ON IRREDUCIBLE BINARY POLYNOMIALS

by

PINAR ONGAN

Submitted to the Graduate School of Engineering and Natural Sciences
in partial fulfillment of
the requirements for the degree of
Master of Science

Sabancı University
Spring 2011

ON IRREDUCIBLE BINARY POLYNOMIALS

APPROVED BY:

Prof. Dr. Henning Stichtenoth ....
(Thesis Supervisor)

Prof. Dr. Alev Topuzoğlu ....

Assoc. Prof. İlker Birbil ....

Assoc. Prof. Wilfried Meidl ....

Asst. Prof. Gökhan Göğüş ....Gökhan..........

DATE OF APPROVAL: 07/06/2011

ON IRREDUCIBLE BINARY POLYNOMIALS

Pınar Ongan

Mathematics, Master Thesis, 2011

Thesis Supervisor: Prof. Dr. Henning Stichtenoth

Keywords: finite fields, irreducible polynomials, group actions, general linear group of degree two, permutations.

ABSTRACT

In the article [1], Michon and Ravache define a group action of S_3 on the set of irreducible polynomials of degree ≥ 2 over $\mathbb{F}_2$, and seeing that the orbits can have 1, 2, 3, or 6 elements, they give answers to the following two questions: Which polynomials have $i \in \{1,\ 2,\ 3,\ 6\}$ elements in their orbits? Within the orbits of the irreducible polynomials of degree n ≥ 2, how many of them consist of $i \in \{1,\ 2,\ 3,\ 6\}$ elements? After their article, the next step seems to generalize their results to the $\mathbb{F}_q$-case, however, their definition of the group action is not so suitable for such an extension. Therefore it is defined in a slightly different approach in this master thesis so that it can be easily generalized to the $\mathbb{F}_q$-case later. Furthermore, the results of the article [1] are reacquired using the new definition. Additionally, in the light of the articles [2] by Meyn and [3] by Michon and Ravache, the construction of irreducible polynomials of a higher degree which remain invariant under the group action of a given element forms a part of this thesis.

İNDİRGENEMEZ İKİLİ POLİNOMLAR ÜZERİNE

Pınar Ongan

Matematik, Yüksek Lisans Tezi, 2011

Tez Danışmanı: Prof. Dr. Henning Stichtenoth

Anahtar Kelimeler: sonlu cisimler, indirgenemez polinomlar, grup etkileri, 2 × 2 terslenebilir matrisler, permütasyonlar.

ÖZET

$\mathbb{F}_q$, q elemanlı bir sonlu cisim; $\mathrm{GL}_2[\mathbb{F}_2]$, öğeleri $\mathbb{F}_2$'ye ait 2×2 terslenebilir matrisler grubu ve S_3, 3 elemanın permütasyon grubu olsun.

Michon ve Ravache, makale [1]'de S_3'ten $\mathbb{F}_2[x]$'teki (derecesi 1'den büyük) indirgenemez polinomlar kümesi üzerine bir grup etkisi tanımlıyor ve bir yörüngenin 1, 2, 3, ya da 6 elemanlı olabileceğini gözlemleyerek şu soruları cevaplıyor: Hangi polinomların yörüngesinde $i \in \{1,\ 2,\ 3,\ 6\}$ eleman bulunur? Derecesi $n \geq 2$ olan indirgenemez polinomların kaçının yörüngesi $i \in \{1,\ 2,\ 3,\ 6\}$ elemanlıdır? Onların bu makalesinin ardından bir sonraki adım, sonuçlarının $\mathbb{F}_q$'ya genellenmesi olarak görünse de, makaledeki grup etkisi tanımı bu tarz bir genişlemeye pek uygun değil. Dolayısıyla, bu yüksek lisans tezinde grup etkisi bir parça farklı bir biçimde tanımlanıyor ki daha sonra $\mathbb{F}_q$'ya kolayca genellenebilsin. Ayrıca, makale [1]'in sonuçları da yeni grup etkisi tanımı kullanılarak tekrar elde ediliyor. Dahası, Meyn'ın yazdığı makale [2] ve yine Michon ve Ravache'ın çalşması olan makale [3]'ün ışığında; daha yüksek dereceye sahip ve verilen bir grup elemanının etkisinde sabit kalan indirgenemez polinomların inşaası da bu tezin bir parçasını oluşturuyor.

ACKNOWLEDGEMENTS

My first and foremost gratitude is to Henning Stichtenoth for his support in preparation of this master thesis and for his momentous contribution in shaping the way I do mathematics. It was an honor and a pleasure to be a student of him.

I would like to thank Alev Topuzoğlu and Buket Özkaya for their valuable help and suggestions in the phase of writing this thesis. I would also like to thank Wilfried Meidl for his comments during the finalization of this work.

I have been very much aided by the instruction and direction of Cem Güneri throughout my master study, for this I am very much obliged.

I am grateful to Nilgün Işık for believing in me at the most difficult phase of my education; and I am indebted to Ender Abadoğlu for urging me forward since day one during my first year in the undergraduate education.

I am deeply thankful to my parents Emine and İsmail Ongan for their self-sacrifice, help and support.

Finally, it's a joy to express here my special thanks to Ali Ongan, Volkan Yılmaz, Burcu Doğan and Sinan Eden for their love and honesty to me. Their existence in my life made the things easier.

TABLE OF CONTENTS

1 Introduction

Given a group G and a nonempty set X; G is said to *act on* X if there exists a map $\cdot : G \times X \to X$ defined as $\cdot(g, x) := g \cdot x$ satisfying

$$g_2 \cdot (g_1 \cdot x) = (g_2 g_1) \cdot x \;\; and \;\; e \cdot x = x, \; \forall g_1, g_2 \in G \; \forall x \in X,$$

where e is the identity of G. One can naturally define an equivalence relation on X as

$$x \sim y \;\Leftrightarrow\; g \cdot x = y, \; for \; some \; g \in G,$$

where $x, \; y \in X$. So, for any $x \in X$, we can talk about the equivalence class of x according to this relation, which is named *the orbit of* x and denoted as $Orb(x)$ in the course of this study. Also, the set of elements in G fixing x is called *the stabilizer of* x *in* G and the notation used for it in this text is $Stab_G(x)$. Moreover, this set is, in fact, a subgroup of G; and the *Orbit-Stabilizer Theorem* gives us

$$|G| = |Orb(x)| \, |Stab_G(x)| \, , \; for \; any \; x \in X.$$

In the next section of this study, using these basic notions, we will define a group action of $\mathrm{GL}_2[\mathbb{F}_2]$ on the set $\mathcal{I}$ of irreducible polynomials of degree ≥ 2 over $\mathbb{F}_2$. In fact, in the article [1], Michon and Ravache define a similar group action of $\mathcal{S}_3$ on the same set $\mathcal{I}$ and work on the orbits of irreducible binary polynomials. Although a generalization of the results of [1] to the $\mathbb{F}_q$-case will be a further step, since the definition of the group action in [1] is not so suitable for such a generalization, it will be defined in a slightly different approach in this master thesis so that it can be easily generalized to the $\mathbb{F}_q$-case later.

In Section 3, we will first realize several facts about the group $\mathrm{GL}_2[\mathbb{F}_2]$ and the action of this group on the set $\mathcal{I}$. Then, seeing that an orbit of an irreducible polynomial of degree ≥ 2 can contain $1, \; 2, \; 3$ or 6 elements, we will focus on the following two questions for a given $i \in \{1, \; 2, \; 3, \; 6\}$ and a given integer $n \geq 2$: *Which polynomials have* i *elements in their orbit? Within the orbits of irreducible polynomials of degree* n*, how many of them consists of* i *elements?* Indeed, Michon and Ravache answer these questions in [1] and their results will be reacquired in this study using our group action defined in Section 2.

Lastly, we will study on the construction of invariant irreducible binary polynomials of a higher degree in Section 4. To be more precise, let an irreducible binary polynomial f of degree $n \geq 3$ and a matrix $A \in \mathrm{GL}_2[\mathbb{F}_2]$ be given, we will define several transformations $\tau : \mathbb{F}_2[x] \to \mathbb{F}_2[x]$ such that $deg(\tau(f)) > n$ and $\tau(f)$ is fixed by the matrix A; we will and answer the question when $\tau(f)$ is irreducible over $\mathbb{F}_2$. Intrinsically, the main goal of this section is studied in [3] by Michon and Ravache; and, basically, the articles [2] by Meyn together with [3] shed light on this section.

2 The Definition of the Action of $\mathrm{GL}_2[\mathbb{F}_2]$ on Irreducible Polynomials

Let $G := \mathrm{GL}_2[\mathbb{F}_2]$ and $\mathcal{M}$ be the set of polynomials f over $\mathbb{F}_2$ of degree ≥ 2 such that f has no root in $\mathbb{F}_2$. Define a group action of G on the set $\mathcal{M}$ as:

$$(A \cdot f)(x) := (bx+d)^n f\left(\frac{ax+c}{bx+d}\right), \tag{2.1}$$

where $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in G$ and $f(x) \in \mathcal{M}$ with $deg(f) = n$.

Lemma 1. *Let $A, B \in G$ and $f \in \mathcal{M}$. Then*

a. *$deg(A \cdot f) = deg(f)$ and $A \cdot f \in \mathcal{M}$.*

b. *$A \cdot (B \cdot f) = (AB) \cdot f$.*

c. *$I \cdot f = f$, where I is the identity matrix of G.*

Proof. $A, B \in G$ and $f \in \mathcal{M}$.

a. Let $f(x) = \sum_{i=0}^{n} a_i x^i$. Then

$$(A \cdot f)(x) = \sum_{i=0}^{n} a_i (ax+c)^i (bx+d)^{n-i},$$

implying that the coefficient of x^n in $(A \cdot f)(x)$ is

$$a_0 b^n + a_1 a b^{n-1} + \ ... + \ a_{n-1} a^{n-1} b + a_n a^n.$$

If $b = 0$, then this coefficient is $a_n a^n$. Since $ad - bc \neq 0$, by assumption on the matrix A; we already have $a \neq 0$. Furthermore, $deg(f) = n$ implies $a_n \neq 0$. So $deg(A \cdot f) = n$ in this case. On the other hand, if $b = 1$, assume that the coefficient of x^n in $(A \cdot f)(x)$ is equal to 0. This implies

$$f(a) = f\left(\frac{a}{b}\right) = 0$$

which is a contradiction since f has no root in $\mathbb{F}_2$, by assumption. Hence

$$deg(A \cdot f) = n$$

in any case.

Now, assume $k \in \mathbb{F}_2$ is a root of $A \cdot f$. If $bk + d = 0$, then

$$0 = (A \cdot f)(k) = \sum_{i=0}^{n} a_i(ak + c)^i(bk + d)^{n-i} = a_n(ak + c)^n$$

will imply $ak + c = 0$. So we obtain

$$0 = a(bk + d) = b(ak) + ad = bc + ad$$

which is a contradiction since $A \in G$.

If $bk + d = 1$, then

$$0 = (A \cdot f)(k) = (bk + d)^n f\left(\frac{ak + c}{bk + d}\right),$$

i.e. f has a root $\frac{ak+c}{bk+d} \in \mathbb{F}_2$ which contradicts with the assumption $f \in \mathcal{M}$.

Hence $A \cdot f$ has no root in $\mathbb{F}_2$.

b. On one hand,

$$A \cdot (B \cdot f) = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \left(\begin{bmatrix} e & k \\ g & h \end{bmatrix} \cdot f(x) \right) = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \left((kx + h)^n f\left(\frac{ex + g}{kx + h}\right) \right)$$

$$= ((ak + bh)x + (ck + dh))^n f\left(\frac{(ae + bg)x + (ce + dg)}{(ak + bh)x + (ck + dh)}\right).$$

On the other hand,

$$(AB) \cdot f(x) = \begin{bmatrix} ae + bg & ak + bh \\ ce + dg & ck + dh \end{bmatrix} \cdot f(x)$$

$$= ((ak + bh)x + (ck + dh))^n f\left(\frac{(ae + bg)x + (ce + dg)}{(ak + bh)x + (ck + dh)}\right).$$

c. By definition.

□

Hence, we know that G acts on $\mathcal{M}$ by definition (2.1).

Lemma 2. *For all $A \in G$ and $f, g \in \mathcal{M}$, we have $A \cdot (fg) = (A \cdot f)(A \cdot g)$.*

Proof. Let $f(x) = \sum_{i=0}^{n} a_i x^i$ and $g(x) = \sum_{j=0}^{r} b_j x^j$. Then, on one hand,

$$A \cdot (fg) = A \cdot \left(\sum_{k=0}^{n+r} \sum_{i+j=k} (a_i b_j) x^k \right) = (bx+d)^{n+r} \sum_{k=0}^{n+r} \sum_{i+j=k} (a_i b_j) \left(\frac{ax+c}{bx+d} \right)^k .$$

On the other hand, the right side of the equation is

$$(bx+d)^{n+r} f\left(\frac{ax+c}{bx+d} \right) g\left(\frac{ax+c}{bx+d} \right) = (bx+d)^{n+r} \sum_{k=0}^{n+r} \sum_{i+j=k} (a_i b_j) \left(\frac{ax+c}{bx+d} \right)^k .$$

□

Corollary 3. *For $A \in G$ and $f \in \mathcal{M}$, we have*

$$A \cdot f \textit{ is irreducible over } \mathbb{F}_2 \Leftrightarrow f \textit{ is irreducible over } \mathbb{F}_2.$$

Proof. $\Rrightarrow$: If f is reducible over $\mathbb{F}_2$, then $f = gh$, for some g and h in $\mathcal{M}$. So $A \cdot f$ must also be reducible since

$$A \cdot f = A \cdot (gh) = (A \cdot g)(A \cdot h).$$

$\Lleftarrow$: Obvious by a similar approach to the converse part, since A is invertible. □

Now, define the set $\mathcal{I} := \{f(x) \in \mathcal{M} \mid f \textit{ is irreducible over } \mathbb{F}_2\}$. Then, using the previous corollary, one can restrict the definition of the group action in (2.1) to an action of G on $\mathcal{I}$. (*In this paper, we're mainly interested in this group action of G on $\mathcal{I}$.*)

3 Orbits of Irreducible Polynomials

Proposition 4. *G is isomorphic to $\mathcal{S}_3$.*

Proof. Let $A \in G$, then, by definition of the general linear group G, A maps the elements of the vector space ${\mathbb{F}_2}^2$ to the elements in the same vector space and fixes the zero element of ${\mathbb{F}_2}^2$. Take the subset

$$\mathcal{J} := \{e_1 := (1,0),\ e_2 := (0,1),\ e_3 := (1,1)\}$$

of ${\mathbb{F}_2}^2$ and consider $\varpi : G \to \mathcal{S}_{\mathcal{J}}$ defined as

$$\varpi(A) := \sigma_A, \ where \ \sigma_A(e_i) := Ae_i, \ \forall i \in \{1, \ 2, \ 3\}.$$

For $A, \ B \in G$ and $1 \leq i \leq 3$,

$$\sigma_{AB}(e_i) = AB(e_i) = A(Be_i) = A\sigma_B(e_i) = \sigma_A(\sigma_B(e_i))$$

implies that ϖ is an injective homomorphism since the matrices in G act nontrivially on the basis vectors e_1 and e_2. Furthermore, the number of elements in G is 6 proves that ϖ is an isomorphism. On the other hand, the set $\mathcal{J}$ consists of 3 elements, which implies $\mathcal{S}_{\mathcal{J}} = \mathcal{S}_3$. Hence $G \cong \mathcal{S}_3$. □

Let f be a polynomial in $\mathcal{I}$, then, since $Stab_G(f)$ is a subgroup of G, $|Stab_G(f)|$ must divide 6, by Lagrange's Theorem. Also, since $\mathcal{S}_3$ is a non-commutative group that has

- one subgroup of order 1,
- three cyclic subgroups of order 2,
- one cyclic subgroup of order 3,
- one subgroup of order 6

and no other subgroup, we can say

$$|Stab_G(f)| \neq 6 \Rightarrow Stab_G(f) \ is \ cyclic.$$

Furthermore, Orbit-Stabilizer Theorem gives us the following result:

$$|Orb(f)| = 1, \ 2, \ 3 \ or \ 6, \ \forall f \in \mathcal{I}.$$

Definition 5. *For a polynomial f in $\mathcal{I}$, the number of elements in the orbit of f is called* ***the length of*** *$Orb(f)$.*

Also, since every polynomial in an orbit must have the same degree, the following definition makes sense:

Definition 6. *For a polynomial $f \in \mathcal{I}$,* ***the degree of*** *$Orb(f)$ is defined as the degree of f.*

So, for a given $i \in \{1, \ 2, \ 3, \ 6\}$ and $n \geq 2$, one can ask the following two questions:

- Which polynomials have orbit length i?
- How many orbits of degree n have orbit length i?

The rest of this section is dedicated to answer these questions in sequel, but before that, we need a proposition to use later:

Proposition 7. *G is generated by the matrices $S = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ and $T = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$.*

Proof. We have

$$S^2 = I = T^2, \text{ i.e. } ord_G(S) = ord_G(T) = 2.$$

Moreover,

$$TS = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \ TST = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \ (TS)^2 = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, \ (TS)^2T = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

and $(TS)^3 = I$. i.e. $ord_G(TS) = 3$, which completes the proof since $|G| = 6$. □

3.1 Polynomials of a given orbit length

Knowing that an orbit length may be $1, \ 2, \ 3$ or 6, we are looking for an answer to the question: "Which polynomials have orbit length i?" for i taking the values $1, \ 2, \ 3$ and 6 in this subsection. First of all, let's look at the polynomials in $\mathcal{I}$ of orbit length 1:

Proposition 8. *$f \in \mathcal{I}$ has orbit length 1 if and only if $f(x) = x^2 + x + 1$.*

Proof. For the sufficiency, let f be a polynomial in $\mathcal{I}$ of degree n satisfying $|Orb(f)| = 1$. Then, by Orbit-Stabilizer Theorem, $|Stab_G(f)| = 6$, and since $Stab_G(f)$ is a subgroup of G, we have $Stab_G(f) = G$. So, by Proposition 7,

$$f = S \cdot f = T \cdot f.$$

And the definition of the action gives that

$$f(x) = x^n f\left(\frac{1}{x}\right) = f(x+1).$$

Now, let α be a root of f, then all the roots of f in $\overline{\mathbb{F}_2}$ are $\alpha, \ \alpha^2, \ \alpha^{2^2}, \ ..., \ \alpha^{2^{n-1}}$, and

$$0 = f(\alpha) = \alpha^n f\left(\frac{1}{\alpha}\right) = f(\alpha + 1).$$

Since $\alpha \neq 0$, $\alpha+1$ and $\frac{1}{\alpha}$ must also be roots of f:

$$\alpha + 1 = \alpha^{2^k} \textit{ and } \alpha^{-1} = \alpha^{2^s}, \textit{ for some } 0 < k, s < n. \tag{3.1}$$

On one hand, by taking the $(2^k)^{th}$ power of the first equation, we get

$$\alpha^{2^{2k}} = (\alpha^{2^k})^{2^k} = (\alpha+1)^{2^k} = \alpha^{2^k} + 1 = (\alpha+1)+1 = \alpha.$$

So $2k \equiv 0 \mod n$. On the other hand, by taking the $(2^s)^{th}$ power of the second equation in (3.1), we obtain

$$\alpha^{2^{2s}} = (\alpha^{2^s})^{2^s} = (\alpha^{-1})^{2^s} = (\alpha^{2^s})^{-1} = (\alpha^{-1})^{-1} = \alpha.$$

So $2s \equiv 0 \mod n$, and since $0 < k, s < n$, we have $k = \frac{n}{2} = s$ implying that $k = s$. Thus $\alpha + 1 = \alpha^{-1}$, which gives us the equation $\alpha^2 + \alpha + 1 = 0$. Therefore α is a root of the polynomial $x^2 + x + 1$, and so $f(x)$ must divide $x^2 + x + 1$ since f is the minimal polynomial of α over $\mathbb{F}_2$. However, this means $f(x) = x^2 + x + 1$ since $deg(f) \geq 2$.

For the necessity, consider the polynomial $f(x) = x^2 + x + 1 \in \mathcal{I}$. To show that it has orbit length 1, it's enough to show that f is fixed by every element of G. Since

$$S \cdot (x^2 + x + 1) = x^2\left(\frac{1}{x^2} + \frac{1}{x} + 1\right) = x^2 + x + 1$$

and

$$T \cdot (x^2 + x + 1) = (x+1)^2 + (x+1) + 1 = x^2 + x + 1,$$

by Proposition 7, the proof is complete. □

In the analysis of the polynomials in $\mathcal{I}$ of orbit length $\neq 1$, the following two theorems will be crucial:

Theorem 9. *If $f \in \mathcal{I}$ of degree $n \geq 3$, $A \in G$ such that $ord_G(A) = m \geq 2$ and $A \cdot f = f$, then $n \equiv 0 \mod m$.*

Theorem 10. *If $f \in \mathcal{I}$ such that $deg(f) \geq 3$ and $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in Stab_G(f)$, then $f(x)$ must divide the polynomial $bx^{2^s+1} + ax^{2^s} + dx + c$, for some $0 \leq s \leq n-1$.*

However, the proofs of these theorems will require some additional work. First, define a group action of G on $\overline{\mathbb{F}_2} \setminus \mathbb{F}_2$ as follows:

$$A \cdot \alpha := \frac{d\alpha + c}{b\alpha + a}, \tag{3.2}$$

where $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in G$ and $\alpha \in \overline{\mathbb{F}_2} \setminus \mathbb{F}_2$.

Lemma 11. *Let $A, B \in G$ and $\alpha \in \overline{\mathbb{F}_2} \setminus \mathbb{F}_2$. Then*

a. $A \cdot \alpha \in \overline{\mathbb{F}_2} \setminus \mathbb{F}_2$.

b. $A \cdot (B \cdot \alpha) = (AB) \cdot \alpha$.

c. $I \cdot \alpha = \alpha$, *where I is the identity matrix of G.*

Proof. $A, B \in G$ and $\alpha \in \overline{\mathbb{F}_2} \setminus \mathbb{F}_2$.

a. Assume $A \cdot \alpha = k \in \mathbb{F}_2$. Using (2.2),

$$d\alpha + c = bk\alpha + ak$$

$$i.e.\ (bk + d)\alpha = ak + c.$$

Thus, if $bk = d$, then $ak = c$, and so

$$ad + bc = a(bk) + b(ak) = 0$$

which gives a contradiction since $A \in G$. Hence $bk \neq d$. However, at that time,

$$\alpha = \frac{ak + c}{bk + d} \in \mathbb{F}_2$$

which contradicts to the definition of α.

b. On one hand,

$$A \cdot (B \cdot \alpha) = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \left(\begin{bmatrix} e & f \\ g & h \end{bmatrix} \cdot \alpha \right) = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \frac{h\alpha + g}{f\alpha + e} = \frac{(cf + dh)\alpha + ce + dg}{(af + bh)\alpha + (ae + bg)}.$$

On the other hand,

$$(AB) \cdot \alpha = \begin{bmatrix} ae + bg & af + bh \\ ce + dg & cf + dh \end{bmatrix} \cdot \alpha = \frac{(cf + dh)\alpha + (ce + dg)}{(af + bh)\alpha + (ae + bg)}.$$

c. By definition.

□

By Lemma 11, we know that the group G acts on the set $\overline{\mathbb{F}_2} \setminus \mathbb{F}_2$. Now, let us investigate the connection between the definitions (2.1) and (3.2):

Lemma 12. *If α is a root of f, then $A \cdot \alpha$ must be a root of $A \cdot f$.*

Proof. $f(\alpha) = 0$ implies that

$$(A \cdot f)(A \cdot \alpha) = (bx+d)^n f\left(\frac{ax+c}{bx+d}\right)(A \cdot \alpha) = (b(A \cdot \alpha)+d)^n f\left(\frac{a(A \cdot \alpha)+c}{b(A \cdot \alpha)+d}\right)$$

$$= \left(b\left(\frac{d\alpha+c}{b\alpha+a}\right)+d\right)^n f\left(\frac{a(d\alpha+c)+c(b\alpha+a)}{b(d\alpha+c)+d(b\alpha+a)}\right) = \left(\frac{ad+bc}{b\alpha+a}\right)^n f(\alpha) = 0.$$

□

Now, we are ready to prove the theorems stated above.

Proof of Theorem 9. Let α be a root of f. Assume that $A \cdot f = f$, then

$$A^j \cdot f = A \cdot (A \cdot (A \cdot ...(A \cdot f)...)) = f,$$

for all $j \in \mathbb{N}$ by Lemma 1. Also, using Lemma 12,

$$f(A^j \cdot \alpha) = (A^j \cdot f)(A^j \cdot \alpha) = 0.$$

So the group $< A >$ generated by A acts on the roots of f in $\overline{\mathbb{F}_2}$.
Claim: This action is without fixed points.
Assume $A^k \cdot \alpha = A^i \cdot \alpha$, for some $0 \leq i < k \leq m-1$. Then

$$A^l \cdot \alpha = \alpha,$$

where $l = k - i$ and $0 < l < m$. Say A^l is equal to the matrix $\begin{bmatrix} a_l & b_l \\ c_l & d_l \end{bmatrix}$, then

$$\alpha = A^l \cdot \alpha = \frac{d_l\alpha + c_l}{b_l\alpha + a_l}$$

which implies

$$b_l\alpha^2 + (a_l + d_l)\alpha + c_l = 0.$$

If $b_l = 0$, then this equation turns into

$$(a_l + d_l)\alpha = c_l.$$

In this case, either $a_l + d_l = 0$ or $\alpha \in \mathbb{F}_2$ gives a contradiction. So take $a_l = d_l$. Then

$$0 \neq a_l d_l + b_l c_l = (a_l)^2 + 0 = a_l$$

implies $A^l = I$. However, that is impossible since $l < m$. So b_l cannot be 0, i.e. α is a root of a second degree nontrivial equation over $\mathbb{F}_2$ which is contradictory since f is the minimal polynomial of α of degree ≥ 3, by assumption.

Thus the group $< A >$ acts without fixed points on the set of roots of f and the list

$$A \cdot \alpha,\ A^2 \cdot \alpha,\ ..., A^m \cdot \alpha$$

consists of m distinct roots of f. Say α^{2^s} is a root of f which is not in the list. Then the list

$$A \cdot \alpha,\ A^2 \cdot \alpha,\ ..., A^m \cdot \alpha,\ A \cdot \alpha^{2^s},\ A^2 \cdot \alpha^{2^s},\ ..., A^m \cdot \alpha^{2^s}$$

consists of $2m$ distinct roots of f. By continuing this argument, we conclude that there exist $n = mk$ roots of f in total, for some $k \in \mathbb{N}$.

□

Proof of Theorem 10. Let $A \cdot f = f$ and α be a root of f in $\overline{\mathbb{F}_2} \setminus \mathbb{F}_2$. Then all the roots of f are $\alpha,\ \alpha^2,\ \alpha^{2^2},\ ...,\ \alpha^{2^{n-1}}$. By Lemma 12, $A \cdot \alpha$ is a root of $A \cdot f = f$. So one can find $0 \leq s \leq n-1$ satisfying

$$\alpha^{2^s} = A \cdot \alpha = \frac{d\alpha + c}{b\alpha + a}$$

which is equal to

$$b\alpha^{2^s+1} + a\alpha^{2^s} + d\alpha + c = 0.$$

Thus α is a root of $x^{2^s+1} + ax^{2^s} + dx + c$, for some $0 \leq s \leq n-1$. On the other hand, by definition of $\mathcal{I}$, we know that f is the minimal polynomial of α over $\mathbb{F}_2$. So f has to divide $bx^{2^s+1} + ax^{2^s} + dx + c$, for some $0 \leq s \leq n-1$.

□

For the polynomials in $\mathcal{I}$ of orbit length 2, the proposition below is a direct consequence of the Orbit-Stabilizer Theorem.

Proposition 13. *$|Orb(f(x))| = 2$ if and only if $(ST) \cdot f = f$ and $S \cdot f \neq f$.*

Proof. Let f be a polynomial in $\mathcal{I}$ such that $|Orb(f)| = 2$. We know this is possible only if $|Stab_G(f)| = 3$. So $Stab_G(f) =< A >$, for some $A \in G$ satisfying $ord_G(A) = 3$. By definition of G, A can be TS or ST. And, in both cases, we must have

$$(ST) \cdot f = f$$

since $TS \in Stab_G(f)$ implies

$$ST \cdot f = ST \cdot (TS \cdot f) = f.$$

If, moreover, $S \cdot f = f$, then $f = S \cdot f = T \cdot f$ which is a contradiction by Proposition 7. Hence

$$S \cdot f \neq f.$$

□

Corollary 14. *If a polynomial $f \in \mathcal{I}$ has orbit length 2, then $deg(f) \equiv 0 \mod 3$.*

Proof. Since the matrix ST has order 3 in G, this corollary is a direct consequence of Proposition 13 and Theorem 9. □

Theorem 15. *ST is in the stabilizer of the polynomial $f \in \mathcal{I}$ of degree n if and only if $f(x)$ is an irreducible factor of the polynomial*

$$B_k(x) := x^{2^k+1} + x + 1, \tag{3.3}$$

for some $k \in \mathbb{N}$ satisfying $0 \leq k \leq n - 1$.

Proof. If $f \in \mathcal{I}$ of degree n is fixed by ST, then by Theorem 10, $f(x)$ must divide $B_k(x)$, for some $k \in \mathbb{N}$ satisfying $0 \leq k \leq n - 1$.

For the converse, let f be an irreducible factor of B_k, for some $0 \leq k \leq n$.
Case1: If f is a factor of B_0, then $f(x) = x^2 + x + 1 = B_0(x)$, by definition of B_k. So f is fixed by every element in G.
Case 2: If f is an irreducible factor of B_k, for some $1 \leq k \leq n$, then any root of f must also be a root of B_k. Let α be a root of f, then all the roots of f are α, α^2, α^{2^2}, ..., $\alpha^{2^{n-1}}$, where $deg(f) = n$. Also, since α has to be a root of B_k, we have $\alpha^{2^k+1} + \alpha + 1 = 0$ implying that $\alpha^{2^k} = 1 + \frac{1}{\alpha}$. So $1 + \frac{1}{\alpha}$ is a root of f, too. Moreover,

$$(ST \cdot f)(\alpha) = \alpha^n f\left(1 + \frac{1}{\alpha}\right) = 0.$$

Thus, for any root α of f, α must also be a root of $ST \cdot f$. □

Let $f \in \mathcal{I}$ be a polynomial of degree n fixed by the matrix ST. If $n = 2$, then $f(x) = x^2 + x + 1$ and $|Orb(f)| = 1$, by Proposition 8. Otherwise, since S will not be in the stabilizer of f, the orbit length of f will be equal to 2. Thus, the previous theorem implies that, for some $k \in \mathbb{N}$, every irreducible factor of B_k other than $x^2 + x + 1$ must be a polynomial in $\mathcal{I}$ of orbit length 2. In fact, one can use MAGMA to calculate these factors. For example, the table below consisting of the irreducible factors of B_k $(0 \leq k \leq 7)$ is obtained using this program, and we can say that all the polynomials appearing on the right column other than $x^2 + x + 1$ must be a polynomial of orbit length 2.

k	all irreducible factors of B_k
0	$x^2 + x + 1.$
1	$x^3 + x + 1.$
2	$x^2 + x + 1,\ x^3 + x^2 + 1.$
3	$x^9 + x + 1.$
4	$x^2 + x + 1,\ x^3 + x + 1,\ x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^6 + x^4 + x + 1.$
5	$x^3 + x^2 + 1,\ x^{15} + x^{10} + x^9 + x^8 + x^4 + x^3 + x^2 + x + 1,$ $x^{15} + x^{14} + x^{13} + x^{11} + x^{10} + x^7 + x^6 + x^3 + 1.$
6	$x^2 + x + 1,\ x^9 + x^8 + 1,$ $x^{18} + x^{14} + x^{13} + x^{12} + x^{11} + x^7 + x^6 + x^5 + x^4 + x^2 + 1,$ $x^{18} + x^{17} + x^{15} + x^{14} + x^{13} + x^9 + x^7 + x^6 + x^3 + x + 1,$ $x^{18} + x^{17} + x^{16} + x^{15} + x^{12} + x^{11} + x^9 + x^5 + x^4 + x^3 + x^2 + x + 1.$
7	$x^3 + x + 1,\ x^{21} + x^{17} + x^{16} + x^{15} + x^{13} + x^{12} + x^{10} + x^9 + x^7 + x^6 + x^5 + x + 1,$ $x^{21} + x^{19} + x^{18} + x^{15} + x^{14} + x^{13} + x^{11} + x^9 + x^6 + x^5 + x^2 + x + 1,$ $x^{21} + x^{20} + x^{15} + x^{14} + x^{11} + x^8 + x^6 + x^4 + 1,$ $x^{21} + x^{20} + x^{18} + x^{17} + x^{16} + x^{15} + x^{14} + x^{12} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^3 + 1,$ $x^{21} + x^{20} + x^{19} + x^{15} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^3 + x^2 + 1,$ $x^{21} + x^{20} + x^{19} + x^{18} + x^{17} + x^{16} + x^{15} + x^{12} + x^{10} + x^8 + x^7 + x^6 + x^4 + x^2 + 1.$

Now, let us consider the polynomials $f \in \mathcal{I}$ of orbit length 3. We already know that its stabilizer consists of 2 elements, and $Stab_G(f)$ is generated by a matrix $B \in G$, by Proposition 4. Because of this, the order of B in G must be equal to 2 and all the matrices in G satisfying this condition are S, T, and STS. Therefore we have the following proposition:

Proposition 16. *$f \in \mathcal{I}$ has orbit length 3 if and only if $Stab_G(f)$ is generated by either S or T or STS.*

Moreover, since $ord_G S = ord_G T = ord_G STS = 2$, by Theorem 9, the following corollary is obvious:

Corollary 17. *If $f \in \mathcal{I}$ has orbit length 3, then the degree of f must be even.*

Also, using Theorem 10, one can conclude additional results for the polynomials fixed by either S, or T or STS:

Corollary 18. *Let $f \in \mathcal{I}$ be a polynomial of degree n.*

- *If $S \cdot f = f$, then f must divide the polynomial $x^{2^k+1} + 1$, for some $k \in \mathbb{N}$ satisfying $0 \leq k \leq n-1$.*
- *If $T \cdot f = f$, then f must divide the polynomial $x^{2^k} + x + 1$, for some $k \in \mathbb{N}$ satisfying $0 \leq k \leq n-1$.*
- *If $STS \cdot f = f$, then f must divide the polynomial $x^{2^k} + x^{2^k-1} + 1$, for some $k \in \mathbb{N}$ satisfying $0 \leq k \leq n-1$.*

Finally, let $f \in \mathcal{I}$ be a polynomial of orbit length 6. Then the order of $Stab_G(f)$ must be equal to 1, meaning that $Stab_G(f) = \{I\}$ since $Stab_G(f)$ is a subgroup of G. So we get:

Proposition 19. *$f \in \mathcal{I}$ has orbit length 6 if and only if $A \cdot f \neq f$, for all $A \in G \backslash \{I\}$.*

3.2 The number of orbits of a given degree and orbit length

In this subsection, for i taking the values $1,\ 2,\ 3$ and 6, we look for an answer to the question "How many orbits of length i and degree n exist according to the group action definition (2.1)?". Let $N^{(i)}(n)$ denote the number of the orbits of degree n and orbit length i. So the total number of orbits of degree n is equal to

$$N^{(1)}(n) + N^{(2)}(n) + N^{(3)}(n) + N^{(6)}(n)$$

and, we are trying to find the numbers $N^{(1)}(n)$, $N^{(2)}(n)$, $N^{(3)}(n)$ and $N^{(6)}(n)$.

First, as a direct consequence of Proposition 8, we already have the following result for the number of orbits of degree n and orbit length 1:

Corollary 20.

$$N^{(1)}(n) = \begin{cases} 1 & \text{if } n = 2, \\ 0 & \text{if } n \geq 3. \end{cases}$$

Secondly, Proposition 13 and Theorem 15 will be useful in finding the number $N^{(2)}(n)$. By these two results of the previous subsection, counting the number of irreducible factors of degree n of B_k's will be enough to calculate the number of orbits of degree $n \geq 3$ and orbit length 2. To continue, let us observe some results on the polynomial B_k.

Proposition 21. *If a polynomial $f \in \mathcal{I}$ is of degree $3m$ and orbit length 2, then it must divide exactly one of B_m and B_{2m}.*

Proof. Let α be a root of f. Since f divides B_k, for some $0 < k < n$, we already have $\alpha^{2^k} = 1 + \frac{1}{\alpha}$. By taking the $(2^k)^{th}$ power of this equation, we get

$$\alpha^{2^{2k}} = (\alpha^{2^k})^{2^k} = \left(1 + \frac{1}{\alpha}\right)^{2^k} = 1 + \frac{1}{\alpha^{2^k}} = 1 + \frac{\alpha}{\alpha + 1} = \frac{1}{1+\alpha}.$$

Again, by taking the $(2^k)^{th}$ power of this equation, we see

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

So $3k \equiv 0 \mod n$, and k is equal to $\frac{n}{3} = m$ or $\frac{2n}{3} = 2m$ since $0 < k < n$. Therefore f must divide B_m or B_{2m}. Now, assume f divides both B_m and B_{2m}. Then,

$$B_{2m}(\alpha) = \alpha^{2^{2m}+1} + \alpha + 1 = 0$$

and

$$B_m(\alpha) = \alpha^{2^m+1} + \alpha + 1 = 0$$

imply $\alpha^{2^m+1} = \alpha$. However, this means $\alpha \in \mathbb{F}_{2^{m+1}}$ which is a contradiction since $2^m + 1$ is odd. □

Definition 22. *Let $f \in \mathcal{I}$ such that $(ST) \cdot f = f$ and $deg(f) = 3m$. f is said to be*

- *of **type 1** if f divides B_m.*
- *of **type 2** if f divides B_{2m}.*

Proposition 23. *f and $S \cdot f$ have distinct types.*

Proof. Let f be of type 1 such that $deg(f) = 3m$ and α be a root of f. Then since f divides B_m, we have $\alpha^{2^m+1} + \alpha + 1 = 0$ implying that $\alpha^{2^m} = 1 + \frac{1}{\alpha}$.
On the other hand, α is a root of f implies that $\frac{1}{\alpha}$ is a root of $f(\frac{1}{x})$, and so a root of $S \cdot f = x^n f(\frac{1}{x})$. Say $\beta = \frac{1}{\alpha}$, so β is a root of $S \cdot f$.

$\Rightarrow \beta^{-2^m} = \alpha^{2^m} = 1 + \frac{1}{\alpha} = 1 + \beta$.
$\Rightarrow \beta^{2^m} = (1+\beta)^{2^m} = \frac{1}{1+\beta}$.
$\Rightarrow \beta^{2^{2m}} = (\beta^{2^m})^{2^m} = (\frac{1}{1+\beta})^{2^m} = \frac{1}{1+\beta^{2^m}} = 1 + \frac{1}{\beta}$.
$\Rightarrow \beta^{2^{2m}+1} + \beta + 1 = 0$.
$\Rightarrow S \cdot f$ divides B_{2m}, i.e. $S \cdot f$ is of type 2. □

Corollary 24. *Among all polynomials $f \in \mathcal{I}$ of degree $3m$ satisfying $(ST) \cdot f = f$, half of them divides B_m while the other half divides B_{2m}.*

Proposition 25. *B_k has no multiple roots.*

Proof. Since $B_k^{'}(x) = x^{2^k} + 1 = (x+1)^{2^k}$, the unique root of $B_k^{'}$ is 1 with multiplicity 2^k. However, 1 is not a root of B_k, so B_k and $B_k^{'}$ have no common roots. □

Proposition 26. *$x^2 + x + 1$ divides B_k if and only if k is even.*

Proof. Let α be a root of $x^2 + x + 1$, then $\alpha^3 = \alpha^2 + \alpha = 1$, and so $\alpha^2 = \alpha^{-1}$. Since $B_k(\alpha) = \alpha^{2^k+1} + \alpha + 1 = \alpha^{(-1)^k+1} + \alpha + 1$, we conclude that:

- if k is even, then $B_k(\alpha) = \alpha^2 + \alpha + 1 = 0$;
- if k is odd, then $B_k(\alpha) = \alpha^0 + \alpha + 1 = \alpha$.

□

Now, we are ready to prove the following theorem on the factors of B_k:

Theorem 27. *Let f be a polynomial in $\mathcal{I}$ of degree $3m$. Then f divides B_k if and only if f satisfies the following three conditions:*

- *$(ST) \cdot f = f$;*
- *m divides k;*
- *$\frac{k}{m} \mod 3$ is equal to the type of f.*

Proof. Let f be a polynomial in $\mathcal{I}$ of degree $3m$.
$\Leftarrow$: Say $k = ml$ and $l \equiv t \mod 3$ with f is of type t. Let α be a root of f. Since f divides $B_{tm} = x^{2^{tm}+1} + x + 1$, we have α is a root of B_{tm}. So

$$\alpha^{2^k} = \alpha^{2^{ml}} = \alpha^{2^{tm}} = 1 + \frac{1}{\alpha}$$

implying that

$$\alpha^{2^k+1} + \alpha + 1 = 0,$$

i.e. α is a root of B_k. Thus f divides B_k.
$\not\Rightarrow$: Let f divide B_k, then $(ST)\cdot f = f$. Also, if α is a root of f, as seen in the proof of Theorem 21, $\alpha^{2^{3k}} = \alpha$, and so $\alpha \in \mathbb{F}_{2^{3k}}$. Thus $\mathbb{F}_2 \subset \mathbb{F}_{2^{3m}} \subset \mathbb{F}_{2^{3k}}$ since $deg(f) = 3m$ and α is a root of f. Hence m divides k.
Now, let $k = ml$, for some $l \in \mathbb{Z}$. Then Theorem 21 implies that f divides B_m or B_{2m}.
If f divides B_m, then any root α of f has to be a root of B_m, so $\alpha^{2^m+1} + \alpha + 1 = 0$, i.e. $\alpha^{2^m} = 1 + \frac{1}{\alpha}$.
Furthermore, since f divides B_k, we also have $\alpha^{2^k} = 1 + \frac{1}{\alpha}$ implying that

$$\alpha^{2^m} = 1 + \frac{1}{\alpha} = \alpha^{2^k} = \alpha^{2^{ml}} = \alpha^{2^{(m+m(l-1))}} = (\alpha^{2^m})^{2^{m(l-1)}}.$$

On the other hand, f has $3m$ distinct roots: $\alpha,\ \alpha^2,\ \alpha^{2^2},\ ...,\ \alpha^{2^{3m-1}}$
$\Rightarrow m(l-1) \equiv 0 \mod (3m)$.
$\Rightarrow 3m$ divides $m(l-1)$, i.e. $l \equiv 1 \mod 3$.
$\Rightarrow \frac{k}{m} \equiv 1 \mod 3$.
If f divides B_{2m}, then for any root α of f, $\alpha^{2^{2m}+1} + \alpha + 1 = 0$ which gives

$$\alpha^{2^{2m}} = 1 + \frac{1}{\alpha} = \alpha^{2^k} = \alpha^{2^{ml}} = \alpha^{2^{2m+m(l-2)}}.$$

And similarly this equality implies $l \equiv 2 \mod 3$. Hence $\frac{k}{m} \equiv 2 \mod 3$. □

At last, we can have a result on the number $N^{(2)}(n)$:

Lemma 28. *For any $k \geq 1$:*

$$2^k - (-1)^k = \sum_{\substack{d|k \\ \frac{k}{d}\not\equiv 0 \mod 3}} (3d)N^{(2)}(3d).$$

Proof. Let $EB_k := \{f \in \mathcal{I} \ :\ deg(f) \geq 3 \ \wedge\ f|B_k\}$.
$\Rightarrow EB_k = \{f \in \mathcal{I} \ :\ deg(f) \equiv 0 \mod 3 \ \wedge\ f|B_k\}$.
If $deg(f) = 3d$, then f is of type 1 or type 2, by Proposition 21; and $(ST)\cdot f = f$, $d|k$, $\frac{k}{d} \mod 3$ is equal to the type of f, by Theorem 27. So

$$EB_k = \bigcup_{d|k,\ \frac{k}{d}\equiv 1 (mod 3)} \{f \in \mathcal{I} \ :\ deg(f) = 3d \ \wedge\ (ST)\cdot f = f \ \wedge\ f|B_k\} \ \cup$$

$$\bigcup_{d|k,\ \frac{k}{d}\equiv 2 (mod 3)} \{f \in \mathcal{I} \ :\ deg(f) = 3d \ \wedge\ (ST)\cdot f = f \ \wedge\ f : B_k\}.$$

Let $E_i(3d) := \{f \in \mathcal{I} \ : \ deg(f) = 3d \ \wedge \ (ST)\cdot f = f \ \wedge \ f|B_k \ \wedge \ f \ is \ of \ type \ i\}$ for $i = 1, \ 2$. Then

$$EB_k = \bigcup_{d|k, \ \frac{k}{d}\equiv 1(mod3)} E_1(3d) \ \cup \ \bigcup_{d|k, \ \frac{k}{d}\equiv 2(mod3)} E_2(3d).$$

By multiplying all elements in the sets of both sides and taking the degrees, the right hand side of the equation gives

$$\sum_{d|k, \ \frac{k}{d}\equiv 1(mod3)} \{deg(f) \ : \ f \in E_1(3d)\} \ + \sum_{d|k, \ \frac{k}{d}\equiv 2(mod3)} \{deg(f) \ : \ f \in E_2(3d)\}$$

$$= \sum_{d|k, \ \frac{k}{d}\equiv 1(mod3)} (3d)\,|E_1(3d)| \ + \sum_{d|k, \ \frac{k}{d}\equiv 2(mod3)} (3d)\,|E_2(3d)|$$

$$= \sum_{d|k, \ \frac{k}{d}\equiv 1(mod3)} (3d)N^{(2)}(3d) \ + \sum_{d|k, \ \frac{k}{d}\equiv 2(mod3)} (3d)N^{(2)}(3d)$$

$$= \sum_{d|k, \ \frac{k}{d}\not\equiv 0(mod3)} (3d)N^{(2)}(3d).$$

while, using Proposition 26, the left hand side becomes

- $deg(\frac{x^{2^k+1}+x+1}{x^2+x+1}) = 2^k - 1$ if k is even, since $(x^2+x+1)|B_k$ in this case.
- $deg(x^{2^k+1}+x+1) = 2^k + 1$ if k is odd.

□

Theorem 29.

$$N^{(2)}(n) = \begin{cases} \frac{1}{3m}\sum_{\substack{d|m \\ d\neq 0 \mod 3}} \mu(d)(2^{\frac{m}{d}} - (-1)^{\frac{m}{d}}) & if \, n = 3m, \\ 0 & if \, 3 \ does \ not \ divide \ n. \end{cases}$$

Proof. By Corollary 14, we know that if $f \in \mathcal{I}$ such that $|Orb(f)| = 2$, then $deg(f) \equiv 0 \mod 3$. So $N^{(2)}(n) = 0$ for $n \not\equiv 0 \mod 3$.
Now, let $n \equiv 0 \mod 3$, say $n = 3m$. Defining $H(m) := 2^m - (-1)^m$ and $h(m) := 3mN^{(2)}(3m)$, for all $m \in \mathbb{N}^+$, Theorem 28 gives the equality

$$H(m) = \sum_{d|m, \ d\not\equiv 0(mod3)} h(d), \ \forall m \geq 1.$$

Thus, by Moebius Inversion Formula, we have

$$h(m) = \sum_{d|m,\ d\neq 0(mod3)} \mu(d)H\left(\frac{m}{d}\right),\ \forall m \geq 1$$

which is

$$N^{(2)}(n) = \frac{1}{3m} \sum_{\substack{d|m \\ d\neq 0(mod3)}} \mu(d)(2^{\frac{m}{d}} - (-1)^{\frac{m}{d}}),\ \forall m \geq 1.$$

□

Next, we want to calculate the number of orbits in $\mathcal{I}$ of degree n and length 3.

Proposition 30. *Each orbit of length 3 contains a polynomial $h \in \mathcal{I}$ satisfying $S \cdot h = h$.*

Proof. Let f be a polynomial in $\mathcal{I}$ such that $|Orb(f)| = 3$, then $|Stab_G(f)| = 2$. Say $I \neq A \in Stab_G(f)$. Then we must have $A \cdot f = f$, $A \neq I$ and $A^2 = I$. Since

$$S = BAB^{-1},\ for\ some\ B \in GL_2(\mathbb{F}_2),$$

for $h = B \cdot f$, we obtain

$$S \cdot h = (BAB^{-1}) \cdot (B \cdot f) = B \cdot (A \cdot f) = B \cdot f = h.$$

□

Clearly, by the previous proposition, finding the number $N^{(3)}(n)$ is the same as counting the number of polynomials $h \in \mathcal{I}$ satisfying $S \cdot h = h$. And, the following theorem of Meyn in the article [2] makes possible to count the number of polynomials of this kind:

Theorem 31.

a. *Each polynomial $f \in \mathcal{I}$ of degree $2n$ $(n \geq 1)$ satisfying $S \cdot f = f$ is a factor of the polynomial*

$$H_n(x) = x^{2^n+1} + 1.$$

b. *Each irreducible factor of degree ≥ 2 of H_n is a polynomial $f \in \mathcal{I}$ of degree $2d$ satisfying $S \cdot f = f$, where d divides n and $\frac{n}{d}$ is odd.*

Proof.

a. Let $f \in \mathcal{I}$ be a polynomial of degree $2n$ which is fixed by S. Say α is a root of f. Then Theorem 10 implies that f has to divide the polynomial $x^{2^s+1}+1$, for some $0 \leq s \leq 2n-1$. So α must be a root of $x^{2^s+1}+1$, too, which can be stated as $\alpha^{-1} = \alpha^{2^s}$. Then

$$\alpha^{2^{2s}} = (\alpha^{2^s})^{2^s} = (\alpha^{-1})^{2^s} = (\alpha^{2^s})^{-1} = (\alpha^{-1})^{-1} = \alpha,$$

gives us $\alpha \in \mathbb{F}_{2^{2s}}$. Therefore, we conclude

$$\mathbb{F}_{2^{2n}} = \mathbb{F}_2(\alpha) \subseteq \mathbb{F}_{2^{2s}},$$

so $2n$ must divide $2s$, i.e. $n = s$.

b. Let $g \in \mathcal{I}$ be of degree ≥ 2 such that $g|H_n$. Say α is a root of g. Then $\alpha^{2^n+1}+1 = 0$, i.e. $\alpha^{-1} = \alpha^{2^n}$. So for every root α of g, we have α^{-1} is a root of g. Moreover,

$$S \cdot g(\alpha) = \alpha^{deg(g)} g(\alpha^{-1}) = 0$$

implies that g divides $S \cdot g$. Similarly, for any root β of $S \cdot g$, we can write

$$0 = S \cdot g(\beta) = \beta^{deg(g)} g(\beta^{-1}).$$

Therefore β^{-1} is root of g, and $(\beta^{-1})^{-1} = \beta$ is also a root of g. Hence g is fixed by S, and by Theorem 9, $deg(g)$ must be even. Say $deg(g) = 2d$, for some $d \in \mathbb{N}$. Then by Part a, g has to be a factor of H_d. Also,

$$\alpha^{2^{2n}} = (\alpha^{2^n})^{2^n} = (\alpha^{-1})^{2^n} = (\alpha^{2^n})^{-1} = (\alpha^{-1})^{-1} = \alpha$$

since $g|H_n$, so $\alpha \in \mathbb{F}_{2^{2n}}$. But, since g is an irreducible polynomial over $\mathbb{F}_2$ of degree $2d$, we already have $\mathbb{F}_{2^{2d}} = \mathbb{F}_2(\alpha)$. So

$$\mathbb{F}_{2^{2d}} = \mathbb{F}_2(\alpha) \subseteq \mathbb{F}_{2^{2n}},$$

gives us that $d|n$. Moreover,

$$\alpha^{2^n} = (...((\alpha^{2^d})^{2^d})^{\cdots})^{2^d},$$

where there exist $\frac{n}{d}$ -many 2^d powers on the right hand side since $n = \frac{n}{d}d$.

Hence

$$\alpha^{2^n} = \begin{cases} \alpha & \text{if } \frac{n}{d} \textit{ is even}, \\ \alpha^{-1} & \text{if } \frac{n}{d} \textit{ is odd}. \end{cases}$$

However, since we already have $\alpha^{-1} = \alpha^n$, we conclude that $\frac{n}{d}$ cannot be even.

□

Again, one can use MAGMA to compute the factors of H_n's. For instance, the table below is obtained using this program for $1 \leq n \leq 7$.

n	all irreducible factors of H_n
1	$x+1,\ x^2+x+1.$
2	$x+1,\ x^4+x^3+x^2+x+1.$
3	$x+1,\ x^2+x+1,\ x^6+x^3+1.$
4	$x+1,\ x^8+x^5+x^4+x^3+1,\ x^8+x^7+x^6+x^4+x^2+x+1.$
5	$x+1,\ x^2+x+1,\ x^{10}+x^7+x^5+x^3+1,\ x^{10}+x^9+x^5+x+1,$ $x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1.$
6	$x+1,\ x^4+x^3+x^2+x+1,\ x^{12}+x^8+x^7+x^6+x^5+x^4+1,$ $x^{12}+x^{10}+x^7+x^6+x^5+x^2+1,$ $x^{12}+x^{10}+x^9+x^8+x^6+x^4+x^3+x^2+1,$ $x^{12}+x^{11}+x^9+x^7+x^6+x^5+x^3+x+1,$ $x^{12}+x^{11}+x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1.$
7	$x+1,\ x^2+x+1,\ x^{14}+x^9+x^7+x^5+1,$ $x^{14}+x^{10}+x^8+x^7+x^6+x^4+1,$ $x^{14}+x^{11}+x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+1,$ $x^{14}+x^{12}+x^9+x^8+x^7+x^6+x^5+x^2+1,$ $x^{14}+x^{12}+x^{10}+x^7+x^4+x^2+1,$ $x^{14}+x^{13}+x^{10}+x^8+x^7+x^6+x^4+x+1,$ $x^{14}+x^{13}+x^{11}+x^7+x^3+x+1,$ $x^{14}+x^{13}+x^{12}+x^9+x^8+x^7+x^6+x^5+x^2+x+1,$ $x^{14}+x^{13}+x^{12}+x^{11}+x^{10}+x^9+x^7+x^5+x^4+x^3+x^2+x+1.$

Here, notice that the only irreducible factor of H_n over $\mathbb{F}_2$ of odd degree is $x+1$. In fact, every root β of the polynomial H_n satisfies the equation

$$0 = \beta^{2^n+1} + 1 = \beta^{2^n}\beta + 1 = \beta^2 + 1 = (\beta+1)^2.$$

So we conclude that $x+1$ divides the polynomial H_n, for all n.

Now, before going further, it is good to emphasize that Theorem 31 can be reformalized in a similar way to Theorem 27:
Let $f \in \mathcal{I}$ be of degree $2n$, where $n > 1$. Then f divides H_n if and only if f satisfies the following three conditions:

- *$S \cdot f = f$;*
- *d divides n;*
- *$\frac{n}{d}$ is odd.*

It would be more useful to recall this formalization when we refer to Theorem 31 for the rest of this subsection.

Lemma 32. *For any $n \geq 1$;*

$$2^n = \sum_{\substack{d|n \\ \frac{n}{d} \equiv 1 \mod 2}} (2d) N^{(3)}(2d).$$

Proof. Let $EH_n := \{f \in \mathcal{I} \ : \ deg(f) \geq 2 \ \wedge \ f|H_n\}$. Then

$$EH_n = \{f \in \mathcal{I} \ : \ deg(f) \equiv 0 \mod 2 \ \wedge \ f|H_n\}.$$

$$= \bigcup_{d|n, \ \frac{n}{d} \equiv 1 (mod 2)} \{f \in \mathcal{I} \ : \ deg(f) = 2d \ \wedge \ S \cdot f = f \ \wedge \ f|H_n\},$$

by Theorem 31. Let $E(2d) := \{f \in \mathcal{I} \ : \ deg(f) = 2d \ \wedge \ S \cdot f = f \ \wedge \ f|H_n\}$, then

$$EH_n = \bigcup_{d|n, \ \frac{n}{d} \equiv 1 (mod 2)} E(2d).$$

By multiplying all elements in the sets of both sides and taking the degrees, the right hand side of the equation gives

$$\sum_{d|n, \ \frac{n}{d} \equiv 1 (mod 2)} \{deg(f) \ : \ f \in E(2d)\} = \sum_{d|n, \ \frac{n}{d} \equiv 1 (mod 2)} (2d) \left| E(2d) \right|$$

$$= \sum_{d|n, \ \frac{n}{d} \equiv 1 (mod 2)} (2d) N^{(3)}(2d)$$

while, using Theorem 31, the left hand side becomes

$$deg\Bigg(\prod_{f \in EH_n} f\Bigg) = deg\Bigg(\frac{x^{2^n+1}+1}{x+1}\Bigg) = 2^n.$$

Hence the proof is complete. □

Theorem 33.

$$N^{(3)}(n) = \begin{cases} \frac{1}{2m}\sum_{\substack{d|m \\ \frac{m}{d}\equiv 1 \mod 2}} \mu(d)2^{\frac{m}{d}} & \textit{if } n = 2m, \\ 0 & \textit{if } 2 \textit{ does not divide } n. \end{cases}$$

Proof. Define $H(m) := 2^m$ and $h(m) := 2mN^{(3)}(2m)$, for all $m \in \mathbb{N}^+$. Then Lemma 32 gives the equality

$$H(m) = \sum_{d|m,\ \frac{m}{d}\equiv 1(mod2)} h(d),\ \forall m \geq 1,$$

and; using Moebius Inversion Formula,

$$h(m) = \sum_{d|m,\ \frac{m}{d}\equiv 1(mod2)} \mu(d) H\left(\frac{m}{d}\right),\ \forall m \geq 1$$

which is

$$N^{(3)}(2m) = \frac{1}{2m} \sum_{\substack{d|m \\ \frac{m}{d}\equiv 1 \mod 2}} \mu(d)2^{\frac{m}{d}},\ \forall m \geq 1.$$

The other case is trivial by Corollary 17. □

Finally, to compute the number of orbits of degree n and orbit length 6, one can use the following corollary.

Corollary 34. $N^{(6)}(n) = \frac{1}{6}\left(\frac{1}{n}\sum_{d|n} 2^{\frac{n}{d}} - N^{(1)}(n) - 2N^{(2)}(n) - 3N^{(3)}(n)\right)$.

Proof. On one hand, if $N_2(n)$ denotes the number of irreducible polynomials over $\mathbb{F}_2$ of degree n, then it can be calculated using the techniques in [5] as

$$N_2(n) = \frac{1}{n}\sum_{d|n} 2^{\frac{n}{d}}.$$

And, on the other hand, one can count this number $N_2(n)$ in the following way

$$N_2(n) = N^{(1)}(n) + 2N^{(2)}(n) + 3N^{(3)}(n) + 6N^{(6)}(n).$$

□

4 The Construction of Invariant Irreducible Polynomials of a Higher Degree

Let f be a polynomial in $\mathcal{I}$ of degree n. In [3], Michon and Ravache study on finding several transformations $\tau : \mathbb{F}_2[x] \to \mathbb{F}_2[x]$ satisfying

- $\tau(f) \in \mathcal{I}$
- $deg(\tau(f)) > deg(f)$
- $|Orb(\tau(f))| = i$

at the same time, where $i \in \{1,\ 2,\ 3,\ 6\}$. In fact, we can formalize their problem in the following way:

Consider a matrix $A \in G$. Then f remains invariant under A if and only if $A \in Stab_G(f)$. Therefore, if we have a transformation $\tau : \mathbb{F}_2[x] \to \mathbb{F}_2[x]$ such that $\tau(f)$ is irreducible and $deg(Orb(\tau(f))) > n$, then $|Orb(\tau(f))|$ will be equal to the number $\frac{6}{k}$, where $k = ord_G(A)$.

In this section, we will see several examples of transformations satisfying the three properties given above.

4.1 To be invariant under ST or TS

Consider the following transformation defined in the article [3].

Definition 35. *For $f \in \mathbb{F}_2[x]$ of degree $n \geq 3$, define $\psi : \mathbb{F}_2[x] \to \mathbb{F}_2[x]$ as*

$$\psi(f(x)) := (x^2 + x)^n f\left(x + \frac{1}{x} + \frac{1}{x+1}\right). \tag{4.1}$$

Clearly, for any polynomial $f \in \mathbb{F}_2[x]$ of degree n, $\psi(f)$ will be a polynomial of degree $3n$. Also, $\psi(f)$ remains invariant under ST, by the following proposition.

Proposition 36. $(ST) \cdot \psi(f) = \psi(f)$.

Proof. Since $ST = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$, using (2.1),

$$ST \cdot \psi(f(x)) = (x+1)^{2n+n} \left(\left(\frac{1}{x+1} \right)^2 + \frac{1}{x+1} \right)^n f\left(\frac{1}{x+1} + x + 1 + \frac{x+1}{1+(x+1)} \right)$$

$$= \psi(f)(x).$$

□

The main question at this point is, for $f \in \mathcal{I}$, when $\psi(f)$ is irreducible over $\mathbb{F}_2$.

Let $f \in \mathcal{I}\backslash\{x^2+x+1\}$ be any irreducible polynomial of degree n. Consider the irreducible polynomial x^2+x+1 over $\mathbb{F}_2$, say ε is a root of it, i.e. $\varepsilon^2 = \varepsilon + 1$. Then all the roots of x^2+x+1 are ε and ε^2. Moreover, if $f(\varepsilon) = 0$, then ε will be a root of an irreducible polynomial of degree $n > 2$ which is a contradiction since $\varepsilon \in \mathbb{F}_2(\varepsilon) = \mathbb{F}_{2^2}$. Hence $f(\varepsilon) \in \{\ 1,\ \varepsilon,\ \varepsilon^2 = \varepsilon + 1\ \}$.

In fact, for a given $f \in \mathcal{I}$, a necessary and sufficient condition for $\psi(f)$ to be irreducible over $\mathbb{F}_2$ is that $f(\epsilon) \neq 1$. However, this task requires some work which we pursue below.

Since f is irreducible, we know that the splitting field of f over $\mathbb{F}_2$ is $\mathcal{K} := \mathbb{F}_{2^n}$. Let δ be a root of $\psi(f)$, then $\alpha := \delta + \frac{1}{\delta} + \frac{1}{\delta+1}$ must be a root of f. Moreover, all the roots of f are $\alpha,\ \alpha^2,\ \alpha^{2^2},\ ...,\alpha^{2^{n-1}}$; and so, $\mathcal{K} \subset \mathcal{K}(\delta)$.

Define a polynomial $T_\alpha \in \mathcal{K}[x]$ as

$$T_\alpha(x) := x^3 + (1+\alpha)x^2 + \alpha x + 1, \tag{4.2}$$

then δ will also be a root of T_α.

Proposition 37. *The roots of the polynomial T_α are*

$$\delta_i = 1 + \alpha + \varepsilon^i\omega + \frac{\alpha^2+\alpha+1}{\varepsilon^i\omega},$$

with $i \in \{0,\ 1,\ 2\}$ where ω is a cubic root of $(\varepsilon+\alpha)(\varepsilon+\alpha^2)$. Moreover, they satisfy the relations $\delta_1 = (\delta_0+1)^{-1}$ and $\delta_2 = 1 + {\delta_0}^{-1}$.

Proof. Set $y = 1 + \alpha + x$, then

$$T_\alpha(x) = (1+\alpha+y)^3 + (1+\alpha)(1+\alpha+y)^2 + \alpha(1+\alpha+y) + 1 = y^3 + (1+\alpha+\alpha^2)y + (1+\alpha+\alpha^2).$$

Let $b = \alpha^2+\alpha+1$ and $u,\ v$ be two variables such that $y = u + v$, then

$$T_\alpha(x) = (u+v)^3 + b(u+v) + b = (u^3+v^3) + (uv+b)(u+v) + b.$$

By choosing $uv = b$, we get

$$T_\alpha(x) = (u^3+v^3) + b,$$

so solving $T_\alpha(x) = 0$ is the same thing with solving the system of equations: $uv = b$ and $u^3 + v^3 = b$.

Writing $z = u^3$, we obtain

$$b^3 = u^3v^3 = zv^3 = z(u^3 + b) = z^2 + bz, \ i.e. \ z^2 + bz + b^3 = 0,$$

and by letting $t = \frac{z}{b}$,

$$0 = \frac{1}{b^2}(z^2 + bz + b^3) = t^2 + t + b = (t + \alpha)^2 + (t + \alpha) + 1$$

since $b = \alpha^2 + \alpha + 1$. Then $\alpha + \varepsilon^2$ is a solution for t. And

$$(\alpha + \varepsilon^2)b = (\alpha + \varepsilon^2)(1 + \alpha + \alpha^2) = (\alpha + \varepsilon^2)(\alpha + \varepsilon)(\alpha + \varepsilon^2) = (\alpha^2 + \varepsilon)(\alpha + \varepsilon)$$

is a solution for $z = u^3$ since $\varepsilon^3 = 1$. So, for $u = \omega$ and $v = \frac{b}{\omega}$,

$$x = y + \alpha + 1 = (u + v) + \alpha + 1 = 1 + \alpha + \omega + \frac{b}{\omega} = \delta_0$$

is a root of T_α. This implies

$$T_\alpha\left(1 + \frac{1}{\delta_0}\right) = \frac{1}{{\delta_0}^3}({\delta_0}^3 + (1 + \alpha){\delta_0}^2 + \alpha\delta_0 + 1) = 0 \tag{4.3}$$

and

$$T_\alpha\left(\frac{1}{1 + \delta_0}\right) = \frac{1}{1 + {\delta_0}^3}({\delta_0}^3 + (1 + \alpha){\delta_0}^2 + \alpha\delta_0 + 1) = 0. \tag{4.4}$$

Moreover, $T_\alpha(\delta_0) = 0$ means

$$\delta_0({\delta_0}^2 + (1 + \alpha)\delta_0 + \alpha) = 1$$

implying that

$$1+\frac{1}{\delta_0} = {\delta_0}^2+(1+\alpha)\delta_0+\alpha+1 = \left(1+\alpha+\omega+\frac{b}{\omega}\right)^2+(1+\alpha)\left(1+\alpha+\omega+\frac{b}{\omega}\right)+\alpha+1,$$

by definition of δ_0. Then

$$1 + \frac{1}{\delta_0} = 1 + \alpha^2 + \omega^2 + \frac{b^2}{\omega^2} + (1 + \alpha) + \alpha + \alpha^2 + (1 + \alpha)\omega + \frac{b(1 + \alpha)}{\omega} + \alpha + 1$$

$$= \omega^2\frac{b\omega}{b\omega} + \frac{b^2}{\omega^2}\frac{\omega}{\omega} + (1 + \alpha)\omega + (1 + \alpha)\frac{b}{\omega} + \alpha + 1$$

$$= \left(\frac{b^2}{\omega^3} + 1 + \alpha\right)\omega + \left(\frac{\omega^3}{b} + 1 + \alpha\right)\frac{b}{\omega} + \alpha + 1.$$

And, since $\omega^3 = (\varepsilon+\alpha)(\varepsilon+\alpha^2)$ and $b = \alpha^2+\alpha+1 = (\varepsilon+\alpha)(\varepsilon^2+\alpha)$, we get

$$\frac{b^2}{\omega^3}+1+\alpha = \frac{(\varepsilon+\alpha)^2(\varepsilon^2+\alpha)^2}{(\varepsilon+\alpha)(\varepsilon+\alpha^2)}+1+\alpha = \frac{\varepsilon^2+\alpha^2}{\varepsilon+\alpha}+1+\alpha = \frac{\varepsilon^2+\varepsilon+\alpha+\alpha\varepsilon}{\varepsilon+\alpha}$$

$$= \frac{\varepsilon(\varepsilon+\alpha)+(\varepsilon+\alpha)}{\varepsilon+\alpha} = \frac{(\varepsilon+\alpha)(\varepsilon+1)}{\varepsilon+\alpha} = \varepsilon+1 = \varepsilon^2,$$

using the equation $\varepsilon^2+\varepsilon+1=0$; while, on the other hand, we have

$$\frac{\omega^3}{b}+1+\alpha = \frac{(\varepsilon+\alpha)(\varepsilon+\alpha^2)}{(\varepsilon+\alpha)(\varepsilon^2+\alpha)}+1+\alpha = \frac{\varepsilon+\alpha^2+\varepsilon^2+\alpha+\alpha\varepsilon^2+\alpha^2}{\varepsilon^2+\alpha}$$

$$= \frac{\varepsilon+\varepsilon^2+\alpha+\alpha\varepsilon^2}{\varepsilon^2+\alpha}.\frac{\varepsilon^2}{\varepsilon^2} = \frac{1+\varepsilon+\alpha\varepsilon^2+\alpha\varepsilon}{\varepsilon+\alpha\varepsilon^2} = \frac{(1+\alpha\varepsilon)(1+\varepsilon)}{\varepsilon(1+\alpha\varepsilon)} = \frac{\varepsilon^2}{\varepsilon}.\frac{\varepsilon}{\varepsilon} = \frac{1}{\varepsilon^2}.$$

Thus we conclude

$$\delta_2 = 1+\frac{1}{\delta_0}$$

is a root of T_α, using (4.3). By several similar calculations, one can easily conclude

$$\delta_1 = \frac{1}{1+\delta_0}$$

is a root of T_a, using (4.4). □

Lemma 38. *If $f \in \mathcal{I}$ of degree $n > 2$, then $\psi(f)(x)$ must be equal to*

$$\prod_{0\le k\le n-1} T_{\alpha^{2^k}}(x),$$

where $\alpha \in \mathcal{K}$ is a root of f.

Proof. For any root δ of $\psi(f)$, we have

$$\frac{1}{\delta+1}+\frac{1}{\frac{1}{\delta+1}}+\frac{1}{\frac{1}{\delta+1}+1} = \frac{1}{\delta+1}+\delta+1+\frac{\delta+1}{\delta} = \delta+\frac{1}{\delta}+\frac{1}{\delta+1}$$

and

$$\left(1+\frac{1}{\delta}\right)+\frac{1}{(1+\frac{1}{\delta})}+\frac{1}{(1+\frac{1}{\delta})+1} = 1+\frac{1}{\delta}+\frac{\delta}{\delta+1}+\delta = \delta+\frac{1}{\delta}+\frac{1}{\delta+1}.$$

So we can say that for any root δ of $\psi(f)$, $\frac{1}{\delta}$ and $\frac{1}{\delta+1}$ are also roots of $\psi(f)$. Furthermore, using the previous proposition and the fact that any root of $\psi(f)$ is also a root of T_α, we can write the following equalities in $\mathbb{F}_{2^n}$

$$\psi(f)(x) = \prod_{\psi(f)(\delta)=0} (x-\delta) = \prod_{f(\delta+\frac{1}{\delta}+\frac{1}{\delta+1})=0} (x-\delta)\left(x-\frac{1}{\delta}\right)\left(x-1-\frac{1}{1+\delta}\right)$$

$$= \prod_{f(\alpha)=0} T_\alpha(x) = \prod_{0\le k\le n-1} T_{\alpha^{2^k}}(x).$$

□

Lemma 39. *Let $f(\varepsilon)=1$. Then $(\varepsilon+1)(\varepsilon+a^2)$ has cubic roots in*

- *$\mathcal{K}$ if n is even,*
- *$\mathcal{K}(\varepsilon)$ if n is odd.*

Proof. If n is even, then there will be an integer m such that $n=2m$. Let α be a root of f, then

$$f(\varepsilon) = (\varepsilon+\alpha)(\varepsilon+\alpha^2)(\varepsilon+\alpha^{2^2})...(\varepsilon+\alpha^{2^{2m-1}}).$$

Using $\varepsilon^4=(\varepsilon+1)^2=\varepsilon^2+1=\varepsilon$,

$$f(\varepsilon) = [(\varepsilon+\alpha)(\varepsilon+\alpha^2)][(\varepsilon^4+\alpha^4)(\varepsilon^4+\alpha^8)]...[(\varepsilon^{2^{2m-2}}+\alpha^{2^{2m-2}})(\varepsilon^{2^{2m-2}}+\alpha^{2^{2m-1}})]$$

$$= [(\varepsilon+\alpha)(\varepsilon+\alpha^2)][(\varepsilon+\alpha)(\varepsilon+\alpha^2)]^4...[(\varepsilon+\alpha)(\varepsilon+\alpha^2)]^{2^{2m-2}}$$

$$= [(\varepsilon+\alpha)(\varepsilon+\alpha^2)]^{\frac{2^n-1}{3}}$$

since $1+4+...+4^{m-1}=\frac{4^m-1}{4-1}=\frac{2^n-1}{3}$. Let ω be a cubic root of $(\varepsilon+\alpha)(\varepsilon+\alpha^2)$ in some extension of $\mathbb{F}_2$, then

$$\omega^{2^n-1} = (\omega^3)^{\frac{2^n-1}{3}} = [(\varepsilon+\alpha)(\varepsilon+\alpha^2)]^{\frac{2^n-1}{3}} = f(\varepsilon) = 1,$$

by assumption. So ω is a $(2^n-1)^{th}$ root of unity implying that $\omega\in\mathbb{F}_{2^n}=\mathcal{K}$.

If n is odd, then there will be an integer k such that $n=2k+1$, and for a root α of f, we will have

$$f(\varepsilon) = (\varepsilon+\alpha)(\varepsilon+\alpha^2)(\varepsilon+\alpha^4)...(\varepsilon+\alpha^{2^{2k}}). \tag{4.5}$$

Since $\alpha\in\mathbb{F}_{2^n}$, by Fermat's Little Theorem, we have $\alpha=\alpha^{2^{2k+1}}$ and so

$$f(\varepsilon) = (\varepsilon+\alpha^{2^{2k+1}})(\varepsilon+\alpha^{2^{2k+2}})...(\varepsilon+\alpha^{2^{4k}})(\varepsilon+\alpha^{2^{4k+1}}). \tag{4.6}$$

By multiplying the equations (4.5) and (4.6), we obtain

$$[f(\varepsilon)]^2 = [(\varepsilon+\alpha)(\varepsilon+\alpha^2)][(\varepsilon+\alpha)(\varepsilon+\alpha^2)]^4 ... [(\varepsilon+\alpha)(\varepsilon+\alpha^2)]^{4^{2k}}$$

$$= [(\varepsilon+\alpha)(\varepsilon+\alpha^2)]^{\frac{2^{2n}-1}{3}}$$

since $1+4+...+4^{2k} = \frac{4^{2k+1}-1}{4-1} = \frac{2^{2n}-1}{3}$. Thus

$$\omega^{2^{2n}-1} = \omega^{3\frac{2^{2n}-1}{3}} = [(\varepsilon+\alpha)(\varepsilon+\alpha^2)]^{\frac{2^{2n}-1}{3}} = [f(\varepsilon)]^2 = 1.$$

So ω is a $(2^{2n}-1)^{th}$ root of unity, i.e. $\omega \in \mathbb{F}_{2^{2n}}$. On the other hand,

$$[\mathcal{K}(\varepsilon) : \mathbb{F}_2] = [\mathcal{K}(\varepsilon) : \mathcal{K}][\mathcal{K} : \mathbb{F}_2] = 2n$$

gives us $\mathcal{K}(\varepsilon) = \mathbb{F}_{2^{2n}}$, so $\omega \in \mathcal{K}(\varepsilon)$.

□

Now, by combining the results of the previous two lemmas, one can conclude the following corollary:

Corollary 40. *If $f \in \mathcal{I}$ of degree n is such that $f(\varepsilon) = 1$, then $\psi(f)$ is reducible.*

Proof. If n is even, then $\omega \in \mathcal{K}$, by Lemma 39. Since we already have $\alpha \in \mathcal{K}$ and $\varepsilon \in \mathbb{F}_{2^2} \subset \mathbb{F}_{2^n} = \mathcal{K}$, by Proposition 37, all the roots of T_α are in $\mathcal{K}$. And, by definition of T_α, we conclude all the roots of $\psi(f)$ are in $\mathcal{K} = \mathbb{F}_{2^n}$. However, $deg(\psi(f)) = 3n \neq n$. So $\psi(f)$ cannot be irreducible over $\mathbb{F}_2$.
If n is odd, then $\omega \in \mathcal{K}(\varepsilon)$, by Lemma 39, and since $\mathcal{K}(\varepsilon) = \mathbb{F}_{2^n}(\varepsilon) = \mathbb{F}_{2^{2n}}$, by a similar argumentation to the previous part, we have all the roots of $\psi(f)$ are in $\mathbb{F}_{2^{2n}}$. However, $deg(\psi(f)) = 3n \neq 2n$. Thus, $\psi(f)$ must be reducible over $\mathbb{F}_2$. □

Proposition 41. *If $f \in \mathcal{I}$ of degree $n > 2$ satisfies that $\psi(f)$ is reducible over $\mathbb{F}_2[x]$, then $\psi(f) = g(ST \cdot g)(TS \cdot g)$, for some $g \in \mathcal{I}$ of degree n such that $ST \cdot g \neq g$.*

Proof. Let δ be a root of $\psi(f)$. Say $g(x) \in \mathbb{F}_2[x]$ be the minimal polynomial of δ. Then $n | deg(g)$ since $\mathcal{K} \subset \mathcal{K}$, and $n \leq deg(g) < 3n$ since $\psi(f)$ is assumed to be reducible over $\mathbb{F}_2$. Also any irreducible factor of $\psi(f)$ in $\mathbb{F}_2[x]$ has to be of degree $\geq n$ since g is the minimal polynomial of δ. So

$$\psi(f)(x) = g(x)h(x),\ for\ some\ g \in \mathcal{I}\ :\ deg(g) = n\ and\ h \in \mathbb{F}_2[x]\ deg(h) = 2n.$$

Consider $ST \cdot g(x) = (x+1)^n g(\frac{1}{x+1})$ and $TS \cdot g(x) = x^n g(\frac{x+1}{x})$. Since the roots of $ST \cdot g$ and $TS \cdot g$ are $\frac{1}{\delta+1}$ and $1 + \frac{1}{\delta}$ which are the roots of $\psi(f)$, we conclude

$ST \cdot g | \psi(f)$ and $TS \cdot g | \psi(f)$.

If $ST \cdot g \neq g$, then $\psi(f)(x) = g(x)(ST \cdot g)(x)(TS \cdot g)(x)$.

Let $ST \cdot g = g$, then δ, $\frac{1}{1+\delta}$, $1 + \frac{1}{\delta}$ will be distinct roots of $ST \cdot g = g = TS \cdot g$; and so, we get $T_\alpha(x)$ divides $g(x)$ for $\alpha = \delta + \frac{1}{\delta} + \frac{1}{\delta+1}$. Since all roots of g are δ, δ^2, δ^{2^2}, ..., $\delta^{2^{n-1}}$, we get $T_{\alpha^{2^k}}$ divides g for all k. However, this means $g(x)$ has $3n$ distinct roots δ^{2^k}, $\frac{1}{\delta^{2^k}+1}$, $1 + \frac{1}{\delta^{2^k}}$ for $0 \leq k \leq n-1$, by the previous lemma, which is a contradiction. So $ST \cdot g \neq g$. i.e.

$$\psi(f) = g(x)(x+1)^n g\left(\frac{1}{x+1}\right) x^n g\left(1 + \frac{1}{x}\right)$$

with $g \in \mathcal{I} \setminus \{x^2 + x + 1\}$ such that $ST \cdot g \neq g$. So

$$\psi(f)(\varepsilon) = g(\varepsilon)\left[(\varepsilon+1)^n g\left(\frac{1}{\varepsilon+1}\right)\right]\left[\varepsilon^n g\left(\frac{\varepsilon+1}{\varepsilon}\right)\right] = [g(\varepsilon)]^3.$$

We already know $g(\varepsilon) \neq 0$ and one can see that $[g(\varepsilon)] = 1$, for all $g(\varepsilon) \in \{1,\ \varepsilon,\ \varepsilon^2\}$. On the other hand,

$$\psi(f)(\varepsilon) = (\varepsilon^2 + \varepsilon)^n f\left(\varepsilon + \frac{1}{\varepsilon} + \frac{1}{\varepsilon+1}\right) = f(\varepsilon^2).$$

So $f(\varepsilon^2) = 1$. Furthermore,

$$f(\varepsilon^2) = a_0 + a_1\varepsilon^2 + a_2(\varepsilon^2)^2 + ... + a_n(\varepsilon^2)^n = {a_0}^2 + {a_1}^2\varepsilon^2 + {a_2}^2(\varepsilon^2)^2 + ... + {a_n}^2(\varepsilon^2)^n$$

$$= (a_0 + a_1\varepsilon + a_2\varepsilon^2 + ... + a_n\varepsilon^n)^2 = [f(\varepsilon)]^2,$$

where $f(x) := a_0 + a_1 x + a_2 x^2 + ... + a_n x^n$, since the characteristic of the field is 2. So $f(\varepsilon) = 1$. □

Theorem 42. *Let $f \in \mathcal{I}$ be of degree $n \geq 3$. If $f(\varepsilon) \neq 1$, then $\psi(f)$ is an irreducible polynomial such that $ST \cdot \psi(f) = \psi(f)$.*

Proof. Let $f \in \mathcal{I}$ be of degree $n > 2$ such that $f(\varepsilon) \neq 1$. Then $\psi(f)$ is irreducible, by the contrapositive of the previous proposition; and Proposition 21 completes the proof.

□

Corollary 43. *For $f \in \mathcal{I}$, $\psi(f)$ is irreducible if and only if $f(\varepsilon) \neq 1$.*

Proof. It's a direct conclusion of the previous theorem and Proposition 36. □

Thus, if $f \in \mathcal{I}$ of degree $n \geq 3$ satisfies $f(\varepsilon) \neq 1$, we can use the transformation ψ to get an irreducible polynomial of a greater degree which is invariant under ST.

Now, let $f \in \mathcal{I}$ be a polynomial invariant under the action of ST. Then it must be invariant under TS since

$$TS \cdot f = TS \cdot (ST \cdot f) = T \cdot (S^2) \cdot T \cdot f = T^2 \cdot f = f.$$

Therefore, the way described above is valid to obtain an irreducible polynomial of a greater degree which is invariant under TS, too.

4.2 To be invariant under S

The study of Meyn in [2] carries a great importance for the polynomials $f \in \mathcal{I}$ fixed by S, and the following transformation is defined in this study of Meyn.

Definition 44. *Define a transformation $\phi : \mathbb{F}_2[x] \to \mathbb{F}_2[x]$ as*

$$\phi(f(x)) := x^n f\left(x + \frac{1}{x}\right), \ \forall f \in \mathbb{F}_2[x] \ : \ deg(f) = n. \tag{4.7}$$

Proposition 45. *For any polynomial $f \in \mathbb{F}_2[x]$, we have $S \cdot \phi(f) = \phi(f)$. Moreover, $\phi(f)$, $T \cdot \phi(f)$ and $ST \cdot \phi(f)$ are all distinct polynomials.*

Proof. Let f be given in $\mathbb{F}_2[x]$. Then

$$S \cdot \phi(f)(x) = S\left(\cdot x^n f\left(x + \frac{1}{x}\right)\right) = x^{2n}\left(\frac{1}{x}\right)^n f\left(x + \frac{1}{x}\right) = x^n f\left(x + \frac{1}{x}\right) = \phi(f)(x)$$

using (2.1) and (4.9). Also, one can easily obtain

$$T \cdot \phi(f) = (x+1)^n f\left(x + 1 + \frac{1}{x+1}\right) = (x+1)^n f\left(\frac{x^2+x+1}{x+1}\right)$$

and

$$ST \cdot \phi(f) = S \cdot (x+1)^n f\left(\frac{x^2+x+1}{x+1}\right) = x^{2n}\left(\frac{1}{x}+1\right)^n f\left(\frac{(\frac{1}{x})^2 + \frac{1}{x} + 1}{\frac{1}{x}+1}\right)$$

$$= (x^2+x)^n f\left(\frac{x^2+x+1}{x^2+x}\right),$$

which complete the proof. □

So the question is when $\phi(f)$ is irreducible over $\mathbb{F}_2$.

Lemma 46. *If $f \in \mathcal{I}$ of degree n, then either $S \cdot \phi(f) = \phi(f)$ or $\phi(f) = g_1 g_2$, where $g_1, g_2 \in \mathcal{I}$.*

Proof. Let β be a root of $\phi(f)$. Then

$$0 = \phi(f)(\beta) = \beta^n f\left(\beta + \frac{1}{\beta}\right)$$

gives that $\alpha := \beta + \frac{1}{\beta}$ is a root of f; and so, the splitting field of f over $\mathbb{F}_2$ is $\mathbb{F}_{2^n} = \mathbb{F}_2(\alpha)$. If β were a root of a polynomial $h \in \mathcal{I}$ of degree m where $m < n$, then

$$\mathbb{F}_{2^m} = \mathbb{F}_2(\beta) = \mathbb{F}_2(\alpha) = \mathbb{F}_{2^n}$$

would imply the contradiction: $m = n$ and $m < n$. So β cannot be a root of a polynomial whose degree is less than n. Since β is already a root of $\phi(f)$, we conclude that the irreducible decomposition of $\phi(f)$ cannot contain a polynomial of degree less than n. Since $deg(\phi(f)) = 2n$, this means that either $\phi(f) \in \mathcal{I}$ or there exist $g_1, g_2 \in \mathcal{I}$ such that $\phi(f)(x) = g_1(x)g_2(x)$. □

Lemma 47. *With the notations fixed in the previous lemma, we have the following result: $\phi(f) \in \mathcal{I}$ if and only if $g(x) = x^2 - \alpha x + 1 \in \mathbb{F}_{2^n}[x]$ is irreducible.*

Proof. β is a root of g since

$$g(\beta) = \beta^2 - \alpha\beta + 1 = \beta^2 - \left(\beta + \frac{1}{\beta}\right)\beta + 1 = \beta^2 - \beta^2 - 1 + 1 = 0.$$

On the other hand, we know $\phi(f) \in \mathcal{I}$ if and only if $ord_{\mathbb{F}_2}(\beta) = deg(\phi(f)) = 2n$. If g is reducible, then β will be a root of a polynomial of degree 1 over $\mathbb{F}_{2^n}$, and so $ord_{\mathbb{F}_2}(\beta)$ becomes n. Hence $\phi(f) \in \mathcal{I}$ if and only if g is irreducible. □

Proposition 48. *There exists a normal basis $\{\gamma,\ \gamma^2,\ ,\gamma^{2^2},\ ...,\gamma^{2^{n-1}}\}$ of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ with $\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(\gamma) = 1$.*

Proof. By Normal Basis Theorem, there exists a normal basis $\{\rho,\ \rho^2,\ \rho^{2^2},\ ...,\rho^{2^{n-1}}\}$ of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$. First, we want to show that $\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(\rho^{2^k}) \neq 0$, for some $0 \leq k \leq n-1$. Assume it is not true, and say $\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(\rho^{2^s}) = 0$, for all $0 \leq s \leq n-1$. For any $\eta \in \mathbb{F}_{2^n}$, we have $\eta = \sum_{0 \leq i \leq n-1} a_i \rho^{2^i}$, for some $a_i \in \mathbb{F}_2$, and

$$\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(\eta) = \mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}\left(\sum_{i=0}^{n-1} a_i \rho^{2^i}\right) = \sum_{i=0}^{n-1} a_i \mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(\rho^{2^i}) = 0,$$

i.e. $\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(\mathbb{F}_{2^n}) = \{0\}$. However, this is a contradiction since the trace map is onto.
Thus there exists an integer k such that $0 \leq k \leq n-1$ and $\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(\rho^{2^k}) = 1$, for some $0 \leq k \leq n-1$. Define $\gamma := \rho^{2^k}$, then

$$\rho^{2^i} = \gamma^{2^{n-k+i}}, \forall i: \ 0 \leq i \leq k-1$$

and

$$\rho^{2^{k+j}} = \rho^{2^j}, \forall j: \ 0 \leq j \leq n-k-1$$

implies that the set

$$\{\rho, \ \rho^2, \ \rho^{2^2}, \ ..., \rho^{2^{n-1}}\} = \{\gamma, \ \gamma^2, \ \gamma^{2^2}, \ ..., \gamma^{2^{n-1}}\}$$

is a normal basis $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$. □

Proposition 49. *The quadratic equation $x^2 + x + \xi = 0$, where $\xi \in \mathbb{F}_{2^n}$ has*

- *two roots in $\mathbb{F}_{2^n}$ if $\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(\xi) = 0$.*
- *no root in $\mathbb{F}_{2^n}$ if $\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(\xi) = 1$.*

Proof. First, we will prove the second part of the proposition, by showing the contrapositive of the statement is true.
Let $\{\gamma, \ \gamma^2, \ , \gamma^{2^2}, \ ..., \gamma^{2^{n-1}}\}$ be a normal basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ such that $\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(\gamma) = 1$. Then there exist $b_0, \ b_1, \ ..., b_{n-1} \in \mathbb{F}_2$ and $x_0, \ x_1, \ ..., x_{n-1} \in \mathbb{F}_2$ satisfying

$$\xi = b_0\gamma + b_1\gamma^2 + b_2\gamma^{2^2} + ... + b_{n-1}\gamma^{2^{n-1}}, \ x = x_0\gamma + x_1\gamma^2 + x_2\gamma^{2^2} + ... + x_{n-1}\gamma^{2^{n-1}};$$

and so

$$x^2 + x = (x_0\gamma^2 + x_1\gamma^{2^2} + x_2\gamma^{2^3} + ... + x_{n-1}\gamma^{2^n}) + (x_0\gamma + x_1\gamma^2 + x_2\gamma^{2^2} + ... + x_{n-1}\gamma^{2^{n-1}})$$

$$= (x_{n-1} + x_0)\gamma + (x_0 + x_1)\gamma^2 + ... + (x_{n-2} + x_{n-1})\gamma^{2^{n-1}}.$$

Also, having $0 = x^2 + x + \xi$, we get the following equations:

$$x_{n-1} + x_0 = b_0; \ x_0 + x_1 = b_1, \ ..., x_{n-2} + x_{n-1} = b_{n-1}$$

implying that

$$b_0 + b_1 + ... + b_{n-1} = (x_{n-1} + x_0) + (x_0 + x_1) + ... + (x_{n-2} + x_{n-1}) = 0.$$

On the other hand, if we compute $\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(\xi)$, using the representation of ξ as a combination of vectors in the normal basis, easily seen that it is equal to

$$(b_0\gamma+b_1\gamma^2+...+b_{n-1}\gamma^{2^{n-1}})+(b_{n-1}\gamma+b_0\gamma^2+...+b_{n-2}\gamma^{2^{n-1}})+...+(b_1\gamma+b_2\gamma^2+...+b_0\gamma^{2^{n-1}})$$

$$= (b_0 + b_1 + ...b_{n-1})(\gamma + \gamma^2 + ... + \gamma^{2^{n-1}}) = (b_0 + b_1 + ...b_{n-1})$$

since $\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(\gamma) = 1$. So we conclude that

$$0 = b_0 + b_1 + ... + b_{n-1} = \mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(\xi).$$

To prove the first part of the proposition, assume that $\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(\xi) = 0$. Then it is easily verified that

$$x_0 = \kappa,\ x_1 = \kappa + b_1,\ x_2 = \kappa + b_1 + b_2,\ ..., x_{n-1} = \kappa + b_1 + b_2 + ... + b_{n-1},$$

where $\kappa = 0$ or 1. So there are two solutions of the equation $x^2 + x + \xi = 0$. □

Theorem 50. *With the notations fixed in the previous two lemmas, we have the following result:* $\phi(f) \in \mathcal{I}$ *if and only if* $\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(\alpha) = 1$.

Proof. We already know that $\phi(f) \in \mathcal{I}$ if and only if $g(x) = x^2 - \alpha x + 1 \in \mathbb{F}_{2^n}[x]$ is irreducible, by Lemma 39. To use the previous proposition; multiply the polynomial g by α^{-2}, define $y := -\frac{x}{\alpha}$ and $\xi := \frac{1}{\alpha^2}$:

$$\frac{x^2}{\alpha^2} - \frac{x}{\alpha} + \frac{1}{\alpha^2} = y^2 + y + \xi.$$

So this polynomial is irreducible if and only if $\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(\frac{1}{\alpha^2}) = \mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(\xi) = 1$. Finally,

$$\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}\left(\frac{1}{\alpha}\right) = \frac{1}{\alpha} + \frac{1}{\alpha^2} + \frac{1}{\alpha^{2^2}} + ... + \frac{1}{\alpha^{2^{n-1}}} = \frac{1 + \alpha^2 + \alpha^{2^2} + ... + \alpha^{2^{n-1}}}{\alpha}$$

gives us the desired result, using the facts $\alpha^{2^n} = \alpha$ and $\mathrm{Tr}_{F/\mathbb{F}_2}(\vartheta^2) = \vartheta,\ \forall\vartheta \in F$. □

Hence, for a given polynomial $f \in \mathcal{I}$ of degree n, if $\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(\alpha) = 1$, then we can use the transformation ψ to obtain an irreducible polynomial of degree $2n$, which is invariant under S.

4.3 To be invariant under T or STS

Definition 51. *Define transformations ϕ_T and ϕ_{ST} from $\mathbb{F}_2[x]$ to $\mathbb{F}_2[x]$ as $\phi_T(f(x)) := (T \cdot \phi(f))(x)$ and $\phi_{ST}(f(x)) := (ST \cdot \phi(f))(x)$, for all $f(x) \in \mathbb{F}_2[x]$.*

Proposition 52. *For $f(x) \in \mathbb{F}_2[x]$, we have*

a. *$STS \cdot \phi_T(f) = \phi_T(f)$ and $T \cdot \phi_{ST}(f) = \phi_{ST}(f)$.*

b. *$\phi_T(f)$ and $\phi_{ST}(f)$ are both of degree $2n$.*

Proof.

a. By Proposition 45, we get

$$STS \cdot \phi_T(f) = TST \cdot (T \cdot \phi(f)) = T \cdot (S \cdot \phi(f)) = T \cdot \phi(f) = \phi_T(f)$$

and

$$T \cdot \phi_{ST}(f) = T \cdot (ST \cdot \phi(f)) = ST \cdot (S \cdot \phi(f) = ST \cdot \phi(f) = \phi_{ST}(f).$$

b. Clear by Lemma 1, since $\phi(f)$ is of degree $2n$.

□

Proposition 53. *For all $f \in \mathbb{F}_2[x]i$ the following statements are equivalent:*

i. *$\phi(f)$ is irreducible over $\mathbb{F}_2$.*

ii. *$\phi_T(f)$ is irreducible over $\mathbb{F}_2$.*

iii. *$\phi_{ST}(f)$ is irreducible over $\mathbb{F}_2$.*

Proof. First, we will prove the statement *ii.* implies *i.* by showing the contrapositive of it. Let $\phi(f)$ be reducible over $\mathbb{F}_2$, then $\phi(f) = gh$, for some nonconstant polynomials g and h in $\mathbb{F}_2[x]$. So, we get

$$\phi_T(f) = T \cdot (\phi(f)) = T \cdot (gh) = (T \cdot g)(T \cdot g),$$

where both of the polynomials on the right hand side are nonconstant, by Lemma 1. So the reducibility of $\phi(f)$ implies the reducibility of $\phi_T(f)$.

In fact, all other implications can be shown easily using a similar approach. □

So, for a given polynomial $f \in \mathcal{I}$ of degree n, if $Tr_{\mathbb{F}_2^n/\mathbb{F}_2}(\alpha) = 1$, one can use the transformation ϕ_{ST} to find an irreducible polynomial of degree $2n$ which is invariant under T, and the transformation ϕ_T to find an irreducible polynomial of degree $2n$ which is invariant under STS.

5 Conclusion

Consequently, we defined a group action of the group $\mathrm{GL}_2(\mathbb{F}_2)$ on the set of irreducible binary polynomials of degree ≥ 2, studied on the orbits of the polynomials taken from the set and also on the construction of several invariant polynomials of higher degree, in the light of three articles.

In short, this master thesis can be considered as a half step for the generalization of the results of *Michon* and *Ravache* in [1] and [3] to the $\mathbb{F}_q$-case, but it is also nourished by the article [2] of Meyn. After all, one can extend (2.1) to a definition of group action of $\mathrm{GL}_2[\mathbb{F}_q]$ on the set of irreducible polynomials of degree $n \geq 2$ over $\mathbb{F}_q$ in a natural way. Then similar results to the $\mathbb{F}_2$-case will be valid in this generalization, too.

References

[1] J.F. Michon and P. Ravache, “On different families of irreducible polynomials over $\mathbb{F}_2$”, *Finite Fields and Their Applications 16(3)* (2010) 163-174.

[2] H. Meyn, “On construction of irreducible self-reciprocal polynomials over finite fields”, *Appl. Algebra Engrg. Comm. Comput. 1* (1990), 43-53.

[3] J.F. Michon and P. Ravache, “Transformations on irreducible binary polynomials”, *C. Carlet and A. Pott (Eds.): SETA 2010, LNCS 6338* (2010), 166-180.

[4] W. Bosma, J. Cannon and C. Playoust, “The Magma Algebra System I. The user language”, *J. Symbolic Comput., vol. 24* (1997), 235-265.

[5] R. Lidl and H. Niederreiter, “Finite Fields”, *Encyclopedia of Mathematics and Its Applications, 2nd Edition: Cambridge University Press* (1997), 37-106.

[6] F.J. MacWilliams and N.J.A. Sloane, “The theory of error-correcting codes”, *Amsterdam: North-Holland* (1977), 277-278.