



HAL
open science

Transformations on Irreducible Binary Polynomials

Jean Francis Michon, Philippe Ravache

► **To cite this version:**

Jean Francis Michon, Philippe Ravache. Transformations on Irreducible Binary Polynomials. 6th International Conference Sequences and Their Applications - SETA 2010, Sep 2023, Paris, France. pp.166-180, 10.1007/978-3-642-15874-2_13 . hal-04156219

HAL Id: hal-04156219

<https://hal.science/hal-04156219v1>

Submitted on 7 Jul 2023

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



Distributed under a Creative Commons Attribution - NonCommercial - NoDerivatives 4.0 International License

Transformations on Irreducible Binary Polynomials

Jean-Francis Michon and Philippe Ravache

Université de Rouen, LITIS EA 4108
BP 12 - 76801 Saint-Étienne du Rouvray cedex, France.
{jean-francis.michon, philippe.ravache}@litislab.fr

Abstract. Using the natural action of $GL_2(\mathbb{F}_2) \simeq \mathfrak{S}_3$ over $\mathbb{F}_2[X]$, one can define different classes of polynomials strongly analogous to self-reciprocal irreducible polynomials. We give transformations to construct polynomials of each kind of invariance and we deal with the question of explicit infinite sequences of invariant irreducible polynomials in $\mathbb{F}_2[X]$. We generalize results obtained by Varshamov, Wiedemann, Meyn and Cohen and we give sequences of invariant irreducible polynomials. Moreover we explain what happens when the given constructions fail. We also give a result on the order of the polynomials of one of the classes: the alternate irreducible polynomials.

Keywords: irreducible polynomials, finite fields, sequences of irreducible invariant polynomials.

1 Introduction

In [6], we studied the natural action of the 6 elements group $\mathfrak{S}_3 \simeq GL_2(\mathbb{F}_2) \simeq PGL_2(\mathbb{F}_2)$ on the set

$$\mathcal{I} = \{P \in \mathbb{F}_2[X] \mid P \text{ irreducible}\} \setminus \{X, X+1\}.$$

This action of \mathfrak{S}_3 on \mathcal{I} , is defined by the two operations

$$P^+(X) = P(X+1)$$
$$P^*(X) = X^{\deg P} P\left(\frac{1}{X}\right).$$

The action of all other elements of \mathfrak{S}_3 are obtained by compositions of these two operations. We shall write for example P^{**+} for $(P^*)^+$.

Definition 1 *The **hexagon** of $P \in \mathcal{I}$ is the orbit of P :*

$$Hex(P) = \{P^\sigma \mid \sigma \in \mathfrak{S}_3\}.$$

*The **degree** of a hexagon is the degree of its polynomials. When $Card(Hex(P)) < 6$ we say that the hexagon is **degenerate**.*

Such an orbit has 1, 2, 3 or 6 elements according to the isotropy subgroup of P . In \mathfrak{S}_3 , apart from the trivial subgroups, we have 3 subgroups of order 2, and one of order 3. Each of them will give a family of invariant irreducible polynomials. The case of 1 element hexagon is easy : $\mathcal{I}(2) = \{X^2 + X + 1\}$ is the only 1 element degenerate hexagon. This polynomial is the only fixed point of the action.

Let us define for any integer $n > 1$

$$\mathcal{I}(n) = \{P \in \mathcal{I} \mid \deg P = n\},$$

then this grading of \mathcal{I} is stable under the action (but this is not true for $n = 1$).

2 Self-reciprocity and the 3 Elements Degenerate Hexagons

Self-reciprocal polynomials are invariant under the action of one subgroup of order 2 (generated by $*$ operation). In fact there is no reason to focus on one subgroup because they are all conjugate.

2.1 The Invariant Polynomials

Definition 2 Let P be a polynomial, P is said to be **self-reciprocal** (resp. **periodic**, **median**) if $P^* = P$ (resp. $P^+ = P$, $P^{**} = P^{**} = P$). We easily check that these polynomials are of even degree.

Definition 3 Let P and Q , $P \neq Q$, be two polynomials of \mathcal{I} , $\{P, Q\}$ is said to be a **reciprocal pair** (resp. **periodic pair**, **median pair**) if $Q = P^*$ (resp. $Q = P^+$, $Q = P^{**}$). As the polynomials of a pair have the same degree, by extension, it will also be the degree of the pair.

Definition 4 A **3 elements degenerate hexagon** is made of a self-reciprocal irreducible polynomial P , a median irreducible polynomial Q and a periodic irreducible polynomial R such that:



The next theorem extends Meyn's one (see [4], Theorem 1) to the periodic and median polynomials:

Theorem 1 *i) Each self-reciprocal (resp. periodic, median) irreducible polynomial of degree $2n$ ($n \geq 1$) is a factor of the polynomial*

$$H_{r,n}(X) = X^{2^n+1} + 1$$

$$\text{(resp. } H_{p,n}(X) = X^{2^n} + X + 1, \quad H_{m,n}(X) = X^{2^n} + X^{2^n-1} + 1).$$

ii) Each irreducible factor of degree ≥ 2 of $H_{r,n}$ (resp. $H_{p,n}$, $H_{m,n}$) is a self-reciprocal (resp. periodic, median) polynomial of degree $2d$, where d divides n such that n/d is odd.

Proof. In [4], Meyn proves the theorem for self-reciprocal polynomials. We trivially extend it to the periodic (resp. median) polynomials noting that, on the one hand, $H_{p,n} = H_{r,n}^{+*}$ (resp. $H_{m,n} = H_{r,n}^+$) and on the other hand, a periodic (resp. median) irreducible polynomial is obtained from a self-reciprocal one, applying the transformation $+^*$ (resp. $+$) on it.

2.2 The Quadratic Transformations

Definition 5 We define the maps $\phi_p, \phi_m, \phi_r: \mathbb{F}_2[X] \rightarrow \mathbb{F}_2[X]$ by

$$\begin{aligned}\phi_p(P) &= P(X^2 + X) \\ \phi_m(P) &= \phi_p(P)^* = X^{2n} P\left(\frac{X+1}{X^2}\right) \\ \phi_r(P) &= \phi_p(P)^{*+} = (X^2 + 1)^n P\left(\frac{X}{X^2 + 1}\right).\end{aligned}$$

The image by ϕ_p (resp. ϕ_m, ϕ_r) of a polynomial of $\mathcal{I}(n)$ is a periodic (resp. median, self-reciprocal) polynomial of degree $2n$ but is not always irreducible.

Proposition 1 Let $\mathcal{P} \subset \mathbb{F}_2[X]$ be the subset of periodic polynomials, then \mathcal{P} is a sub algebra of $\mathbb{F}_2[X]$ and $\phi_p: \mathbb{F}_2[X] \rightarrow \mathcal{P}$ is an algebra isomorphism.

Proof. Only ϕ_p surjectivity deserves proof. Let Q be a periodic polynomial, its degree is an even integer $2n$. Then, $Q + (X^2 + X)^n$ is a periodic polynomial of degree $< 2n$. Iterating this process, we obtain a polynomial P of degree n such that $\phi_p(P) = Q$.

We call **trace** of a polynomial $P \neq 0$ of degree n , and write $Tr(P)$, the X^{n-1} coefficient.

The following theorem and corollary can be seen as an extension of Meyn's Lemma (see [4], Lemma 4):

Theorem 2 Let $P \in \mathcal{I}(n)$. If $Tr(P) = 1$, then $\phi_p(P)$ is a periodic irreducible polynomial of degree $2n$, else, $\phi_p(P)$ is the product of two irreducible polynomials of degree n , which form a periodic pair.

Conversely, let Q be an irreducible periodic polynomial of degree $2n$ (resp. $\{R, R^+\}$ a periodic pair of degree n), then, there exists a unique $P \in \mathcal{I}(n)$ such that $\phi_p(P) = Q$ (resp. $\phi_p(P) = RR^+$).

Proof. Let $P \in \mathcal{I}(n)$ and let h be a root of $\phi_p(P)$, then $h^2 + h$ is a root of P by definition and generates the field \mathbb{F}_{2^n} . This implies that $\mathbb{F}_2[h] \supset \mathbb{F}_2[h^2 + h] = \mathbb{F}_{2^n}$. In turn h cannot be a root of a polynomial whose degree is $< n$. We conclude that the irreducible decomposition of $\phi_p(P)$ contains only polynomials of degree $\geq n$. This leaves only two cases: $\phi_p(P)$ is irreducible of degree $2n$ or is the product of two irreducible polynomials A and B of degree n .

Suppose we are in the second case : AB being periodic, we have two possibilities: $B = A^+$ or A and B are themselves periodic. This last event cannot

occur because if $\phi_p(P) = AB$ with A and B periodic and irreducible, then by Proposition 1, there exist U and V such that $\phi_p(U) = A$ and $\phi_p(V) = B$. Then $\phi_p(P) = \phi_p(U)\phi_p(V) = \phi_p(UV)$ and $P = UV$. This would contradict the irreducibility of P .

We now prove that the trace dispatches the two cases. Suppose $\phi_p(P) = AB$, then we have $h \in \mathbb{F}_{2^n}$. We call $a = h^2 + h \in \mathbb{F}_{2^n}$, then $Tr(a) = Tr(h^2) + Tr(h) = 0$ and $Tr(P) = 0$ because a is a root of P . Conversely if $Tr(P) = 0$ then $Tr(a) = 0$ for any root a of P . Then it is well known that the equation $X^2 + X = a$ has roots in \mathbb{F}_{2^n} (using the "half-trace"). This means that $\phi_p(P)$ has a root in \mathbb{F}_{2^n} , so it is reducible.

We prove now the "conversely" part of the theorem.

Let Q be an irreducible periodic polynomial of degree $2n$ and let h be a root of Q , then, $h+1$ is also a root of Q and, from Theorem 1, we know that $h+1 = h^{2^n}$. Now, if

$$\mathcal{E} = \{h^{2^i} \mid 0 \leq i < n\},$$

$$Q = \prod_{h \in \mathcal{E}} (X + h)(X + h + 1) = \prod_{h \in \mathcal{E}} (X^2 + X + h(h + 1)).$$

We take

$$P = \prod_{h \in \mathcal{E}} (X + h(h + 1)),$$

it is then clear that $\phi_p(P) = Q$. Let $h(h + 1)$ be a root of P , then any other root can be written $h^{2^k}(h^{2^k} + 1) = [h(h + 1)]^{2^k}$ for some integer $k \geq 1$. In other terms, the roots of P are conjugate by Frobenius. This implies that $P \in \mathbb{F}_2[X]$. If P is reducible, say $P = ST$ then $\phi_p(P) = \phi_p(S)\phi_p(T) = Q$. This decomposition is trivial because Q is irreducible. This forces S or T to be trivial and P to be irreducible. Now, if P is not unique, there exists another irreducible polynomial S such that $\phi_p(S) = Q$, then $h(h + 1)$ is a root of S by definition, so S and P have the same roots and consequently, $S = P$.

In the same manner, let $\{R, R^+\}$ be a periodic pair of degree n and \mathcal{F} be the set of the n roots of R then taking

$$P = \prod_{a \in \mathcal{F}} (X + a(a + 1)),$$

we obtain a $P \in \mathbb{F}_2[X]$ such that $\phi_p(P) = RR^+$.

Suppose $P = ST$ with two non constant polynomials in $\mathbb{F}_2[X]$, then $\phi_p(P) = \phi_p(S)\phi_p(T) = RR^+$. Consequently, we can write $\phi_p(S) = R$ and this is a contradiction because $\phi_p(S)$ is periodic and R is not, so P is irreducible. The unicity of P is proved like previously.

Corollary 1 *Let $P \in \mathcal{I}(n)$, if $Tr(P) = 1$, then, $\phi_r(P)$ (resp. $\phi_m(P)$) is a self-reciprocal (resp. median) irreducible polynomial of degree $2n$, else, it is the product of two irreducible polynomials of degree n , which form a reciprocal (resp. median) pair.*

Conversely, let Q be an irreducible self-reciprocal (resp. median) polynomial of degree $2n$, then, there exists $P \in \mathcal{I}(n)$ such that $\phi_r(P) = Q$ (resp. $\phi_m(P) = Q$). In the same way, let $\{R, R^*\}$ (resp. $\{R, R^{**}\}$) be a reciprocal (resp. median) pair of degree n , then, there exists a unique $P \in \mathcal{I}(n)$ such that $\phi_r(P) = RR^*$ (resp. $\phi_m(P) = RR^{**}$).

Proof. We prove the corollary only for the self-reciprocal case, the median case being similar.

If $Tr(P) = 1$, from Theorem 2, we know that $\phi_p(P)$ is periodic in $\mathcal{I}(2n)$. Using Definitions 4 and 5, we see that $\phi_r(P)$ is self-reciprocal in $\mathcal{I}(2n)$. If $Tr(P) = 0$, there exists a periodic pair $\{S, S^+\}$ of degree n such that $\phi_p(P) = SS^+$. Now, as the transformations $*$ and $+$ are distributive with regard to the multiplication in $\mathbb{F}_2[X]$, $\phi_r(P) = (SS^+)^{*+} = S^{*+}S^{+**} = S^{*+}(S^{**})^*$, which is a reciprocal pair of degree n .

Using Theorem 2, Definitions 4 and 5, the proof of the second part is obvious.

We get a simple way to construct 3 and 6 elements hexagons: let P be an irreducible polynomial of degree n such that $Tr(P) = 1$, then $\{\phi_r(P), \phi_m(P), \phi_p(P)\}$ is a 3 elements degenerate hexagon of degree $2n$. This is illustrated by the left-side diagram. If $Tr(P) = 0$, we have the right-side diagram, where $\{Q_1, Q_2\}$, $\{Q_3, Q_4\}$ and $\{Q_5, Q_6\}$ are the pairs such that $\phi_r(P) = Q_1Q_2$, $\phi_m(P) = Q_3Q_4$ and $\phi_p(P) = Q_5Q_6$ respectively.

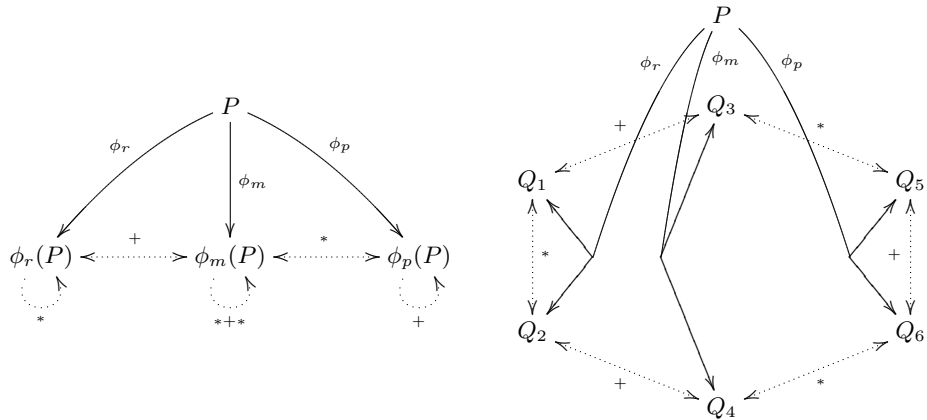


Fig. 1. Construction of hexagons by ϕ_r , ϕ_m and ϕ_p from an irreducible polynomial P such that $Tr(P) = 1$ (left) and $Tr(P) = 0$ (right).

2.3 Infinite Sequences of Self-reciprocal, Median and Periodic Irreducible Polynomials

Let $P \in \mathcal{I}(n)$, we denote $c_1(P)$ the coefficient of X in P .

Sequences of invariant irreducible polynomials appear implicitly in Varshamov [8] and more explicitly in Wiedemann [9], Meyn [4] and Cohen [1]. These sequences appear in papers devoted to a more general problem: the construction of irreducible polynomials (see Kyuregyan [2] and [3] for recent references).

Our approach shows that, actually, there are three strongly analogous families of invariant irreducible polynomials corresponding to the three conjugated 2-groups of \mathfrak{S}_3 . The following theorem is an easy extension of the construction of sequences of self-reciprocal irreducible polynomials given by Meyn and Cohen to the median and periodic cases.

Theorem 3 *Let $P \in \mathcal{I}(n)$ be such that $c_1(P) = \text{Tr}(P) = 1$. Starting from $\phi_r(P)$ (resp. $\phi_m(P)$, $\phi_p(P)$) and iterating the transformation $P \rightarrow \phi_r(P)$ (resp. $P \rightarrow \phi_m(P^+)$, $P \rightarrow \phi_p(P^{*+})$) one generates an infinite sequence of self-reciprocal (resp. median, periodic) irreducible polynomials of degree $2^i n$, $i > 0$.*

Proof. We know by Theorem 2 that $\phi_r(P)$ is self-reciprocal and irreducible. By explicit computation, we see that $\text{Tr}(\phi_r(P)) = 1$ and because of self-reciprocity, $c_1(\phi_r(P)) = 1$. So by recurrence, we get a sequence of self-reciprocal irreducible polynomials. Then, using the Definitions 4 and 5, we obtain sequences of median and periodic polynomials.

2.4 Equivalent Transformations

In Definition 5 we defined ϕ_m and ϕ_r from ϕ_p in a natural way. Other transformations can be used instead of ϕ_p . They are obtained by choosing one "right" action by an element of the group \mathfrak{S}_3 before applying ϕ_p .

We construct in this way new transformation ϕ'_p and consequently new ϕ'_m and ϕ'_r . We recover in this way the transformation ϕ'_r quoted in Section 2.3 which is more frequently used in the mathematical literature for constructing self-reciprocal polynomial. The results of the preceding sections can be transposed with small changes. The following table lists these transformations:

ϕ'_p	$\phi'_m = * \circ \phi'_p$	$\phi'_r = + \circ * \circ \phi'_p$
$P(X^2 + X + 1) = \phi_p(P^+)$	$X^{2n} P(\frac{X^2+X+1}{X^2})$	$(X^2 + 1)^n P(\frac{X^2+X+1}{X^2+1})$
$(X^2 + X + 1)^n P(\frac{1}{X^2+X+1}) = \phi_p(P^{*+})$	$(X^2 + X + 1)^n P(\frac{X^2}{X^2+X+1})$	$(X^2 + X + 1)^n P(\frac{X^2+1}{X^2+X+1})$
$(X^2 + X + 1)^n P(\frac{X^2+X}{X^2+X+1}) = \phi_p(P^{+++})$	$(X^2 + X + 1)^n P(\frac{X+1}{X^2+X+1})$	$(X^2 + X + 1)^n P(\frac{X}{X^2+X+1})$
$(X^2 + X)^n P(\frac{X^2+X+1}{X^2+X}) = \phi_p(P^{**})$	$(X + 1)^n P(\frac{X^2+X+1}{X+1})$	$X^n P(\frac{X^2+X+1}{X})$
$(X^2 + X)^n P(\frac{1}{X^2+X}) = \phi_p(P^*)$	$(X + 1)^n P(\frac{X^2}{X+1})$	$X^n P(\frac{X^2+1}{X})$

Table 1. Equivalent quadratic transformations.

3 Alternate Polynomials and 2 Elements Degenerate Hexagons

We introduced in [6] the class of alternate polynomials over \mathbb{F}_2 :

- Definition 6** – A polynomial P is said to be **alternate** if $P^{*+} = P^{+*} = P$.
- Let $P \in \mathcal{I}$, if P is not alternate, then $\{P, P^{*+}, P^{+*}\}$ is said to be an **alternate triplet**. P, P^{*+} and P^{+*} are of the same degree, so by extension, the degree of an alternate triplet is the degree of its polynomials.
 - A **2 elements degenerate hexagon** is made of two distinct alternate irreducible polynomials P and Q such that:

$$P \overset{+/*}{\longleftrightarrow} Q .$$

We refer again to [6] for the details of the following :

Proposition 2 The irreducible alternate polynomials are exactly the irreducible factors of the polynomials

$$B_k(X) = X^{2^k+1} + X + 1,$$

for $k \in \mathbb{N}$.

If P is alternate then $\deg P \equiv 0 \pmod{3}$ or $P = X^2 + X + 1$. If $\deg P = 3m$ then either P divides B_m and B_{2m}^* , or P divides B_m^* and B_{2m} . In the first case we say that P has **type 1**, in the second P has **type 2**.

Corollary 2 The order of an alternate irreducible polynomial of degree $3n$ divides $2^{2^n} + 2^n + 1$.

Proof. Let $P \in \mathcal{I}(n)$ be alternate. We suppose P is of type 1. Let a be a root of P , then, from Proposition 2, $a^{2^n+1} + a + 1 = 0$. We put this equation to the 2^n , we get $a^{2^n(2^n+1)} + a^{2^n} + 1 = 0$. Now, multiplying by a , we have $a^{2^n(2^n+1)+1} + a^{2^n+1} + a = 0$. Finally, we replace the term in the middle using the first equation, we obtain $a^{2^n(2^n+1)+1} + 1 = 0$.

If P is of type 2, then P^* is of type 1 and as P and P^* have same order, this concludes the proof.

3.1 The Cubic Transformation

Let $P \in \mathbb{F}_2[X]$ of degree n , we define the map $\psi : \mathbb{F}_2[X] \rightarrow \mathbb{F}_2[X]$ by

$$\psi(P)(X) = (X^2 + X)^n P\left(\frac{X^3 + X^2 + 1}{X^2 + X}\right).$$

We verify that $\psi(P)$ is alternate.

Let ϵ and ϵ^2 be the roots of $X^2 + X + 1$. For any irreducible $P \neq X^2 + X + 1$ in $\mathbb{F}_2[X]$ we have $P(\epsilon) \in \{1, \epsilon, \epsilon^2\}$. The main result of this section is:

- Theorem 4** – Let $P \in \mathcal{I}(n)$, $n > 2$. If $P(\epsilon) \neq 1$ then $\psi(P)$ is an irreducible alternate polynomial of degree $3n$, else, $\psi(P) = RST$, where $\{R, S, T\}$ is an alternate triplet of degree n .
- Conversely, let $Q \in \mathcal{I}(3n)$, $n > 1$ be an alternate polynomial (resp. $\{R, R^{*+}, R^{*+}\}$ an alternate triplet of degree n), then there exists a unique $P \in \mathcal{I}(n)$ such that $\psi(P) = Q$ (resp. $\psi(P) = RR^{*+}R^{*+}$).

To complete the theorem, we precise that the irreducible (alternate) polynomials of degree 3 are obtained from X and $X + 1$:

$$\psi(X) = X^3 + X^2 + 1 \text{ and } \psi(X + 1) = X^3 + X + 1,$$

and for the particular case $X^2 + X + 1$ (whose value in ϵ is 0), we have:

$$\psi(X^2 + X + 1) = (X^2 + X + 1)^3.$$

Before going into the proof of Theorem 4, we need to establish some results.

Let us take $P \in \mathcal{I}(n)$ with $n > 2$, $K = \mathbb{F}_{2^n}$ the splitting field of P , and h a root of $\psi(P)$, then $h \neq 0, 1$ and

$$a = \frac{h^3 + h^2 + 1}{h^2 + h} = h + \frac{1}{h} + \frac{1}{h + 1} \quad (1)$$

is a root of P . This implies $K \subset K(h)$.

As $h \neq 0, 1$, h is a root of the polynomial

$$T_a(X) = X^3 + (1 + a)X^2 + aX + 1. \quad (2)$$

3.2 Proof of the First Part of Theorem 4

Proposition 3 Let w be a cubic root of $(\epsilon + a)(\epsilon + a^2)$, then the roots of (2) are

$$h_i = 1 + a + \epsilon^i w + \frac{b}{\epsilon^i w},$$

with $i = 0, 1$ or 2 , and $b = a^2 + a + 1$. Moreover, they verify the relations $h_1 = 1/(h_0 + 1)$ and $h_2 = 1 + 1/h_0$.

Proof. The formulas for the h_i are obtained by the classical Cardan's method:

The first step is to cancel the X^2 coefficient in

$$X^3 + (a + 1)X^2 + aX + 1 = 0.$$

We take $X' = X + 1 + a$ and $b = 1 + a + a^2$:

$$X'^3 + bX' + b = 0.$$

The second step is to use two variables u, v and take $X' = u + v$:

$$u^3 + v^3 + (u + v)(uv + b) + b = 0.$$

Choosing $uv = b$, if we can solve

$$\begin{cases} uv = b \\ u^3 + v^3 = b \end{cases}$$

in \overline{K} , we will have the roots of (2), they would be the

$$1 + a + u + v.$$

We can write:

$$\begin{cases} u^3v^3 = b^3 \\ u^3 + v^3 = b, \end{cases}$$

which is equivalent to a second degree problem. If $Y = u^3$ then:

$$Y^2 + bY + b^3 = 0,$$

and dividing by b^2 we get:

$$\frac{Y^2}{b^2} + \frac{Y}{b} + b = 0.$$

We take $Z = Y/b$ (because $b \neq 0$):

$$Z^2 + Z + b = 0$$

$$Z^2 + Z + 1 + a + a^2 = 0$$

$$(Z + a)^2 + (Z + a) + 1 = 0.$$

So the solutions are $Z = a + \epsilon$ and $Z = a + \epsilon^2$. And we find:

$$u^3 = (1 + a + a^2)(a + \epsilon^2),$$

which can be written equivalently:

$$\begin{aligned} u^3 &= (a + \epsilon)(a + \epsilon^2)(a + \epsilon^2) \\ &= (a + \epsilon)(a^2 + \epsilon). \end{aligned}$$

So we can choose u as one of the three cubic roots of $(a + \epsilon)(a^2 + \epsilon)$. The quantity $v = b/u$ is then determined uniquely. The roles of v and u can be exchanged.

We now establish the relations between the roots:

$$\begin{aligned} 1 + \frac{1}{h_0} &= h_0^2 + (1 + a)h_0 + a + 1 \quad (\text{from (2)}) \\ &= w^2 + \frac{b^2}{w^2} + (1 + a)\left(w + \frac{b}{w}\right) + a + 1 \\ &= \frac{w^3}{w} + \frac{b^2w}{w^3} + (1 + a)\left(w + \frac{b}{w}\right) + a + 1 \\ &= \left[\frac{b^2}{w^3} + 1 + a\right]w + \left[\frac{w^3}{b} + 1 + a\right]\frac{b}{w} + a + 1. \end{aligned}$$

Then using $b = (\epsilon + a)(\epsilon^2 + a)$ and $w^3 = (\epsilon + a)(\epsilon + a^2)$ we find:

$$1 + \frac{1}{h_0} = \epsilon^2 w + \frac{b}{\epsilon^2 w} + a + 1 = h_2.$$

The first relation can be obtained by the same trick.

Lemma 1 *If $P(\epsilon) = 1$ and n is even (resp. odd), then $(\epsilon + a)(\epsilon + a^2)$ has cubic roots in $K = \mathbb{F}_{2^n}$ (resp. $K(\epsilon)$).*

Proof. Case n even: If $n = 2m$

$$\begin{aligned} P(\epsilon) &= (\epsilon + a)(\epsilon + a^2)(\epsilon + a^4)(\epsilon + a^8) \dots (\epsilon + a^{2^{2m-2}})(\epsilon + a^{2^{2m-1}}) \\ &= (\epsilon + a)(\epsilon + a^2)((\epsilon + a)(\epsilon + a^2))^4 \dots ((\epsilon + a)(\epsilon + a^2))^{2^{2m-2}}. \end{aligned}$$

So $P(\epsilon) = [(\epsilon + a)(\epsilon + a^2)]^k$ with

$$k = 1 + 4 + \dots + 2^{2(m-1)} = \frac{2^n - 1}{3}.$$

Let w be a cubic root of $(\epsilon + a)(\epsilon + a^2)$ in some extension of \mathbb{F}_2 (it always exists). Then, from what we have just said:

$$w^{2^n - 1} = w^{3 \cdot \frac{2^n - 1}{3}} = P(\epsilon) = 1,$$

so $w \in K$.

Case n odd: let $n = 2m + 1$, we write $P(\epsilon)$ in two different ways, using Fermat's little theorem:

$$\begin{aligned} P(\epsilon) &= (\epsilon + a)(\epsilon + a^2)(\epsilon + a^4)(\epsilon + a^8) \dots (\epsilon + a^{2^{2m-2}})(\epsilon + a^{2^{2m-1}})(\epsilon + a^{2^{2m}}) \\ P(\epsilon) &= (\epsilon + a^{2^{2m+1}})(\epsilon + a^{2^{2m+2}})(\epsilon + a^{2^{2m+3}})(\epsilon + a^{2^{2m+4}}) \dots (\epsilon + a^{2^{4m}})(\epsilon + a^{2^{4m+1}}). \end{aligned}$$

Multiplying these equalities, we get

$$\begin{aligned} P(\epsilon)^2 &= [(\epsilon + a)(\epsilon + a^2)][(\epsilon + a)(\epsilon + a^2)]^4 \dots [(\epsilon + a)(\epsilon + a^2)]^{2^{4m}} \\ &= [(\epsilon + a)(\epsilon + a^2)]^k, \end{aligned}$$

with

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

Then

$$w^{2^{2n} - 1} = w^{3 \cdot \frac{2^{2n} - 1}{3}} = P(\epsilon)^2 = 1,$$

and $w \in K(\epsilon)$ because $[K(\epsilon) : \mathbb{F}_2] = 2n$.

Proposition 4 *Let $P \in \mathcal{I}(n)$ be such that $P(\epsilon) = 1$, then, $\psi(P)$ is reducible.*

Proof. If n is even this is a direct consequence of the preceding Lemma and Proposition 3.

If n is odd, $w \in K(\epsilon)$ by the preceding lemma, so by Proposition 3 we have $K(h) \subset K(\epsilon)$. If $\psi(P)$ is irreducible then for any of its root h we have $[K(h) : \mathbb{F}_2] = 3n$ and $[K(h) : K] = 3$. This is a contradiction so $\psi(P)$ is reducible.

Proposition 5 *Let $P \in \mathcal{I}(n)$, $n > 2$, the polynomial $\psi(P)$ has $3n$ distinct roots and*

$$\psi(P) = \prod_{k=0}^{n-1} T_{a^{2^k}}(X),$$

where $a \in K$ is any root of P .

Proof. If a is a root of P and if h is a root of T_a , then h is a root of $\psi(P)$. Let a' be another root of P , distinct from a , then, the set of roots of T_a is disjoint from the set of roots of $T_{a'}$ because of (1). As P is irreducible, all the roots of P are conjugate and distinct, which concludes the proof of the proposition.

Proposition 6 *Let $P \in \mathcal{I}(n)$, $n > 2$, if $\psi(P)$ is reducible in $\mathbb{F}_2[X]$ then $\psi(P) = RST$, where $\{R, S, T\}$ is an alternate triplet of degree n , moreover $P(\epsilon) = 1$.*

Proof. Let h be a root of $\psi(P)$, we have seen that $K \subset K(h)$. Thus, the degree of the minimal polynomial of h is divisible by n and is $\leq 3n$. This implies that the irreducible factors of $\psi(P)$ in $\mathbb{F}_2[X]$ are at least of degree n , $< 3n$ and multiples of n . Consequently, one of the irreducible factor of $\psi(P)$ is of degree n . Let R be such a factor.

We consider R^{*+} and R^{+*} . They are polynomials of $\mathbb{F}_2[X]$ of degree n and their roots are roots of $\psi(P)$, thus, they divide $\psi(P)$. If R is not alternate, then we obtain an alternate triplet $\{R, R^{*+}, R^{+*}\}$ of degree n , as expected.

If R is alternate let h be a root of R and a such that

$$a = \frac{h^3 + h^2 + 1}{h^2 + h},$$

then, like previously, a is a root of P and $T_a(X)|R$ because $h, \frac{1}{h+1}$ and $\frac{h+1}{h}$ are distinct roots of R . As $R \in \mathbb{F}_2[X]$ is irreducible of degree n , its roots are the h^{2^k} , with $0 \leq k \leq n-1$. So, as Frobenius commutes with our group transformations, $T_{a^{2^k}}|R$ for every k . The $T_{a^{2^k}}$ are distinct because of the preceding proposition. It follows that R has $3n$ distinct roots which is a contradiction, so R cannot be alternate.

We can explicit the decomposition:

$$\psi(P) = R(X)(X+1)^n R\left(\frac{1}{X+1}\right) X^n R\left(\frac{X+1}{X}\right),$$

with $R \in \mathbb{F}_2[X]$ irreducible of degree $n > 2$, so $\psi(P)(\epsilon) = \epsilon^{3n} R(\epsilon)^3 = R(\epsilon)^3 = 1$.

Then, taking $X = \epsilon$ in the definition of ψ , we get $\psi(P)(\epsilon) = P(\epsilon^2)$. Consequently, $P(\epsilon^2) = P(\epsilon)^2 = 1$ and $P(\epsilon) = 1$.

The Propositions 4 and 6 give a demonstration of the first part of Theorem 4.

3.3 Proof of the Second Part of Theorem 4

Proposition 7 *let $Q \in \mathcal{I}(3n)$, $n > 1$ be an alternate polynomial (resp. $\{R, R^{+*}, R^{*+}\}$ an alternate triplet of degree n), then, there exists a unique $P \in \mathcal{I}(n)$ such that $\psi(P) = Q$ (resp. $\psi(P) = RR^{+*}R^{*+}$).*

Proof. Let a be a root of Q , suppose $\text{type}(Q) = 1$ (type 2 is similar), then, $1/(1+a)$ and $1+1/a$ are also roots of Q , moreover, from Proposition 2, we know that $1+1/a = a^{2^n}$ and that $1/(1+a) = a^{2^{2n}}$. Now, we take

$$\mathcal{E} = \{a^{2^i} \mid 0 \leq i < n\},$$

from what we have just seen, we can write

$$\begin{aligned} Q &= \prod_{a \in \mathcal{E}} (X+a)(X+1+\frac{1}{a})(X+\frac{1}{1+a}) \\ &= (X^2+X)^n \prod_{a \in \mathcal{E}} \left(\frac{X^3+X^2+1}{X^2+X} + \frac{a^3+a^2+1}{a^2+a} \right). \end{aligned}$$

We take

$$P = \prod_{a \in \mathcal{E}} \left(X + \frac{a^3+a^2+1}{a^2+a} \right),$$

it is then clear that $\psi(P) = Q$. Let $\frac{a^3+a^2+1}{a^2+a}$ be a root of P , then any other root can be written $a^{2^k}(1+1/a^{2^k})(1/(1+a^{2^k})) = [a(1+1/a)(1/(1+a))]^{2^k}$ for some integer $k \geq 1$. In other terms, the roots of P are conjugate by Frobenius. This implies that $P \in \mathbb{F}_2[X]$.

To show that P is irreducible, we suppose that $P = ST$, with two non constant polynomials in $\mathbb{F}_2[X]$, then, as $\deg ST = \deg S + \deg T$:

$$\psi(P) = \psi(S)\psi(T) = Q,$$

and this decomposition is non trivial. This is impossible because Q is irreducible, so P is irreducible.

And to show that P is unique, we suppose that there exists another irreducible polynomial P_1 such that $\psi(P_1) = Q$, then, $\frac{a^3+a^2+1}{a^2+a}$ is a root of P_1 by definition, so P and P_1 have the same roots and $P = P_1$.

In the same way, let $\{R, R^{+*}, R^{*+}\}$ be an alternate triplet of degree n and \mathcal{F} the set of the n roots of R , then, taking

$$P = \prod_{a \in \mathcal{F}} \left(X + \frac{a^3+a^2+1}{a^2+a} \right),$$

we obtain a P such that $\psi(P) = RR^{+*}R^{*+}$ and $P \in \mathbb{F}_2[X]$.

If P is reducible, we can write $P = ST$, with two non constant polynomials in $\mathbb{F}_2[X]$, then

$$\psi(P) = \psi(S)\psi(T) = RR^{+*}R^{*+}.$$

Consequently, we can write $\psi(S) = R$ and this is a contradiction because $\psi(S)$ is alternate and R is not, so P is irreducible. Finally, we can show that P is unique as we did in the first part.

This completes the proof of Theorem 4.

As we did in the previous section, we propose a simple way to construct 2 elements hexagons: let $P \in \mathcal{I}(n)$ be such that $P(\epsilon) \neq 1$, then, using the fact that $\psi \circ + = + \circ \psi$ (the demonstration is obvious), we deduce that $\{\psi(P), \psi(P^+)\}$ is a 2 elements degenerate hexagon of degree $3n$. This is illustrated by the left-side diagram. On the other hand, if $P(\epsilon) = 1$, we have the right-side diagram, where $\{Q_1, Q_3, Q_5\}$ and $\{Q_2, Q_4, Q_6\}$ are the alternate triplets such that $\psi(P) = Q_1Q_3Q_5$ and $\psi(P^+) = Q_2Q_4Q_6$ respectively:

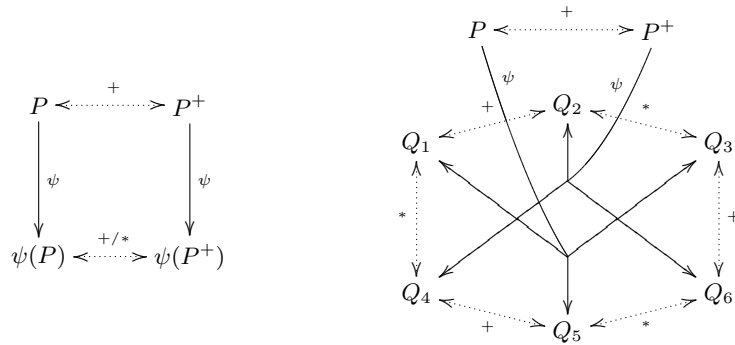


Fig. 2. Construction of hexagons by ψ from an irreducible polynomial P such that $P(\epsilon) \neq 1$ (left) and $P(\epsilon) = 1$ (right).

3.4 Infinite Sequences of Irreducible Alternate Polynomials

Proposition 8 *If P is an irreducible alternate polynomial of degree > 2 , then $\psi(P)$ is an irreducible alternate polynomial.*

Proof. Let P be an irreducible alternate polynomial, by Theorem 4, $P = \psi(Q)$ for some irreducible Q , then $P(\epsilon) = \epsilon$ or ϵ^2 . By the same theorem $\psi(P)$ is irreducible and alternate.

Theorem 5 *Let $P \in \mathcal{I}(n)$ be such that $P(\epsilon) = \epsilon$ or ϵ^2 , then the iteration ψ on P generates a sequence of alternate irreducible polynomials of degree $3^i n$, $i > 0$.*

Proof. Theorem 4 and Proposition 8 prove this theorem.

3.5 Computation of the Type of the Alternate Irreducible Polynomials

Another consequence of Theorem 4 is that it gives a simple way to compute the type:

Theorem 6 *Let Q be an alternate irreducible polynomial of degree > 2 then its type is 1 (resp. 2) if and only if $Q(\epsilon) = \epsilon$ (resp. $Q(\epsilon) = \epsilon^2$).*

Proof. If $\deg Q = 3$, we verify the theorem by calculus. We now suppose that $\deg Q = 3n$, $n > 1$. We know from the preceding that $Q = \psi(P) \in \mathcal{I}(3n)$ for some irreducible polynomial P and $Q(\epsilon) = P(\epsilon)^2$.

If n is even, let h_0 be a root of Q , then with the notations used in Proposition 3 we have $h_0 = 1 + a + w + \frac{b}{w}$. Consequently:

$$h_0^{2^n} = 1 + a + w^{2^n} + \frac{b}{w^{2^n}}.$$

From the demonstration of Lemma 1 we have $w^{2^n} = P(\epsilon)w$, and

$$h_0^{2^n} = 1 + a + P(\epsilon)w + \frac{b}{P(\epsilon)w}.$$

If $Q(\epsilon) = \epsilon$ (resp. ϵ^2), then $P(\epsilon) = \epsilon^2$ (resp. ϵ) and using again Theorem 4:

$$h_0^{2^n} = 1 + \frac{1}{h_0} \quad (\text{resp. } h_0^{2^n} = \frac{1}{h_0 + 1}).$$

This is equivalent to say that Q is of type 1 (resp. type 2).

If n is odd the demonstration follows the same line except that we must use $w^{2^{2n}} = P(\epsilon)^2w = Q(\epsilon)w$. We compute:

$$h_0^{2^{2n}} = 1 + a + Q(\epsilon)w + \frac{b}{Q(\epsilon)w}.$$

If $Q(\epsilon) = \epsilon$ (resp. ϵ^2), then $P(\epsilon) = \epsilon^2$ (resp. ϵ). We obtain:

$$h_0^{2^{2n}} = \frac{1}{h_0 + 1} \quad (\text{resp. } h_0^{2^{2n}} = 1 + \frac{1}{h_0}).$$

This implies (by iteration for example) that:

$$h_0^{2^n} = 1 + \frac{1}{h_0} \quad (\text{resp. } h_0^{2^n} = \frac{1}{h_0 + 1}),$$

and Q has type 1 (resp. 2).

3.6 Equivalent Transformations

Other cubic transformations can be used instead of ψ . As previously, they are obtained by a right action of the group elements on ψ .

ψ'
$(X^2 + X)^n P\left(\frac{X^3+X+1}{X^2+X}\right) = \psi(P^+)$
$(X^3 + X + 1)^n P\left(\frac{X^2+X}{X^3+X+1}\right) = \psi(P^{*+})$
$(X^3 + X + 1)^n P\left(\frac{X^3+X^2+1}{X^3+X+1}\right) = \psi(P^{+++})$
$(X^3 + X^2 + 1)^n P\left(\frac{X^3+X+1}{X^3+X^2+1}\right) = \psi(P^{**})$
$(X^3 + X^2 + 1)^n P\left(\frac{X^2+X}{X^3+X^2+1}\right) = \psi(P^*)$

Table 2. Equivalent cubic transformations.

4 Conclusion

To conclude, in this paper, we defined the different classes of irreducible polynomials obtained by the action of $GL_2(\mathbb{F}_2)$ on $\mathbb{F}_2[X]$. We gave transformations to get invariant polynomials of each class, ways to generate infinite sequences of them and we showed the perfect analogy between self-reciprocal irreducible polynomials and alternate ones.

Now, the perspectives would be to study the action of $GL_2(\mathbb{F}_q)$ on $\mathbb{F}_q[X]$. For that, the first step would be the action of $GL_2(\mathbb{F}_{2^n})$ on $\mathbb{F}_{2^n}[X]$.

Acknowledgment For our computations, we used the open source Mathematics software SAGE [7], so, we would like to thank the developers and contributors of SAGE. We also thank the reviewers for helping us to clarify the paper.

References

1. Cohen, S.D.: The Explicit Construction of Irreducible Polynomials over Finite Fields. *Designs, Codes and Cryptography* 2, pp. 169-174 (1992)
2. Kyuregyan, M.: Recurrent Methods for Constructing Irreducible Polynomials over GF(2s). *Finite Fields and Their Applications* 8:3, pp. 52-68 (2002)
3. Kyuregyan, M.: Iterated Constructions of Irreducible Polynomials over Finite Fields with Linearly Independent Roots. *Finite Fields and Their Applications* 10:1, pp. 323-341 (2004)
4. Meyn, H.: On the Construction of Irreducible Self-reciprocal Polynomials over Finite Fields. *Appl. Algebra Eng. Comm. Comp.* 1, pp. 43-53 (1990)
5. Meyn, H., Götz, W.: Self-reciprocal Polynomials over Finite Fields. *Publ. I.R.M.A. Strasbourg* 413/S-21, pp. 82-90 (1990)
6. Michon, J.-F., Ravache, P.: On Different Families of Invariant Irreducible Polynomials over GF(2). *Finite Fields and Their Applications* 16:3, pp. 163-174 (2010)
7. SAGE, <http://www.sagemath.org>
8. Varshamov, R.R.: A General Method of Synthesis for Irreducible Polynomials over Galois Fields. *Soviet Math. Dokl.* 29, pp. 334-336 (1984)
9. Wiedemann, D.: An Iterated Quadratic Extension of GF(2). *Fibonacci Quart.* 26, pp. 290-295 (1988)