Dickson Polynomials that are Involutions.

Pascale Charpin, Sihem Mesnager, Sumanta Sarkar

Chapter 1

Dickson Polynomials that are Involutions

Pascale Charpin

INRIA-Paris, 2 rue Simone Iff 75012, Paris, France,
Pascale.Charpin@inria.fr.

Sihem Mesnager

University of Paris VIII and University of Paris XIII, LAGA, CNRS and Télécom ParisTech, Paris, France, *smesnager@univ-paris8.fr*

Sumanta Sarkar

TCS Innovation Labs, Hyderabad 500081, India, Sumanta@atc.tcs.com.

Abstract. Dickson polynomials which are permutations are interesting combinatorial objects and well studied. In this paper, we describe Dickson polynomials of the first kind in $\mathbb{F}_2[x]$ that are involutions over finite fields of characteristic 2. Such description is obtained using modular arithmetic's tools. We give results related to the cardinality and the number of fixed points (in the context of cryptographic application) of this corpus. We also present infinite classes of Dickson involutions. We study Dickson involutions which have a minimal set of fixed points.

Keywords: Dickson polynomials, permutation, involution, fixed point, Jacobi symbol, quadratic residue.

1.1 Introduction

We start with the question related to cryptography: can decryption algorithm be the same as the encryption algorithm? The answer is yes, and in fact, the classic example of this kind of cryptosystem is Enigma. The advantage of having the same encryption and decryption algorithm is that the same implementation of the encryption algorithm works for the decryption also, and hence reduces the implementation cost. Suppose a uniformly chosen permutation $E : X \to X$ is applied as the encryption, where X is the message space, with the additional property that $E(E(x)) = x$ for all $x \in X$, i.e., $E^{-1} = E$. Then E serves for both the encryption and decryption.

Let $\mathbb{F}_{2^n}$ be the finite field of 2^n elements. If the polynomial $F(x)$ defined over $\mathbb{F}_{2^n}$ induces a permutation of $\mathbb{F}_{2^n}$, then $F(x)$ is called a permutation polynomial. Permutations are invertible functions, i.e., for a permutation polynomial $F(x)$ there exists a unique polynomial $F'(x)$ such that $F' \circ F(x) = F \circ F'(x) = x$, for all x. The polynomial $F'(x)$ is called the compositional inverse of F and is generally denoted by F^{-1}. Permutation polynomial is well known for its application in cryptography, coding theory, combinatorial design, etc. For instance, in block ciphers, a permutation F is used as an S-box to build the confusion layer during the encryption process, while in the decryption the inverse of F is required.

A permutation polynomial $F(x)$ for which $F \circ F(x) = x$ is called *involution*, and from the above discussions, it is clear that involution property is important in applications. Dickson polynomials form an important class of permutation polynomials. We would like to refer to the book of Lidl, Mullen and Turnwald [8], where the work on Dickson polynomials, and its developments are presented. Our results are widely derived from those of [8, Chapter 2-3]. Moreover, the Dickson permutations that decompose in cycles of same length are generally studied in [11]; more applications are presented in [12]. Our purpose is to describe precisely this corpus in the case of cycles of length 2, for such permutations over any finite field of characteristic 2. Some proofs are given for clarity; our aim is to propose a clear understanding in order to use easily Dickson involutions.

The Dickson polynomials have been extensively investigated in recent years under different contexts (see for instance [2, 5, 6, 9, 10, 13]). In this paper we treat *Dickson polynomials of the first kind* defined on a finite field of order 2^n.

Definition 1.1. The Dickson polynomial of the first kind of degree k in indeterminate x and with parameter $a \in \mathbb{F}_{2^n}^*$ is defined by

$$D_k(x,a) = \sum_{i=0}^{\lfloor k/2 \rfloor} \frac{k}{k-i} \binom{k-i}{i} a^k x^{k-2i},\ k \geq 2 \tag{1.1}$$

where $\lfloor k/2 \rfloor$ denotes the largest integer less than or equal to $k/2$.

We treat here the polynomials $D_k(x,1)$ that we will denote by $D_k(x)$ throughout this paper. The set of k such that D_k is a permutation of a given finite field $\mathbb{F}_{2^n}$ is well-known.

Our aim, in this paper, is the study of such polynomials $D_k(x)$ which induce an involution of any fixed finite field. After some preliminaries, in Section 1.2, the characterization of Dickson involutions is presented in Section 1.3 (see Theorem 1.3). Section 1.4 is devoted to the study of the corpus of involutions. We notably show that it consists in equivalence classes of size 4 and we compute the number of such classes. We also exhibit two infinite classes of Dickson involutions (Theorem 5). In Section 1.5, we study the fixed points of Dickson involutions. Our study reveals that they generally have a high number of fixed points. We propose lower bounds on this number. We give a precise description of the set of fixed points of Dickson involutions and study the case where this set has a minimal size, when $n = 2m$ with m even. We prove that such minimal set is equal to $\mathbb{F}_{2^{\frac{m}{2}}}$ and we characterize the Dickson involutions which have such set of fixed points (Section 1.5.3). At the end we give some numerical results.

1.2 Basic properties

Here we introduce some useful properties, on the Dickson polynomials of $\mathbb{F}_2[x]$. Note that they are known in many different contexts. Dickson polynomial $D_k \in \mathbb{F}_2[x]$ are recursively defined by

$$\begin{array}{l} D_0(x) = 0 \text{ and } D_1(x) = x; \\ D_{i+2}(x) = xD_{i+1}(x) + D_i(x). \end{array} \tag{1.2}$$

Using this definition it is easy to prove the next properties which we use in the sequel.

Proposition 1.1. *The polynomials defined by (1.2) satisfy:*

- $\deg(D_i) = i$,
- $D_{2i}(x) = (D_i(x))^2$,

- $D_{ij}(x) = D_i(D_j(x))$,
- $D_i(x + x^{-1}) = x^i + x^{-i}$,

for all x, for any integer $i, j > 0$.

In this paper, we identify a polynomial on $\mathbb{F}_{2^n}$ (for some n) with its corresponding mapping $x \mapsto F(x)$ from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$; F is a permutation when this mapping is bijective. Concerning the Dickson polynomials, we have the following fundamental result.

Theorem 1.1. [8, Theorem 3.2] *The Dickson polynomial $D_k \in \mathbb{F}_2[x]$ is a permutation on $\mathbb{F}_{2^n}$ if and only if* $\gcd(k, 2^{2n} - 1) = 1$.

Some permutations are *involutive* and are then called *involutions*.

Definition 1.2. We say that F is an involution on $\mathbb{F}_{2^n}$ when it satisfies

$$F \circ F(x) = x, \quad \text{for all } x \in \mathbb{F}_{2^n}.$$

Note that an involution is equal to its compositional inverse. We will use later the *Jacobi symbols*. We now give its definition and some of its basic properties. Recall that an integer a is a *quadratic residue modulo a prime* p if and only if there is an integer u such that $a \equiv u^2 \pmod p$.

Definition 1.3. Let P be an odd integer, $P > 2$, and $P = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$ be the decomposition of P in prime factors. Let a be any integer. The Jacobi symbol of a is

$$Jac(a, P) = \left(\frac{a}{P}\right) = \left(\frac{a}{p_1}\right)^{a_1} \dots \left(\frac{a}{p_k}\right)^{a_k}.$$

where $\left(\frac{a}{p_i}\right)$, called a *Legendre symbol*, is as follows defined : it is equal to 0 if p_i divides a; otherwise we have:

$$\left(\frac{a}{p_i}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue modulo } p_i, \\ & \textit{i.e.,} \text{ there is } k > 0 \text{ such that } a \equiv k^2 \pmod{p_i}; \\ -1 & \text{if } a \text{ is not a quadratic residue modulo } p_i. \end{cases}$$

And we have these well-known formula on the values $Jac(a, P)$ where a and b are any integer.

$$\left(\frac{ab}{P}\right) = \left(\frac{a}{P}\right)\left(\frac{b}{P}\right). \tag{1.3}$$

$$\left(\frac{-1}{P}\right) = (-1)^{\frac{P-1}{2}} \quad \text{and} \quad \left(\frac{2}{P}\right) = (-1)^{\frac{P^2-1}{8}}. \tag{1.4}$$

$$a \equiv b \pmod P \implies \left(\frac{a}{P}\right) = \left(\frac{b}{P}\right). \tag{1.5}$$

Note that if $Jac(a, P) = -1$ then a is a quadratic nonresidue modulo P.

1.3 Dickson polynomials which induce involutions

A priori, the Dickson permutations cannot be involutive since they are obtained recursively. However they are permutations on a specific finite field. Let $n = 2m$ and k such that $\gcd(k, 2^n - 1) = 1$. Then D_k permutes $\mathbb{F}_{2^m}$. What happens when we compute $D_k \circ D_k$?

From Proposition 1.1, we have $D_k(D_k(x)) = D_{k^2}(x)$. Thus D_k is an involution on $\mathbb{F}_{2^m}$ if and only if $D_{k^2}(x) \equiv x \pmod{x^{2^m} + x}$. For instance, for $m = 2\ell$,

$$D_{2^\ell} \ : \ x \mapsto x^{2^\ell} \text{ is an involution on } \mathbb{F}_{2^m}.$$

We are going to describe the set of k such that D_k is an involution on $\mathbb{F}_{2^m}$, for any fixed m. The proofs of Theorem 1.2 and Corollary 1.1 below are derived from the results of [8, Chapters 2-3]. We give these proofs for clarity.

Lemma 1.1. *For all $x \in \mathbb{F}_{2^m}$ there is $\gamma \in \mathbb{F}_{2^n}^*$, $n = 2m$, such that $x = \gamma + \gamma^{-1}$. Moreover such a γ satisfies either $\gamma^{2^m-1} = 1$ or $\gamma^{2^m+1} = 1$.*

Proof. We denote by Tr the absolute trace on $\mathbb{F}_{2^n}$. For any $x \in \mathbb{F}_{2^m}$, there is γ such that $x = \gamma + \gamma^{-1}$ if and only if the equation $\gamma^2 + \gamma x + 1 = 0$ has a solution in $\mathbb{F}_{2^n}^*$. And this is equivalent to $Tr(1/x) = 0$ which is satisfied for all $x \in \mathbb{F}_{2^m}$.

We have $\gamma + \gamma^{-1}$ in $\mathbb{F}_{2^m}$ if and only if

$$\left(\gamma + \frac{1}{\gamma}\right)^{2^m} = \gamma + \frac{1}{\gamma}, \text{ or equivalently } \ (\gamma^{2^m} + \gamma)(\gamma^{2^m+1} + 1) = 0,$$

completing the proof. □

Theorem 1.2. *Let k, ℓ be two nonzero integers. Then*

$$D_k(x) \equiv D_\ell(x) \pmod{x^{2^m} + x}$$

if and only if

$$\begin{array}{l} k \equiv \ell \pmod{2^m - 1} \text{ or } k \equiv -\ell \pmod{2^m - 1} \\ \text{and} \\ k \equiv \ell \pmod{2^m + 1} \text{ or } k \equiv -\ell \pmod{2^m + 1}. \end{array}$$

Proof. Let us suppose that $D_k(x) \equiv D_\ell(x)$ for any $x \in \mathbb{F}_{2^m}$. From Lemma 1.1, this is to say that for any $x = \gamma + \gamma^{-1}$

$$D_k(x) = \gamma^k + \left(\frac{1}{\gamma}\right)^k \equiv D_\ell(x) = \gamma^\ell + \left(\frac{1}{\gamma}\right)^\ell, \tag{1.6}$$

applying Proposition 1.1, where $\gamma \in \mathbb{F}_{2^n}^*$ such that $\gamma^{2^m-1} = 1$ or $\gamma^{2^m+1} = 1$. Now (1.6) can be written

$$\gamma^\ell(\gamma^{2k}+1) + \gamma^k(\gamma^{2\ell}+1) = 0 \;\Leftrightarrow\; (\gamma^\ell+\gamma^k)(\gamma^{\ell+k}+1) = 0.$$

Thus (1.6) is equivalent to $\gamma^{\ell+k} = 1$ or $\gamma^{k-\ell} = 1$. Let α be a primitive root of $\mathbb{F}_{2^n}$. We know that we have to consider two forms for γ: $\gamma = \alpha^{s(2^m-1)}$ and $\gamma = \alpha^{t(2^m+1)}$ for some s, t. Then (1.6) holds for any γ is if and only if the two following conditions are satisfied:

- if $\gamma = \alpha^{s(2^m-1)}$ then $k \pm \ell \equiv 0 \pmod{2^m+1}$;
- if $\gamma = \alpha^{t(2^m+1)}$ then $k \pm \ell \equiv 0 \pmod{2^m-1}$.

□

Now we can describe that cases where $D_k(x) \equiv x \pmod{x^{2^m}+x}$. The next corollary can be viewed as an instance of [8, Theorem 3.8].

Corollary 1.1. *Let $n = 2m$. Let us define*

$$K_n = \{\ k \mid 1 \le k \le 2^n - 1,\ D_k(x) \equiv x \pmod{x^{2^m}+x}\ \}.$$

Then $K_n = \{\ 1,\ 2^m,\ 2^n - 2^m - 1,\ 2^n - 2\ \}$.

Proof. Applying Theorem 1.2 to the case $\ell = 1$, k must be a solution of one of the four systems of congruences modulo $2^n - 1$:

$$\begin{array}{l}
(i)\ k \equiv 1 \pmod{2^m-1} \text{ and } k \equiv 1 \pmod{2^m+1} \\
(ii)\ k \equiv 1 \pmod{2^m-1} \text{ and } k \equiv -1 \pmod{2^m+1} \\
(iii)\ k \equiv -1 \pmod{2^m-1} \text{ and } k \equiv 1 \pmod{2^m+1} \\
(iv)\ k \equiv -1 \pmod{2^m-1} \text{ and } k \equiv -1 \pmod{2^m+1}.
\end{array}$$

If $k < 2^m - 1$ then $k = 1$ (case (i)). Moreover $k = 2^m$ is a solution of (ii). We now assume that $2^m < k$.

Now (i) implies that (2^m-1) and (2^m+1) divide $k-1$. Since (2^m-1) and (2^m+1) are odd and coprime, only $k = 2^n$ is a solution of (i) and $2^n \equiv 1$ modulo (2^n-1). Similarly, (iv) implies that $2^n - 1$ divides $k+1$ so that only $k = 2^n - 2$ is a solution of (iv).

The congruence (ii) implies that (2^m-1) divides $k-1$ and (2^m+1) divides $k+1$. Thus there is b such that

$$k = b(2^m-1)+1 = b(2^m+1)-2b+1,\ \textit{i.e.},\ k+1 \equiv -2b+2 \pmod{2^m+1},$$

implying $b \equiv 1 \pmod{2^m+1}$ so that $b = 1$. Further $k = 2^m$.

The congruence (iii) implies that (2^m-1) divides $k+1$ and (2^m+1) divides $k-1$. Thus there is b such that

$$k = b(2^m+1)+1 = b(2^m-1)+2b+1, \ i.e., \ k+1 \equiv 2b+2 \pmod{2^m-1},$$

implying $b \equiv -1 \pmod{2^m-1}$ so that $b = 2^m-2$. Further

$$k = (2^m-2)(2^m+1)+1 = 2^{2m}-2^m+1.$$

□

Now we are able to describe the set of Dickson involutions. We first need to eliminate the elements of K_n which are not quadratic residues modulo 2^n-1.

Lemma 1.2. *Let $n = 2m$. Then*

- 2^n-2^m-1 *and* 2^n-2 *are quadratic nonresidues modulo* 2^n-1.
- 2^m *is a quadratic residue modulo* 2^n-1 *if and only if* m *is even and the square roots are* $2^{m/2}S_n$ *where* S_n *are the square roots of* 1 *modulo* 2^n-1.

Proof. Since $2^n-1 \equiv 3 \pmod 4$, $2^{n-1}-1$ is an odd integer. Thus we have

$$\left(\frac{-1}{2^n-1}\right) = (-1)^{\frac{(2^n-1)-1}{2}} = (-1)^{2^{n-1}-1} = -1.$$

On the other hand, one has that $2^n-1 \equiv 7 \pmod 8$ for every $n \geq 3$ which implies that $\frac{(2^n-1)^2-1}{8}$ is an even integer. Thus

$$\left(\frac{2}{2^n-1}\right) = (-1)^{\frac{(2^n-1)^2-1}{8}} = 1.$$

by applying (1.4). Thus 2^m-2 is a quadratic nonresidue modulo 2^n-1, using (1.5), since $-1 \equiv 2^m-2 \pmod{2^n-1}$. That implies also

$$\left(\frac{2^n-2^m-1}{2^n-1}\right) = \left(\frac{-2^m}{2^n-1}\right) = \left(\frac{-1}{2^n-1}\right)\left(\frac{2}{2^n-1}\right)^m = -1,$$

since $-2^m \equiv 2^n-2^m-1 \pmod{2^n-1}$. Thus 2^n-2^m-1 is a quadratic nonresidue modulo 2^n-1.

Secondly, since n is even, 3 divides 2^n-1. Now, 2 is a quadratic nonresidue modulo 3 that is $\left(\frac{2}{3}\right) = -1$ which implies that $\left(\frac{2^m}{3}\right) = (-1)^m = 1$ if and only if m is even. Therefore, according to the preceding result, if m is odd, 2^m is a quadratic nonresidue modulo 2^n-1. If m is even, 2^m is clearly a quadratic residue since $(2^{m/2})^2 \equiv 2^m$ modulo 2^n-1. Now, set

$$S_n = \{\ u \mid 1 \leq u \leq 2^n-2, \ u^2 \equiv 1 \pmod{2^n-1}\ \}. \tag{1.7}$$

Note that the map $k \mapsto 2^{m/2}k$ is a one-to-one map from the set S_n of all square roots of 1 modulo 2^n-1 to the set of all square roots of 2^m modulo 2^n-1. □

Theorem 1.3. *Consider the Dickson polynomials D_k, $1 \leq k \leq 2^n-1$, $n=2m$ with $m \geq 2$. Let S_n be defined by (1.7). Then D_k is an involution on $\mathbb{F}_{2^m}$ if and only if*

- *$k \in S_n$, when m is odd;*
- *$k \in S_n \cup 2^{m/2}S_n$ if m is even.*

Proof. We will always consider $D_k(x) \pmod{x^{2^m}+x}$. This polynomial induces an involution if and only if

$$D_k \circ D_k(x) = D_{k^2}(x) = x, \quad \text{for all } x \in \mathbb{F}_{2^m}.$$

From Corollary 1.1, this is to say that $k^2 \in \{\ 1,\ 2^m,\ 2^n-2^m-1,\ 2^n-2\ \}$ where k^2 is computed modulo 2^n-1. According to Lemma 1.2, that is equivalent to $k \in S_n$ if m is odd and $k \in S_n \cup 2^{m/2}S_n$ if m is even. □

Remark 1.1. For all $u \in S_n$, $u^2 \equiv 1 \pmod{2^n-1}$ implies $\gcd(u, 2^n-1) = 1$. Therefore, we have, for even m, $\gcd(2^{m/2}u, 2^n-1) = 1$. This is to say that the hypothesis $\gcd(k, 2^n-1) = 1$ is not necessary in the previous theorem.

1.4 The set of Dickson involutions

We consider involutions of $\mathbb{F}_{2^m}$ and $n=2m$ in all this section. There are some immediate observations. Let S_n be defined by (1.7) and

$$K_n = \{\ 1,\ 2^m,\ 2^n-2^m-1,\ 2^n-2\ \} \equiv \{\pm 1, \pm 2^m\} \pmod{2^n-1}$$

Note that K_n is a multiplicative subgroup of S_n. Define an equivalence relation over S_n:

$$s_1 \sim s_2 \quad \text{if and only if} \quad \frac{s_1}{s_2} \in K_n. \tag{1.8}$$

Lemma 1.3. *Denote by $\sigma(s)$ the class of $s \in S_n$, according to the relation (1.8). Then $\sigma(s) = \{s, -s, 2^m s, -2^m s\}$ and we have*

$$D_t(x) \equiv D_s(x) \pmod{x^{2^m}+x}, \quad \textit{for any } t \in \sigma(s).$$

Proof. One simply observe that if s and t belong to the same class then D_s and D_t induce the same permutation on $\mathbb{F}_{2^m}$. Indeed, in this case there exists $k \in K_n$ such that $t = ks$. Therefore, according to Corollary 1.1 and to Proposition 1.1, we have for all $x \in \mathbb{F}_{2^m}$

$$D_t(x) = D_{sk}(x) = D_s \circ D_k(x) = D_s \circ D_1(x) = D_s(x) \pmod{x^{2^m} + x}.$$

□

Hence each class different from the class of 1 leads to a different non-trivial involution. We will give the exact number of such classes for a fixed n in the next subsection. The Dickson polynomials are closed with respect to composition of polynomials. Moreover the commutativity of integers imply that this composition is commutative. Thus for two non trivial involutions D_s and D_t of $\mathbb{F}_{2^m}$ we have

$$(D_s \circ D_t)^{-1} = D_t^{-1} \circ D_s^{-1} = D_t \circ D_s = D_{ts} = D_{st},$$

proving that D_{st} is an involution too. Now, if s and t are in the same class then $D_{st} = D_{s^2}$, from Lemma 1.3, where s is a square root of 1 so that $D_{st}(x) \equiv x \pmod{x^{2^m} + x}$. Now suppose that $t \notin \sigma(s)$. If m is even and $t \in \sigma(2^{m/2}s)$ then $D_{st} = (D_{s^2})^{2^{m/2}}$ so that $D_{st}(x) \equiv x^{m/2} \pmod{x^{2^m} + x}$. Otherwise, in other cases, there are more than 4 classes and $st \pmod{2^n - 1} = r$ where r is not in the classes $\{s, t, 2^{m/2}, 2^{m/2}s\}$ (see Example 1.2 later). We summarize these results with the next lemma.

Lemma 1.4. *If D_s and D_t are two Dickson involutions of $\mathbb{F}_{2^m}$ then $D_s \circ D_t = D_{st}$ is an involution too. Moreover:*

- *If $t \in \sigma(s)$ then $st \pmod{2^n - 1} \in \sigma(1)$.*
- *If $t = 2^{m/2}$ (m even) then $st \in \sigma(2^{m/2}s)$.*
- *If $t \in \sigma(2^{m/2}s)$ (m even) then $st \pmod{2^n - 1} \in \sigma(2^{m/2})$.*
- *Otherwise, and assuming that s, t are two representatives of non trivial classes we get $st \pmod{2^n - 1} = r$ where r is in another nontrivial class.*

Remark 1.2. Note that the three first assertions are in fact equivalences since $st \in \sigma(u)$ is equivalent to $t \in \sigma(us^{-1}) \pmod{2^n - 1} = \sigma(us)$ (s being a quadratic residue of 1 modulo $2^n - 1$, its inverse modulo $2^n - 1$ is itself).

Example 1.1. n=6, m=3: $K_6 = \{1, 8, 55, 62\} = S_6$. For any $k \in K_6$, $D_k(x) = x$ modulo $(x^8 + x)$. For example

$$D_{55}(x) = x+x^{33}+x^9+x^{41}+x^{49}+x^5+x^{37}+x^{53}+x^7+x^{39}+x^{55} \equiv x \pmod{x^8+x}.$$

n=8, m=4:
$K_8 = \{1, 16, 239, 254\}$ while $S_8 = \{1, 16, 86, 101, 154, 169, 239, 254\}$. Note that $-86 = 169$, $86 * 16 = 101$ and $86 * (-16) = 154$. Here the non trivial involutions are the $D_k(x) \pmod{x^{16} + x}$ with k in $(S_8 \cup 4S_8) \setminus K_8$. Thus, according to (1.8), we get three such D_k which are the representatives of the three classes:

$$k \in \{4, 64, 191, 251\} \cup \{86, 101, 154, 169\} \cup \{89, 149, 106, 166\}$$

For instance

$$D_4(x) = x^4 \pmod{x^{16} + x}$$

$$\begin{aligned} D_{86}(x) &= x^2 + x^6 + x^{10} + x^{18} + x^{22} + x^{34} + x^{38} + x^{42} + x^{86} + x^{74} + x^{82} + x^{66} + x^{70} \\ &= x^2 + x^3 + x^4 + x^8 + x^{12} + x^{11} + x^{14} \pmod{x^{16} + x}. \end{aligned}$$

while, with $89 \equiv 86 * 4 \pmod{255}$

$$D_{89}(x) = (D_{86}(x))^4 = x^2 + x^3 + x^{12} + x^8 + x^{11} + x + x^{14} \pmod{x^{16} + x}.$$

n=10, m=5: $K_{10} = \{1, 32, 991, 1022\}$ while

$$S_{10} = \{1, 32, 340, 373, 650, 683, 991, 1022\}$$

Here we have a unique non trivial involution over $\mathbb{F}_{2^5}$: D_{340}.

1.4.1 *The number of Dickson involutions*

We now compute the number of Dickson polynomials which induce involutions on $\mathbb{F}_{2^m}$. To this end, we begin with a technical result.

Lemma 1.5. *The number of quadratic residues of* 1 *modulo* $2^n - 1$ *is equal to* 2^τ *where* τ *is the number of the prime factors in the prime decomposition of* $2^n - 1$.

Proof. Given a positive integer p, let us denote $\rho(p)$ the number of square roots of unity modulo p, that is, the number of solutions of the congruence equation : $x^2 \equiv 1 \pmod{p}$. Let us show that

$$\rho(pq) = \rho(p)\rho(q), \quad \text{when } p \text{ and } q \text{ are coprime.} \tag{1.9}$$

To this end, note that according to Chinese's Theorem, $\mathbb{Z}/(pq)\mathbb{Z}$ is isomorphic to $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ via the isomorphism

$$\psi \ : \ x \in \mathbb{Z}/(pq)\mathbb{Z} \ \mapsto \ (x \pmod{p}, \ x \pmod{q}).$$

By construction, in $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$, $(a,b)^2 = (c,d)$ is equivalent to $a^2 = c$ and $b^2 = d$ so that $\psi(x^2) = (x^2 \pmod p,\ x^2 \pmod q)$, proving (1.9).

Now, one has $\rho(p^\alpha) = 2$ for any odd prime number p and positive integer α. Indeed, suppose that $x^2 \equiv 1 \pmod{p^\alpha}$. Then

$$x^2 - 1 = (x+1)(x-1) \equiv 0 \pmod{p^\alpha}.$$

and this is equivalent to

$$x + 1 \equiv 0 \pmod{p^\alpha} \text{ or } x - 1 \equiv 0 \pmod{p^\alpha},$$

that is $x \equiv \pm 1 \mod p^\alpha$. Since $2^n - 1$ is an odd number, we can write

$$2^n - 1 = \prod_{i=1}^{\tau} p_i^{\alpha_i}, \quad p_i \text{ is a prime factor,}$$

and the α_i's are positive integers. Then $\rho(2^n - 1) = \prod_{i=1}^{\tau} \rho(p_i^{\alpha_i}) = 2^\tau$. □

Then we have the following result on the number of Dickson polynomials that are involutions. Recall that for any such involution D_k there are four elements $k' \in \sigma(k)$ providing the same involution (see Lemma 1.3). Thus, the number of Dickson involutions is the number of such classes $\sigma(.)$. The class of 1 is said *trivial* since $D_1(x) = x$.

Theorem 1.4. *Let m be a positive integer such that $m > 1$ and set $n = 2m$. Let τ be the number of prime factors in the decomposition of $2^n - 1$. Then the number of (non trivial) Dickson polynomials over $\mathbb{F}_{2^m}$ which are involutions is equal to*

$$2^{\tau-2} - 1 \text{ if } m \text{ is odd and } 2^{\tau-1} - 1 \text{ if } m \text{ is even.}$$

Proof. Suppose that m is odd. According to Theorem 1.3, D_k is an involution if and only if $k \in S_n$, that is k is a quadratic residue of 1 modulo $2^n - 1$. The number of such k is equal to 2^τ by Lemma 1.5 . Now, according to (1.8) and Lemma 1.3, the number of pairwise different Dickson polynomial is equal to $2^\tau/4 = 2^{\tau-2}$ since K_n is of cardinality 4. Suppose that m is even. One can repeat again similar arguments as those of the odd case except that, in the even case, D_k is an involution if and only $k \in S \cup 2^{m/2}S$. It means that we have to replace 2^τ by $2^{\tau+1}$ in the preceding calculation. We then conclude by excluding the class of 1. □

Remark 1.3. When m is odd, non trivial Dickson involutions exist for $\tau > 2$. Since $n = 2m$, $2^n - 1 = (2^m - 1)(2^m + 1)$. If $2^m - 1$ is prime and $2^m + 1$ is a power of 3 then $\tau = 2$, implying that non trivial Dickson involutions do not exist. It is the case for $n = 4, 6$. We prove below that this never holds for $m > 3$.

Proposition 1.2. *Let τ be the number of Dickson involutions on $\mathbb{F}_{2^m}$. Then $\tau \geq 3$ for any $m > 3$, i.e., for any $m > 3$ non trivial Dickson involutions do exist.*

Proof. We assume that $m > 3$. When m is even we have

$$2^n - 1 = (2^m + 1)(2^{m/2} - 1)(2^{m/2} + 1)$$

implying $\tau \geq 3$. From now on m is odd. Thus 3 divides $2^m + 1$ and we have $2^m + 1 \equiv 3m \pmod 9$ because

$$\begin{aligned} 2^m + 1 &= (3-1)^m + 1 \\ &= 3^m + \binom{m}{1} 3^{m-1}(-1) + ... + \binom{m}{m-1} 3(-1)^{m-1}. \end{aligned}$$

If 3 does not divide m then $2^m + 1 = 3\ell$ where ℓ is coprime with 3 and with $2^m - 1$. In this case, we conclude that $2^n - 1$ has at least three prime divisors.

Now suppose that $m = 3^i p$, for some odd p which is coprime with 3. Then 9 divides $2^m + 1$. If $p > 1$ then $2^3 - 1$ and $2^p - 1$, which are coprime, both divide $2^m - 1$ providing at least three prime divisors of $2^n - 1$. If $p = 1$ then $i \geq 2$ so that $2^9 - 1$ divides $2^m - 1$. Since $2^9 = 17 \times 73$, we get again three prime divisors of $2^n - 1$. □

Example 1.2.

$n = 4, 6$ We seen above that $\tau = 2$. There is no Dickson polynomials which are involutions except $D_1(x) = x$.

$n = 8$, $m = 4$, $2^n - 1 = 255 = 17 \times 5 \times 3$, $\tau = 3$. The number of nontrivial Dickson polynomials which are involutions is equal to $2^{\tau-1} - 1 = 3$.

$n = 10$, $m = 5$, $2^n - 1 = 1023 = 31 \times 11 \times 3$, $\tau = 3$. The number of nontrivial Dickson polynomials which are involutions is equal to $2^{\tau-2} - 1 = 1$.

$n = 12$, $m = 6$, $2^n - 1 = 4095 = 3^2 \times 5 \times 7 \times 13$, $\tau = 4$. The number of Dickson polynomials which are involutions is equal to $2^{\tau-1} = 8$ if we include the trivial class $\sigma(1)$. A set of representatives of these classes is:

$$\{\ 1, 181, 1574, 1756\ \} \cup \{\ 8, 1448, 307, 1763\} \subset S_{12} \cup 8 * S_{12}.$$

Note that $181 * 1574 = -1756$ modulo 4095.

1.4.2 *Dickson involutions of very high degree*

Our previous results show that it is generally easy to get a Dickson involution on $\mathbb{F}_{2^m}$ by computation. However, for a very high m it could be difficult to obtain such involution which is neither trivial nor equal to $x^{m/2}$ (m even). Also, it could be convenient to have the use of specific k such that D_k is an involution which is not trivial. To explain that this is possible, we exhibit below several infinite class of Dickson involutions.

Theorem 1.5. *Let $n = 2m$, $m \geq 4$. Assume that $\gcd(m, 3) = 1$ and set $n = 3r + e$, $e \in \{1, 2\}$. Then the polynomial*

$$D_k(x) \pmod{x^{2^m} + x}, \quad \text{where } k = \begin{cases} (2^n - 1)/3 + 1 & \text{if } e = 2 \\ (2^n - 1)/3 - 1 & \text{if } e = 1 \end{cases},$$

is an involution of $\mathbb{F}_{2^m}$, such that $k \notin \sigma(1)$; moreover for even m, $k \notin \sigma(2^{m/2})$. Consequently, the Dickson monomial $D_k(x) = x^k$ is also an involution.

Proof. We first prove that $k^2 = 1$ modulo $2^n - 1$:

$$\begin{aligned} k^2 - 1 &= \left(\frac{2^n - 1}{3} \pm 1\right)^2 - 1 = \left(\frac{2^n - 1}{3}\right)^2 \pm \frac{2(2^n - 1)}{3} \\ &= (2^n - 1)\left(\frac{2^n - 1 \pm 6}{9}\right) \end{aligned}$$

with $2^n = 2^e(2^3 + 1 - 1)^r \equiv 2^e(-1)^r \pmod 9$. Let $a = 2^n - 1 \pm 6 \pmod 9$. We have to examine when a is zero modulo 9.

Note that, by hypothesis, $e \neq 0$ since a cannot be 0 modulo 9 when $e = 0$. When $e = 2$ (r even), we get $2^n \equiv 4 \pmod 9$; thus $a \in \{0, -3\}$. The value -3, obtained from $a \equiv 4 - 1 - 6 \pmod 9$ is not suitable. Hence, for $e = 2$ we take $a \equiv 4 - 1 + 6 \pmod 9$, that is $k = (2^n - 1)/3 + 1$. Similarly, if $e = 1$ (r odd) then $2^n \equiv -2 \pmod 9$ and $a \in \{3, 0\}$. In this case, only $k = (2^n - 1)/3 - 1$ is suitable.

Now, k is given by its binary expansion. With this representation, the *weight of k*, say $w(k)$, is the number of terms of this expression. Here we have $w(k) = m$ for $e = 1$ and $w(k) = m + 1$ for $e = 2$. Recall that the class of 1 is $K_n = \{\pm 1, \pm 2^m\}$. Clearly the corresponding weights are $\{1, n - 1\}$ and this holds for the class of $2^{m/2}$ too (for even m). This completes the proof. □

Example 1.3. The first pairs (n, k), obtained by Theorem 1.5 are: $(8, 86)$, $(10, 340)$, $(14, 5462)$ and $(16, 21844)$. According to Theorem 1.3, we have also $(8, 2^2 * 86)$, and $(16, 2^4 * 21844)$.

Theorem 1.6. *Let ℓ be any even integer ($\ell > 0$). Set $n = \ell(2^\ell + 1)$ and $m = n/2$. Then the polynomial*

$$D_k(x), \quad (\text{mod } x^{2^m} + x) \quad \textit{where } k = \sum_{i=1}^{2^\ell} 2^{i\ell},$$

is an involution of $\mathbb{F}_{2^m}$, such that $k \notin \sigma(1)$; moreover for even m, $k \notin \sigma(2^{m/2})$. Consequently, the Dickson monomial $D_k(x) = x^k$ is also an involution.

Proof. First, it is easy to prove that $k^2 = 1$ modulo $2^n - 1$, since

$$2^n - 1 = (2^\ell - 1)(2^{\ell 2^\ell} + 2^{\ell(2^\ell - 1)} + \cdots + 2^\ell + 1) = (2^\ell - 1)(k + 1).$$

Hence we have

$$\begin{aligned} k^2 - 1 &= \left(\frac{2^n - 1}{2^\ell - 1} - 1\right)^2 - 1 = \left(\frac{2^n - 1}{2^\ell - 1}\right)^2 - 2\frac{2^n - 1}{2^\ell - 1} \\ &= (2^n - 1)\left(\frac{2^n - 1 - 2(2^\ell - 1)}{(2^\ell - 1)^2}\right) = (2^n - 1)\left(\frac{k - 1}{2^\ell - 1}\right). \end{aligned}$$

But $k = \sum_{i=1}^{2^\ell} \left((2^\ell - 1) + 1\right)^i \equiv 1 \pmod{2^\ell - 1}$. Hence $2^n - 1$ divides $k^2 - 1$.

Now, k is given by its binary expansion. With this representation, the *weight of* k is $w(k) = 2^\ell = (n - \ell)/\ell$ where $\ell \geq 2$. As in the proof of Theorem 1.5, this completes the proof. □

Remark 1.4. The first value of n, in Theorem 1.6, is $n = 10$, for $\ell = 2$. In this case we check that $k = 340$, as explained in Example 1.1. This value is also obtained by Theorem 1.5 but the two classes are different. Note that in Theorem 1.6 the condition $\gcd(m, 3) = 1$ is not necessary.

1.5 Fixed points of the Dickson involutions

A *fixed point* of any polynomial $P(x)$ is an element ρ such that $P(\rho) = \rho$. In [14], an empirical study on the number of fixed points of involutions and general permutations were made. Permutations are important building blocks in block ciphers, and for a secure design purpose S-boxes are chosen with very good cryptographic properties. The observation in [14] was that the number of fixed points is correlated to the cryptographic properties like nonlinearity and the maximum XOR entry table. Precisely, lower is the number of fixed points better is the value of nonlinearity and the maximum XOR entry table. Thus the authors proposed to choose permutation S-boxes with a few fixed points.

1.5.1 *General description*

The number of fixed points of polynomials $D_k(x)$ on $\mathbb{F}_{2^m}$ is computed in [8] as a function of m and k. We give this result in our context with a sketch of proof.

Theorem 1.7. [8, Theorem 3.34] *Denote by $\mathcal{F}(k,m)$ the set of fixed points of the Dickson polynomial D_k (over $\mathbb{F}_{2^m}$). Then the cardinality of $\mathcal{F}(k,m)$ is*

$$|\mathcal{F}(k,m)| = \frac{1}{2}\left(\gcd(2^m+1,k+1) + \gcd(2^m-1,k+1) + \gcd(2^m+1,k-1) + \gcd(2^m-1,k-1)\right) - 1. \quad (1.10)$$

Sketch of Proof. According to Lemma 1.1, any $x \in \mathbb{F}_{2^m}$ can be written

$$x = \gamma + \frac{1}{\gamma},\ \gamma \in \mathbb{F}_{2^n}^*,\ \gamma^{2^m+1} = 1 \ \text{ or } \ \gamma^{2^m-1} = 1 \quad (1.11)$$

Thus $D_k(x) = D_k(\gamma+\gamma^{-1}) = \gamma^k + \gamma^{-k}$. Further, x is a fixed point of D_k if and only if

$$\gamma^k + \gamma^{-k} = \gamma + \gamma^{-1},\ \textit{i.e.},\ (\gamma^{k+1}-1)(\gamma^{k-1}-1) = 0.$$

Note that γ and γ^{-1} provide the same x. ◇

The proof of Theorem 1.7 gives explicitly the fixed points of D_k : x is written as in (1.11) and either $\gamma^{k-1} = 1$ or $\gamma^{k+1} = 1$. We can be more precise in the case where D_k is an involution. Set

$$\begin{aligned} r_1 &= \gcd(2^m-1,k-1),\ r_2 = \gcd(2^m-1,k+1), \\ s_1 &= \gcd(2^m+1,k-1),\ s_2 = \gcd(2^m+1,k+1). \end{aligned} \quad (1.12)$$

providing $|\mathcal{F}(k,m)| = (r_1+r_2+s_1+s_2)/2 - 1$. From Theorem 1.3 and its proof, we must distinguish two cases:

- $k \in S_n$ where we have $k^2 \equiv 1 \pmod{2^n-1}$, *i.e.*, 2^n-1 divides k^2-1;
- for even m, let $k \in 2^{m/2}S_n$; in this case, we have $k^2 = 2^m s^2$ where $s \in S_n$. Hence $k^2 \equiv 2^m \pmod{2^n-1}$ and then

$$k^2 - 1 = (k+1)(k-1) \equiv 2^m - 1 \pmod{2^n-1}.$$

These properties will be used respectively in Corollaries 1.2 and 1.3.

Corollary 1.2. *Consider any involution D_k on $\mathbb{F}_{2^m}$ as described by Theorem 1.3 with $k \in S_n$. We assume that D_k is not the identity modulo*

$(x^{2^m}+x)$, i.e., $k \notin \{\pm 1,\ \pm 2^m\}$. Let α be a primitive root of $\mathbb{F}_{2^n}$, $n=2m$. Then $2^m-1=r_1r_2$ and $2^m+1=s_1s_2$. Moreover $\mathcal{F}(k,m)$ is the set of $\gamma+\gamma^{-1}$ where

$$\gamma \in \left\{ \begin{array}{l} \alpha^{ir_2(2^m+1)},\ 0 \le i \le (r_1-1)/2,\ \alpha^{jr_1(2^m+1)},\ 0 \le j \le (r_2-1)/2 \\ \alpha^{\ell s_2(2^m-1)},\ 0 \le \ell \le (s_1-1)/2,\ \alpha^{ts_1(2^m-1)},\ 0 \le t \le (s_2-1)/2 \end{array} \right\}.$$

Proof. Since 2^n-1 divides k^2-1, we get directly from the definition (see (1.12)): $2^m-1=r_1r_2$, $2^m+1=s_1s_2$ and

$$\gcd(2^n-1,k-1)=r_1s_1,\ \ \gcd(2^n-1,k+1)=r_2s_2.$$

Now we have two cases:

- If $\gamma^{2^m-1}=1$ then $\gamma=\alpha^{u(2^m+1)}=\alpha^{us_1s_2}$ for some u. If $\gamma^{k-1}=1$ then $u=ir_2$, $0 \le i \le r_1-1$. If $\gamma^{k+1}=1$ then $u=jr_1$, $0 \le j \le r_2-1$.
- If $\gamma^{2^m+1}=1$ then $\gamma=\alpha^{u(2^m-1)}=\alpha^{ur_1r_2}$ for some u. If $\gamma^{k-1}=1$ then $u=\ell s_2$, $0 \le \ell \le s_1-1$. If $\gamma^{k+1}=1$ then $u=ts_1$, $0 \le t \le s_2-1$.

We observe that $\alpha^{(r_1-i)r_2s_1s_2}=\alpha^{-ir_2s_1s_2}$ and this holds for the three other kinds of α^e above, completing the proof. □

Remark 1.5. Define M_n, $n=2m$, the set of factors of 2^n-1,as follows:

$$M_n=\{p_i^{e_i} \mid i=1,\dots s\} \ \text{ with } \ 2^n-1=\prod_{i=1}^{s} p_i^{e_i},\ p_i \text{ is prime.}$$

Clearly, for any i, $p_i^{e_i}$ is a factor either of 2^m-1 or of 2^m+1. Such a factor divides either $k-1$ or $k+1$ when 2^n-1 divides k^2-1. Thus, all elements of M_n are involved in the computation of $|\mathcal{F}(k,m)|$ when $k \in S_n$.

Remark 1.6. It is to be noted that in Theorem 3.36 of [8], a lower bound on the number of fixed points of Dickson polynomials which are permutations has been given. For characteristic 2, this lower bound equals 2. Throughout our results it appears that such a lower bound is higher for Dickson involutions.

We now include the case where $k \in 2^{m/2}S_n$. We notably give a count of the fixed points of the Dickson involution D_k, $k \in \sigma(2^{m/2})$.

Corollary 1.3. *Let $n=2m$ where m is even. Consider any involution D_k on $\mathbb{F}_{2^m}$ such that $k \in 2^{\frac{m}{2}}S_n$. Then 2^m-1 divides k^2-1 and we have $2^m-1=r_1r_2$,*

$$s_1=s_2=1 \text{ so that } \ |\mathcal{F}(k,m)|=\frac{r_1+r_2}{2}.$$

In particular the cardinality of the set of fixed points of D_k, $k \in \sigma(2^{\frac{m}{2}})$, equals $2^{\frac{m}{2}}$.

Moreover, $\mathcal{F}(k,m)$ is the set of $\gamma + \gamma^{-1}$ where

$$\gamma \in \left\{ \alpha^{ir_2(2^m+1)},\ 0 \le i \le (r_1-1)/2 \right\} \cup \left\{ \alpha^{jr_1(2^m+1)},\ 0 \le j \le (r_2-1)/2 \right\}$$

(where α is a primitive root of $\mathbb{F}_{2^n}$ and s_i, r_i are given by (1.12)).

Proof. Recall that the number of fixed points of D_k is:

$$(r_1 + r_2 + s_1 + s_2)/2 - 1,$$

where r_1, r_2, s_1 and s_2 are from (1.12).

As noticed at the beginning of this section, $2^m - 1$ divides $k^2 - 1$ for $k \in 2^{\frac{m}{2}} S_n$. More precisely $k^2 \equiv 2^m \pmod{2^n - 1}$, *i.e.,*

$$(k-1)(k+1) = \ell(2^n - 1) + 2^m - 1, \text{ for some } \ell > 0.$$

Thus $\gcd(2^m+1, k^2-1) = \gcd(2^m+1, 2^m-1) = 1$, proving that $s_1 = s_2 = 1$. Since $\gcd(2^m - 1, k^2 - 1) = 2^m - 1$, $2^m - 1 = r_1 r_2$. Further

$$|\mathcal{F}(k,m)| = (r_1 + r_2 + 2)/2 - 1 = (r_1 + r_2)/2.$$

If $k \in \sigma(2^{\frac{m}{2}})$ then $k = 2^{\frac{m}{2}} s$ with $s \in K_n$ (see Lemma 1.3). Note $\mathcal{F}(k,m) = \mathcal{F}(k',m)$ for any element of $k' \in \sigma(k)$. Thus, we can assume that $k = 2^{\frac{m}{2}}$. Since $k^2 - 1 = 2^m - 1$, we have directly $r_1 = 2^{\frac{m}{2}} - 1$ and $r_2 = 2^{\frac{m}{2}} + 1$. Then

$$|\mathcal{F}(2^{\frac{m}{2}}, m)| = \frac{2^{\frac{m}{2}} - 1 + 2^{\frac{m}{2}} + 1}{2} = 2^{\frac{m}{2}}.$$

To compute the set $\mathcal{F}(k,m)$ we proceed as previously, for Corollary 1.2:

- If $\gamma^{2^m-1} = 1$ then $\gamma = \alpha^{u(2^m+1)}$ for some u. If $\gamma^{k-1} = 1$ then $u = ir_2$, $0 \le i \le r_1 - 1$. If $\gamma^{k+1} = 1$ then $u = jr_1$, $0 \le j \le r_2 - 1$.
- If $\gamma^{2^m+1} = 1$ then $\gamma = \alpha^{u(2^m-1)}$ for some u. But $\gcd(k^2 - 1, 2^m + 1) = 1$ implies that $\gamma^{k-1} = 1$ (resp. $\gamma^{k+1} = 1$) if and only if $2^m + 1$ divides u. Thus $\gamma = \alpha^{(2^m+1)(2^m-1)} = 1$.

□

Example 1.4. Let $n = 12$ and $k = 181$. We have

$$N = 2^{12} - 1 = 63 \times 65 = (9 \times 7) \times (5 \times 13) \text{ and}$$

$$180 = 4 \times 5 \times 9, \quad 182 = 2 \times 7 \times 13.$$

With notation of Corollary 1.2, $r_1 = 9$, $r_2 = 7$, $s_1 = 5$ and $s_2 = 13$. Thus the cardinality of $\mathcal{F}(181, 12)$ equals $(7 + 13 + 9 + 5)/2 - 1 = 16$. and, α being a primitive root of $\mathbb{F}_{2^{12}}$,

$$\mathcal{F}(181,12) = \left\{ \alpha^d + \alpha^{-d},\ d \in \left\{ 0, \frac{N}{9}, \ldots, \frac{4N}{9}, \frac{N}{7}, \ldots, \frac{3N}{7}, \frac{N}{5}, \frac{2N}{5}, \frac{N}{13}, \ldots, \frac{6N}{13} \right\} \right\}.$$

Now we take $k = 2^3 \times 181 \equiv 1448 \pmod{2^{12} - 1}$. We have $2^6 - 1 = r_1 r_2$ with $r_1 = 1$ and $r_2 = 63$. Moreover $s_1 = s_2 = 1$. Then the cardinality of $\mathcal{F}(1448, 12)$ equals $64/2 = 32$. According to Corollary 1.3, we have

$$\mathcal{F}(1448,12) = \left\{ \alpha^d + \alpha^{-d},\ d \in \{0, 65, 2 * 65, \ldots, 31 * 65\} \right\}.$$

1.5.2 *Bounds on the number of fixed points*

Below we give the proof that for even m, the minimum value of $|\mathcal{F}(k, m)|$ is $2^{\frac{m}{2}}$.

Theorem 1.8. *Let I be the index set such that for all $k \in I$, D_k is an involution on $\mathbb{F}_{2^m}$. Then for even m,*

$$\min_{k \in I} |\mathcal{F}(k, m)| = |\mathcal{F}(2^{\frac{m}{2}}, m)| = 2^{\frac{m}{2}}.$$

Proof. Let $n = 2m$. Since m is even, $k \in S_n$ or $k \in 2^{\frac{m}{2}} S_n$. We treat the proof in two cases.

Case 1: $k \in 2^{\frac{m}{2}} S_n$.

Following Corollary 1.3, the minimum value of $|\mathcal{F}(k, m)|$ is the minimum value that $(r_1 + r_2)/2$ can have with the constraint $r_1 r_2 = 2^m - 1$. So now we have to deal with an optimization problem. To deal with this we consider the following related optimization problem over positive real numbers.

Minimize $f(x, y) = x + y$

Subject to :

$$xy = 2^m - 1,$$

where x, y are positive real numbers.

Using *Lagrange multiplier method* [1, Section 3.1.3], we get that the minimum value of $f(x, y)$ is $2\sqrt{2^m - 1}$ which is obtained at $x = \sqrt{2^m - 1}$ and $y = \sqrt{2^m - 1}$.

So if r_1 and r_2 were real numbers then the minimum value of $(r_1 + r_2)$ would have been $2\sqrt{2^m - 1}$. Note that the closest integer to $\sqrt{2^m - 1}$ is $2^{\frac{m}{2}}$ and $2 \cdot 2^{\frac{m}{2}} = (2^{\frac{m}{2}} + 1) + (2^{\frac{m}{2}} - 1)$. If $k = 2^{\frac{m}{2}}$, then $r_1 = 2^{\frac{m}{2}} + 1$ and $r_2 = 2^{\frac{m}{2}} - 1$ for which $r_1 r_2 = 2^m - 1$, and hence the minimum value of $(r_1 + r_2)/2$ is $2^{\frac{m}{2}}$.

Case 2: $k \in S_n$.
In this case $k^2-1 \equiv 0 \pmod{2^n-1}$. Therefore, $2^m-1 = r_1r_2$ and $2^m+1 = s_1s_2$. Now we have to consider the optimization problem:

Minimize $(r_1 + r_2 + s_1 + s_2)/2 - 1$

Subject to :

$$r_1r_2 = 2^m - 1,$$
$$s_1s_2 = 2^m + 1.$$

More precisely, we need to minimize the value (r_1+r_2) subject to $r_1r_2 = 2^m - 1$, and $(s_1 + s_2)$ subject to $s_1s_2 = 2^m + 1$. It is clear that one of s_1 and s_2 is greater than 1, *i.e.,* $(s_1 + s_2) > 2$. We already have seen in the previous case that the minimum value of $r_1 + r_2$ is $2 \cdot 2^{\frac{m}{2}}$. Therefore, the minimum value of $(r_1 + r_2 + s_1 + s_2)/2 - 1$ is greater than $2^{\frac{m}{2}}$.

Thus from the two cases the proof is clear. □

For odd m, the exact minimum value of $|\mathcal{F}(k, m)|$ is not clear. However, we can derive a lower bound on the minimum value of $|\mathcal{F}(k, m)|$ that we present below. Note that if m is odd, then $3|(2^m + 1)$.

Theorem 1.9. *Let I be the index set such that for all $k \in I$, D_k is an involution on $\mathbb{F}_{2^m}$, where m is odd. Then*

(1) $\min_{k\in I} |\mathcal{F}(k, m)| > 2^{m-1} + \lceil\sqrt{2^m + 1}\rceil - 1$, *when $2^m - 1$ is prime,*
(2) $\min_{k\in I} |\mathcal{F}(k, m)| > \lceil(\sqrt{2^m - 1} + \sqrt{2^m + 1})\rceil - 1$, *when $2^m - 1$ is composite,*

Proof. Since m is odd, $k \in S_n$. Consider r_1, r_2, s_1, s_2 as they are given in (1.12). Since 2^n-1 divides k^2-1, we have $r_1r_2 = 2^m-1$ and $s_1s_2 = 2^m+1$. To find the minimum value of $|\mathcal{F}(k, m)|$, we need to minimize the value of $(r_1 + r_2 + s_1 + s_2)/2 - 1$ subject to the constraints $r_1r_2 = 2^m - 1$ and $s_1s_2 = 2^m+1$. Note that we can consider this optimization problem over the set of real numbers, that will give us a lower bound of the minimum value of $(r_1+r_2+s_1+s_2)/2-1$ Therefore we consider the following optimization problem:

Minimize $(r_1 + r_2 + s_1 + s_2)/2 - 1$

Subject to :

$$r_1r_2 = 2^m - 1,$$
$$s_1s_2 = 2^m + 1.$$

First we prove *(i)*, i.e., when $2^m - 1$ is prime. In this case, $r_1 + r_2 = 2^m$. If s_1 and s_2 were real valued, the minimum of $s_1 + s_2$ would have

been $2\sqrt{2^m+1}$ (using the Lagrange Multiplier method), and the minimum value of $(r_1+r_2+s_1+s_2)/2-1$ would be $2^{m-1}+\sqrt{2^m+1}-1$. Since r_1, r_2, s_1, s_2 are all integers, thus the actual minimum value is greater than $2^{m-1}+\lceil\sqrt{2^m+1}\rceil-1$.

For *(ii)*, we have that 2^m-1 is composite. Then considering all of r_1, r_2, s_1, s_2 as real numbers, and using the Lagrange Multiplier method, we get the minimum value of $(r_1+r_2+s_1+s_2)/2-1$ is $\sqrt{2^m-1}+\sqrt{2^m+1}-1$. Since r_1, r_2, s_1, s_2 are all integers, we have that the actual minimum value is greater than $\lceil(\sqrt{2^m-1}+\sqrt{2^m+1})\rceil-1$. □

Remark 1.7. Theorem 1.8 and 1.9 clearly says that the Dickson involutions $D_k(x)$ have high number of fixed points jeopardizing their use as S-boxes in block ciphers. However the structure of the set of fixed points is of interest allowing to have easy methods to reduce its size. A special example is studied in the next section.

Let us see how good these bounds are. In Table 1.1, we compare the lower bound obtained in Theorem 1.9 and the exact minimum value of $|\mathcal{F}(k,m)|$ for some odd m.

m	Lower bound of $\lvert\mathcal{F}(k,m)\rvert$ from Theorem 1.9	Exact minimum value of $\lvert\mathcal{F}(k,m)\rvert$
5	21	22
7	75	86
9	45	62
11	90	398

1.5.3 *Minimal sets of fixed points*

In this section m is even and we consider Dickson involutions D_k over $\mathbb{F}_{2^n}$ such that $k \in 2^{m/2}S_n$ where S_n, defined by (1.7), is the set of $1 \le u \le 2^n-2$ such that $u^2 \equiv 1 \pmod{2^n-1}$. From Theorem 1.8, we know that the minimal size of $\mathcal{F}(k,m)$ is $2^{m/2}$. It is exactly $2^{m/2}$ for those $k \in \sigma(2^{\frac{m}{2}})$ and we will point out that other k satisfy this property. We study these special cases now. And first we have to precise that in this case the set $\mathcal{F}(k,m)$ is the subfield of order $2^{\frac{m}{2}}$.

Proposition 1.3. *Let $n=2m=4t$ and k is such that D_k is an involution.*

Then $|\mathcal{F}(k,m)| = 2^t$ *if and only if* $k = 2^t s$ *with* $s^2 \equiv 1 \pmod{2^n - 1}$ *and either (i) or (ii) holds:*

(i) $r_1 = 2^t - 1$ *and* $r_2 = 2^t + 1$ *;*
(ii) $r_1 = 2^t + 1$ *and* $r_2 = 2^t - 1$*,*

where r_1, r_2 *are as given in (1.12).*

Proof. It is clear that if $k = 2^t s$ and (i) or (ii) holds, then

$$|\mathcal{F}(k,m)| = \frac{r_1 + r_2}{2} = 2^t.$$

Next assume that $|\mathcal{F}(k,m)| = 2^t$. From Case 2 of Theorem 1.8, we get that if $k \in S_n$, then $|\mathcal{F}(k,m)| > 2^t$. Therefore, it is necessary to have $k = 2^t s$, where $s \in S_n$. Moreover, from Corollary 1.3 we have $r_1 r_2 = 2^m - 1$ and $r_1 + r_2 = 2^{t+1}$. Thus r_1 and r_2 are the integer roots of the equation

$$X^2 - 2^{t+1}X + 2^m - 1 = 0 \iff (X - 2^t)^2 = 1$$

Hence $(r_1, r_2) = (2^t - 1, 2^t + 1)$ or $(r_1, r_2) = (2^t + 1, 2^t - 1)$, completing the proof. □

Remark 1.8. We could give a more general result following Corollary 1.3 by studying the roots of $X^2 + 2EX + 2^m - 1 = 0$, where $E = |\mathcal{F}(k,m)|$. One can say that E is suitable if and only if $D = E^2 - (2^m - 1)$ is a square. If it is we get r_1 and r_2. Further, the problem is to know if such k exists.

Lemma 1.6. *Let* $n = 2m = 4t$*,* $k = 2^t s$ *with* $s^2 \equiv 1 \pmod{2^n - 1}$*.*
Then $\mathcal{F}(k,m) = \mathbb{F}_{2^t}$ *if and only if either (i) or (ii) (of Proposition 1.3) holds.*

Proof. We apply Corollary 1.3 assuming that (i) holds. Let $x = \gamma + \gamma^{-1}$ be a fixed point of D_k. Note that $\gamma^{2^m - 1} = 1$ which means $\gamma \in \mathbb{F}_{2^m}$. The cardinality of $\mathcal{F}(k,m)$ is

$$\frac{r_1 + r_2}{2} = \frac{2^t + 1 + 2^t - 1}{2} = 2^t.$$

If $\gamma = \alpha^{ir_2(2^m+1)}$ then $\gamma^{2^t - 1} = 1$ so that $\gamma \in \mathbb{F}_{2^t}$. If $\gamma = \alpha^{jr_1(2^m+1)}$ then $\gamma^{2^t+1} = 1$ so that $\gamma^{-1} = \gamma^{2^t}$. Hence $\gamma \mapsto \gamma + \gamma^{-1}$ is a function from $\mathbb{F}_{2^m}$ to $\in \mathbb{F}_{2^t}$. Thus in both cases we have $x \in \mathbb{F}_{2^t}$. The proof is completed since $|\mathcal{F}(k,m)| = 2^t$. The proof assuming that (ii) holds is similar, by exchanging r_1 and r_2.

Conversely, if $\mathcal{F}(k,m) = \mathbb{F}_{2^t}$ then $|\mathcal{F}(k,m)| = 2^t$ and we apply Proposition 1.3. □

Now, considering $k = 2^t s$ we want to identify those s such that D_k is an involution with fixed points set $\mathbb{F}_{2^t}$. In the following we avoid the trivial cases $s \in \sigma(1)$. The case $k = 2^t$ was treated before (Corollary 1.3).

Theorem 1.10. *Let $n = 2m = 4t$. Let $k \equiv 2^t s \pmod{2^n - 1}$, $s \notin \sigma(1)$. Then $s^2 \equiv 1 \pmod{2^n - 1}$ and $\mathcal{F}(k, m) = \mathbb{F}_{2^t}$ if and only if either (a) or (b) holds:*

(a) *$s - 1 = (2^m - 1)L$ where $0 < L < 2^m$ and $L^2 - L \equiv 0 \pmod{2^m + 1}$;*
(b) *$s + 1 = (2^m - 1)L$ where $0 < L < 2^m$ and $L^2 + L \equiv 0 \pmod{2^m + 1}$.*

Moreover if s satisfies (a) then there is $s' \in \sigma(s)$ which satisfies (b) and vice versa.

Proof. Assume that (a) holds. Then $s + 1 = (2^m - 1)L + 2$ and

$$s^2 - 1 = (2^m - 1)L(s + 1),$$

where

$$\begin{aligned} L(s+1) &= L^2(2^m - 1) + 2L = L^2(2^m + 1 - 2) + 2L \\ &\equiv -2(L^2 - L) \equiv 0 \pmod{2^m + 1}. \end{aligned} \tag{1.13}$$

Therefore $s^2 \equiv 1 \pmod{2^n - 1}$. Also, we have

$$k - 1 = 2^t(2^m - 1)L + 2^t - 1 \equiv 2^t - 1 \pmod{2^m - 1}$$

and

$$k + 1 = 2^t(2^m - 1)L + 2^t + 1 \equiv 2^t + 1 \pmod{2^m - 1},$$

that is, we are in the case (i) of Proposition 1.3. Thus $\mathcal{F}(k, m) = \mathbb{F}_{2^t}$ from Lemma 1.6. Similarly, if (b) holds then $s - 1 = (2^m - 1)L - 2$ and

$$L((2^m - 1)L - 2) = L^2(2^m + 1 - 2) - 2L \equiv -2(L^2 + L) \pmod{2^m + 1}.$$

We prove Proposition 1.3),(ii), by computing $k \pm 1$ using $s = (2^m - 1)L - 1$. To conclude this part of proof, note that if s satisfies (a) then

$$(-s) + 1 = -((2^m - 1)L + 1) + 1 = (2^m - 1)R \text{ where } R = (-L).$$

Then $R^2 + R = L^2 - L \equiv 0 \pmod{2^m + 1}$ showing that $-s$ (which is in $\sigma(s)$) satisfies (b).

Conversely, assume that $s^2 \equiv 1 \pmod{2^n - 1}$ and $\mathcal{F}(k, m) = \mathbb{F}_{2^t}$. From Lemma 1.6, either (i) or (ii) holds. Assume that (i) holds; so $r_1 = \gcd(2^m - 1, k - 1) = 2^t - 1$. This implies

$$k - 1 = 2^t s - 1 = (2^t - 1)s + (s - 1) \text{ where } (2^t - 1) \text{ divides } s - 1.$$

Similarly, $k+1 = (2^t+1)s - (s-1)$ where (2^t+1) divides $s-1$, since $r_2 = \gcd(2^m-1, k+1) = 2^t+1$. Hence 2^m-1 divides $s-1$. Moreover we have $s-1 < 2^n-2$. Then $s-1 = (2^m-1)L$ where $L < 2^m$. Now we have $L(s+1) \equiv 0 \pmod{2^m+1}$, because $s^2-1 = (2^m-1)L(s+1)$. This implies $L^2 - L \equiv 0 \pmod{2^m+1}$, since as shows (1.13) $L(s+1) \equiv -2(L^2-L) \pmod{2^m+1}$. The proof is similar (symmetric) if we suppose that (ii) holds. □

Remark 1.9. By Theorem 1.10 we have a partial characterization of those $k \in 2^t S_n$ whose set of fixed points equals 2^t. Clearly we have a good algorithm by computing $(2^m-1)L$ such that

$$L^2 \pm L - R(2^m+1) = 0, \quad \text{has integer solutions } L.$$

If there are solutions, one is negative and then is not suitable. The main question is : for which R the integer $1 + 4R(2^m+1)$ is a square?

Example 1.5. We give here the (non trivial) involutions D_k which are such that $k \in 2^t S_n$ and $\mathcal{F}(k,m) = \mathbb{F}_{2^t}$ $(m = 2t)$, for $m \leq 14$. For $2 \leq t \leq 6$ we found zero or one such k:

n=12, t=3: $k = 307 = 2^3 s$ where $s+1 = 1574+1 = 63*25$.
n=20, t=5: $k = 51118 = 2^5 s$ where $s+1 = (2^{10}-1)*450$.
n=24, t=6: $k = 6908201 = 2^6 s$ where $s+1 = (2^{12}-1)*1445$.

For $n = 28$ we found three classes whose representatives are $k = 2^7 s$ where $s = (2^{14}-1)L+1$, $L \in \{1131, 6555, 7685\}$.

Several observations arise, since our numerical results.

If 2^m+1 is prime then 2^m+1 must divide L or $s+1$ (resp. $s-1$) which is impossible unless $s = 2^m$. Indeed $L < 2^m$ and $s+1 = (2^m-1)L+2$ in case (a) (resp. $s-1 = (2^m-1)L-2$ in case (b)). When $s+1 \equiv -2L+2 \pmod{2^m+1}$ 2^m+1 divides $s+1$ only if $L = 1$, that is $s = 2^m$. Respectively $s-1 \equiv -2L-2 \pmod{2^m+1}$ and 2^m+1 cannot divide $s-1$. This explains why we have no result for $m = 4$ and $m = 8$, two cases where 2^m+1 is prime.

Proposition 1.4. *Let $n = 2m = 4t$. If D_k is such that $\mathcal{F}(k,m) = \mathbb{F}_{2^t}$, $k = 2^t s$ with $s \in S_n$, then $|\mathcal{F}(s,m)| > 2^{m-1}$.*

Proof. Recall that r_i and s_i, $i = 1, 2$, are given by (1.12), replacing k by s. From Theorem 1.10, we have either $r_1 = 2^m-1$ or $r_2 = 2^m-1$ and,

respectively, $r_2 = 1$ or $r_1 = 1$. According to Theorem 1.7 and Corollary 1.2, we get

$$|\mathcal{F}(s,m)| = \frac{(2^m-1)+1}{2} + \frac{s_1+s_2}{2} - 1 = 2^{m-1} + \frac{s_1+s_2}{2} - 1$$

where $s_1 s_2 = 2^m + 1$. □

1.6 Numerical results

In Table 1.6, we present some numerical results related to number of equivalence classes of Dickson involutions and the respective number of fixed points. Notation is as follows: m is the dimension of the field, $\mathcal{N}_m$ is the total number of Dickson involutions over $\mathbb{F}_{2^m}$, k is such that D_k is a Dickson involution on $\mathbb{F}_{2^m}$, where k represents one equivalence class as described in (1.8), and $|\mathcal{F}(k,m)|$ is the corresponding number of fixed points.

From Table 1.6, note that for odd m, the minimum value of $|\mathcal{F}(k,m)|$ is much larger than $2^{\frac{m}{2}}$, considering $2^{\frac{m}{2}}$ as a real value.

m	$\mathcal{N}_m$	k	$\lvert\mathcal{F}(k,m)\rvert$	m	$\mathcal{N}_m$	k	$\lvert\mathcal{F}(k,m)\rvert$
4	16	1	16	7	8	1	128
		4	4			5333	86
		86	12				
		89	8				
5	8	1	32				
		340	22				
6	32	1	64	8	32	1	256
		8	8			16	16
		181	16			9011	44
		307	8			12851	156
		1448	32			17749	28
		1574	40			21589	172
		1756	40			30584	144
		1763	32			30599	128

Table 1.6 - Dickson involutions of 1st kind over $\mathbb{F}_{2^m}$, $4 \le m \le 8$, and their fixed points.

Some Dickson involutions. We do not give the polynomials D_k where k is in the classes of 1 and of $2^{m/2}$. Polynomials are given modulo $(x^{2^m}+x)$. Involutions on $\mathbb{F}_{2^m}$ for $m = 3, 4$ are given in Example 1.1. Recall that $D_{2^{m/2}s}(x) = (D_s(x))^{2^{m/2}}$ where we compute only D_s. When $m = 5$ we

have only one non trivial involution:

$$D_{340}(x) = x^4 + x^5 + x^6 + x^8 + x^9 + x^{16} + x^{17} + x^{21} + x^{24} + x^{28} + x^{30}.$$

Let $m = 6$. We have $\{181, 1574, 1756\}$ from S_{12} and $\{1448, 307, 1763\}$ in $2^3 S_{12}$, respectively.

$$\begin{aligned} D_{181}(x) &= x + x^2 + x^4 + x^6 + x^7 + x^9 + x^{10} + x^{12} + x^{13} + x^{33} + x^{39} \\ &\quad + x^{41} + x^{45} + x^{49} + x^{55}. \\ D_{1574}(x) &= x^2 + x^8 + x^9 + x^{10} + x^{12} + x^{13} + x^{32} + x^{33} + x^{41} + x^{45} \\ &\quad + x^{48} + x^{49} + x^{56} + x^{60} + x^{62}. \\ D_{1756}(x) &= x^4 + x^6 + x^7 + x^8 + x^{32} + x^{39} + x^{48} + x^{55} + x^{56} + x^{60} + x^{62}. \end{aligned}$$

For $m = 7$ we have only one non trivial involution:

$$\begin{aligned} D_{5333}(x) &= x + x^2 + x^3 + x^4 + x^8 + x^{10} + x^{11} + x^{16} + x^{18} + x^{19} + x^{20} + x^{32} \\ &\quad + x^{34} + x^{35} + x^{36} + x^{40} + x^{42} + x^{43} + x^{64} + x^{67} + x^{75} + x^{83} + x^{96} \\ &\quad + x^{112} + x^{120} + x^{124} + x^{126}. \end{aligned}$$

1.7 Conclusion

In this paper we have characterized Dickson polynomials of the first kind, with the constant $a = 1$, that are involutions. We studied some properties of Dickson involutions over $\mathbb{F}_{2^m}$, for a fixed m, trying to have a clear description of this corpus. In particular, we show that its size increases with the number of prime divisors of $2^n - 1$. We have studied the set of fixed points and noticed that the number of fixed points of a Dickson involution is generally *high*. Nevertheless, we have obtained a precise description of such points. In particular, we have described the set of Dickson involutions whose set of fixed point is $\mathbb{F}_{2^t}$ ($t = \frac{n}{4}$). Removing many of those fixed points in such a way that keeps the involution property intact will give involution with a few fixed points. Actually, several techniques exist to reduce the number of fixed points [3, 4].

Acknowledgment

The third author did this work while he was at the Centre of Excellence in Cryptology at Indian Statistical Institute, Kolkata.

Bibliography

[1] D. P. Bertsekas. Nonlinear Programming (Second ed.), 1999, Cambridge, MA.: Athena Scientific.

[2] P. Charpin and G. Gong. Hyperbent functions, Kloosterman sums and Dickson polynomials. *IEEE Transactions on Information Theory*, Vol. 54, No. 9, pages 4230-4238, September 2008.

[3] P. Charpin, S. Mesnager and S. Sarkar. On involutions of finite fields, *Proceedings of 2015 IEEE International Symposium on Information Theory, ISIT 2015*, Hong-Kong, 2015.

[4] P. Charpin, S. Mesnager and S. Sarkar. Involutions over the Galois field $\mathbb{F}_{2^n}$, *IEEE Transactions on Information Theory*. To appear, 2016.

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

[6] J. F. Dillon and H. Dobbertin. New cyclic difference sets with Singer parameters. *Finite Fields and their Applications*, vol. 10, n. 3, pages 342-389, 2004.

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

[8] R. Lidl, G.L. Mullen and G. Turnwald, *Dickson Polynomials*, Pitman Monographs in Pure and Applied Mathematics, Vol. 65, Addison-Wesley, Reading, MA 1993.

[9] S. Mesnager, Bent and Hyper-bent functions in polynomial form and their link with some exponential sums and Dickson Polynomials. *IEEE Transactions on Information Theory*, Vol 57, No 9, pages 5996-6009, 2011.

[10] S. Mesnager, Semi-bent functions from Dillon and Niho exponents, Kloosterman sums and Dickson polynomials. *IEEE Transactions on Information Theory*, Vol 57, No 11, pages 7443-7458, 2011.

[11] I.M. Rubio, G.L. Mullen, C. Corrada and F. N. Castro, Dickson permutation polynomials that decompose in cycles of the same length, *Finite fields and applications*, 229239, *Contemp. Math.*, 461, Amer. Math. Soc., Providence, RI, 2008.

[12] A. Sakzad, M.-R. Sadeghi and D. Panario, Cycle structure of permutation

functions over finite fields and their applications, *Advances in Math. Communications* 6, 2012.

[13] G. Wu, N. Li, T. Helleseth and Y. Zhang, Some classes of monomial complete permutation polynomials over finite fields of characteristic two, *Finite Fields and Their Applications*, Volume 28, July 2014, Pages 148-165.

[14] A.M. Youssef, S.E. Tavares and H.M. Heys, A new class of substitution-permutation networks, Proceedings of *selected Areas in Cryptography, SAC-96*, pp 132-147.