SEQUENCES OF BINARY IRREDUCIBLE POLYNOMIALS

S. UGOLINI

Abstract. In this paper we construct an infinite sequence of binary irreducible polynomials starting from any irreducible polynomial \( f_0 \in \mathbb{F}_2[x] \). If \( f_0 \) is of degree \( n = 2^l \cdot m \), where \( m \) is odd and \( l \) is a non-negative integer, after an initial finite sequence of polynomials \( f_0, f_1, \ldots, f_s \), with \( s \leq l + 3 \), the degree of \( f_{i+1} \) is twice the degree of \( f_i \) for any \( i \geq s \).

1. Introduction

Constructing binary irreducible polynomials of arbitrary large degree is of fundamental importance in many applications. If \( f \) is a binary polynomial, namely \( f \in \mathbb{F}_2[x] \) where \( \mathbb{F}_2 \) is the field with two elements, and has degree \( n \), then its \( Q \)-transform is the polynomial \( f^Q(x) = x^n \cdot f(x + x^{-1}) \) of degree \( 2n \). The \( Q \)-transform of \( f \) is a self-reciprocal polynomial, namely \( f^Q \) is equal to its reciprocal polynomial (we remind that, if \( g \) is a polynomial of degree \( d \), then its reciprocal polynomial is \( g^*(x) = x^d \cdot g(x^{-1}) \)).

In [RRV69] the following result was proved.

**Theorem 1.1.** Let \( f(x) = x^n + \cdots + a_1 x + 1 \) be an irreducible polynomial of \( \mathbb{F}_2[x] \). Then \( f^Q(x) \) is irreducible if and only if \( a_1 = 1 \).

Later Meyn proved in [Mey90] the following result.

**Theorem 1.2.** If \( f(x) = x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + 1 \) is an irreducible polynomial of degree \( n \) over \( \mathbb{F}_2 \) such that \( a_{n-1} = a_1 = 1 \), then \( f^Q(x) = x^{2n} + b_{2n-1} x^{2n-1} + \cdots + b_1 x + 1 \) is a self-reciprocal irreducible polynomial of \( \mathbb{F}_2[x] \) of degree \( 2n \).

We classify any irreducible polynomial \( f(x) = x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{F}_2[x] \) as follows.

- \( f \) is of type \((A, n)\) if \( a_{n-1} = a_1 = 1 \).
- \( f \) is of type \((B, n)\) if \( a_{n-1} = 0 \) and \( a_1 = 1 \).
- \( f \) is of type \((C, n)\) if \( a_{n-1} = 1 \) and \( a_1 = 0 \).
- \( f \) is of type \((D, n)\) if \( a_{n-1} = a_1 = 0 \).

If \( n \) is any positive integer, then we can write \( n = 2^l \cdot m \), for some odd integer \( m \) and non-negative integer \( l \). As pointed out by Meyn, if \( f_0 \) is of type \((A, n)\), then by means of repeated applications of the \( Q \)-transform we can construct an infinite sequence of irreducible polynomials setting
$f_{i+1} := f_i^Q$, for $i \geq 0$. We notice that, for any $i$, the degree of $f_{i+1}$ is twice the degree of $f_i$.

One can wonder what happens if $f_0$ is not of type $(A, n)$. In this paper we will prove that, if $f_0$ is of type $(B, n)$, $(C, n)$ or $(D, n)$, then it is possible to construct an infinite sequence $\{f_i\}_{i \geq 0}$ of binary irreducible polynomials such that, after an initial finite sequence $f_0, f_1, \ldots, f_s$ with $s \leq l + 3$, for $i \geq s$ the degree of $f_{i+1}$ is twice the degree of $f_i$ (see the Subsections 3.1 and 3.2). To prove this fact we will rely upon the properties of the graphs associated with the map $\vartheta(x) = x + 1$ over finite fields of characteristic two (see [Ugo12]) and some properties of the $Q$-transform.

2. Background

Given a positive integer $n$, it is possible to construct a graph associated with the map $\vartheta$ over $\mathbb{P}^1(\mathbb{F}_{2^n}) = \mathbb{F}_{2^n} \cup \{\infty\}$, being $\mathbb{F}_{2^n}$ the field with $2^n$ elements. If $\alpha \in \mathbb{P}^1(\mathbb{F}_{2^n})$, then

$$\vartheta(\alpha) = \begin{cases} \infty & \text{if } \alpha = 0 \text{ or } \infty \\ \alpha + 1 & \text{otherwise.} \end{cases}$$

The vertices of the graph are labelled by the elements of $\mathbb{P}^1(\mathbb{F}_{2^n})$ and an arrow connects the vertex $\alpha$ to the vertex $\beta$ if $\beta = \vartheta(\alpha)$. We will denote the graph constructed in such a way by $\text{Gr}_n$. The elements of $\mathbb{P}^1(\mathbb{F}_{2^n})$ can be partitioned in two sets,

$$A_n = \{ \alpha \in \mathbb{F}_{2^n}^* : \text{Tr}_n(\alpha) = \text{Tr}_n(\alpha^{-1}) \} \cup \{0, \infty\}$$

$$B_n = \{ \alpha \in \mathbb{F}_{2^n}^* : \text{Tr}_n(\alpha) \neq \text{Tr}_n(\alpha^{-1}) \},$$

where $\text{Tr}_n(\alpha) = \sum_{i=0}^{n-1} \alpha^{2^i}$ denotes the absolute trace of $\alpha \in \mathbb{F}_{2^n}$. We notice that, if $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in \mathbb{F}_2[x]$ is the minimal polynomial of an element $\alpha \in \mathbb{F}_{2^n}$, then $a_{n-1} = \text{Tr}_n(\alpha)$. Moreover, if $n > 1$, then $a_1 = \text{Tr}_n(\alpha^{-1})$.

In Section 4 of [Ugo12] the structure of the graph $\text{Gr}_n$ is analysed in depth. If $\alpha$ is an element of $\mathbb{P}^1(\mathbb{F}_{2^n})$ such that $\vartheta^k(\alpha) = \alpha$ for some positive integer $k$, then $\alpha$ is $\vartheta$-periodic. In the case an element $\alpha$ is not $\vartheta$-periodic, it is preperiodic, namely some iterate of $\alpha$ is $\vartheta$-periodic.

Here we summarize the properties of the graph $\text{Gr}_n$ we will use later.

- Two or zero arrows enter a vertex.
- The elements belonging to a connected component of the graph are all in $A_n$ or all in $B_n$.
- A connected component having elements in $A_n$ is formed by a cycle, whose vertices are roots of reversed binary trees of depth $l + 2$, where $2^l$ is the greatest power of 2 which divides $n$. Moreover, any vertex belonging to a non-zero level smaller than $l + 2$ of a tree has exactly two children.
3. Construction of sequences of binary irreducible polynomials

The following, which is a special case of Lemma 4 in [Mey90], holds.

Lemma 3.1. If \( f \) is an irreducible polynomial of \( \mathbb{F}_2[x] \) of degree \( n > 1 \) then either \( f^q \) is a self-reciprocal irreducible polynomial of degree \( 2n \) or \( f^q \) is the product of a reciprocal pair of irreducible polynomials of degree \( n \) which are not self-reciprocal.

We prove some technical lemmas.

Lemma 3.2. Suppose that \( g(x) = x^{2n} + b_{2n-1}x^{2n-1} + \cdots + b_1x + b_0 \) is a self-reciprocal binary polynomial of degree \( 2n \) which factors as \( g(x) = f(x) \cdot f^*(x) \), where \( f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \) is irreducible in \( \mathbb{F}_2[x] \). Then one of the following holds:

- if \( b_{2n-1} = b_1 = 0 \), then \( a_{n-1} = a_1 \);
- if \( b_{2n-1} = b_1 = 1 \), then \( f \) is of type \((B,n)\) and \( f^* \) is of type \((C,n)\) or viceversa.

Proof. Expanding the product \( f(x) \cdot f^*(x) \) we get a polynomial whose coefficients of the terms of degree 1 and 2 are both equal to \( a_{n-1} + a_1 \). The thesis follows equating the coefficients of the terms of degrees \( 2n - 1 \) and 1 of \( f(x) \cdot f^*(x) \) to \( b_{2n-1} \) and \( b_1 \) respectively. \(\square\)

Lemma 3.3. Let \( f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \) be an irreducible binary polynomial of degree \( n \) and \( g(x) = f^Q(x) = x^{2n} + b_{2n-1}x^{2n-1} + \cdots + b_1x + b_0 \) its \( Q \)-transform. The following holds.

- If \( a_{n-1} = 1 \), then \( b_{2n-1} = b_1 = 1 \).
- If \( a_{n-1} = 0 \), then \( b_{2n-1} = b_1 = 0 \).

Proof. We notice that, if \( k \) is a positive integer, then in the expansion of the term \((x + x^{-1})^k\) only monomials \(x^e\), with \(-k \leq e \leq k\), appear. Therefore, the coefficients \( b_{2n-1} \) and \( b_1 \) of degrees \( 2n - 1 \) and 1 of \( g \) are affected only by the expansions of \((x + x^{-1})^n\) and \((x + x^{-1})^{n-1}\).

If \( a_{n-1} = 1 \), then

\[
g(x) = x^n \cdot [(x + x^{-1})^n + (x + x^{-1})^{n-1} + \cdots + a_0].
\]

Hence, \( g(x) = x^{2n} + x^{2n-1} + \cdots + x + 1 \), namely \( b_{2n-1} = b_1 = 1 \).

Viceversa, if \( a_{n-1} = 0 \), then \( g(x) = x^{2n} + 0 \cdot x^{2n-1} + \cdots + 0 \cdot x + 1 \), namely \( b_{2n-1} = b_1 = 0 \). \(\square\)

Lemma 3.4. If \( f \) is a binary irreducible polynomial of degree \( n \) with a root \( \alpha \in \mathbb{F}_{2^n} \) and \( \vartheta(\beta) = \alpha \) for some \( \beta \in \mathbb{F}_{2^{2n}} \), then \( \beta \) is root of \( f^Q \).

Proof. Since \( f(\alpha) = 0 \), then \( f^Q(\beta) = \beta^n \cdot f(\beta + \beta^{-1}) = \beta^n \cdot f(\alpha) = 0 \). \(\square\)

Now we prove some theorems which relate the types of a polynomial and its \( Q \)-transform.
Theorem 3.5. If \( f \) is a polynomial of type \((B, n)\), for some integer \( n \) greater than 1, then \( f^Q \) is a polynomial of type \((D, 2n)\). If is of type \((B, 1)\), then \( f(x) = x \) and \( f^Q \) splits as \( f^Q(x) = (x + 1)^2 \).

Proof. If \( n > 1 \), then by Theorem 1.1 the polynomial \( f^Q \) is irreducible of degree \( 2n \). The conclusion follows from Lemma 3.3.

If \( n = 1 \), then \( f(x) = x \) and \( f^Q(x) = x^2 + 1 = (x + 1)^2 \). \(\square\)

Theorem 3.6. If \( f \) is a polynomial of type \((C, n)\), then \( f^Q \) can be factored into the product of a reciprocal pair of distinct irreducible polynomials \( g_1, g_2 \) of degree \( n \). Up to renaming, \( g_1 \) is of type \((B, n)\), while \( g_2 \) is of type \((C, n)\).

Proof. By Theorem 1.1 the polynomial \( f^Q \) is not irreducible. Hence it splits into the product of a pair of reciprocal irreducible polynomials, \( g_1 \) and \( g_2 \), of degree \( n \). If \( f^Q(x) = x^{2n} + b_{2n-1}x^{2n-1} + \cdots + b_1x + b_0 \), then, by Lemma 3.3 \( b_{2n-1} = b_1 = 1 \). Since \( f^Q(x) = g_1(x) \cdot g_2(x) \), equating the coefficients we get the thesis. \(\square\)

Remark 3.7. As a consequence of Theorem 3.6 if \( f \) is a polynomial of type \((C, n)\), then one of the irreducible factors of \( f^Q \), which has been called \( g_1 \), is of type \((B, n)\). Then, by Theorem 3.5 \( g_1^Q \) is a polynomial of type \((D, 2n)\). Summing all up, starting from a polynomial \( f \) of type \((C, n)\), we have constructed a polynomial of type \((D, 2n)\).

Theorem 3.8. Let \( f \) be a polynomial of type \((D, n)\). Then, \( f^Q \) splits into the product of a reciprocal pair of distinct irreducible polynomials \( g_1, g_2 \) which are both of type \((A, n)\) or both of type \((D, n)\). Moreover, at least one of them is the minimal polynomial of an element \( \beta \in \mathbb{F}_{2^n} \) which is not \( \vartheta \)-periodic.

Proof. We notice that the roots of \( f \) belong to \( A_n \), because \( f \) is of type \((D, n)\). Moreover, by Theorem 1.1 and Lemma 3.1 \( f^Q \) splits into the product of a reciprocal pair of distinct irreducible polynomials \( g_1, g_2 \). Since \( f \) is of type \((D, n)\), by Lemma 3.3 and Lemma 3.2 the polynomials \( g_1 \) and \( g_2 \) are both of type \((D, n)\) or both of type \((A, n)\).

Consider a root \( \beta \in \mathbb{F}_{2^n} \) of the polynomial \( g_1 \). Then, \( \beta^{-1} \) is root of \( g_2 \) and \( \alpha = \vartheta(\beta) \) is root of \( f \). If \( \alpha \) is not \( \vartheta \)-periodic, then both \( \beta \) and \( \beta^{-1} \) are not \( \vartheta \)-periodic. On the contrary, if \( \alpha \) is \( \vartheta \)-periodic, then one between \( \beta \) and \( \beta^{-1} \), say \( \beta \), belongs to the first level of the tree rooted at \( \alpha \). All considered, in any case \( \beta \) is not \( \vartheta \)-periodic. \(\square\)

3.1. **An iterative procedure.** Let \( n' \) be a positive integer and \( 2^l \), for some \( l \geq 0 \), the greatest power of 2 dividing \( n' \). The following iterative procedure takes as input a binary irreducible polynomial \( p_0 \) of type \((D, n')\) having a root \( \alpha \in \mathbb{F}_{2^{n'}} \) which is not \( \vartheta \)-periodic and produces a finite sequence of polynomials \( p_0, \ldots, p_\varphi \), where \( p_\varphi \) is of type \((A, n')\). After setting \( i := 0 \), we proceed as follows.
(1) Factor $p_i^Q$ into the product of two irreducible polynomials $g_1, g_2$ of degree $n'$.
(2) Set $i := i + 1$ and $p_i := g_1$.
(3) If $p_i$ is of type $(A, n')$, then break the iteration. Otherwise, since $p_i$ is of type $(D, n')$, go to step (1).

The procedure breaks if and only if for some $i$ the polynomial $p_i$ is of type $(A, n')$. Actually, this is the case, as stated below.

**Theorem 3.9.** Using the notations introduced above, there exists a positive integer $s' \leq l' + 1$ such that $p_{s'}$ is a polynomial of type $(A, n')$. In addition, if $n' = 2m'$ and $p_0 = g^Q$, for some polynomial of type $(B, m')$, then $s' \leq l'$.

**Proof.** The element $\alpha$ belongs to a positive level $j$ of the reversed binary tree rooted at some element of $A_{n'}$. We want to prove that, for any $0 \leq k \leq l' + 2 - j$, the polynomial $p_k$ is the minimal polynomial (of type $(A, n')$ or $(D, n')$) of an element $\gamma \in F_{2n'}$ such that $\vartheta^k(\gamma) = \alpha$. This is true if $k = 0$. Therefore, consider $k < l' + 2 - j$ and suppose that the assertion is true for $p_k$. This means that $p_k$ is the minimal polynomial of an element $\gamma \in F_{2n'}$ such that $\vartheta^k(\gamma) = \alpha$. Since $\gamma$ is not a leaf of the tree, then there exists an element $\gamma' \in F_{2n'}$ such that $\vartheta(\gamma') = \gamma$. By Lemma 3.4, the element $\gamma'$ is root of $p_k^Q$. Hence $p_k^Q$ splits into the product of a reciprocal pair of distinct irreducible polynomials and $p_{k+1}$ is equal to one of these two polynomials. Moreover, $\gamma'$ or $(\gamma')^{-1}$ is a root of $p_{k+1}$.

Finally, consider $p_d$, where $d = l' + 2 - j$. This polynomial has a root $\gamma' \in F_{2n'}$ such that $\vartheta^d(\gamma) = \alpha$. We want to prove that $p_d$ is of type $(A, n')$. Suppose on the contrary that it is of type $(D, n')$. Then, $p_d^Q$ splits into the product of two irreducible polynomials of degree $n'$. One of these polynomials has a root $\gamma' \in F_{2n'}$ such that $\vartheta(\gamma') = \gamma$. Hence $\vartheta^{d+1}(\gamma') = \alpha$. Since $\alpha$ belongs to the level $j$ of the tree, then $\gamma'$ belongs to the level $l' + 3$ of the tree. But this is not possible, because the tree has depth $l' + 2$. Hence, setting $s' := d \leq l + 1$, the polynomial $p_{s'}$ is of type $(A, n')$.

Suppose now that $n' = 2m'$ and $p_0 = g^Q$, for some polynomial $g$ of type $(B, m')$. Then, $p_0$ is self-reciprocal and $\beta = \vartheta(\alpha) = \vartheta(\alpha^{-1}) < F_{2n'}$ is root of $g$. Moreover, $\beta$ is not $\vartheta$-periodic, since its only two preimages with respect to the map $\vartheta$ are $\alpha, \alpha^{-1}$, which are not $\vartheta$-periodic. If none of the polynomials $p_0, \ldots, p_{s'}$ constructed with the previous iterative procedure is of type $(A, n')$ and $\gamma \in F_{2n'}$ is a root of $p_{s'}$, then $\alpha$ (root of $p_0$) belongs to some tree of $Gr_{n'}$ of depth greater than $l' + 2$. Since this is an absurd, we deduce that in this case $s' \leq l'$.

**3.2. Conclusions.** Using the results of Subsection 3.1, if $f_0$ is any irreducible polynomial of degree $n$ over $F_2$ and $2^j$ is the greatest power of 2 dividing $n$, then we can construct an infinite sequence of binary
irreducible polynomials. In particular, the initial segment $f_0, \ldots, f_s$, with $s \leq l + 3$, is constructed as explained below.

- If $f_0$ is of type $(A, n)$, then $s = 0$.
- If $f_0$ is of type $(B, n)$, with $n > 1$, then, by Theorem 3.5, $f_0^Q$ is of type $(D, 2n)$. Set $p_0 := f_0^Q, n' := 2n$ and $l' := l + 1$. Then, by Theorem 3.9, it is possible to construct a finite sequence $p_0, \ldots, p_{s'}$, where $s' \leq l' = l + 1$ and $p_{s'}$ is of type $(A, 2n)$. Setting $f_i := p_{i-1}$, for $1 \leq i \leq s' + 1 \leq l + 2$, we are done.

  If $f_0$ is of type $(B, 1)$, then $f_0^Q(x) = x^2 + 1 = (x + 1)^2$. In this case we set $f_1(x) = x + 1$ and notice that $f_1$ is of type $(A, 1)$. Then, $s = 1$.

- If $f_0$ is of type $(C, n)$, then, proceeding as explained in Remark 3.7 it is possible to construct a polynomial $f_1$ of type $(B, n)$ and then another polynomial $f_2$ of type $(D, 2n)$. Set $p_0 := f_2, n' := 2n$ and $l' := l + 1$. Then, by Theorem 3.9, it is possible to construct a finite sequence $p_0, \ldots, p_{s'}$, where $s' \leq l' = l + 1$ and $p_{s'}$ is of type $(A, 2n)$. Setting $f_i := p_{i-2}$, for $2 \leq i \leq s' + 2 \leq l + 3$, we are done.

- If $f_0$ is of type $(D, n)$ and $f_0^Q$ does not split into the product of two polynomials of type $(A, n)$, then one of the two irreducible factors $h_1, h_2$ of $f_0^Q$ is a polynomial of type $(D, n)$ having a root $\alpha \in \mathbb{F}_{2^n}$ which is not $\vartheta$-periodic. A priori we do not know which of these two polynomials has such a root. Firstly, we set $n' := n$, $l' := l$ and $p_0 := h_1$. Iterating the procedure described in the previous Subsection we construct a sequence of polynomials $p_0, p_1, \ldots, p_{s'}$, where $s' \leq l' + 1$. If none of the polynomials $p_i$ is of type $(A, n)$, then we break the iterations, set $p_0 := h_2$ and construct a new sequence. This new sequence $p_0, p_1, \ldots, p_{s'}$ ends with a polynomial of type $(A, n)$, as proved in Theorem 3.9. Setting $f_i := p_{i-1}$ for $1 \leq i \leq s' + 1 \leq l + 2$, we are done.

In all cases the polynomial $f_s$ is of type $(A, n)$ or $(A, 2n)$. We can inductively construct all other terms of the sequence setting $f_{i+1} := f_i^Q$ for $i \geq s$. It is worth noting that for any $i$ the degree of $f_{i+1}$ is twice the degree of $f_i$. Moreover, if $n$ is odd, namely $l = 0$, then $s \leq 3$.

References

[3.5] H. Meyn, On the construction of irreducible self-reciprocal polynomials over finite fields, AAECC 1 (1990), 43–53.

[3.7] G. A. Garakov R. R. Varshamov, On the theory of selfdual polynomials over a Galois field (Russian), Bull. Math. Sci. Math. R. S. Roumanie (N. S.) 13 (1969), 403–415.

[S. Ugolini, Graphs associated with the map $x \mapsto x + x^{-1}$ in finite fields of characteristic two, Theory and Applications of Finite Fields, Contemp. Math., vol. 579, Amer. Math. Soc., Providence, RI, 2012.
E-mail address: sugolini@gmail.com