2^{n-2}$	0	2^{n-2}
Kasami	$2^{2t} - 2^t + 1$ $\gcd(t, n) = 2$	$2^n - 2^{n-2}$	0	2^{n-2}
Inverse	$2^{n-1} - 1$ n even	$2^{n-1} + 1$	$2^{n-1} - 2$	1
Bracken, Leander	$2^{2k} + 2^k + 1$ $n = 4k$	$5 \cdot 2^{4k-3} - 2^{3k-3}$	$2^{3k-2}(2^k + 1)$	$2^{3k-3}(2^k - 1)$

Table 2.4. Known differentially 4-uniform power functions in $\mathbb{F}_{2^n}$ and their spectra.

2.4.2 Previously Known Differentially 6-Uniform Monomials

Differentially 6-uniform monomials have been studied in [BCC11] and experiments lead to the conjecture that apart from a finite set of monomials in fields of small size, all differentially 6-uniform monomials have exponent $2^t - 1$ for some t. We shall denote these monomials $G_t(x) = x^{2^t-1}$. It was also proved that $x \mapsto x^{2^t-1}$ with $t = (n+3)/2$ for n odd is differentially 6-uniform and that for $t = (n-1)/2$, $x \mapsto x^{2^t-1}$ is locally differentially 6-uniform.

The complete differential spectrum when $t = 3$ was extracted in [BCC11]. It corresponds to the monomial $G_3 : x \mapsto x^7$. The expression found depends on the

Kloosterman sum; its numerical value for $n = 10$ is given in Table 2.1 (bold line).

Definition 22. *We denote by $K(1)$ the so-called Kloosterman sum defined as*

$$K(1) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathbf{Tr}(x+x^{-1})}, \tag{2.2}$$

where $(-1)^{\mathbf{Tr}(x+x^{-1})}$ is set to 1 when $x = 0$. Carlitz showed in [Car69] that $K(1)$ is also given by the following expression:

$$K(1) = 1 + \frac{(-1)^{n-1}}{2^{n-1}} \sum_{i=0}^{\lfloor n/2 \rfloor} (-1)^i \binom{n}{2i} 7^i. \tag{2.3}$$

Theorem 2 (Theorem 5 of [BCC11])**.** *$G_3 : x \mapsto x^7$ is differentially 6-uniform and its differential spectrum $\{\omega_0, \omega_2, \omega_4, \omega_6\}$ is as follows.*

- *If n is odd, then:*

$$\begin{aligned}
\omega_0 &= 2^{n-2} + \frac{2^n + 1}{3} - \frac{K(1)}{4}, \\
\omega_2 &= \frac{3 \cdot 2^{n-2} - 1}{2} + 3 \cdot \frac{K(1)}{8}, \\
\omega_4 &= 0, \\
\omega_6 &= \frac{2^{n-2} + 1}{6} - \frac{K(1)}{8}.
\end{aligned}$$

- *If n is even, then:*

$$\begin{aligned}
\omega_0 &= 2^{n-2} + \frac{2^n - 1}{3} + \frac{K(1)}{4}, \\
\omega_2 &= 3 \cdot \left(2^{n-3} - \frac{K(1)}{8}\right), \\
\omega_4 &= 1, \\
\omega_6 &= \frac{2^{n-2} - 4}{6} + \frac{K(1)}{8}.
\end{aligned}$$

In the same paper, the following theorem was also proved. It gives the value of the coefficients $\delta(0)$ and $\delta(1)$ for $G_t : x \mapsto x^{2^t - 1}$ for any t.

Theorem 3 (Theorem 1 from [BCC11] (end))**.** *Let G_t be defined by $G_t(x) = x^{2^t-1}$. Then the corresponding values of $\delta(0)$ and $\delta(1)$ are given by*

$$\begin{aligned}
\delta(0) &= 2^{\gcd(t,n)} - 2 \\
\delta(1) &= 2^{\gcd(t-1,n)}.
\end{aligned}$$

Note in particular that G_t is a bijection if and only if $\delta(0) = 0$.

In the same paper, a relation between G_t and G_s where $s = n - t + 1$ is also given.

Theorem 4 (Corollary 2 from [BCC11])**.** *Let t be in $[1, n-1]$ and $s = n-t+1$ and let $\delta^w(b)$ be the number of solutions of $G_w(x)+G_w(x+1) = b$. Then G_s and G_t have the same restricted differential spectrum and the values $\delta^t(0), \delta^t(1)$ and $\delta^s(0), \delta^s(1)$ are related as follows:*

$$\begin{array}{rcl}\delta^s(0) & = & \delta^t(1) - 2 \\ \delta^s(1) & = & \delta^t(0) + 2.\end{array}$$

G_s is the called the symmetric *of G_t.*

An important implication of this theorem is that computing the differential spectrum of a monomial G_t always gives, as an immediate corollary, the one of G_s where $s = n - t + 1$. In particular, Blondeau *et al.* used it to derive the differential spectrum of $G_s : x \mapsto x^{2^{n-2}-1}$ ($t = 3$ implies $s = n - 2$). Table 2.5 shows the restricted differential spectrum of G_t for all t for $n = 10$. As we can see, the line between $t = 5$ and $t = 6$ is an axis of symmetry for the whole table.

t	Restricted spectrum of G_t
2	$\omega_0 = 512,\ \omega_2 = 510$
3	$\omega_0 = 582,\ \omega_2 = 405,\ \omega_6 = 35$
4	$\omega_0 = 582,\ \omega_2 = 405,\ \omega_6 = 35$
5	$\omega_0 = 527,\ \omega_2 = 495$
6	$\omega_0 = 527,\ \omega_2 = 495$
7	$\omega_0 = 582,\ \omega_2 = 405,\ \omega_6 = 35$
8	$\omega_0 = 582,\ \omega_2 = 405,\ \omega_6 = 35$
9	$\omega_0 = 512,\ \omega_2 = 510$

Table 2.5. The restricted spectrum of G_t in $\mathbb{F}_{2^{10}}$ for every value of t.

Other families of locally differentially 6-uniform monomials are now known. First conjectured by Blondeau in [Blo11], these differential spectra are given in Section 2.5. The proof of Theorem 2 in [BCC11] is long and complicated, it is derived from many lemmas and propositions. Nevertheless, the proofs presented in the next chapter present a structure similar to this one so we give an outline of this proof.

Proof sketch of Theorem 2. The proof made by Blondeau *et al.* consists in the following steps.

1. First step: the values of $\delta(0)$ and $\delta(1)$ are computed separately using Theorem 3.

2. Second step: the problem is modified so as to make it possible to count its solutions. To achieve this, it is shown that the equation $(x+1)^{2^t-1}+x^{2^t-1}=b$ has twice as many solutions as the system

$$\begin{cases} \sum_{i=1}^{t-1} y^{2^i} = \beta y \\ \mathbf{Tr}(y) = 0 \end{cases} \tag{2.4}$$

with $\beta = b+1$ for any t.

3. Third step (the longest): the number of β such that the system has no solutions is counted. First, t is fixed to 3 so the polynomial $Q_\beta(y) = y^{-1}\big(\sum_{i=1}^{3-1} y^{2^i} + \beta y\big) = y^3+y+\beta$ is studied. Note that a polynomial of degree 3 has either 0, 1 or 3 solutions so we study these cases separately.

   - If Q_β has three roots (y_1, y_2, y_3), then exactly one or three satisfy $\mathbf{Tr}(i) = 0$ because $y_1+y_2+y_3 = 0$ (recall that Q_β is a linear polynomial divided by x).
   - A result from the appendices of [KHCJ96] gives the number M_0 of values of β such that Q_β has no roots.
   - A result from [BRS67] gives a condition necessary and sufficient for Q_β to have a unique root: it must hold that $\mathbf{Tr}(\beta^{-1}) \neq \mathbf{Tr}(1)$.

   The number of β such that System 2.4 has no solutions is therefore $M_0 + |\mathcal{B}_1|$ where $\mathcal{B}_1$ is the set of the β such that Q_β has a unique solution y which does not satisfy the trace condition $\mathbf{Tr}(y) = 0$.

   The aim then is to compute the size of $\mathcal{B}_1$. Q_β has only one root if and only if $\mathbf{Tr}(\beta^{-1}) \neq \mathbf{Tr}(1)$ and $Q_\beta(y) = 0$ if and only if $\beta = y + y^3$. Therefore, $\mathcal{B}_1$ can be written as follows:

$$\mathcal{B}_1 = \left\{ (y+y^3) \in \mathbb{F}_{2^n}^*, \mathbf{Tr}\Big(\frac{1}{y+y^3}\Big) \neq \mathbf{Tr}(1), \mathbf{Tr}(y) = 1 \right\}.$$

   Computations then show that the size of $\mathcal{B}_1$ is equal to this:

$$|\mathcal{B}_1| = \{y \in \mathbb{F}_{2^n}^*,\ \mathbf{Tr}(y^{-1}) \neq \mathbf{Tr}(1),\ \mathbf{Tr}(y) = 1\}$$

   This size turns out to be closely related to the Kloosterman sum (see Definition 22).

$$\begin{aligned} K(1) - 2 &= \sum_{y \in \mathbb{F}_{2^n} \backslash \mathbb{F}_2} (-1)^{\mathbf{Tr}(y+y^{-1})} \\ &= |\{y \in \mathbb{F}_{2^n} \backslash \mathbb{F}_2, \mathbf{Tr}(y+y^{-1}) = 0\}| - |\{y \in \mathbb{F}_{2^n} \backslash \mathbb{F}_2, \mathbf{Tr}(y+y^{-1}) = 1\}| \\ &= 2^n - 2 - 4|\{y \in \mathbb{F}_{2^n} \backslash \mathbb{F}_2,\ \mathbf{Tr}(y^{-1}) = 0,\ \mathbf{Tr}(y) = 1\}|. \end{aligned}$$

   Depending on the parity of n, the size of $\{y \in \mathbb{F}_{2^n} \backslash \mathbb{F}_2,\ \mathbf{Tr}(y^{-1}) = 0,\ \mathbf{Tr}(y) = 1\}$ is either equal to $|\mathcal{B}_1|$ or to $2^{n-1} - |\mathcal{B}_1|$. This leads to the conclusion that System (2.4) has no solutions for $M_0 + 2^{n-2} + (-1)^n K(1)/4$ values of β. Furthermore, recall that Ω_0 is equal to the number of β such that System (2.4) has no solutions. Therefore:

$$\Omega_0 = \frac{2^n - (-1)^n}{3} + 2^{n-2} + (-1)^n \frac{K(1)}{4}.$$

4. Fourth step: using the values of $\delta(0)$ and $\delta(1)$ extracted during the first step and the equations given by Lemma 2, the whole spectrum is deducted.

□

2.5 New Locally Differentially 6-Uniform Monomials

We conclude this chapter on the known differential spectra by giving the ones we extracted. The proofs of these spectra are the topic of the next chapter and of [BP13]. They were first conjectured by Blondeau in [Blo11] at the end of Chapter 8 ("*Spectre différentiel des monômes*"); here are translations of these conjectures.

Conjecture 1. *Let k be such that $n + k \equiv 0 \mod 3$. Then the function $G_t(x) = x^{2^t-1}$ with $t = (n + k)/3$ has the same restricted spectrum as $G_3(x) = x^7$.*

Conjecture 2. *The function $G_t(x) = x^{2^t-1}$ with $t = (n - 1)/2$ has the same restricted spectrum as $G_3(x) = x^7$.*

Both turned out to be correct. The values of $\delta(0)$ and $\delta(1)$, computed separately, complete the spectra. A list of all the locally differentially 6-uniform monomials G_t for some t is given in Table 2.6. They all have the same restricted spectrum.

t	condition over n	permutation	reference
3	Always	yes if $n \not\equiv 0 \mod 3$	[BCC11]
$\frac{kn+1}{3}$	$n \not\equiv 0 \mod 3$	yes	Theorem 7
$\frac{n-1}{2}$	n odd	yes	Theorem 11
$\frac{n+3}{2}$	n odd	yes if $n \not\equiv 3 \mod 6$	Theorem 12
$\frac{jn+2}{3}$	$n \not\equiv 0 \mod 3$	yes if $n \equiv \pm 1 \mod 6$	Theorem 8
$n - 2$	Always	yes if $n \equiv 1 \mod 2$	[BCC11]

Table 2.6. Values of t for which the power functions G_t is known to be locally differentially 6-uniform.

Note that we studied $t = (kn + 1)/3$ and $t = (jn + 2)/3$ instead of $t = (n + k)/3$ as stated in the conjecture. The values of t considered are actually the same in both cases, a discussion as for why we preferred the new expression over the one in the conjecture is given in Section 3.2.1.

Chapter 3

On the 2^{t-1} Exponent Family

We are interested in the differential spectrum of monomials $G_t(x) = x^{2^t-1}$ in $\mathbb{F}_{2^n}$. In this Thesis, we shall study the differential spectrum of two families of monomials: those with $t = (n-1)/2$ when n is odd and those with exponent $t = (kn+1)/3$ when $kn \equiv 2 \pmod 3$. These results will also give us the differential spectra of polynomials related to these, namely those of the monomials $G_s : x \mapsto x^{2^s-1}$ where $s = ((3-k)n+2)/3$ and $s = (n+3)/2$. The values of these spectra were conjectured by Blondeau in [Blo11]. Roughly speaking, these conjectures state that the differential spectrum of these families of monomials is essentially the same as that of x^7 (see Conjectures 1 and 2).

3.1 Outline of the Proofs of the Differential Spectra

The general structure of the proofs we found for $t = (n-1)/2$ and $t = (n+k)/3$ follows the same general flow as that found by Blondeau *et al.* for Theorem 2. We shall give a common outline for both our proofs and point out the main difference they have with that of [BCC11] but first, let us introduce a theorem crucial for this study.

In our approach, we modify the problem statement to exhibit its relation with the number of roots of the polynomial $\mathcal{L}_\beta : x \mapsto x^{2^t+1} + x + \beta$. Polynomials of the structure $x^{p^l+1} + x + \beta$ where p is the characteristic of the field have been studied by several researchers. Bluher published a paper [Blu04] giving general properties of such polynomials in any field and Helleseth and Kholosha gave more specific properties in characteristic 2 [HK08]. In particular, this last paper gives two theorems which we shall use in this work. A combined statement of these two theorems is Theorem 5.

Theorem 5. *(From [HK08]) Let t be a positive integer such that $t \leq n$ and $\gcd(t,n) = 1$. For any $a \in \mathbb{F}_{2^n}^*$, the polynomial $\mathcal{L}_a(x) = x^{2^t+1} + x + a$ has either none, one or three roots in $\mathbb{F}_{2^n}$. Further $\mathcal{L}_a$ has exactly one zero in $\mathbb{F}_{2^n}^*$, namely x_0, if and only if* $\mathbf{Tr}\left((1 + x_0^{-1})^\tau\right) = 1$.

Let $M_i = \#\{a \in \mathbb{F}_{2^n}^* \mid \mathcal{L}_a$ *has* i *roots*$\}$.

- *For* n *odd:* $M_0 = \dfrac{2^n+1}{3},\ M_1 = 2^{n-1}-1,\ M_3 = \dfrac{2^{n-1}-1}{3}$.
- *For* n *even:* $M_0 = \dfrac{2^n-1}{3},\ M_1 = 2^{n-1},\ M_3 = \dfrac{2^{n-1}-2}{3}$.

Outline of the proof of the differential spectrum of G_t. Here is a common outline for both our proofs of the differential spectra of G_t for $t = (n-1)/2$ and $t = (kn+1)/3$.

1. First step: we compute $\delta(0)$ and $\delta(1)$ are easily computed using direct formulas. Indeed, cases were $b = 0, 1$ would require a special treatment in the general approach. Thus, we compute these separately.

2. Second step: we rewrite the equation $(x+1)^d + x^d = b$ as a new system having half its number of solution using new variables v and β:

$$\begin{cases} \mathcal{L}_\beta(v) & = 0 \\ \mathbf{Tr}(v^q) & = \epsilon. \end{cases} \tag{3.1}$$

   In this system, v is the image of $x + x^2$ and β is that of b by some bijections; q is a constant, $\epsilon \in \{0, 1\}$ is also a constant and $\mathcal{L}_\beta$ is a simple polynomial:

$$\mathcal{L}_\beta(x) = x^{2^t+1} + x + \beta. \tag{3.2}$$

   In [BCC11], the polynomial $\mathcal{L}_\beta$ is replaced by $x \mapsto x^3 + x + \beta$.

3. Third step: we count the number of β such that System (3.1) has no solutions. As in the proof of Blondeau *et al.* for $t = 3$, we have the following cases to consider.

   - If $\mathcal{L}_\beta$ has three roots, we show that exactly one or three satisfy the trace condition $\mathbf{Tr}(v^q) = \epsilon$.
   - A theorem (Theorem 5) gives us the number of cases where $\mathcal{L}_\beta$ has no solutions.
   - If $\mathcal{L}_\beta$ has one root, we count how many of these do not satisfy the trace condition. This part is the most complicated and the arguments used differ greatly from those used in [BCC11]. They are also very different if $t = (n-1)/2$ or $t = (kn+1)/3$.

4. The number of cases where System (3.1) has no roots is equal to Ω_0. Thus, we have all we need at this point to compute the whole spectrum. That of the symmetric exponents $2^s - 1$ with $s = n - t + 1$ is also derived using Theorem 4.

□

3.2 The Case $t = (kn + 1)/3$

Recall Conjecture 1: monomials with exponent $2^t - 1$ with $t = (n + k)/3$ are thought to have the same restricted spectrum as G_3. This section is a proof of this conjecture. Complete expressions of the spectra of these functions and their symmetric are given at the end of this section in Theorems 7 and 8.

3.2.1 Statement of the Problem

Conjecture 1 is about exponent $t_1 = (n + k)/3$ but, instead of considering this particular value, we shall focus on $t_2 = (kn + 1)/3$. If $k = 1$, then $kn + 1 = n + k$ so the corresponding exponents are strictly identical ($t_1 = t_2$). If $k = 2$, then $s_1 = n - t_1 + 1$ turns out to be $s_1 = (2n + 1)/3 = t_2$ so, according to Theorem (4), this monomial has the same restricted differential spectrum.

Furthermore, $(kn+1)/3$ is invertible modulo n so Theorem 1 gives us the inverse τ of $2^t - 1$ modulo $2^n - 1$: $\tau = 1 + 2^t + 2^{2t}$. Another consequence of this is that G_t is always a bijection, unlike $(n + k)/3$.

Therefore, instead of proving Conjecture 1 directly, we shall prove Theorem 7 which gives the differential spectrum of G_t with $t = (kn + 1)/3$. In what follows, we let t be:

$$t = \frac{kn + 1}{3} \ , \ k \equiv 3 - n \mod 3.$$

Recall that in order to compute the differential spectrum of $x \mapsto x^{2^t-1}$, we need to know for every k the number ω_k of b such that the number $\delta(b)$ of solutions of the following equation is equal to k:

$$(x + 1)^{2^t-1} + x^{2^t-1} = b. \tag{3.3}$$

To prove this theorem, we shall use the same structure for our proof as for that of the spectrum of $x \mapsto x^7$. First, we shall compute $\delta(0)$ and $\delta(1)$ separately (Section 3.2.2). Then, we shall rewrite the equation defining the spectrum, i.e. $(x + 1)^{2^t-1} + x^{2^t} = b$, in a way which will allow us to compute the number of roots it has (Section 3.2.3). In a third step, we count the number of b's such that the system has no solutions (Section 3.2.4) and then, using this information, we extract the whole spectrum and give it in Section 3.2.5.

3.2.2 Step 1: Computing $\delta(0)$ and $\delta(1)$

From Theorem 3, we know that

$$\begin{aligned} \delta(0) &= 2^{\gcd(t,n)} - 2 \\ \delta(1) &= 2^{\gcd(t-1,n)}. \end{aligned}$$

As (t, n) are co-prime, $\delta(0) = 0$.[1] The value of $\delta(1)$ depends on the congruence of n modulo 6.

$$\begin{aligned} \delta(0) &= 0 \\ \delta(1) &= \begin{cases} 2 & \text{if } n \equiv \pm 1 \mod 6 \\ 4 & \text{if } n \equiv \pm 2 \mod 6. \end{cases} \end{aligned} \tag{3.4}$$

Now that these cases have been taken care of, we can assume that $x \neq 0$ and/or that $x \neq 1$ in what follows. Indeed, if $x = 0$ or $x = 1$ then $x^{2^t-1} + (x+1)^{2^t-1} = 1$: these cases are treated.

3.2.3 Step 2: Rewriting the Equation

It has been proved by Blondeau *et al.* (Theorem 3 of [BCC11]) that the number of solutions of Equation (3.3) which are not 0 or 1 is equal to the number of non-zero solutions of the following system:[2]

$$\begin{cases} Q(y) &= by \\ \mathbf{Tr}(y) &= 0 \end{cases} \tag{3.5}$$

where

$$Q(y) = \sum_{i=0}^{t-1} y^{2^i}.$$

Our aim now is to compute the number of non-zero b such that this system has ℓ solutions, and do so for all ℓ. To do this, we shall first modify the expression of this system using the following lemma.

Lemma 4. *We notice that the sum $\sum_{i=0}^{2} Q(y)^{2^{it}}$ can be expressed in a simple way using the trace of y:*

$$Q(y) + Q(y)^{2^t} + Q(y)^{2^{2t}} = y + k \cdot \mathbf{Tr}(y)$$

where $k = 1$ or $k = 2$ is such that $t = (kn+1)/3$ is an integer.

Proof. This lemma is a direct consequence of the following observation:

$$\begin{aligned} Q(y) + Q(y)^{2^t} + Q(y)^{2^{2t}} &= \sum_{i=0}^{t-1} y^{2^i} + \sum_{i=0}^{t-1} y^{2^{i+t}} + \sum_{i=0}^{t-1} y^{2^{i+2t}} \\ &= \sum_{i=0}^{t-1} y^{2^i} + \sum_{i=t}^{2t-1} y^{2^i} + \sum_{i=2t}^{3t-1} y^{2^i} \\ &= \sum_{i=0}^{3t-1} y^{2^i}. \end{aligned}$$

[1] Note that $\delta(0) = 0$ is equivalent to the monomial being a bijection.

[2] A new and different method to derive this system is discussed in Section 4.1.2.

As $3t = kn + 1$, this sum is equal to:

$$\begin{aligned}\sum_{i=0}^{kn} y^{2^i} &= \sum_{i=0}^{n-1} y^{2^i} + \sum_{i=n}^{kn} y^{2^i} \\ &= \mathbf{Tr}(y) + \sum_{i=n}^{kn} y^{2^i}.\end{aligned}$$

If $k = 1$, then $\sum_{i=n}^{kn} y^{2^i} = y^{2^n} = y$. Else, i.e. if $k = 2$, $\sum_{i=n}^{kn} y^{2^i} = \sum_{i=0}^{n-1} y^{2^i} + y^{2^n} = \mathbf{Tr}(y) + y$.

It therefore holds that $Q(y) + Q(y)^{2^t} + Q(y)^{2^{2t}} = k \cdot \mathbf{Tr}(y) + y$. □

A direct consequence of this lemma is that if $Q(y) = by$ and $\mathbf{Tr}(y) = 0$, then

$$Q(y) + by + \left(Q(y) + by\right)^{2^t} + \left(Q(y) + by\right)^{2^{2t}} = y + by + (by)^{2^t} + (by)^{2^{2t}}.$$

The following lemma states the converse is true.

Lemma 5. *The following two systems have exactly the same solutions and, in particular, the same number of solutions:*

$$\left\{\begin{array}{l} Q(y) = by \\ \mathbf{Tr}(y) = 0 \end{array}\right. , \left\{\begin{array}{l} y + by + (by)^{2^t} + (by)^{2^{2t}} = 0 \\ \mathbf{Tr}(y) = 0\ . \end{array}\right.$$

Proof. The fact that $Q(y) = by$ and $\mathbf{Tr}(y) = 0$ is, as stated before, a direct consequence of Lemma 4.

Let L_1 be the polynomial defined by $L_1(x) = x + x^{2^t} + x^{2^{2t}}$. If we prove that $L_1(x) = 0$ is equivalent to $x = 0$, then the lemma will immediately follow.

The expression of the polynomial L_1 can be written as follows:[3]

$$\begin{aligned}L_1(x) &= x + x^{2^t} + x^{2^{2t}} \\ &= x\left(1 + x^{2^t-1} + x^{(2^t-1)(2^t+1)}\right) \\ &= x\mathcal{L}_1(x^{2^t-1})\end{aligned}$$

Since $x \mapsto x^{2^t-1}$ is a bijection, we now need to show that $\mathcal{L}_1$ has no root; which we shall do using [HK08]. First of all, it is shown that $\mathcal{L}_1$ has either 0, 1 or 3 solutions. Proposition 5 of this paper states that $\mathcal{L}_1$ has three roots if and only if, using their notations, $C_n(1) = 0$. Proposition 4 states that it has exactly one root if and only if $Z_n(1) = 0$ and $C_n(1) \neq 0$ where $C_i(x)$ is defined for $1 \leq i \leq n-1$ by the following induction

$$\begin{aligned}C_1(x) &= 1 \\ C_2(x) &= 1 \\ C_{i+2}(x) &= C_{i+1}(x) + x^{2^{it}} C_i(x)\end{aligned} \tag{3.6}$$

[3] Recall that $\mathcal{L}_a$ was defined in Equation (3.2): $\mathcal{L}_a = x^{2^t+1} + x + a$.

and $Z_n(x)$ is a function of $C_{n-1}(x)$ and $C_{n+1}(x)$:

$$Z_n(x) = C_{n+1}(x) + xC_{n-1}^{2^{2t}}(x). \tag{3.7}$$

For $x = 1$, the expression of $C_i(1)$ can be computed easily. We have:

$$\begin{aligned}
C_1(1) &= 1\\
C_2(1) &= 1\\
C_3(1) &= 1 + 1 = 0\\
C_4(1) &= 0 + 1 = 1\\
C_5(1) &= 1 + 0 = 1\\
C_6(1) &= 1 + 1 = 0\\
C_7(1) &= 1 + 0 = 1\\
&\dots
\end{aligned}$$

$C_n(1)$ is equal to zero if and only if 3 divides n. Since we consider cases where 3 does not divide n (recall that $kn = 3t + 1$), we always have $C_n(1) = 1$. Hence, $\mathcal{L}_1$ cannot have three solutions.

Furthermore, $Z_n(1) = C_{n-1}(1) + C_{n+1}(1)$. Since 3 does not divide n, it must divide exactly one of $n-1$ and $n+1$. Thus, $Z_n(1) = 1$, which means that $\mathcal{L}_1$ cannot have one root either.

This concludes the proof. □

We can modify the system by introducing a new variable $z = by$. In this case,

$$y + by + (by)^{2^t} + (by)^{2^{2t}} = (1 + b^{-1})z + z^{2^t} + z^{2^{2t}}.$$

Note that $y+by+(by)^{2^t}+(by)^{2^{2t}} = y+z+z^{2^t}+z^{2^{2t}}$ so if $y+by+(by)^{2^t}+(by)^{2^{2t}} = 0$ and $\mathbf{Tr}(y) = 0$ then $\mathbf{Tr}(z) = 0$. Conversely, if $y + z + z^{2^t} + z^{2^{2t}} = 0$ and $\mathbf{Tr}(z) = 0$ then $\mathbf{Tr}(y) = 0$. Furthermore, if $b \mapsto 1+b^{-1}$ is a bijection of $\mathbb{F}_{2^n} \backslash \{1\}$. Consequently, the following lemma holds.

Lemma 6. *The System (3.5) has exactly the same number of solutions as*

$$\begin{cases} \beta z + z^{2^t} + z^{2^{2t}} = 0\\ \mathbf{Tr}(z) = 0 \end{cases}$$

for $b \neq 0$ and $\beta = 1 + b^{-1}$.

At last, we introduce a new variable $v = x^{2^t-1}$ using that $x \mapsto x^{2^t-1}$ is a bijection and this equality

$$\beta z + z^{2^t} + z^{2^{2t}} = z \cdot \left(\beta + z^{2^t-1} + z^{(2^t-1)(2^t+1)}\right)$$

to obtain the following theorem. Note that $z = 0$ implies $by = 0$, which means that $y = 0$ since we only consider $b \neq 0$ but we are only interested in non-zero solutions of Equation (3.5), so we can safely remove the solution $z = 0$.

Theorem 6. *The number of solutions $x \neq 0,1$ of the differential equation $(x+1)^{2^t-1} + x^{2^t-1} = b$ for $b \neq 0$ is twice that of the following system for $\beta = 1 + b^{-1}$:*

$$\begin{cases} \mathcal{L}_\beta(v) = 0 \\ \mathbf{Tr}(v^\tau) = 0. \end{cases} \tag{3.8}$$

This system has the same structure as the one presented at the end of the second step of our sketch of proof (Section 3.1, System (3.1)), namely

$$\begin{cases} \mathcal{L}_\beta(v) & = 0 \\ \mathbf{Tr}(v^q) & = \epsilon. \end{cases}$$

Indeed, setting $\epsilon = 0$ and $q = \tau$ gives System (3.8).

3.2.4 Step 3: Computing Ω_0

Theorem 6 tells us that counting the solutions of System (3.8) for all $\beta \neq 0,1$ will give us the differential spectrum of G_t. We know from Theorem 5 that $\mathcal{L}_\beta$ has either 0,1 or 3 solutions, so System (3.8) has at most 3 solutions. In other words, G_t is locally differentially 6-uniform. Furthermore, the differential spectrum satisfies Lemma 2 so all we need to know is the value of ω_0: we can compute others from it. At last, since we already know the value of $\delta(0)$ and $\delta(1)$, we just need the value of Ω_0 i.e. the number of $b \neq 0,1$ such that $(x+1)^{2^t-1} + x^{2^t-1} = b$ has no solutions. We showed it is equal to the number of β such that System (3.8) has no solutions. There are three possibilities for an element β to be such that System (3.8) has no solutions.

- If $\mathcal{L}_\beta$ has no root.
- If $\mathcal{L}_\beta$ has a unique root v_0 such that $\mathbf{Tr}(v_0^\tau) \neq 0$.
- If $\mathcal{L}_\beta$ has three roots v_1, v_2, v_3, none of which satisfies the trace condition: $\mathbf{Tr}(v_1^\tau) = \mathbf{Tr}(v_2^\tau) = \mathbf{Tr}(v_3^\tau) \neq 0$.

First of all, let us rule out the third case.

Lemma 7. *If $\mathcal{L}_\beta$ has three roots v_1, v_2, v_3, then exactly one or three of them satisfy the trace condition $\mathbf{Tr}(v_i^\tau) = 0$.*

Proof. If v_i (i in $\{1,2,3\}$) is a root of $\mathcal{L}_\beta$, then $v_i^{(2^t-1)(2^t+1)} + v_i^{2^t-1} + \beta = 0$. Thus, the v_i's are roots of a linear polynomial $L_\beta : x \mapsto x^{2^{2t}} + x^{2^t} + \beta x$ having four roots: three non-zero roots (these v_i^τ's) and zero. As it is a linear polynomial, it holds that $v_1^\tau + v_2^\tau + v_3^\tau = 0$ so $\mathbf{Tr}\big(v_1^\tau + v_2^\tau + v_3^\tau\big) = 0$. The only possibilities for this to happen are (up to permutation of the indices) the following.

- $\mathbf{Tr}(v_1^\tau) = 0$ and $\mathbf{Tr}(v_2^\tau) = \mathbf{Tr}(v_3^\tau) = 1$, so exactly one satisfies the trace condition.

- $\mathbf{Tr}(v_1^\tau) = \mathbf{Tr}(v_2^\tau) = \mathbf{Tr}(v_3^\tau) = 0$, so all three of them satisfy the trace condition.

This proves the lemma. □

As a consequence of this lemma, we can claim that the set U_0 of $\beta \neq 1$ such that System (3.8) has no solution has the following structure:

$$U_0 = \{\beta,\ \mathcal{L}_\beta \text{ has no roots}\} \cup \{\beta \neq 1,\ \mathcal{L}_\beta \text{ has a unique root } v,\ \mathbf{Tr}(v^\tau) \neq 0\}. \quad (3.9)$$

These two sets are disjoint, so the size of U_0 (which is equal to Ω_0) is the sum of the sizes of these sets.

We know the size of the first set from Theorem 5:

$$|\{\beta,\ \mathcal{L}_\beta \text{ has no roots}\}| = \frac{2^n + (-1)^{n+1}}{3}. \quad (3.10)$$

However, finding the size of the second one requires more work. Recall that Theorem 5 gives a necessary and sufficient condition for any element v to be the unique root of some polynomial $\mathcal{L}_\beta$: it must hold that

$$\mathbf{Tr}\big((1+v^{-1})^\tau\big) = 1. \quad (3.11)$$

Therefore, the size of the second set in Equation (3.9) is equal to the size of $\mathcal{V}$ where

$$\mathcal{V} \ = \ \{v \in \mathbb{F}_{2^n} \backslash \mathbb{F}_2,\ \mathbf{Tr}\big((1+v^{-1})^\tau\big) = 1,\ \mathbf{Tr}(v^\tau) = 1\}. \quad (3.12)$$

As $x \mapsto x^\tau$ is a bijection, the size of this set is the same as that of

$$\begin{aligned} \mathcal{B} \ &= \ \{v \in \mathbb{F}_{2^n} \backslash \mathbb{F}_2,\ \mathbf{Tr}(1+v^{-1}) = 1,\ \mathbf{Tr}(v) = 1\} \\ &= \ \{v \in \mathbb{F}_{2^n} \backslash \mathbb{F}_2,\ \mathbf{Tr}(v^{-1}) = \mathbf{Tr}(1) + 1,\ \mathbf{Tr}(v) = 1\}, \end{aligned}$$

which is the same as that found in [BCC11]. Note in particular the presence of $\mathbf{Tr}(1)$ in the trace condition v^{-1} must satisfy: it is reason of the alternating sign depending on the parity of n in the size of $\mathcal{V}$. For the sake of completeness, we recall how the size can be computed here.

Recall the definition of the Kloosterman sum (Definition 2.2):

$$\begin{aligned} K(1) - 2 &= \sum_{x \in \mathcal{F}} (-1)^{\mathbf{Tr}(x+x^{-1})} \\ &= |\mathbb{F}_{2^n} \backslash \mathbb{F}_2| - 2 \times |\{x \in \mathbb{F}_{2^n} \backslash \mathbb{F}_2, \mathbf{Tr}(x+x^{-1}) = 1\}| \\ &= 2^n - 2 - 2 \times |\{x \in \mathbb{F}_{2^n} \backslash \mathbb{F}_2, \mathbf{Tr}(x+x^{-1}) = 1\}| \\ &= 2^n - 2 - 4 \times |\{x \in \mathbb{F}_{2^n} \backslash \mathbb{F}_2, \mathbf{Tr}(x) = 1, \mathbf{Tr}(x^{-1}) = 0\}|. \end{aligned}$$

If n is odd, $\mathbf{Tr}(1) = 1$ so x is in $\mathcal{B}$ if and only if $\mathbf{Tr}(x) = 1$ and $\mathbf{Tr}(x^{-1}) = 0$. In the same way, if n is even then x is in $\mathcal{B}$ if and only if $\mathbf{Tr}(x) = 1$ and $\mathbf{Tr}(x^{-1}) = 1$. In the case where n is even, we have:

$$\begin{aligned} &|\{x \in \mathbb{F}_{2^n} \backslash \mathbb{F}_2, \mathbf{Tr}(x) = \mathbf{Tr}(x^{-1}) = 1\}| \\ = \ &|\{x \in \mathbb{F}_{2^n} \backslash \mathbb{F}_2, \mathbf{Tr}(x) = 1\}| - |\{x \in \mathbb{F}_{2^n} \backslash \mathbb{F}_2, \mathbf{Tr}(x) = 1, \mathbf{Tr}(x^{-1}) = 0\}| \\ = \ &2^{n-1} - |\{x \in \mathbb{F}_{2^n} \backslash \mathbb{F}_2, \mathbf{Tr}(x) = 1, \mathbf{Tr}(x^{-1}) = 0\}|. \end{aligned}$$

We deduce the following from these observations.

- If n is odd, then $K(1) = 2^n - 4 \times |\mathcal{B}|$.
- If n is even, then $K(1) = 2^n - 4 \times (2^{n-1} - |\mathcal{B}|) = 4 \times |\mathcal{B}| - 2^n$.

We therefore conclude that the size of $\mathcal{V}$ (which is equal to the size of $\mathcal{B}$) is given by:

$$|\mathcal{V}| = 2^{n-2} + (-1)^n \frac{K(1)}{4}.$$

As a consequence, the number of b such that $G_t(x+1) + G_t(x) = b$ has no solutions for $b \neq 0, 1$ is equal to Ω_0 where

$$\Omega_0 = \frac{2^n + (-1)^{n+1}}{3} + 2^{n-2} + (-1)^n \frac{K(1)}{4}.$$

This concludes the third step of the proof. All that is left to do is to deduce the whole spectrum, which is done in the next section.

3.2.5 Step 4: Extracting the Whole Differential Spectrum

Using the value of Ω_0 found in the previous section, the values of $\delta(0)$ and $\delta(1)$ found in Section 3.2.2 and the equations the spectrum must satisfy given by Lemma 2, we compute the complete spectrum of G_t. It is given in the following theorem.

Theorem 7. *Let G_t be the monomial $x \mapsto x^{2^t - 1}$ from $\mathbb{F}_{2^n}$ to itself where 3 does not divide n, $t = \frac{kn+1}{3}$ and $k = 1$ or 2 is such that t is an integer. The function G_t is a differentially 6-uniform permutation. Let $K(1)$ be as defined in Definition 22. The differential spectrum of G_t is $\{\omega_0, \omega_2, \omega_4, \omega_6\}$ and is determined as follows:*

- *If $n \equiv \pm 1 \mod 6$, then:*

$$\begin{aligned}
\omega_0 &= 2^{n-2} + \frac{2^n + 1}{3} - \frac{K(1)}{4} \\
\omega_2 &= \frac{3 \cdot 2^{n-2} - 1}{2} + 3 \cdot \frac{K(1)}{8} \\
\omega_4 &= 0 \\
\omega_6 &= \frac{2^{n-2} + 1}{6} - \frac{K(1)}{8}
\end{aligned}$$

- *If $n \equiv \pm 2 \mod 6$, then:*

$$\begin{aligned}
\omega_0 &= 2^{n-2} + \frac{2^n - 1}{3} + \frac{K(1)}{4} \\
\omega_2 &= 3 \cdot \left(2^{n-3} - \frac{K(1)}{8}\right) \\
\omega_4 &= 1 \\
\omega_6 &= \frac{2^{n-2} - 4}{6} + \frac{K(1)}{8}
\end{aligned}$$

Using Theorem 4 about symmetric functions, we also deduce the spectrum of G_s with $s = n - t + 1 = ((3-k)n+2)/3$.

Theorem 8. *Let G_s be the monomial $x \mapsto x^{2^s-1}$ from $\mathbb{F}_{2^n}$ to itself with $s = \frac{(3-k)n+2}{3}$ and $k = 1$ or 2 depending on n. The function G_s is differentially 6-uniform and is a permutation if and only if $n \equiv \pm 1 \mod 6$. Let $K(1)$ be as defined in Definition 22. The differential spectrum of G_s is $\{\omega_0, \omega_2, \omega_4, \omega_6\}$ and is determined as follows:*

- *If $n \equiv \pm 1 \mod 6$, then:*

$$\begin{aligned}
\omega_0 &= 2^{n-2} + \frac{2^n+1}{3} - \frac{K(1)}{4} \\
\omega_2 &= \frac{3 \cdot 2^{n-2} - 1}{2} + 3 \cdot \frac{K(1)}{8} \\
\omega_4 &= 0 \\
\omega_6 &= \frac{2^{n-2}+1}{6} - \frac{K(1)}{8}
\end{aligned}$$

- *If $n \equiv \pm 2 \mod 6$, then:*

$$\begin{aligned}
\omega_0 &= 2^{n-2} + \frac{2^n-4}{3} + \frac{K(1)}{4} \\
\omega_2 &= 3 \cdot \left(2^{n-3} - \frac{K(1)}{8}\right) + 2 \\
\omega_4 &= 0 \\
\omega_6 &= \frac{2^{n-2}-4}{6} + \frac{K(1)}{8}
\end{aligned}$$

Even though some of the quantities dealt with in these theorems are not integers — for instance, in the first case, $(2^{n-2}+1)/6$ is not an integer — the values of the ω_i are integers.

3.3 The Case $t = (n-1)/2$

3.3.1 Statement of the Problem

Recall Conjecture 2 which states that the restricted spectrum of G_t for $t = (n-1)/2$ and for n odd is the same as that of G_3.

This section is a proof of this conjecture, i.e. of Theorem 11. While the statement of this theorem is essentially the same as the one for $t = (kn+1)/3$ but for another exponent, its proof turns out to be extremely different. Indeed, the proof for $t = (kn+1)/3$ relied on simplification of the system using Equation (4); a method we cannot use this time.

Since $\gcd(2^t-1, 2^n-1) = 2^{\gcd(n,t)}-1$ and $\gcd(n, (n-1)/2) = 1$, G_t is a bijection: its inverse is well defined and we denote it Γ_t:

$$\Gamma_t(x) = x^{\tau},$$

where τ is as before the inverse of $2^t - 1$ modulo $2^n - 1$ and is given by the formula in Theorem 1. Here, τ has the following value:

$$\tau = -2 - 2^{t+1}.$$

Studying Γ_t gives us the differential spectrum of G_t because of Lemma 3. Therefore, we do not look at the number of solutions of $(x+1)^{2^t-1} + x^{2^t-1} = b$ but to that of $(x+1)^\tau + x^\tau = b$.

3.3.2 Step 1: Computing $\delta(0)$ and $\delta(1)$

As Γ_t is a bijection, $\delta(0) = 0$. $\delta(1)$ requires more computations but it turns out to be the same as for G_t which was extracted in [Blo11], namely

$$\delta(1) = \begin{cases} 8, & \text{if } n \equiv 0 \mod 3 \\ 2, & \text{otherwise.} \end{cases}$$

Lemma 8. *The number $\delta(1)$ of solutions of $\Gamma_t(x) + \Gamma_t(x+1) = 1$ is the same as that of $G_t(x) + G_t(x+1) = 1$, namely $2^{\gcd(t-1,n)}$.*

Proof. We know that G_t is a permutation, so $\Gamma_t(x+1) + \Gamma_t(x) = 1$ is equivalent to $G_t(\Gamma_t(x+1) + \Gamma_t(x)) = 1$. Furthermore,

$$\begin{aligned}
&((x+1)^\tau + x^\tau)^{2^t-1} = 1 \\
\Leftrightarrow\ &(x+1)^{2^t\tau} + x^{2^t\tau} = (x+1)^\tau + x^\tau \\
\Leftrightarrow\ &(x+1)^{\tau+1} + x^{\tau+1} = (x+1)^\tau + x^\tau \\
\Leftrightarrow\ &(x+1)^\tau(1 + x + 1) + x^\tau(x+1) = 0 \\
\Leftrightarrow\ &((x+1)^{\tau-1} + x^{\tau-1})x(x+1) = 0,
\end{aligned}$$

so this equations has $\delta(1) = N + 2$ solutions where N is the number of solutions $x \neq 0, 1$ of $(x+1)^{\tau-1} + x^{\tau-1} = 0$. Since 0,1 are not solutions of this equation, N is exactly the number of solutions of the following one:

$$\begin{aligned}
&(x+1)^{\tau-1} = x^{\tau-1} \\
\Leftrightarrow\ &(x+1)^{(\tau-1)(2^t-1)} = x^{(\tau-1)(2^t-1)} \\
\Leftrightarrow\ &(x+1)^{2-2^t} = x^{2-2^t} \\
\Leftrightarrow\ &(x+1)^{2^{t-1}-1} + x^{2^{t-1}-1} = 0.
\end{aligned}$$

Hence, N is equal to the $\delta(0)$ of G_{t-1}, i.e. $2^{\gcd(t-1,n)} - 2$. As a consequence, $\delta(1) = 2^{\gcd(t-1,n)}$. □

3.3.3 Step 2: Rewriting the Equation

Before else, note that $1^{2^t-1}+0^{2^{t-1}}=(1+1)^{2^t-1}+1^{2^t-1}=1$ so $x=0$ and $x=1$ are not a solution of the equation unless $b=1$. Since we shall look at the restricted spectrum in this section ($\delta(0)$ and $\delta(1)$ have been computed separately), x is never equal to 0 or 1. Thus, in the following calculations, we can safely multiply a fraction by (x^2+x).

The differential in 1 for Γ_t can be rewritten in the following way:

$$\begin{aligned}\Gamma_t(x+1)+\Gamma_t(x) &= (x+1)^{-2^{t+1}-2}+x^{-2^{t+1}-2}\\ &= \frac{1}{(x+1)^{2^{t+1}+2}}+\frac{1}{x^{2^{t+1}+2}}\\ &= \frac{x^{2^{t+1}+2}+(x+1)^{2^{t+1}+2}}{(x^2+x)^{2^{t+1}+2}}\\ &= \frac{x^{2^{t+1}+2}+(x+1)^{2^{t+1}}(x^2+1)}{(x^2+x)^{2^{t+1}+2}}\\ &= \frac{x^{2^{t+1}+2}+(x^{2^{t+1}}+1)(x^2+1)}{(x^2+x)^{2^{t+1}+2}}\\ &= \frac{x^{2^{t+1}+2}+x^{2^{t+1}+2}+x^{2^{t+1}}+x^2+1}{(x^2+x)^{2^{t+1}+2}}\\ &= \frac{x^{2^{t+1}}+x^2+1}{(x^2+x)^{2^{t+1}+2}}.\end{aligned}$$

Consequently, $\delta(b)$, the number of solutions of $\Gamma_t(x+1)+\Gamma_t(x)=b$ for b in $\mathbb{F}_{2^n}\backslash\mathbb{F}_2$, is equal to the number of solutions of:

$$\frac{x^{2^{t+1}}+x^2+1}{(x^2+x)^{2^{t+1}+2}}=b.$$

The number of solutions of the following equation is also equal to $\delta(b)$:

$$x^{2^{t+1}}+x^2+1+b(x^2+x)^{2^{t+1}+2}=0.$$

If we let c be $b^{2^{n-1}}$, we can further simplify by taking the "square root" of the equation. We obtain a new polynomial which we call P_c and whose number of roots for a given b is equal to $\delta(b^{2^{n-1}})$:

$$P_c(x)=x^{2^t}+x+1+c(x^2+x)^{2^t+1}. \tag{3.13}$$

Since $x\mapsto x^{2^{n-1}}$ is a permutation mapping 0 and 1 to themselves, finding the number of $c\neq 0,1$ such that the previous equation has k roots will also give Ω_k.

Our aim is now to find the number of roots of P_c in $\mathbb{F}_{2^n}\backslash\mathbb{F}_2$, i.e. the number of solutions of the following equation for all c in $\mathbb{F}_{2^n}\backslash\mathbb{F}_2$

$$P_c(x)=0.$$

We then go further into the modification of this problem to make it easier to solve. First, we introduce a new variable, $y = x^2 + x$. To see this, we can use the following telescopic sum:

$$\begin{aligned}\sum_{i=0}^{t-1}(x^2+x)^{2^i} &= \sum_{i=0}^{t-1} x^{2^{i+1}} + x^{2^i}\\ &= x^{2^t} + x.\end{aligned}$$

Recall that for the proofs of the spectra of both $x \mapsto x^7$ and $x \mapsto x^{2^t-1}$ for $t = (kn+1)/3$, we performed the same substitution.

Note however that this change of variable implies that $\mathbf{Tr}(y) = 0$. Indeed, it is a condition which is necessary (and sufficient) for the existence of an x such that $x^2 + x + y = 0$ (see [Che82] for instance). Note also that if $y \neq 0$ then $x = 0$ and $x = 1$ is impossible.

Hence, $\delta(b)$ for b not in $\mathbb{F}_2$ is equal to two times the number of solutions of the following system in $\mathbb{F}_{2^n}^*$:

$$\begin{cases} A_c(y) = 0\\ \mathbf{Tr}(y) = 0, \end{cases} \tag{3.14}$$

where A_c is defined by:

$$A_c(y) = cy^{2^t+1} + \sum_{i=0}^{t-1} y^{2^i} + 1.$$

Our aim is now, as explained in the sketch of proof, to rewrite this system so that the polynomial $\mathcal{L}_a(x) = x^{2^t+1} + x + a$ is used. A crucial step toward this goal is the following lemma.

Lemma 9. *Consider the following system of equations:*

$$\begin{cases} B_c(y) &= 0\\ \mathbf{Tr}(cy^{2^t+1}) &= 1, \end{cases} \tag{3.15}$$

where

$$B_c(y) = c^{2^{t+1}} y^{2^t+1} + cy + 1.$$

Then Equations (3.14) and (3.15) have exactly the same number of solutions in $\mathbb{F}_{2^n}^*$.

Proof. First of all, let us compute $\phi_c(y) = A_c(y) + A_c(y)^{2^{t+1}}$. As we shall see, $B_c(y)$

is closely related to this quantity. The value of $\phi_c(y)$ can be expressed as follows:

$$\begin{aligned}\phi_c(y) &= A_c(y) + A_c(y)^{2^{t+1}} \\ &= cy^{2^t+1} + \sum_{i=0}^{t-1} y^{2^i} + 1 + (cy^{2^t+1} + \sum_{i=0}^{t-1} y^{2^i} + 1)^{2^{t+1}} \\ &= cy^{2^t+1} + \sum_{i=0}^{t-1} y^{2^i} + c^{2^{t+1}} y^{(2^t+1)2^{t+1}} + \sum_{i=0}^{t-1} y^{2^{i+t+1}} \\ &= cy^{2^t+1} + c^{2^{t+1}} y^{1+2^{t+1}} + \sum_{i=0}^{t-1} y^{2^i} + \sum_{i=t+1}^{2t} y^{2^i} \\ &= cy^{2^t+1} + c^{2^{t+1}} y^{2^{t+1}+1} + \mathbf{Tr}(y) + y^{2^t} \\ &= y^{2^t}(c^{2^{t+1}} y^{2^t+1} + cy + 1) + \mathbf{Tr}(y) \\ &= y^{2^t} B_c(y) + \mathbf{Tr}(y).\end{aligned}$$

We shall prove that the sets of the solutions of Systems (3.14) and (3.15) are included in each other and thus equal.

- First, let y be a solution of System (3.14). Then $A_c(y) = 0$ and $\mathbf{Tr}(y) = 0$. This implies that $\phi_c(y) = 0$, and that $B_c(y) = 0$. Furthermore, $\mathbf{Tr}(A_c(y)) = 0$ and $\mathbf{Tr}(A_c(y)) = \mathbf{Tr}(cy^{2^t+1}) + t \times \mathbf{Tr}(y) + \mathbf{Tr}(1) = 0$. Thus, we do have that $\mathbf{Tr}(cy^{2^t+1}) = \mathbf{Tr}(1) = 1$ (recall that n is odd, so $\mathbf{Tr}(1) = 1$). In other words, y is also a solution of System (3.15).

- Now suppose that y is a solution of System (3.15) and let us prove that it has to be a solution of System (3.14). It holds that $B_c(y) = 0$ so $\phi_c(y) = \mathbf{Tr}(y)$ and $y^{2^t} B_c(y) = c^{2^{t+1}} y^{2^{t+1}+1} + cy^{2^t+1} + y^{2^t} = 0$. Hence, $\mathbf{Tr}(y^{2^t}) = \mathbf{Tr}(c^{2^{t+1}} y^{2^{t+1}+1}) + \mathbf{Tr}(cy^{2^t+1})$.

  Furthermore, $\mathbf{Tr}(a^{2^k}) = \mathbf{Tr}(a)$ for any a and k. Thus, $\mathbf{Tr}(y^{2^k}) = \mathbf{Tr}(y)$ and $\mathbf{Tr}(cy^{2^t+1}) = \mathbf{Tr}((cy^{2^t+1})^{2^{t+1}}) = \mathbf{Tr}(c^{2^{t+1}} y^{2^{t+1}+1})$. From these observations, we deduce that $\mathbf{Tr}(y) = 2 \times \mathbf{Tr}(cy^{2^t+1}) = 0$. The condition on the trace thus yields. Besides, this means that if y is a solution of System (3.15) then $\mathbf{Tr}(y) = 0$, so $A_c(y) + A_c(y)^{2^{t+1}} = y^{2^t} B_c(y) = 0$; which implies the following:

  $$\begin{aligned}0 &= A_c(y) + A_c(y)^{2^{t+1}} \\ &= A_c(y)(1 + A_c(y)^{2^{t+1}-1}).\end{aligned}$$

  There are two possibilities.

  - Either $A_c(y) = 0$, in which case y is a solution of System (3.14) since we already proved that $\mathbf{Tr}(y) = 0$.

- Either $A_c(y)^{2^{t+1}-1} = 1$, which implies the following[4]:

$$\begin{aligned} & A_c(y)^{2^{t+1}-1} = 1 \\ \implies & A_c(y) = 1 \\ \implies & cy^{2^t+1} + \sum_{i=0}^{t-1} y^{2^i} + 1 = 1 \\ \implies & cy^{2^t+1} + \sum_{i=0}^{t-1} y^{2^i} = 0 \\ \implies & \mathbf{Tr}(cy^{2^t+1}) + t \times \mathbf{Tr}(y) = 0. \end{aligned}$$

  Since we already proved that if y is a solution of System (3.15) then $\mathbf{Tr}(y) = 0$, we have a contradiction. Indeed, it must hold that $\mathbf{Tr}(cy^{2^t+1}) = 1$ by definition of the equation system but the above equation implies that $\mathbf{Tr}(cy^{2^t+1}) = 0$. Therefore, if y is a solution of System (3.15) then we cannot have $A_c(y) = 1$. The only possibility left is $A_c(y) = 0$.

If y is a solution of System (3.14) then it is a solution of System (3.15) and if y is a solution of System (3.15) then it is a solution of System (3.14). In other words, these two systems have exactly the same solutions and, in particular, the same number of solutions; which proves the lemma. □

Polynomial $B_c(y) = c^{2^{t+1}} y^{2^t+1} + cy + 1$ looks like $\mathcal{L}_a(x) = x^{2^t+1} + x + a$. Actually, the only difference between these polynomials is a change of variable we shall give now. But before that, we note that in our case $\gcd(2^t+1, 2^n-1) = 1$ and give the inverse of 2^t+1 modulo 2^n-1.

Lemma 10. *The inverse of* (2^t+1) *modulo* (2^n-1) *is* $2 \times (1-2^t)$. *In particular, it holds that:*

$$(2^t+1) \times 2 \times (2^t-1) = -1.$$

Proof. The proof is straight-forward, we simply check:

$$\begin{aligned} (2^t+1) \times 2 \times (-2^t+1) &\equiv -2^{2t+1} - 2^{t+1} + 2^{t+1} + 2 \mod 2^n - 1 \\ &\equiv -2^n + 2 \mod 2^n - 1 \\ &\equiv 1 \mod 2^n - 1. \end{aligned}$$

This proves the lemma. □

[4] $x \mapsto x^{2^{t+1}-1}$ is a permutation since $\gcd(2^{t+1}-1, 2^n-1) = 2^{\gcd(n,t+1)} - 1$ and $\gcd(n, t+1) = \gcd(n, \frac{n+1}{2}) = \gcd(\frac{n+1}{2}, \frac{n-1}{2}) = 1$.

Let $v = c^{2-2^{t+1}}y$, i.e. $y = vc^{2^{t+1}-2}$. Then $B_c(y)$ can be rewritten as follows:

$$\begin{aligned}
B_c(y) &= c^{2^{t+1}} \cdot (vc^{2^{t+1}-2})^{2^t+1} + c \cdot vc^{2^{t+1}-2} + 1 \\
&= v^{2^t+1}c^{(2^{t+1}-2)(2^t+1)+2^{t+1}} + vc^{2^{t+1}-1} + 1 \\
&= v^{2^t+1}c^{-1+2^{t+1}+2^{t+1}} + vc^{2^{t+1}-1} + 1 \\
&= c^{2^{t+1}-1}(v^{2^t+1} + v + c^{1-2^{t+1}}) \\
&= \beta^{-1}\mathcal{L}_\beta(v)
\end{aligned}$$

where $\beta = c^{1-2^{t+1}}$. Note that $c \mapsto c^{1-2^{t+1}}$ is a bijection because $\gcd(2^{t+1}-1, 2^n - 1) = 2^{\gcd((n+1)/2,n)} - 1 = 1$. Therefore, $B_c(y) = 0$ if and only if $\mathcal{L}_\beta(v) = 0$. Besides, cy^{2^t+1} (whose trace corresponds to the trace condition) becomes

$$\begin{aligned}
cy^{2^t+1} &= c \cdot (vc^{2^{t+1}-1})^{2^t+1} \\
&= c \cdot v^{2^t+1}c^{-1} \\
&= v^{2^t+1}.
\end{aligned}$$

As a consequence of this change of variable, the following theorem holds.

Theorem 9. *Consider the following system of equations:*

$$\begin{cases} \mathcal{L}_\beta(v) &= 0 \\ \mathbf{Tr}(v^{2^t+1}) &= 1, \end{cases} \tag{3.16}$$

where

$$\mathcal{L}_\beta(v) = v^{2^t+1} + v + \beta$$

Then Equations (3.15) and (3.16) have exactly the same number of solutions in $\mathbb{F}_{2^n}^*$.

Remark 1. *The trace condition* $\mathbf{Tr}(v^{2^t+1}) = 1$ *is equivalent in this context to* $\mathbf{Tr}(v) = 1 + \mathbf{Tr}(\beta)$ *as* $\mathcal{L}_\beta(v) = 0$ *imposes that* $\mathbf{Tr}(v) = \mathbf{Tr}(\beta) + \mathbf{Tr}(v^{2^t+1})$.

This concludes the second step of the proof. If we look at the general structure of the system we described in our proof sketch (Section 3.1) which we recall here

$$\begin{cases} \mathcal{L}_\beta(v) &= 0 \\ \mathbf{Tr}(v^q) &= \epsilon, \end{cases}$$

we find that System (3.16) is as expected, with $q = 2^t + 1$ and $\epsilon = 1$.

3.3.4 Step 3 (Beginning): Counting a First Set of Non-Solutions

The system we obtained in the previous section uses again the polynomial $\mathcal{L}_\beta$. We already know from [BCC10b] (Theorem 4) that Γ_t is locally differentially 6-uniform, so our general approach will be the same as before: compute the number of $b \neq 0, 1$

such that where System (3.16) has no solution (Ω_0) and deduce the whole spectrum from it. There are three possibilities for an element β to be such that System (3.16) has no solutions.

1. Either $\mathcal{L}_\beta$ has no root.

2. Or $\mathcal{L}_\beta$ has a unique root v_0 such that $\mathbf{Tr}(v_0^\tau) \neq 0$.

3. Or $\mathcal{L}_\beta$ has three roots v_1, v_2, v_3, none of which satisfies the trace condition: $\mathbf{Tr}(v_1^{2^t+1}) = \mathbf{Tr}(v_2^{2^t+1}) = \mathbf{Tr}(v_3^{2^t+1}) \neq 1$ or, equivalently, $\mathbf{Tr}(v_1) = \mathbf{Tr}(v_2) = \mathbf{Tr}(v_3) \neq 1 + \mathbf{Tr}(\beta)$.

From Theorem 5, we know that the number of β such that $\mathcal{L}_\beta$ has no roots is equal to $(2^n+1)/3$ (n is odd). However, unlike in the previous case, we do not have $\mathbf{Tr}(v^\tau) = 0$ as a trace condition; we have $\mathbf{Tr}(v^{-\tau}) = 1$ instead since $-\tau = 2 + 2^{t+1} = 2 \cdot (2^t + 1)$. The arguments we use to compute the number of elements corresponding to cases 2 and 3 in the previous enumeration are thus different. We shall prove that no β fits in the third category and then compute the number of β in the second one.

Lemma 11. *If $\mathcal{L}_\beta$ has three roots v_1, v_2 and v_3, then exactly one or three of these roots satisfy the trace condition $\mathbf{Tr}(v_i) = 1 + \mathbf{Tr}(\beta)$ (which is equivalent to $\mathbf{Tr}(v_i^{2^t+1}) = 1$).*

Proof. Let β be such that it has three roots v_1, v_2 and v_3. First, we shall prove that $v_1^{-1} + v_2^{-1} + v_3^{-1} = 1$ and then, using this fact, that $\mathbf{Tr}(v_1 + v_2 + v_3) = 1 + \mathbf{Tr}(\beta)$ which will imply the lemma.

First, let us prove that $v_1^{-1} + v_2^{-1} + v_3^{-1} = 1$. If the v_i's are roots of $\mathcal{L}_\beta$, then $L_\beta : x \mapsto x^{2^{2t}} + x^{2^t} + \beta x$ has four roots: $v_1^\tau, v_2^\tau, v_3^\tau$ (none of which is equal to zero) and 0. We deduce the following:

$$\begin{aligned} 0 &= v_1^\tau + v_2^\tau + v_3^\tau \\ &= v_1^{-2(2^t+1)} + v_2^{-2(2^t+1)} + v_3^{-2(2^t+1)} \\ &= \left(v_1^{-(2^t+1)} + v_2^{-(2^t+1)} + v_3^{-(2^t+1)}\right)^2. \end{aligned} \tag{3.17}$$

Now recall that $v_i^{2^t+1} + v_i + \beta = 0$ and that $v_i \neq 0$. We can divide the left hand-side by $v_i^{2^t+1}$ to obtain

$$1 + v_i^{-2^t} + \beta v_i^{-(2^t+1)} = 0$$

and then sum these equations over i, which yields

$$\begin{aligned} 0 &= \left(1 + v_1^{-2^t} + \beta v_1^{-(2^t+1)}\right) + \left(1 + v_2^{-2^t} + \beta v_2^{-(2^t+1)}\right) + \left(1 + v_3^{-2^t} + \beta v_3^{-(2^t+1)}\right) \\ &= 1 + \left(v_1^{-1} + v_2^{-1} + v_3^{-1}\right)^{2^t} + \beta\left(v_1^{-(2^t+1)} + v_2^{-(2^t+1)} + v_3^{-(2^t+1)}\right). \end{aligned}$$

We know from Equation (3.17) that $v_1^{-(2^t+1)} + v_2^{-(2^t+1)} + v_3^{-(2^t+1)} = 0$, so

$$v_1^{-1} + v_2^{-1} + v_3^{-1} = 1.$$

Now let us deduce from this that $\mathbf{Tr}(v_1 + v_2 + v_3) = 1 + \mathbf{Tr}(\beta)$. The v_i's are such that $v_i^{2^t+1} + v_i + \beta = 0$ and are not equal to zero, so we can divide the left hand-side by v_i to obtain

$$v_i^{2^t} + 1 + \frac{\beta}{v_i} = 0$$

which, when summed over i, gives

$$\begin{aligned} 0 &= v_1^{2^t} + 1 + \frac{\beta}{v_1} + v_2^{2^t} + 1 + \frac{\beta}{v_2} + v_3^{2^t} + 1 + \frac{\beta}{v_3} \\ &= (v_1 + v_2 + v_3)^{2^t} + 1 + \beta(\frac{1}{v_1} + \frac{1}{v_2} + \frac{1}{v_3}). \end{aligned}$$

If we take the trace of this equality, we find

$$\mathbf{Tr}(v_1 + v_2 + v_3) = 1 + \mathbf{Tr}(\beta(v_1^{-1} + v_2^{-1} + v_3^{-1})).$$

As we proved that $v_1^{-1} + v_2^{-1} + v_3^{-1} = 1$, this gives

$$\mathbf{Tr}(v_1 + v_2 + v_3) = 1 + \mathbf{Tr}(\beta)$$

which means that an odd number of the v_i's satisfy the trace condition. As only 1 and 3 are odd in $[0, 3]$, we have exactly one or three v_i's satisfying the trace condition, an observation which concludes the proof. □

All that remains to do is to find the number of β that are such that $\mathcal{L}_\beta$ has a unique solution v which do not satisfy the trace condition. To achieve this, we shall find an explicit expression giving all the elements v in $\mathbb{F}_{2^n}^*$ such that v is the unique root of some $\mathcal{L}_\beta$.

3.3.5 An Explicit Expression of the Unique Roots of $x^{2^t+1} + x + \beta$

In this section, we shall give a proof of the following theorem which gives a general expression for the elements v in $\mathbb{F}_{2^n}^*$ that are the unique roots of a polynomial $\mathcal{L}_\beta : x \mapsto x^{2^t+1} + x + \beta$ for some β where $t = (n-1)/2$.

Definition 23. *We denote $\mathcal{F}_0$ the set of the elements of $\mathbb{F}_{2^n}^*$ that have a trace equal to zero:*

$$\mathcal{F}_0 = \{l \in \mathbb{F}_{2^n}^*,\ \mathbf{Tr}(l) = 0\}.$$

Theorem 10. *The set of v in $\mathbb{F}_{2^n}^*$ such that v is the unique root of a polynomial $\mathcal{L}_\beta : x \mapsto x^{2^t+1} + x + \beta$ for some β is the image by Λ' of $\mathcal{F}_0$ by*

$$\Lambda' : \left\{ \begin{array}{l} \mathbb{F}_{2^n}^* \to \mathbb{F}_{2^n} \\ l \mapsto \left(\sum_{i=1}^{t} l^{2^i - 1} \right)^{-1}. \end{array} \right.$$

Remark 2. *Proposition 4 of [HK08] gives an explicit expression for the root of $\mathcal{L}_a$ when $\mathcal{L}_a$ has a unique zero. This expression gives the unique root v as a function of a but it involves a sequence of polynomials and is too cumbersome to use in our context. Note however that our approach requires a particular value of t while the formula found by Helleseth and Kholosha always works.*

The rest of this section, dedicated to the proof of Theorem 10, is organised as follows.

1. Find that the elements v that are the roots of $\mathcal{L}_\beta$ such that $\mathcal{L}_\beta$ has *three* roots are the image of $\mathcal{F}_0$ by a function $\Lambda : l \mapsto 1/\Lambda'(l)$.

2. Explain why the images of $\mathcal{F}_0$ by Λ and by $\Lambda' : l \mapsto 1/\Lambda(l)$ are disjoint.

3. Deduce Theorem 10 using that the set of the roots of polynomials $\mathcal{L}_\beta$ such that $\mathcal{L}_\beta$ has a unique root is the complement of the set of the roots of polynomials $\mathcal{L}_\beta$ having three roots.

Lemma 12. *The set of v in $\mathbb{F}_{2^n}^*$ such that v is a root of some $\mathcal{L}_\beta$ which has three non-zero roots is the image by Λ of $\mathcal{F}_0$ where*

$$\Lambda : \begin{cases} \mathbb{F}_{2^n} \to \mathbb{F}_{2^n} \\ l \mapsto \sum_{i=1}^{t} l^{2^i - 1}. \end{cases}$$

Furthermore, if we let $\alpha, \alpha+1$, be the solutions of $x + x^2 = l$, we have that the three roots of $\mathcal{L}_\beta$ are

$$\begin{cases} v_1 &= \Lambda(l) \\ v_2 &= \Lambda(l) \cdot \alpha^{1-2^{t+1}} \\ v_3 &= \Lambda(l) \cdot (\alpha+1)^{1-2^{t+1}}. \end{cases}$$

Proof. We proceed by showing first that if x is a root of a polynomial $\mathcal{L}_\beta$ having three roots, then $x = \Lambda(l)$ for some l in $\mathcal{F}_0$. In a second part, we prove the other implication, i.e. that if $v_1 = \Lambda(l)$ for some l in $\mathcal{F}_0$ then there exists two other values v_2 and v_3 that are the roots of the same polynomial $\mathcal{L}_\beta$. Explicit expressions for v_2 and v_3 as a function of l are also provided.

- We already know that $\mathcal{L}_\beta$ has either zero, one or three roots. As a consequence, v is a root of $\mathcal{L}_\beta$ with $\mathcal{L}_\beta$ having three roots if and only if there is $\gamma \neq 0, 1$ such that $v^{2^t+1} + v = (\gamma v)^{2^t+1} + \gamma v$.

$$\begin{aligned} & v^{2^t+1} + v = (\gamma v)^{2^t+1} + \gamma v \\ \Leftrightarrow\ & v^{2^t+1}(1 + \gamma^{2^t+1}) = v(1+\gamma) \\ \Leftrightarrow\ & v^{2^t} = \frac{1+\gamma}{1+\gamma^{2^t+1}}. \end{aligned}$$

Let α be such that $\gamma = \alpha^{1-2^{t+1}}$. As $\gamma \neq 0,1$, α is also different from 0,1. Besides, this change of variable is well defined because $\gcd(2^{t+1}-1, 2^n-1) = 1$ in our case.

$$\begin{aligned}
v^{2^t} &= \frac{1+\alpha^{1-2^{t+1}}}{1+\alpha^{(2^t+1)(1-2^{t+1})}} \\
\implies v^{2^t} &= \frac{1+\alpha^{1-2^{t+1}}}{1+\alpha^{-2^t}} \\
\implies v^{2^t} &= \frac{\alpha^{2^{t+1}}+\alpha}{\alpha^{2^{t+1}}+\alpha^{2^t}} \\
\implies v &= \frac{\alpha^2+\alpha^{2^{t+1}}}{\alpha^2+\alpha} \\
\implies v &= \sum_{i=1}^{t}(\alpha+\alpha^2)^{2^i-1} = \Lambda(\alpha+\alpha^2)
\end{aligned}$$

The trace of $\alpha+\alpha^2$ is always equal to zero. Therefore, there must exist l in $\mathcal{F}_0$ such that $v = \Lambda(l)$. This concludes the first part.

- Let $v_1 = \Lambda(l)$ for some l in $\mathcal{F}_0$. We prove here that there exists two other values v_2 and v_3 such that $\mathcal{L}_\beta(v_1) = \mathcal{L}_\beta(v_2) = \mathcal{L}_\beta(v_3) = 0$.

  Since l is in $\mathcal{F}_0$, there exists α such that $l = \alpha+\alpha^2 = (\alpha+1)+(\alpha+1)^2$. The following proves that $v_1 = \Lambda(\alpha+\alpha^2)$, $v_2 = \alpha^{1-2^{t+1}}\Lambda(\alpha+\alpha^2)$ and $v_3 = (\alpha+1)^{1-2^{t+1}}\Lambda(\alpha+\alpha^2)$ are such that $v_1^{2^t+1}+v_1 = v_2^{2^t+1}+v_2 = v_3^{2^t+1}+v_3$.

$$\begin{aligned}
v_2^{2^t+1}+v_2 &= \left(\alpha^{1-2^{t+1}}\Lambda(\alpha+\alpha^2)\right)^{2^t+1} + \alpha^{1-2^{t+1}}\Lambda(\alpha+\alpha^2) \\
&= \alpha^{-2^t}\Lambda(\alpha+\alpha^2)^{2^t+1} + \alpha^{1-2^{t+1}}\Lambda(\alpha+\alpha^2) \\
&= \alpha^{-2^t}\Lambda(\alpha+\alpha^2)\left(\Lambda(\alpha+\alpha^2)^{2^t} + \alpha^{1-2^t}\right) \\
&= \alpha^{-2^t}\Lambda(\alpha+\alpha^2)\left(\Lambda(\alpha+\alpha^2) + \alpha^{2^{t+1}-1}\right)^{2^t}.
\end{aligned}$$

In the same way,

$$v_3^{2^t+1}+v_3 = (\alpha+1)^{-2^t}\Lambda(\alpha+\alpha^2)\left(\Lambda(\alpha+\alpha^2)+(\alpha+1)^{2^{t+1}-1}\right)^{2^t}.$$

Let us now look at $\Lambda(\alpha+\alpha^2)+\alpha^{2^{t+1}-1}$ using another expression of $\Lambda(\alpha+\alpha^2)$:

$$\begin{aligned}\Lambda(\alpha+\alpha^2)+\alpha^{2^{t+1}-1} &= \frac{\alpha^2+\alpha^{2^{t+1}}}{\alpha+\alpha^2}+\frac{\alpha^{2^{t+1}}}{\alpha}\\ &= \frac{\alpha^2+\alpha^{2^{t+1}}+(1+\alpha)\alpha^{2^{t+1}}}{\alpha+\alpha^2}\\ &= \alpha\frac{\alpha+\alpha^{2^{t+1}}}{\alpha+\alpha^2}\\ &= \alpha\sum_{i=0}^{t}(\alpha+\alpha^2)^{2^i-1}\\ &= \alpha(\sum_{i=1}^{t}(\alpha+\alpha^2)^{2^i-1}+1).\end{aligned}$$

Therefore, $v_2^{2^t+1}+v_2$ can be written

$$\begin{aligned}v_2^{2^t+1}+v_2 &= \alpha^{-2^t}\Lambda(\alpha+\alpha^2)(\Lambda(\alpha+\alpha^2)+\alpha^{2^{t+1}-1})^{2^t}\\ &= \alpha^{-2^t}\Lambda(\alpha+\alpha^2)\Big(\alpha(\Lambda(\alpha+\alpha^2)+1)\Big)^{2^t}\\ &= \Lambda(\alpha+\alpha^2)(\Lambda(\alpha+\alpha^2)^{2^t}+1)\\ &= v_1^{2^t+1}+v_1.\end{aligned}$$

If now compute $\Lambda(\alpha+\alpha^2)+(\alpha+1)^{2^{t+1}-1}$, we find the same kind of result:

$$\begin{aligned}\Lambda(\alpha+\alpha^2)+(\alpha+1)^{2^{t+1}-1} &= \frac{\alpha^2+\alpha^{2^{t+1}}}{\alpha+\alpha^2}+\frac{\alpha^{2^{t+1}}+1}{\alpha+1}\\ &= \frac{\alpha^2+\alpha^{2^{t+1}}+\alpha(1+\alpha^{2^{t+1}})}{\alpha+\alpha^2}\\ &= \frac{(\alpha+1)(\alpha+\alpha^{2^{t+1}})}{\alpha+\alpha^2}\\ &= (\alpha+1)\sum_{i=0}^{t}(\alpha+\alpha^2)^{2^i-1}\\ &= (\alpha+1)(\sum_{i=1}^{t}(\alpha+\alpha^2)^{2^i-1}+1),\end{aligned}$$

which implies that $v_3^{2^t+1}+v_3=\Lambda(\alpha+\alpha^2)^{2^t+1}+\Lambda(\alpha+\alpha^2)$. This concludes the proof.

□

Another way to state Lemma 12 is to say that the set of the elements v in $\mathbb{F}_{2^n}^*$ which are roots of a polynomial $\mathcal{L}_\beta$ having three roots is the image by Λ of $\mathcal{F}_0$. Let us now look at some interesting properties of Λ.

Lemma 13. *The following is true for any l of $\mathcal{F}_0$:*

$$\Lambda(l)^{2^t} = l^{1-2^t}(1+\Lambda(l)).$$

Proof. It holds that $\Lambda(l)^{2^t} = \sum_{i=1}^{t} l^{(2^i-1)2^t}$. We deduce that $\Lambda(l)^{2^t} = l^{-2^t}\sum_{i=t+1}^{2t} l^{2^i}$. Since $2t = n-1$ and $\mathbf{Tr}(l) = 0$, we have this:

$$\begin{aligned}
\Lambda(l)^{2^t} &= l^{-2^t}\sum_{i=t+1}^{2t} l^{2^i}\\
&= l^{-2^t}(\sum_{i=0}^{n-1} l^{2^i} + \sum_{i=1}^{t} l^{2^i} + l^{2^0})\\
&= l^{-2^t}(\mathbf{Tr}(l) + l + l\Lambda(l))\\
&= l^{1-2^t}(1+\Lambda(l)).
\end{aligned}$$

This proves the lemma. □

Lemma 14. *Λ is one-to-one.*

Proof. Suppose that there is l and m such that $\Lambda(l) = \Lambda(m)$.

$$\begin{aligned}
\Lambda(l) = \Lambda(m) &\implies \Lambda(l)^{2^t} = \Lambda(m)^{2^t}\\
&\implies l^{1-2^t}(1+\Lambda(l)) = m^{1-2^t}(1+\Lambda(m))\\
&\implies (\frac{l}{m})^{1-2^t} = \frac{1+\Lambda(m)}{1+\Lambda(l)}\\
&\implies (\frac{l}{m})^{1-2^t} = 1.
\end{aligned}$$

Since $x \mapsto x^{1-2^t}$ is a bijection,[5] this implies that $l = m$. □

Remark 3. *Every element x of $\mathbb{F}_{2^n}\backslash\mathbb{F}_2$ is the root of exactly one polynomial $\mathcal{L}_\beta$ (simply set $\beta = x^{2^t+1}+x$). Therefore, if we look at the number μ_k of β such that $\mathcal{L}_\beta$ has at least k roots in $\mathbb{F}_{2^n}\backslash\mathbb{F}_2$, we find that $\mu_1+3\mu_3 = 2^n-2$ and $\mu_0+\mu_1+\mu_3 = 2^n-2$. Furthermore, since Λ is an injection over $\mathcal{F}_0$, we have that $3\mu_3 = |\mathcal{F}_0| = 2^{n-1}-1$. Hence, $\mu_1 = 2^{n-1}-1$ and $\mu_0 = (2^n-2)/3$. Since $\mathcal{L}_1$ has no roots, we can deduce the values of the coefficients M_0, M_1 and M_3 for the case $t = (n-1)/2$ of Theorem 5 independently from it.*

Lemma 15. *The images of $\mathcal{F}_0$ by Λ and $\Lambda' : l \mapsto 1/\Lambda(l)$ are disjoint.*

Proof. We proceed by contradiction. Suppose m in $\mathcal{F}_0$ is such that $\Lambda(m)$ is the inverse of some $\Lambda(l)$ (where l is also in $\mathcal{F}_0$), i.e. $\Lambda(l)\Lambda(m) = 1$.

Let $\lambda(l) = l\cdot\Lambda(l) = \sum_{i=1}^{t} l^{2^i}$. Then $\Lambda(l)\cdot\Lambda(m) = 1$ can also be written as follows for l, n in $\mathcal{F}_0$.

[5] Recall that $G_t : x \mapsto x^{2^t-1}$ is a bijection.

$$\begin{aligned}
lm &= \lambda(l)\lambda(m) \\
&= \Big(\sum_{i=1}^{t} l^{2^i}\Big)\Big(\sum_{i=1}^{t} m^{2^i}\Big) \\
&= \sum_{i=1}^{t}\sum_{j=1}^{i} l^{2^{i-j}} m^{2^j}.
\end{aligned}$$

In order to have the sum of index j starting at zero, we add the value $\sum_{i=1}^{t} l^{2^i} m$ and obtain:

$$\lambda(l)\lambda(m) = \sum_{i=1}^{t}\sum_{j=0}^{i} l^{2^{i-j}} m^{2^j} + \sum_{i=1}^{t} l^{2^i} m.$$

In the same way, we add lm to the double sum to be able to start it from $i = 0$ and to that on the right to be able to start also from $i = 0$. In doing so and since $lm + lm = 0$, we have:

$$\lambda(l)\lambda(m) = \sum_{i=0}^{t}\sum_{j=0}^{i} l^{2^{i-j}} m^{2^j} + \sum_{i=0}^{t} l^{2^i} m.$$

We know that $\lambda(l)\lambda(m) = lm$, so:

$$\begin{aligned}
\sum_{i=0}^{t}\sum_{j=0}^{i} l^{2^{i-j}} m^{2^j} &= lm + \sum_{i=0}^{t} l^{2^i} m \\
&= m\lambda(l).
\end{aligned}$$

As the roles of the variables l and m are symmetric, we can derive that $l\lambda(m)$ is equal to same double sum. Therefore, $m\lambda(l) = l\lambda(m)$. Hence:

$$\begin{aligned}
& l \cdot \lambda(m) = m \cdot \lambda(l) \\
\Leftrightarrow\ & \frac{\lambda(l)}{l} = \frac{\lambda(m)}{m} \\
\Leftrightarrow\ & \Lambda(l) = \Lambda(m).
\end{aligned}$$

Thus, $\Lambda(l)$ is its own inverse. The only element of $\mathbb{F}_{2^n}$ satisfying this is 1 and $\Lambda(l)$ is actually never equal to it. Indeed, suppose $\Lambda(l) = 1$. Then:

$$\begin{aligned}
& \sum_{i=1}^{t} l^{2^i - 1} = 1 \implies \sum_{i=1}^{t} l^{2^i} = l \implies \sum_{i=0}^{t} l^{2^i} = 0 \\
\implies\ & \sum_{i=0}^{t} l^{2^i} + \Big(\sum_{i=0}^{t} l^{2^i}\Big)^{2^t} = \sum_{i=0}^{2t} l^{2^i} + l^{2^t} = 0 \\
\implies\ & l^{2^t} = \mathbf{Tr}(l) = 0.
\end{aligned}$$

This does not happen since l is in $\mathcal{F}_0$. We hence do have a contradiction, which concludes the proof. □

We now have all the lemmas needed to prove Theorem 10. Observe that every element v in $\mathbb{F}_{2^n}\backslash\mathbb{F}_2$ is the root of exactly one polynomial $\mathcal{L}_\beta(v)$ (because $\beta = v^{2^t+1} + v$ always works). Therefore, $\mathbb{F}_{2^n}\backslash\mathbb{F}_2$ is equal to the following union of sets:

$$\mathbb{F}_{2^n}\backslash\mathbb{F}_2 = S_1 \cup S_3$$

where

$$\begin{aligned} S_1 &= \{v \in \mathbb{F}_{2^n}\backslash\mathbb{F}_2, \exists\beta \in \mathbb{F}_{2^n}\backslash\mathbb{F}_2,\ \mathcal{L}_\beta(v) = 0 \text{ and } \mathcal{L}_\beta \text{ has one root}\} \\ S_3 &= \{v \in \mathbb{F}_{2^n}\backslash\mathbb{F}_2, \exists\beta \in \mathbb{F}_{2^n}\backslash\mathbb{F}_2,\ \mathcal{L}_\beta(v) = 0 \text{ and } \mathcal{L}_\beta \text{ has three roots}\}. \end{aligned}$$

As Λ is an injection of $\mathcal{F}_0$ which never maps any element to zero, $\Lambda' : l \mapsto 1/\Lambda(l)$ is also an injection. Thus, the image of $\mathcal{F}_0$ by both these functions is of size $2^{n-1} - 1 = |\mathbb{F}_{2^n}\backslash\mathbb{F}_2|/2$. Furthermore, these images are disjoint (see Lemma 15). If we let I be the image of $\mathcal{F}_0$ by Λ and I' be the image of $\mathcal{F}_0$ by Λ' then

$$\mathbb{F}_{2^n}\backslash\mathbb{F}_2 = I \cup I'$$

and the union is disjoint.

We know from Lemma 12 that $S_3 = I$, so we can conclude that $S_1 = I'$; which is precisely what we intended to prove.

3.3.6 Step 3 (End): Computing Ω_0

Now that we have an explicit expression of the elements v in $\mathbb{F}_{2^n}\backslash\mathbb{F}_2$ such that $\mathcal{L}_\beta(v) = 0$ and $\mathcal{L}_\beta$ has a unique root, we can compute the number of unique solutions which do not satisfy the trace condition $\mathbf{Tr}(v^{2^t+1}) = 1$. Recall that Theorem 10, proved in the previous section, gives an expression for such v: there is l in $\mathcal{F}_0$ such that $v = \Lambda(l)^{-1}$. Therefore, the set of the unique roots of some $\mathcal{L}_\beta$ which do not satisfy the trace condition is

$$\mathcal{B} = \{v \in \mathbb{F}_{2^n}^*,\ \exists l \in \mathbb{F}_{2^n}^*,\ \mathbf{Tr}(l) = 0,\ v = \Lambda(l)^{-1},\ \mathbf{Tr}(\Lambda(l)^{-2^t-1}) \neq 1\}$$

and its size is

$$|\mathcal{B}| = \{l \in \mathbb{F}_{2^n}^*,\ \mathbf{Tr}(l) = 0,\ \mathbf{Tr}(\Lambda(l)^{-2^t-1}) \neq 1\}.$$

Lemma 16. *The following equality is true for any l in $\mathcal{F}_0$:*

$$\mathbf{Tr}(\Lambda(l)^{-2^t-1}) = 1 + \mathbf{Tr}\Big(\frac{1}{l \cdot \Lambda(l))}\Big).$$

Proof. The proof is straight-forward in the sense that it consists only in computations. First of all, recall that from Lemma 13, we have: $\Lambda(l)^{2^t} = l^{1-2^t}(1 + \Lambda(l))$ for any l in $\mathcal{F}_0$.

As a consequence, we obtain:

$$\begin{aligned}
\Lambda(l)^{-1-2^t} &= \frac{1}{\Lambda(l)^{2^t}\Lambda(l)} \\
&= \frac{1}{l^{1-2^t}(1+\Lambda(l))\Lambda(l)} \\
&= \frac{l^{2^t-1}}{\Lambda(l)(1+\Lambda(l))} \\
&= \frac{l^{2^t-1}}{\Lambda(l)} + \frac{l^{2^t-1}}{1+\Lambda(l)}.
\end{aligned}$$

Thus, if we apply the trace to this equality, we obtain the following:

$$\begin{aligned}
\mathbf{Tr}(\Lambda(l)^{-2^t-1}) &= \mathbf{Tr}\Big(\frac{l^{2^t-1}}{\Lambda(l)} + \frac{l^{2^t-1}}{1+\Lambda(l)}\Big) \\
&= \mathbf{Tr}\Big(\frac{l^{2^t-1}}{\Lambda(l)}\Big) + \mathbf{Tr}\Big(\frac{1}{\Lambda(l)^{2^t}}\Big) \\
&= \mathbf{Tr}\Big(\frac{l^{2^t-1}+1}{\Lambda(l)}\Big).
\end{aligned}$$

We then find another expression for $l^{2^t-1}+1$:

$$\begin{aligned}
1 + l^{2^t-1} &= l^{-1}(l + l^{2^t}) \\
&= l^{-1}\sum_{i=0}^{t-1}(l+l^2)^{2^i} \\
&= l^{-1}(l\Lambda(l) + l^{2^{-1}}\Lambda(l^{2^{-1}})) \\
&= \Lambda(l) + l^{2^{-1}-1}\Lambda(l)^{2^{-1}}.
\end{aligned}$$

Using this, we rewrite our expression of $\mathbf{Tr}(\Lambda(l)^{-1-2^{t+1}})$:

$$\begin{aligned}
\mathbf{Tr}(\Lambda(l)^{-1-2^{t+1}}) &= \mathbf{Tr}\Big(\frac{\Lambda(l) + l^{2^{-1}-1}\Lambda(l)^{2^{-1}}}{\Lambda(l)}\Big) \\
&= \mathbf{Tr}(1) + \mathbf{Tr}(l^{2^{-1}-1}\Lambda(l)^{2^{-1}-1}) \\
&= 1 + \mathbf{Tr}(l^{-1}\Lambda(l)^{-1}).
\end{aligned}$$

Indeed, $\mathbf{Tr}(1) = 1$ as n is odd. This concludes the proof. □

Thanks to this lemma, we deduce a new expression of the size of the set $\mathcal{B}$:

$$|\mathcal{B}| = \{l \in \mathbb{F}_{2^n}^*,\ \mathbf{Tr}(l) = 0,\ \mathbf{Tr}((l \cdot \Lambda(l))^{-1}) \neq 0\}.$$

Note that $l \mapsto l \cdot \Lambda(l)$ is injective over $\mathcal{F}_0$. Indeed, suppose that $l \cdot \Lambda(l) = m \cdot \Lambda(m)$ for l, m in $\mathcal{F}_0$. Then:

$$\begin{aligned}
& l \cdot \Lambda(l) = m \cdot \Lambda(m) \\
\implies & l^{2^t} \Lambda(l)^{2^t} = m^{2^t} \Lambda(m)^{2^t} \\
\implies & l^{2^t} l^{1-2^t} (1 + \Lambda(l)) = m^{2^t} m^{1-2^t} (1 + \Lambda(l)) \\
\implies & l + l \cdot \Lambda(l) = m + m \cdot \Lambda(m) \\
\implies & l = m.
\end{aligned}$$

In order to compute the size of the set $\mathcal{B}$, we split our reasoning into two cases depending on the parity of t.

- **If t is odd.** In this case, $\mathbf{Tr}(l \cdot \Lambda(l)) = \mathbf{Tr}(l)$ so $\mathbf{Tr}(l) = 0 \Leftrightarrow \mathbf{Tr}(l \cdot \Lambda(l)) = 0$. Thus, we can write the following:

$$|\mathcal{B}| = |\{l \in \mathbb{F}_{2^n}^*, \mathbf{Tr}(l \cdot \Lambda(l)) = 0, \mathbf{Tr}((l \cdot \Lambda(l))^{-1}) = 1\}|.$$

As $l \mapsto l \cdot \Lambda(l)$ is a bijection over $\mathcal{F}_0$ in this case (it maps it to itself and is injective), we have

$$|\mathcal{B}| = |\{l' \in \mathbb{F}_{2^n}^*, \mathbf{Tr}(l') = 0, \mathbf{Tr}(l')^{-1}) = 1\}|.$$

- **If t is even.** If t is even, then the trace of $l \cdot \Lambda(l)$ is equal to zero for any l in $\mathbb{F}_{2^n}^*$ (recall that $\mathbf{Tr}(l \cdot \Lambda(l)) = \sum_{i=1}^{t} \mathbf{Tr}(l)$). Furthermore, $l \mapsto l \cdot \Lambda(l)$ is in this case 2-to-1 over $\mathbb{F}_{2^n}$:

$$\begin{aligned}
l \cdot \Lambda(l) = 0 \implies & \sum_{i=1}^{t} l^{2^i} = 0 \\
\implies & \sum_{i=1}^{t} l^{2^i} + \Big(\sum_{i=1}^{t} l^{2^i}\Big)^{2^t} = 0 \\
\implies & \sum_{i=1}^{2t} l^{2^i} = 0 \\
\implies & \mathbf{Tr}(l) = l.
\end{aligned}$$

The function $l \mapsto l \cdot \Lambda(l)$ is linear and both $l = 0$ and $l = 1$ are indeed such that $l \cdot \Lambda(l) = 0$. Besides, since the function is an injection of $\mathcal{F}_0$ and maps l and $l + 1$ to the same image, we have:

$$\begin{aligned}
& \{l \in \mathbb{F}_{2^n} \backslash \mathbb{F}_2, \mathbf{Tr}\big((l \cdot \Lambda(l)^{-1})\big) = 1\} \\
& = \{l \in \mathbb{F}_{2^n} \backslash \mathbb{F}_2, \mathbf{Tr}(l) = 0,\ \mathbf{Tr}\big((l \cdot \Lambda(l)^{-1})\big) = 1\} \\
& \quad \cup \{l \in \mathbb{F}_{2^n} \backslash \mathbb{F}_2, \mathbf{Tr}(l) = 1,\ \mathbf{Tr}\big((l \cdot \Lambda(l)^{-1})\big) = 1\} \\
& = \{l' \in \mathbb{F}_{2^n} \backslash \mathbb{F}_2, \mathbf{Tr}(l') = 0,\ \mathbf{Tr}(l'^{-1}) = 1\} \\
& \quad \cup \{l \in \mathbb{F}_{2^n} \backslash \mathbb{F}_2, \mathbf{Tr}(l') = 1,\ \mathbf{Tr}(l'^{-1}) = 1\}
\end{aligned}$$

where we let as before $l' = l \cdot \Lambda(l)$.

Since the size of $\mathcal{B}$ is given by the size of the intersection of

$$\{l \in \mathbb{F}_{2^n} \backslash \mathbb{F}_2, \mathbf{Tr}(l) = 0\}$$

and

$$\{l \in \mathbb{F}_{2^n} \backslash \mathbb{F}_2, \mathbf{Tr}((l \cdot \Lambda(l))^{-1}) = 0\},$$

we also have

$$|\mathcal{B}| = |\{l' \in \mathbb{F}_{2^n}^*, \mathbf{Tr}(l') = 0, \mathbf{Tr}(l')^{-1}) = 1\}|.$$

In both case, we obtain for different reasons that the size of $|\mathcal{B}|$ is that of the following set

$$|\mathcal{B}| = |\{l' \in \mathbb{F}_{2^n}^*, \mathbf{Tr}(l') = 0, \mathbf{Tr}(l')^{-1}) = 1\}|$$

which we shall compute in the same way as in [BCC11].

Recall the definition of the Kloosterman sum K(1) (Definition 22). By removing $x = 0, 1$ from the sum, we have

$$\begin{aligned} K(1) - 2 &= \sum_{x \in \mathbb{F}_{2^n} \backslash \mathbb{F}_2} (-1)^{\mathbf{Tr}(x + x^{-1})} \\ &= |\{x \in \mathbb{F}_{2^n} \backslash \mathbb{F}_2, \mathbf{Tr}(x + x^{-1}) = 0\}| - |\{x \in \mathbb{F}_{2^n} \backslash \mathbb{F}_2, \mathbf{Tr}(x + x^{-1}) = 1\}|. \end{aligned}$$

As these two sets are disjoint and their union is the whole set $\mathbb{F}_{2^n} \backslash \mathbb{F}_2$, we have

$$\begin{aligned} K(1) - 2 &= |\mathbb{F}_{2^n} \backslash \mathbb{F}_2| - 2 \times |\{x \in \mathbb{F}_{2^n} \backslash \mathbb{F}_2, \mathbf{Tr}(x + x^{-1}) = 1\}| \\ &= 2^n - 2 - 2 \times |\{x \in \mathbb{F}_{2^n} \backslash \mathbb{F}_2, \mathbf{Tr}(x + x^{-1}) = 1\}|. \end{aligned}$$

Furthermore, in $\{x \in \mathbb{F}_{2^n} \backslash \mathbb{F}_2, \mathbf{Tr}(x + x^{-1}) = 1\}$, each x appears twice (once when we look at it directly and once when we look at its inverse). Thus,

$$K(1) = 2^n - 4 \times |\{x \in \mathbb{F}_{2^n} \backslash \mathbb{F}_2, \mathbf{Tr}(x) = 0, \ \mathbf{Tr}(x^{-1}) = 1\}|,$$

which means that

$$K(1) = 2^n - 4 \times |\mathcal{B}|.$$

Therefore, the size of $\mathcal{B}$ is given by the following formula:

$$|\mathcal{B}| = 2^{n-2} - \frac{K(1)}{4}$$

which allows us to finally give an expression of the number Ω_0 of β in $\mathbb{F}_{2^n} \backslash \mathbb{F}_2$ such that System (3.16) has no solutions:

$$\Omega_0 = \frac{2^n + 1}{3} + 2^{n-2} - \frac{K(1)}{4}.$$

The rest of the spectrum can be derived using the values we found in Section 3.3.2 for $\delta(0)$ and $\delta(1)$ and the equalities in Lemma 3. We give the full spectrum in the next section.

3.3.7 Step 4: Extracting the Whole Differential Spectrum

As for $t = (kn+1)/3$, we use the value of Ω_0 found in the previous section, the values of $\delta(0)$ and $\delta(1)$ found in section 3.3.2 and the equations the spectrum must satisfy given by Lemma 2, we compute the complete spectrum of G_t. It is given in the following theorem.

Theorem 11. *Let G_t be the monomial $x \mapsto x^{2^t-1}$ from $\mathbb{F}_{2^n}$ to itself with $t = \frac{n-1}{2}$ and n odd. The function G_t is always a locally differentially 6-uniform permutation and is differentially 6- or 8-uniform depending on n. Let $K(1)$ be as defined in Definition 22. The differential spectrum of G_t is $\{\omega_0, \omega_2, \omega_4, \omega_6, \omega_8\}$ and is determined as follows:*

- *If $n \equiv \pm 1 \mod 6$, then:*

$$\begin{aligned}
\omega_0 &= 2^{n-2} + \frac{2^n+1}{3} - \frac{K(1)}{4}\\
\omega_2 &= \frac{3\cdot 2^{n-2}-1}{2} + 3\cdot\frac{K(1)}{8}\\
\omega_4 &= 0\\
\omega_6 &= \frac{2^{n-2}+1}{6} - \frac{K(1)}{8}\\
\omega_8 &= 0
\end{aligned}$$

- *If $n \equiv 3 \mod 6$, then:*

$$\begin{aligned}
\omega_0 &= 2^{n-2} + \frac{2^n+4}{3} - \frac{K(1)}{4}\\
\omega_2 &= 3\cdot\left(2^{n-3} + \frac{K(1)}{8}\right)\\
\omega_4 &= 0\\
\omega_6 &= \frac{2^{n-2}-5}{6} - \frac{K(1)}{8}\\
\omega_8 &= 1
\end{aligned}$$

Again, we use Theorem 4 to deduce the spectrum of G_s with $s = n - t + 1 = (n+3)/2$ for odd n.

Theorem 12. *Let G_s be the monomial $x \mapsto x^{2^s-1}$ from $\mathbb{F}_{2^n}$ to itself with $t = (n+3)/2$ and n odd. The function G_s is differentially 6-uniform and it is a permutation if and only if $n \equiv \pm 1 \mod 6$. Let $K(1)$ be as defined in Definition 22. The differential spectrum of G_t is $\{\omega_0, \omega_2, \omega_4, \omega_6\}$ and is determined as follows:*

- *If* $n \equiv \pm 1 \mod 6$*, then:*

$$\begin{aligned}
\omega_0 &= 2^{n-2} + \frac{2^n+1}{3} - \frac{K(1)}{4} \\
\omega_2 &= \frac{3 \cdot 2^{n-2} - 1}{2} + 3 \cdot \frac{K(1)}{8} \\
\omega_4 &= 0 \\
\omega_6 &= \frac{2^{n-2}+1}{6} - \frac{K(1)}{8}
\end{aligned}$$

- *If* $n \equiv 3 \mod 6$*, then:*

$$\begin{aligned}
\omega_0 &= 2^{n-2} + \frac{2^n+1}{3} - \frac{K(1)}{4} \\
\omega_2 &= 3 \cdot \left(2^{n-3} + \frac{K(1)}{8}\right) + 1 \\
\omega_4 &= 0 \\
\omega_6 &= \frac{2^{n-2}+1}{6} - \frac{K(1)}{8}
\end{aligned}$$

As before, the ω_i are always integers due to the properties of the Kloosterman sum.

Chapter 4

General Remarks

In this chapter, we present several observations we made while investigating the differential properties of differentially 6-uniform power functions. In particular, we discuss the connexions between differential spectrum and Dickson polynomials in Section 4.1. Then, we formulate some conjectures about the differential spectra of all differentially 6-uniform power functions in Section 4.2. A study of the resilience against attacks other than differential provided by the the monomials studied is given in Section 4.3. At last, we observe an interesting connexion between the equations used to extract the spectrum of G_t and G_{t+1} for any t in Section 4.4.

4.1 On Reversed Dickson Polynomials

4.1.1 Definitions

In this section, we emphasize some relation between the problems studied in the previous chapter and the Dickson polynomials. Dickson polynomials where introduced by Dickson in [Dic96]. Their study lead to the definition of the so-called *reversed* Dickson polynomials in [HMSY09]. Dickson polynomials are defined in $\mathbb{Z}$ and in any finite field $\mathbb{F}_{p^k}$ but, in this section, we shall give all the definitions and expressions in $\mathbb{F}_{2^n}$.

Definition 24. *The Dickson polynomial of degree n is a bi-variate polynomial $D_n(z_1, z_2)$ such that for any elements pair of elements (x_1, x_2) in $\mathbb{F}_{2^n}$, the following equality holds:*

$$x_1^n + x_2^n = D_n(x_1 + x_2, x_1 x_2).$$

An explicit expression of these polynomials is given by Waring's formula:

$$D_n(x,y) = \sum_{i=0}^{\lfloor n/2 \rfloor} \frac{n}{n-i} \binom{n-i}{i} (-y)^i x^{n-2i} \tag{4.1}$$

where the coefficients are to be taken modulo 2 since we consider variables in $\mathbb{F}_{2^n}$. They also satisfy a recurrence relation:

$$\begin{cases} D_0(x,y) & = 0, \\ D_1(x,y) & = x, \\ D_n(x,y) & = xD_{n-1}(x,y) + yD_{n-2}(x,y), \text{ for } n \geq 2. \end{cases}$$

The polynomials $x \mapsto D_n(x,a)$ for fixed values of a have been extensively studied (a reference on this topic is [LMT93]). However, it is only in 2009 that Hou *et al.* introduced the reversed Dickson polynomials which we denote RD_n:

$$RD_n(y) = D_n(1,y).$$

These also satisfy a recurrence, namely

$$\begin{cases} RD_0(y) & = 0 \\ RD_1(y) & = 1 \\ RD_m(y) & = RD_{m-1}(y) + y \cdot RD_{m-2}(y). \end{cases} \tag{4.2}$$

Reversed Dickson polynomials are "stable" within cyclotomic classes of exponents $e \equiv 2^i d \mod (2^n-1)$, which means:

$$D_e(1,x) = \left(D_d(1,x)\right)^{2^i}.$$

4.1.2 Connexions Between Reversed Dickson and Differential Spectra

As Hou *et al.* pointed out in their paper, these polynomials have a very close relation with the differential spectrum. Indeed, the differential spectrum of $F_d : x \mapsto x^d$ is defined by counting the solutions of the equation

$$(x+1)^d + x^d = b,$$

for every b in $\mathbb{F}_{2^n}$. The equation can also be written

$$\begin{aligned} b &= (x+1)^d + x^d \\ &= D_n\big((x+1)+x, x(x+1)\big) \\ &= D_n(1, x^2+x) \\ &= RD_n(x^2+x), \end{aligned}$$

for any x in $\mathbb{F}_{2^n}$. The following lemma is a direct consequence from this observation.

Lemma 17. *The number of x in $\mathbb{F}_{2^n}$ (respectively $\mathbb{F}_{2^n} \backslash \mathbb{F}_2$ if we look at the restricted spectrum) such that $(x+1)^d + x^d = b$ is equal to exactly twice the number of y in $\mathbb{F}_{2^n}$ (respectively $\mathbb{F}_{2^n}^*$) such that*

$$\begin{cases} RD_n(y) & = & b \\ \mathbf{Tr}(y) & = & 0. \end{cases}$$

In other words, for a monomial $F_d : x \mapsto x^d$, we have

$$\omega_{2k} = |\{b \in \mathbb{F}_{2^n}, RD_d(y) = b \textit{ has } k \textit{ solutions with } \mathbf{Tr}(y) = 0\}|.$$

Actually, Blondeau *et al.* proved that when the monomial's exponent is $2^t - 1$ for some t, ω_{2k} is equal to the number of b such that System (4.3) has k solutions ([BCC11], Theorem 3):[1]

$$\begin{cases} \sum_{i=0}^{t-1} y^{2^i} & = by \\ \mathbf{Tr}(y) & = 0. \end{cases} \tag{4.3}$$

Gölo<span>ğ</span>u proved in [Göl12] that the reversed Dickson polynomial of degree $2^t - 1$ has the following expression:

$$RD_{2^t-1}(y) \ = \ \sum_{i=0}^{t-1} y^{2^i-1}.$$

So if we divide the first equation of System (4.3) by y, we see that the lemma found by Blondeau *et al.* is equivalent to Lemma 17.

This connexion between differential properties and reversed Dickson polynomials goes further. In [HMSY09], the following proposition was shown.

Proposition 1 (Proposition 4.3 from [HMSY09]). *APN functions in $\mathbb{F}_{2^n}$ and $\mathbb{F}_{2^{2n}}$ are connected by the following relations.*

- *If x^d is an APN function on $\mathbb{F}_{2^{2n}}$ then RD_d is a permutation polynomial on $\mathbb{F}_{2^n}$.*
- *If RD_d is a permutation polynomial on $\mathbb{F}_{2^n}$, then x^d is APN on $\mathbb{F}_{2^n}$.*
- *As a direct consequence, if x^d is an APN function on $\mathbb{F}_{2^{2n}}$ then x^d is APN on $\mathbb{F}_{2^n}$.*

The main consequence of this theorem is that finding an APN function in $\mathbb{F}_{2^{2n}}$ automatically implies finding an APN function in $\mathbb{F}_{2^n}$. Note that the converse is false. Let $n = 7$ and consider the monomial with exponent $d = 2^{n-1} - 1 = 63$. $x \mapsto x^d$ is APN in $\mathbb{F}_{2^n}$ as it is in the cyclotomic class of the inverse function and n is odd. However, this function is locally differentially 14-uniform in $\mathbb{F}_{2^{2n}}$.

4.1.3 Connections with $x^{2^t+1} + x + a$

Recall the definitions of $\mathcal{L}_\beta$

$$\mathcal{L}_\beta : x \mapsto x^{2^t+1} + x + \beta,$$

of $\mathcal{F}_0$

$$\mathcal{F}_0 = \{l \in \mathbb{F}_{2\backslash}\mathbb{F}_2, \mathbf{Tr}(l) = 0\}$$

and of the function Λ

$$\Lambda : l \mapsto \sum_{i=1}^{t} l^{2^i-1}.$$

In Section 3.3, when n is odd and $t = (n-1)/2$, we proved the following results.

[1] We used this property in Section 3.2.3 when computing the spectrum of $x \mapsto x^{2^t-1}$ for $t = (kn+1)/3$.

- Let $S_3 = \{x \in \mathbb{F}_{2^n} \backslash \mathbb{F}_2,\ \mathcal{L}_\beta(x) = 0$ and $\mathcal{L}_\beta$ has 3 roots$\}$. Then S_3 is the image of $\mathcal{F}_0$ by Λ.
- Let $S_1 = \{x \in \mathbb{F}_{2^n} \backslash \mathbb{F}_2,\ \mathcal{L}_\beta(x) = 0$ and $\mathcal{L}_\beta$ has 1 roots$\}$. Then S_1 is the image of $\mathcal{F}_0$ by $l \mapsto 1/\Lambda(l)$.

It is interesting to notice that Λ is almost another reversed Dickson polynomial:

$$\Lambda(l) = 1 + RD_{2^{t+1}-1}(l).$$

This implies two things.

- We can prove that Λ is an injection over $\mathcal{F}_0$ simply by observing that $t+1 = (n+1)/2$ is such that G_{t+1} is locally differentially 2-uniform. Thus, it is necessary that $RD_{2^{t+1}-1}$ is an injection over $\mathcal{F}_0$ and so must be $\Lambda = 1 + RD_{2^{t+1}-1}$.
- This also mean that the roots v of $\mathcal{L}_\beta$ when $\mathcal{L}_\beta$ has three roots are such that $v = RD_{2^{t+1}-1}(y) + 1$ and $\mathbf{Tr}(y) = 0$. This also means that when $\mathcal{L}_\beta$ has a unique root v, then $v = \left(1 + RD_{2^{t+1}-1}(y)\right)^{-1}$ with $\mathbf{Tr}(y) = 0$.

4.2 Other Interesting Spectra

All differential spectra of monomials $G_t : x \mapsto x^{2^t-1}$ for n from 5 to 31 and for t from 2 to $n-1$ have been computed by Blondeau. All the locally differentially 6-uniform mappings in this table fit in one of the categories given in Table 4.1. Furthermore, more simulations lead to the following conjecture.

Conjecture 3. *For $n \geq 20$, all differentially 6-uniform monomials are equivalent to a function in the $2^t - 1$ family. Furthermore, the corresponding value of t is given by one of the formulas in Table 4.1.*

t	$s = n - t + 1$	Condition	Reference
3	n-2	-	[BCC11]
$\frac{n-1}{2}$	$\frac{n+3}{2}$	n odd	Theorem 11
$\frac{kn+1}{3}$	$\frac{(k-3)n+2}{3}$	3 does not divide n	Theorem 7
$\frac{n}{3}$	$\frac{2n}{3}+1$	3 divides n	Unknown
$\frac{2n}{3}$	$\frac{n}{3}+1$	3 divides n	Unknown

Table 4.1. Observed locally differentially 6-uniform monomials $G_t : x \mapsto x^{2^t-1}$ and their symmetric.

The spectra in the first category of Table 4.1 have been proved by Blondeau *et al.* in [BCC11]. The spectra in the next two categories were extracted in the previous chapter. However, the last two cases remain to be studied. Though of a limited cryptographic interest due to their complete (i.e. non-restricted) differential uniformity being equal to 2^t or $2^t - 2$, finding out their spectrum would imply a complete characterization of all families of locally differentially 6-uniform monomials G_t.

We also recall the following conjecture concerning the cases $t = n/3$ and $t = n/3 + 1$. It is a particular case of Conjecture 1 which was first stated by Blondeau in [Blo11].

Conjecture 4. *Let n be divided by 3. For $t = n/3$ and $t = 2n/3$ (respectively $t = n/3 + 1$ and $t = 2n/3 + 1$), $G_t : x \mapsto x^{2^t - 1}$ is differentially 2^t-uniform (respectively $(2^t - 2)$-uniform) and is locally differentially 6-uniform.*

It is interesting to see that these exponents are connected. Indeed, $2n/3 + 1$ is the symmetric of $n/3$ and $2n/3$ is that of $n/3 + 1$. Therefore, only two distinct restricted spectra are concerned by this conjecture.

Furthermore, if $t = n/3$ then $2^t - 1$ is in the same cyclotomic class as $2^{2t}(2^t - 1) = 1 - 2^{2t}$, which corresponds to the multiplicative inverse of $2^{2t} - 1$, the symmetric of $2^{t+1} - 1$. Thus, if our conjecture is correct, G_t and $1/G_t$ have the same restricted spectrum for this particular value of t.[2]

For particular values of n, some of the monomials with exponent $2^t - 1$ are also differentially 6-uniform, although the corresponding values of t are not described in Table 4.1.

- For $n = 13$, G_t for $t = 4$ (and its symmetric $t = 10$) has the same spectrum as G_t for $t = 3$, $t = (2n + 1)/3 = 5$, $t = (n - 1)/2 = 6$ and their symmetric.

- For $n = 17$, G_t for $t = 4$, $t = 5$ and $t = 7$ are differentially 6-uniform. Furthermore, their spectra are identical with each other but also different from all the proved ones. The restricted differential spectrum $\{\omega_i^t\}_{i=0..6}$ of G_t for $t = 3$, $t = 4$ and $n = 17$ is given by:

$$\begin{array}{llllll} \omega_0^3 = & 76484, & \omega_2^3 = & 49114, & \omega_6^3 = & 5474 \\ \omega_0^4 = & 75532, & \omega_2^4 = & 50542, & \omega_6^4 = & 4998. \end{array}$$

- For $n = 19$, G_t for $t = 8$ (and its symmetric $t = 12$) is differentially 6-uniform; its spectrum is different from all the proved ones. As above, we give the

[2] Note that this is wrong in the general case. For instance, for $t = (n-1)/2$ and n odd, we have shown in Section 3.3 that G_t has the same spectrum as $x \mapsto x^\tau$ with $\tau = -2 - 2^{t+1}$, i.e. it has the same spectrum as the function $1/Q$ where $Q : x \mapsto x^{2+2^{t+1}}$. The monomial Q is in the class of $x \mapsto x^{2^t+1}$, a quadratic function which is known (see Tables 2.2, 2.3 and 2.4) to be APN when $\gcd(t, n) = 1$.

spectra for $t = 3$, $t = 8$ and $n = 19$:

$$\begin{array}{llllll} \omega_0^3 = & 306034, & \omega_2^3 = & 196309, & \omega_6^3 = & 21945 \\ \omega_0^8 = & 302310, & \omega_2^8 = & 201895, & \omega_6^8 = & 20083. \end{array}$$

4.3 General Properties of the S-boxes Studied

4.3.1 Resilience Against Linear Attacks

From a cryptographic point of view, the lower the differential uniformity the better. Furthermore, for a constant differential uniformity δ, the lower ω_δ the better too. The monomials we studied thus yield interesting properties which would allow a cipher using them as S-boxes to resist a differential cryptanalysis. However, there are other kinds of attacks.

The second main family of cryptanalysis is that of the linear attacks which consist in extracting linear approximations of the ciphers. These attacks can be prevented by using S-boxes with good non-linearity. Intuitively, the non-linearity gives the distance between a function and the set of the linear functions. The higher this quantity, the harder it is to find a linear approximation of the function.

To give a formal definition of the non-linearity, we first introduce the concept of Walsh spectrum.

Definition 25. *Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a Boolean function. The Walsh coefficient of f at the point u of $\mathbb{F}_2^n$ is denoted $\mathcal{F}(f + \phi_u)$ and is equal to*

$$\mathcal{F}(f + \phi_u) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+u\cdot x}.$$

The Walsh spectrum of the function f is the set

$$\{\mathcal{F}(f + \phi_u), u \in \mathbb{F}_2^n\}.$$

Definition 26. *Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a Boolean function. The non-linearity of f is the Hamming distance between f and the set of the linear functions. It is denoted $\mathcal{NL}(f)$ and is such that:*

$$\mathcal{NL}(f) = 2^{n-1} - \frac{1}{2}\mathcal{L}(f)$$

where

$$\mathcal{L}(f) = \max_{u \in \mathbb{F}_2^n} \left(|\mathcal{F}(f + \phi_u)|\right).$$

The Walsh spectrum of a given function can be computed using SAGE [SJ05] as it contains a module for Boolean functions. Using this tool, we computed the Walsh spectra and the non-linearity of G_t for the values of t we are interested in, namely $t = 3$, $t = (nk + 1)/3$, $t = (n - 1)/2$ and their symmetric.

The results we found were not very interesting in the sense that we were not able to find any pattern which would have helped us to develop a theory. They are given in Table 4.2 for $n = 11$ and $n = 12$.

n	type	t	$\mathcal{L}(G_t)$	Walsh spectrum
11	3	3	128	-128 -96 -64 -32 0 32 64 96 128
11	$\frac{n+1}{3}$	4	128	-128 -96 -64 -32 0 32 64 96 128
11	$\frac{n-1}{2}$	5	136	-120 -104 -88 -80 -72 -64 -56 -48 -40 -32 -24 -16 -8 0 8 16 24 32 40 48 56 64 72 80 88 112 136
11	$\frac{n+3}{2}$	7	128	-128 -112 -96 -80 -64 -48 -32 -16 0 16 32 48 64 80 96 128
11	$\frac{2n+2}{3}$	8	144	-144 -112 -96 -80 -64 -48 -32 -16 0 16 32 48 64 80 96 128
11	$n-2$	9	128	-128 -112 -104 -88 -80 -72 -64 -56 -48 -40 -32 -24 -16 -8 0 8 16 24 32 40 48 56 64 72 80 88 96 104 112
12	3	3	176	-144 -80 -16 48 112 176
12	$\frac{n}{3}$	4	224	-160 -96 -32 32 96 224
12	$\frac{n+3}{3}$	5	192	-192 -176 -160 -144 -128 -112 -96 -80 -64 -48 -32 -16 0 16 32 48 64 80 96 112 128 144 160
12	$\frac{2n}{3}$	8	224	-160 -128 -96 -64 -32 0 32 64 96 128 224
12	$\frac{2n+3}{3}$	9	144	-144 -128 -96 -80 -64 -48 -32 -16 0 16 32 48 64 80 96 112 144
12	$n-2$	10	224	-224 -208 -160 -136 -128 -120 -112 -96 -88 -80 -72 -64 -56 -48 -40 -32 -24 -16 -8 0 8 16 24 32 40 48 56 64 72 80 88 96 120 128 136 160

Table 4.2. The non linearity and the Walsh spectra of G_t for the values of t we studied and $n = 11, 12$.

4.3.2 Resilience Against Algebraic Attacks

Another type of attack is the so-called *algebraic attack* which exploits particular algebraic properties of the S-boxes to derive quadratic equations which must be satisfied by a large set of variables. It was introduced by Courtois and Pieprzyk in [CP02]. These variables can correspond to parts of a plaintext, of a ciphertext and also to the internal state.

A key property to resist this cryptanalysis is the algebraic degree.

Definition 27. *For monomials, the algebraic degree is equal to the Hamming weight of the exponent. If F_d is the monomial $x \mapsto x^d$, we denote by $deg(F_d)$ the algebraic degree of F_d (i.e. the hamming weight of d).*

The higher this quantity, the better the resilience against algebraic attacks. However, having an S-box with high algebraic degree is not enough: its inverse must also have a high algebraic degree. The S-box S of the AES is based on the function $I : x \mapsto x^{-1}$ in $\mathbb{F}_{2^8}$ due to its low differential uniformity. However, since the algebraic degree of its inverse is 1 and in order to prevent such attacks, an affine mapping is also used: $S = L \circ I$ (see the AES specification [DR98]).

The algebraic degree of G_t is simply equal to t. To compute the algebraic degree of their inverse, we use Theorem 7 of [KS12]:

$$wt(G_t^{-1}) \equiv \frac{1}{t} \mod n$$

where $1/t$ is the inverse of t modulo n. A table containing the algebraic degrees, differential uniformities $u(G_t), u(G_s)$ and local differential uniformities $U(G_{t,s})$[3] is given Table 4.3 for all the values t studied in this Thesis as well as for their symmetric and inverse.

t, $deg(G_t)$	s, $deg(G_s)$	$deg(G_t^{-1})$	$deg(G_s^{-1})$	$U(G_{t,s})$	$u(G_t)$	$u(G_s)$	Spectrum
2	$n-1$	$(*, \frac{n+1}{2})$	$n-1$	2	2	(2,4)	Quadratic
$\frac{n+1}{2}$	$\frac{n+1}{2}$	2	2	2	2	2	Inverse of x^{2^t+1}
$\frac{n}{2}$	$\frac{n}{2}+1$	$*$	$\frac{n+2}{2}$	2	$2^{n/2-2}$	$2^{n/2}$	[BCC11]
3	$n-2$	$(*, \frac{jn+1}{3})$	$\frac{n-1}{2}$	6	6	(6,8)	[BCC11]
$\frac{kn+1}{3}$	$\frac{(3-k)n+2}{3}$	3	$(*, 3)$	6	6	6	Theorem 7
$\frac{n-1}{2}$	$\frac{n+3}{2}$	$n-2$	$(*, \frac{jn+2}{3})$	6	(6,8)	6	Theorem 11
$\frac{kn}{3}$	$\frac{(3-k)n+3}{3}$	$*$	$(*, \frac{jn+3}{3})$	6	$2^{n/3}-2$	$2^{n/3}$	Unknown

Table 4.3. Differential Uniformity and Algebraic degree of the function $G_t(x) = x^{2^t-1}$, their symmetric G_s and their inverses G_t^{-1} and G_s^{-1}. We have $1 \leq k, j \leq 2$.

4.3.3 Discussion about the Equivalence of the S-boxes Studied

In [CCZ98], Carlet, Charpin and Zinoviev introduced an equivalence relation for Boolean functions which was then named *CCZ equivalence*.

Definition 28 (CCZ-equivalence [CCZ98]). *Let F and F' be two functions from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$ and let G_F (respectively $G_{F'}$) be the graph of F (respectively F'), i.e.*

[3] Recall Theorem 4: G_t and G_s have the same restricted spectrum and thus the same local differential uniformity

$\{(x, F(x)), x \in \mathbb{F}_{2^n}\}$ *(respectively* $\{(x, F'(x)), x \in \mathbb{F}_{2^n}\}$*). Then* F *and* F' *are called CCZ-equivalent if there exists an affine permutation* L *of* $\mathbb{F}_{2^n} \times \mathbb{F}_{2^m}$ *such that* $G_{F'} = L(G_F)$*.*

A particular case of the CCZ equivalence is the *extended affine* equivalence, or *EA-equivalence*, introduced in the same paper ([CCZ98]).

Definition 29 (EA equivalence [CCZ98])**.** *Let* F *and* F' *be two functions from* $\mathbb{F}_{2^n}$ *to* $\mathbb{F}_{2^m}$*.* F *and* F' *are affine equivalent if there exist affine automorphisms* $L : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ *and* $L' : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ *as well as an affine function* $A : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ *such that*

$$F = L' \circ F \circ L + A.$$

As we can see in Table 4.3, the algebraic degrees of the different functions are related to each other. For instance, we have in some cases that $deg(G^{-1}_{(n-1)/2}) = deg(G_{(jn+2)/3)})$. As the CCZ and EA equivalence preserve the algebraic degree and since these functions also have the same differential uniformity (namely 6), it is natural to ask the question of their equivalence.

However, both these equivalence relation are known to also preserve the Walsh spectrum. Using the Walsh spectra extracted using a computer, we were able to check that these are not equal for n in $[7, 13]$ (see Tale 4.2 for the cases $n = 7$ and $n = 13$). We thus claim that the functions we studied are independent from each other with regards to these relations.

4.3.4 The $x \mapsto x^{2^{(n+3)/2}-1}$ S-box

An other observation one can make from this table is that the monomial[4] G_t for $t = (n + 3)/2$ and $n \equiv \pm 1 \mod 6$ is a bijection, is differentially 6-uniform, which is low enough, has algebraic degree $(n + 3)/2$ which is high enough and and has an inverse with algebraic degree $(jn + 2)/3$ for some $j = 1, 2$, which is also high enough. These properties make it a potentially good candidate for use as an S-box of a substitution-permutation network when the bit-length of the input and output of the S-box is $6l \pm 1$ for some l. One could also use it in the round function of a Feistel network in any field size because in this case, it is not necessary to have a bijection.

For example, if we look at the cases where $n = 7, 11$ and 13. In all these cases, $n \equiv \pm 1 \mod 6$ so G_t is a bijection. The size of a look-up table to implement these functions would contain respectively 128, 2048 and 8192 entries. While high in the last case, this remains reasonable.

In these cases, G_t has the properties given in Table 4.4. The differential uniformities are not given since they are constant and equal to 6 (see Theorem 12). For comparison, we also give the properties of the cubic function and the inverse

[4] It corresponds to the symmetric of $t = (n - 1)/2$ whose differential spectrum was extracted in this Thesis.

function, the latter being widely used (it is for instance at the core of the AES S-box [DR98]).

n	type	$deg(G_t) = t$	$deg(G_t^{-1})$	$\mathcal{NL}(G_t)$
7	$\frac{n+3}{2}$	5	3	44
	Cubic	2	5	56
	Inverse	6	6	54
11	$\frac{n+3}{2}$	7	8	960
	Cubic	3	4	992
	Inverse	10	10	980
13	$\frac{n+3}{2}$	8	5	3936
	Cubic	2	9	4032
	Inverse	12	12	4006

Table 4.4. Properties of $G_t : x \mapsto x^{2^t-1}$ for $t = (n+3)/2$ and $n = 7, 11, 13$.

4.4 Relations Between Exponents $2^t - 1$ and $2^{t+1} - 1$

When trying to derive the differential spectrum of G_t and G_{t+1} for $t = n/3$, we observed an interesting link between the monomials G_t and G_{t+1} which actually holds for any value of t.

Recall that $(x+1)^{2^t-1} + x^{2^t-1} = b$ has $\delta(b)$ solutions and that $P_b^t(x) = x^{2^t} + bx^2 + (b+1)x$ has $\delta(b)+2$ roots. Let x be some element of $\mathbb{F}_{2^n}$ and let b and c be defined by

$$\begin{aligned} b &= (x+1)^{2^t-1} + x^{2^t-1} \\ c &= (x+1)^{2^{t+1}-1} + x^{2^{t+1}-1}. \end{aligned}$$

We thus have that x is a root of both P_b^t and P_c^{t+1}. This implies the following:

$$\begin{aligned} 0 &= P_b^t(x)^2 + P_c^{t+1}(x) \\ &= \left(x^{2^t} + bx^2 + (1+b)x\right)^2 + x^{2^{t+1}} + cx^2 + (c+1)x \\ &= x^{2^{t+1}} + b^2x^4 + (b^2+1)x^2 + x^{2^{t+1}} + cx^2 + (c+1)x \\ &= b^2\left(x^4 + (1 + b^{-2} + cb^{-2})x^2 + b^{-2}(c+1)x\right) \\ &= b^2\left(x^4 + (1 + \frac{c+1}{b^2})x^2 + \frac{c+1}{b^2}x\right). \end{aligned}$$

Let $\gamma = (c+1)/b^2$. Then if $P_b^t(x) = P_c^{t+1}(x) = 0$, we have

$$\begin{aligned} 0 &= x^4 + (1+\gamma)x^2 + \gamma x \\ &= (x^2 + x)(x^2 + x + \gamma). \end{aligned}$$

If $x \neq 0, 1$, then it must hold that $\gamma = x^2 + x = y$. Recall that $P_b^t(x) = 0$ if and only if $RD_{2^t-1}(y) = b$; so we also have

$$\begin{aligned}
& RD_{2^t-1}(y) = b \text{ and } RD_{2^{t+1}-1}(y) = c \\
\Longrightarrow\ & RD_{2^t-1}(y) + RD_{2^{t+1}-1}(y) = b + c \\
\Longrightarrow\ & \sum_{i=0}^{t-1} y^{2^i-1} + \sum_{i=0}^{t} y^{2^i-1} = b + c \\
\Longrightarrow\ & y^{2^t-1} = b + c \\
\Longrightarrow\ & y^{2^t-1} = b^2 \frac{c+1}{b^2} + b + 1 \\
\Longrightarrow\ & y^{2^t-1} = b^2\gamma + b + 1.
\end{aligned}$$

These observations have several consequences.

- $\gamma = x^2 + x$ implies that $\mathbf{Tr}(\gamma) = 0$.
- $\gamma = y$ and $y^{2^t-1} = b^2\gamma + b + 1$ implies that $\gamma^{2^t} + b^2\gamma^2 + (b+1)\gamma = 0$. This polynomial is the adjoined polynomial of P_{b+1}^s, denoted P_{b+1}^{s*}. This polynomial was introduced in [Blo11] and it was proven (Corollary 8.2) that $\{\delta_s(b), b \in \mathbb{F}_{2^n} \backslash \mathbb{F}_2\} = \{\delta_t(b), b \in \mathbb{F}_{2^n} \backslash \mathbb{F}_2\}$.

Conclusion

When designing a symmetric cryptographic primitive, be it a block cipher, a hash function or a message authentication code (MAC), highly non-linear functions called S-boxes are often used. Monomials over fields of characteristic 2 are usually chosen due to their low implementation cost. In order for the primitive to be resilient against differential cryptanalysis and affiliated attacks, the differential properties of the S-box have to be taken into account.

In particular, the differential spectrum (and thus the differential uniformity) of the function must match some criteria. In this Thesis, we extracted the differential spectrum of four monomials, thus proving conjectures made by Blondeau in her PhD Thesis. Some observations related to these proofs have also been made, connecting for instance the differential spectrum with the image of a sub-field by Dickson polynomials or linking the study of monomials with exponents $2^t - 1$ and $2^{t+1} - 1$.

At last, we gave some conjectures. If they are correct, the classification of differentially 6-uniform power functions is now complete and only two yet unproven cases correspond to locally differentially 6-uniform functions.

Bibliography

[BCC10a] C. Blondeau, A. Canteaut, and P. Charpin. Differential properties of power functions. *Int. J. Inform. and Coding Theory*, 1(2):149–170, 2010. Special Issue dedicated to Vera Pless.

[BCC10b] C. Blondeau, A. Canteaut, and P. Charpin. Differential properties of power functions. In *IEEE International Symposium on Information Theory, ISIT 2010, June 13-18, 2010, Austin, Texas, USA, Proceedings*, pages 2478–2482. IEEE, 2010.

[BCC11] C. Blondeau, A. Canteaut, and P. Charpin. Differential properties of $x \mapsto x^{2^t-1}$. *IEEE Transactions on Information Theory*, 57(12):8127–8137, 2011.

[BCCLC06] T. P. Berger, A. Canteaut, P. Charpin, and Y. Laigle-Chapuy. On almost perfect nonlinear functions over $\mathrm{F}_2{}^{\mathrm{n}}$. *IEEE Transactions on Information Theory*, 52(9):4160–4170, 2006.

[BDMW10] K. Browning, J. Dillon, M. McQuistan, and A. Wolfe. An APN permutation in dimension six. In *Finite Fields: Theory and Applications - FQ9*, volume 518 of *Contemporary Mathematics*, pages 33–42. AMS, 2010.

[BDPA11] G. Bertoni, J. Daemen, M. Peeters, and G. V. Assche. The Keccak reference, January 2011. http://keccak.noekeon.org/Keccak-reference-3.0.pdf.

[BKL$^+$07] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. B. Robshaw, Y. Seurin, and C. Vikkelsoe. Present: An ultra-lightweight block cipher. In P. Paillier and I. Verbauwhede, editors, *CHES*, volume 4727 of *Lecture Notes in Computer Science*, pages 450–466. Springer, 2007.

[Blo11] C. Blondeau. *La cryptanalyse différentielle et ses généralisations*. PhD thesis, Université Pierre et Marie Curie, Paris, France, 2011.

[Blu04] A. W. Bluher. On $\mathrm{x}^{\mathrm{q}+1}$+ax+b. *Finite Fields and Their Applications*, 10(3):285–305, 2004.

[BP13] C. Blondeau and L. Perrin. More differentially 6-uniform power functions. In *WCC 2013*, (To appear) 2013.

[BRS67] E. R. Berlekamp, H. Rumsey, and G. Solomon. On the solution of algebraic equations over finite fields. *Information and Control*, 10(6):553–564, 1967.

[BS91] E. Biham and A. Shamir. Differential cryptanalysis of DES-like cryptosystems. *Journal of Cryptology*, 4(1):3–72, 1991.

[Can06] A. Canteaut. *Analyse et conception de chiffrements à clef secrète*. Habilitation à diriger des recherches, Université Pierre et Marie Curie, September 2006.

[Car69] L. Carlitz. Kloosterman sums and finite field extensions. *Acta Arithmetica*, 16(2):179–183, 1969.

[CCZ98] C. Carlet, P. Charpin, and V. Zinoviev. Codes, bent functions and permutations suitable for des-like cryptosystems. *Designs, Codes and Cryptography*, 15(2):125–156, 1998.

[Che82] C.-L. Chen. Formulas for the solutions of quadratic equations over $\mathrm{GF}(2^{\mathrm{m}})$. *IEEE Transactions on Information Theory*, 28(5):792–794, 1982.

[Cop94] D. Coppersmith. The data encryption standard (des) and its strength against attacks. *IBM journal of research and development*, 38(3):243–250, 1994.

[CP02] N. T. Courtois and J. Pieprzyk. Cryptanalysis of block ciphers with overdefined systems of equations. In Y. Zheng, editor, *Advances in Cryptology – ASIACRYPT 2002*, volume 2501 of *Lecture Notes in Computer Science*, pages 267–287. Springer Berlin Heidelberg, 2002.

[Dic96] L. E. Dickson. The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group. *Annals of Mathematics*, 11(1/6):65–120, 1896.

[Dob99a] H. Dobbertin. Almost perfect nonlinear power functions on $GF(2^n)$: the Niho case. *Information and Computation*, 151(1-2):57–72, 1999.

[Dob99b] H. Dobbertin. Almost perfect nonlinear power functions on $GF(2^n)$: the Welch case. *IEEE Transactions on Information Theory*, 45(4):1271–1275, 1999.

[Dob00] H. Dobbertin. Almost perfect nonlinear power functions on $GF(2^n)$: a new class for n divisible by 5. In *Proceedings of Finite Fields and Applications Fq5*, pages 113–121. Springer-Verlag, 2000.

[DR98] J. Daemen and V. Rijmen. The block cipher rijndael. In J.-J. Quisquater and B. Schneier, editors, *CARDIS*, volume 1820 of *Lecture Notes in Computer Science*, pages 277–284. Springer, 1998.

[Göl12] F. Göloğlu. A note on "differential properties of x -> $x^{2^{t}-1}$". *IEEE Transactions on Information Theory*, 58(11):6986–6988, 2012.

[HK08] T. Helleseth and A. Kholosha. On the equation $x^{2^{l}+1}$+x+a=0 over GF(2^{k}). *Finite Fields and Their Applications*, 14(1):159–176, 2008.

[HMSY09] X. Hou, G. L. Mullen, J. A. Sellers, and J. L. Yucas. Reversed dickson polynomials over finite fields. *Finite Fields and Their Applications*, 15(6):748 – 773, 2009.

[Kas71] T. Kasami. The weight enumerators for several classes of subcodes of the second order binary Reed-Muller codes. *Information and Control*, 18:369–394, 1971.

[KHCJ96] P. V. Kumar, T. Helleseth, A. R. Calderbank, and A. R. H. Jr. Large families of quaternary sequences with low correlation. *IEEE Transactions on Information Theory*, 42(2):579–592, 1996.

[KS12] G. M. 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*, pages 1207–1211. IEEE, 2012.

[LMT93] R. Lidl, G. Mullen, and G. Turnwald. Dickson polynomials. 1993. *Pitman Monogr. Surveys Pure Appl. Math*, 1993.

[Nat99] National Institute of Standards and Technology. *FIPS PUB 46-3: Data Encryption Standard (DES).* National Institute for Standards and Technology, October 1999.

[Nyb94] K. Nyberg. Differentially uniform mappings for cryptography. In *Workshop on the theory and application of cryptographic techniques on Advances in cryptology*, EUROCRYPT '93, pages 55–64, Secaucus, NJ, USA, 1994. Springer-Verlag New York, Inc.

[Nyb96] K. Nyberg. Generalized feistel networks. In K. Kim and T. Matsumoto, editors, *ASIACRYPT*, volume 1163 of *Lecture Notes in Computer Science*, pages 91–104. Springer, 1996.

[SJ05] W. Stein and D. Joyner. Sage: System for algebra and geometry experimentation. *Communications in Computer Algebra*, 39(2), 2005.

[Sti05] D. Stinson. *Cryptography: theory and practice, Third Edition.* Chapman & Hall/CRC, 2005.