SEQUENCES OF IRREDUCIBLE POLYNOMIALS OVER ODD PRIME FIELDS VIA ELLIPTIC CURVE ENDO MORPHISMS

S. UGOLINI

Abstract. In this paper we present and analyse a construction of irreducible polynomials over odd prime fields via the transforms which take any polynomial $f \in \mathbb{F}_p[x]$ of positive degree $n$ to $(\frac{x}{k})^n \cdot f(k(x + x^{-1}))$, for some specific values of the odd prime $p$ and $k \in \mathbb{F}_p$.

1. Introduction

Let $f$ be a polynomial of positive degree $n$ defined over the field $\mathbb{F}_p$ with $p$ elements, for some odd prime $p$. We set $q = p^n$ and denote by $\mathbb{F}_q$ the finite field with $q$ elements.

For a chosen $k \in \mathbb{F}_p^*$ we define the $Q_k$-transform of $f$ as

$$f^{Q_k}(x) = \left(\frac{x}{k}\right)^n \cdot f(\vartheta_k(x)),$$

where $\vartheta_k$ is the map which takes any element $x \in \mathbb{P}^1(\mathbb{F}_q) = \mathbb{F}_q \cup \{\infty\}$ to

$$\vartheta_k(x) = \begin{cases} 
\infty & \text{if } x = 0 \text{ or } \infty, \\
\frac{k \cdot (x + x^{-1})}{x} & \text{otherwise.}
\end{cases}$$

The aforementioned $Q_k$-transforms seem a natural generalization of some specific transforms employed by different authors for the synthesis of irreducible polynomials over finite fields. In [3] Meyn used the so-called $Q$-transform, which coincides with the $Q_1$-transform according to the notations of the present paper. Moreover, setting $k = \frac{1}{2}$ we recover the $R$-transform introduced by Cohen [1] and used more recently by us [5] to construct sequences of irreducible polynomials over odd prime fields.

In this paper we would like to take advantage of the knowledge of the dynamics of the maps $\vartheta_k$ for some specific values of $k$ [4] and extend our investigation [5]. In the following we will give a thorough description of the sequences of irreducible polynomials constructed by repeated applications of a $Q_k$-transform, when $k$ belongs to one of the following sets:

- $C_1 = \{\frac{1}{2}, -\frac{1}{2}\}$;
- $C_2 = \{k \in \mathbb{F}_p : k \text{ is a root of } x^2 + \frac{1}{2} \}$, provided that $p \equiv 1 \pmod{4}$;
- $C_3 = \{k \in \mathbb{F}_p : k \text{ is a root of } x^2 + \frac{1}{2}x + \frac{1}{2} \}$, provided that $p \equiv 1, 2, \text{ or } 4 \pmod{7}$;
- $C_3^- = \{-k \in \mathbb{F}_p : -k \text{ is a root of } x^2 + \frac{1}{2}x + \frac{1}{2} \}$, provided that $p \equiv 1, 2, \text{ or } 4 \pmod{7}$.

Indeed, the case $k = \frac{1}{2}$ has been analysed in [5] and we can easily adapt the results of that paper to the case $k = -\frac{1}{2}$ (see the subsequent Remark 2.2). Hence, in this paper we will mainly concentrate on the cases that $k \in C_2 \cup C_3 \cup C_3^-$. 

2. Preliminaries

Let $p$ be an odd prime and $q$ a power of $p$. For a fixed $k \in \mathbf{F}_p^*$, the dynamics of the map $\vartheta_k$ over $\mathbf{P}^1(\mathbf{F}_q)$ can be visualized by means of the graph $G^2_{\vartheta_k}$, whose vertices are labelled by the elements of $\mathbf{P}^1(\mathbf{F}_q)$ and where a vertex $\alpha$ is joined to a vertex $\beta$ if $\beta = \vartheta_k(\alpha)$. As in [4] we say that an element $x \in \mathbf{P}^1(\mathbf{F}_q)$ is $\vartheta_k$-periodic if $\vartheta_k^r(x) = x$ for some positive integer $r$. We will call the smallest of such integers $r$ the period of $x$ with respect to the map $\vartheta_k$. Nonetheless, if an element $x \in \mathbf{P}^1(\mathbf{F}_q)$ is not $\vartheta_k$-periodic, then it is preperiodic, namely $\vartheta_k^r(x)$ is $\vartheta_k$-periodic for some positive integer $r$.

In [4] the reader can find more details about the length and the number of the cycles of $G^2_{\vartheta_k}$, when $k \in C_1 \cup C_2 \cup C_3$. For the purposes of the present paper we are just interested in the structure of the reversed binary trees attached to the vertices of a cycle.

The following lemma shows how the maps $\vartheta_k$ and $\vartheta_{-k}$ are related, for any $k \in \mathbf{F}_p^*$.

**Lemma 2.1.** Let $k \in \mathbf{F}_p^*$ and $x \in \mathbf{P}^1(\mathbf{F}_q)$. The following hold:

1. $\vartheta_k^{2r}(x) = \vartheta_{-k}^{2r}(x)$ for any nonnegative integer $r$;
2. if $\vartheta_k^t(x)$ is $\vartheta_k$-periodic, for some nonnegative integer $t$, then $\vartheta_{-k}^t(x)$ is $\vartheta_{-k}$-periodic too.

**Proof.** We prove separately the statements.

1. We proceed by induction on $r$.
   - If $r = 0$, then $\vartheta_k^0(x) = \vartheta_{-k}^0(x) = x$.
   - For the inductive step, assume that $\vartheta_k^{2(r-1)}(x) = \vartheta_{-k}^{2(r-1)}(x) = \tilde{x}$ for some integer $r > 0$. Therefore,
     \[
     \vartheta_k^{2r}(x) = \vartheta_k^2(\vartheta_k^{2r-2}(x)) = \vartheta_k^2(\tilde{x}) = k \cdot \frac{(k \cdot \tilde{x}^2 + 1)^2}{\tilde{x}} + 1
     \]
     \[
     = -k \cdot \frac{(-k \cdot \tilde{x}^2 + 1)^2}{-k \cdot \tilde{x}^2 + 1} = \vartheta_{-k}^2(\tilde{x}) = \vartheta_{-k}^{2r}(x).
     \]

2. Let $\tilde{x} = \vartheta_k^r(x)$. By hypothesis, $\vartheta_k^r(\tilde{x}) = \tilde{x}$ for some nonnegative integer $r$. Then, $\vartheta_{-k}^r(\tilde{x}) = \vartheta_{-k}^{2r}(\tilde{x}) = \tilde{x}$ according to (1). \qed

**Remark 2.2.** In virtue of Lemma 2.1, the results in [5, Theorem 3.1] still hold replacing $\vartheta_{1/2}$ with $\vartheta_{-1/2}$ and the $R$-transform with the $Q_{-1/2}$-transform.

We introduce the following notations in analogy with [5].

**Definition 2.3.** If $f \in \mathbf{F}_p[x] \setminus \{x\}$ is a monic irreducible polynomial and $\alpha$ is a non-zero root of $f$ in an appropriate extension of $\mathbf{F}_p$, then we denote by $f_{\vartheta_k}$ the minimal polynomial of $\vartheta_k(\alpha)$ over $\mathbf{F}_p$.

**Definition 2.4.** We denote by $\text{Irr}_p$ the set of all monic irreducible polynomials of $\mathbf{F}_p[x]$. If $n$ is a positive integer, then $\text{Irr}_p(n)$ denotes the set of all polynomials of $\text{Irr}_p$ of degree $n$. 

Remark 2.5. The reader can notice a slight difference in the definition of Irr$_p$ with respect to [5] Definition 2.3. Indeed, in [5] we excluded the polynomials $x + 1$ and $x - 1$ from Irr$_p$, because 1 and $-1$ are the only $\vartheta_2$-periodic elements in $G^1_2$ which are not root of any reversed binary tree, for any power $q$ of $p$. If $k \in C_2 \cup C_3 \cup C_3^-$ this phenomenon does not occur, namely any $\vartheta_k$-periodic element is root of a reversed binary tree.

The following lemma and theorems can be proved respectively as [5] Lemma 2.5, Theorem 2.6, Theorem 2.7] using the current more general notations of $\vartheta_k$ and $f^Q_k$ in place of $\vartheta_2$ and $f^R$.

**Lemma 2.6.** Let $f$ be a polynomial of positive degree $n$ in $F_p[x]$. Suppose that $\beta$ is a root of $f$ and that $\beta = \vartheta_k(\alpha)$ for some $\alpha, \beta$ in suitable extensions of $F_p$. Then, $\alpha$ and $\alpha^{-1}$ are roots of $f^Q_k$.

**Theorem 2.7.** Let $f$ be a polynomial of Irr$_p(n)\setminus\{x, x + 1, x - 1\}$, for some positive integer $n$. The following hold.

- If the set of roots of $f$ is not inverse-closed, then $\tilde{f}_{\vartheta_k} \in$ Irr$_p(n)$.
- If the set of roots of $f$ is inverse-closed, then $n$ is even and $\tilde{f}_{\vartheta_k} \in$ Irr$_p(n/2)$.

**Theorem 2.8.** Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in$ Irr$_p(n)$ for some positive integer $n$. The following hold.

- 0 is not a root of $f^Q_k$.
- The set of roots of $f^Q_k$ is closed under inversion.
- Either $f^Q_k \in$ Irr$_p(2n)$ or $f^Q_k$ splits into the product of two polynomials $m_\alpha, m_{\alpha^{-1}}$ in Irr$_p(n)$, which are respectively the minimal polynomial of $\alpha$ and $\alpha^{-1}$, for some $\alpha \in$ F$^{p^n}$. Moreover, in the latter case at least one among $\alpha$ and $\alpha^{-1}$ is not $\vartheta_k$-periodic.

Before dealing with the construction of sequences of irreducible polynomials, we prove some additional results for the dynamics of the maps $\vartheta_k$, when $k$ belongs respectively to $C_2$, $C_3$ or $C_3^-$, such results complement our investigation [4].

2.1. **Case** $k \in C_2$. In this section we fix an odd prime $p \equiv 1 \pmod{4}$ and a root $k$ of $x^2 + \frac{1}{2}$ in $F_p$.

The notations of the current section are the same as in [4] Section 3], except for the symbol $\varphi_2$, which we introduce in the present paper. For the reader’s convenience we review all the relevant notations:

- $R = Z[i]$;
- $\alpha = 1 + \sqrt{-1} \in R$;
- $N$ is the norm function on $R$, which takes any element $a + ib \in Z[i]$ to $N(a + ib) = a^2 + b^2$;
- $E$ is the elliptic curve of equation $y^2 = x^3 + x$ over $F_p$;
- $\pi_p$ is the representation in $R$ of the Frobenius endomorphism of $E$ over $F_p$, namely the map which takes any point $(x, y)$ of $E$ to $(x^p, y^p)$;
- $E(F_{p^n})$ is the group of rational points of $E$ over $F_{p^n}$, for any positive integer $n$, while
  
  $E(F_p)^* = \{O, (0, 0), (i_p, 0), (-i_p, 0)\} \subseteq E(F_{p^n})$,
  
  $E(F_p)^* = \{\infty, 0, i_p, -i_p\} \subseteq P^1(F_{p^n})$,

  being $O$ the point at infinity of $E$ and $i_p$ a square root of $-1$ in $F_p$. 


\begin{itemize}
  \item $\rho_0$ is the element of $R$ defined as
    \[
    \rho_0 = \begin{cases} 
      \alpha, & \text{if } \alpha^{-2} \equiv k \pmod{\pi_p}, \\
      \overline{\alpha}, & \text{if } \overline{\alpha}^{-2} \equiv k \pmod{\pi_p}; 
    \end{cases}
    \]
  \item $P^1(F_{p^n}) = A_n \cup B_n$, where $A_n$ and $B_n$ are two disjoint subsets of $P^1(F_{p^n})$ for any positive integer $n$;
  \item for any positive integer $m$, which we can express as $m = 2^e \cdot f$ for some odd integer $f$ and non-negative integer $e$, we denote by $\nu_2(m)$ the exponent of the greatest power of 2 which divides $m$, namely $\nu_2(m) = e$.
\end{itemize}

According to [4] Lemma 3.2, either all the elements belonging to a connected component of $G^e_{\vartheta_k}$ are in $A_n$ or they are in $B_n$.

In [4] Section 3 we defined the sets
\[
E(F_{p^n})_{A_n} = \{(x, y) \in E(F_{p^n}) : x \in A_n \backslash \{\infty\}\},
\]
\[
E(F_{p^n})_{B_n} = \{(x, y) \in E(F_{p^n}) : x \in B_n \backslash \{\infty\}\}
\]
and proved the existence of two isomorphisms
\[
\psi_n : E(F_{p^n})_{A_n} \cup E(F_p)^* \to R/(\pi_p^n - 1)R,
\]
\[
\overline{\psi}_n : E(F_{p^n})_{B_n} \cup E(F_p)^* \to R/(\pi_p^n + 1)R.
\]

The dynamics of the map $\vartheta_k$ on $A_n$ (resp. $B_n$) can be studied relying upon the iterations of $[\rho_0]$ in $R/(\pi_p^n - 1)R$ (resp. $R/(\pi_p^n + 1)R$). In particular, according to [4] Theorem 3.5, the depth of the trees in a connected component formed by elements of $A_n$ (resp. $B_n$) is equal to $e_0$, being $\rho_0^e$ the greatest power of $\rho_0$ which divides $\pi_p^n - 1$ (resp. $\pi_p^n + 1$). Indeed, since $N(\rho_0) = 2$ and the norm of any irreducible factor of $\pi_p^n - 1$ (resp. $\pi_p^n + 1$) different from $\rho_0$ and $\overline{\rho}_0$ is odd, we have that $e_0 = \nu_2(N(\pi_p^n - 1))$ (resp. $\nu_2(N(\pi_p^n + 1))$).

We prove the following technical lemma.

\textbf{Lemma 2.9.} Let $m$ and $n$ be two positive integers. Then, the following hold:
\begin{enumerate}
  \item $\nu_2(N(\pi_p^n - 1)) \geq 2$;
  \item if $\nu_2(N(\pi_p^n - 1)) = 2$, then $\nu_2(N(\pi_p^n + 1)) \geq 3$;
  \item if $\nu_2(N(\pi_p^n - 1)) \geq 3$, then $\nu_2(N(\pi_p^n + 1)) = 2$;
  \item $\nu_2(N(\pi_p^{2i+1}m - 1)) = \nu_2(N(\pi_p^{2im} - 1)) + 2$, for any positive integer $i$.
\end{enumerate}

\textbf{Proof.} Since $\pi_p^n - 1 \in \mathbb{Z}[i]$, we have that $\pi_p^n - 1 = a + ib$, for some $a, b \in \mathbb{Z}$, and consequently $\pi_p^n + 1 = (a + 2) + ib$. We prove separately the statements.

\begin{enumerate}
  \item Let
    \[
    S = R/\rho_0^e R \times R/\rho_1^f R \cong R/(\pi_p^n - 1)R
    \]
    for some element $\rho_1 \in R$ coprime to $\rho_0$ and some non-negative integers $e_0, e_1$. Consider the following points in $S$:
    \[
    Q = (Q_0, Q_1) = \psi_n(i_p, 0);
    \]
    \[
    P = (P_0, P_1) = \psi_n(0, 0);
    \]
    \[
    \odot = (0, 0) = \psi_n(O).
    \]
    Since $\vartheta_k(i_p) = 0$ and $\vartheta_k(0) = \infty$, we have that $[\rho_0]Q = P$ and $[\rho_0]P = \odot$. Moreover, by the fact that $\rho_0$ and $\rho_1$ are coprime, we deduce that $P_1 = 0$ and $Q_1 = 0$. In addition, $Q_0 \neq 0$ and $P_0 \neq 0$. Therefore, $[\rho_0]Q_0 \neq 0$ in $R/\rho_0^e R$.
    Since this latter is true only if $e_0 \geq 2$, we get the result.
\end{enumerate}
By hypothesis,
\[ N(\pi_p^n - 1) = a^2 + b^2 = 4c, \tag{2.1} \]
for some odd integer \(c\), and consequently \(a\) and \(b\) have the same parity. Indeed, \(a\) and \(b\) are both even. Suppose, on the contrary, that \(a\) and \(b\) are both odd. Then, \(a \equiv \pm 1 \pmod{4}\), \(b \equiv \pm 1 \pmod{4}\) and \(a^2 + b^2 \equiv 2 \pmod{4}\), in contradiction with (2.1).

Evaluating \(N(\pi_p^n + 1)\) we get

\[ N(\pi_p^n + 1) = a^2 + 4a + 4 + b^2 = 4c + 4(1 + a) = 4(1 + a + c). \]

We notice that \(1 + a\) is odd, because \(a\) is even. Therefore, \(1 + a + c\) is even and consequently \(N(\pi_p^n + 1) \equiv 0 \pmod{8}\). Hence, \(\nu_2(N(\pi_p^n + 1)) \geq 3\).

By hypothesis,
\[ N(\pi_p^n - 1) = a^2 + b^2 = 8c, \tag{2.2} \]
for some integer \(c\). In particular, \(a\) and \(b\) are both even, as proved in (2).

We evaluate \(N(\pi_p^n + 1)\) and get

\[ N(\pi_p^n + 1) = a^2 + 4a + 4 + b^2 = 8c + 4(1 + a). \]

We notice that \(1 + a\) is odd, because \(a\) is even. Therefore,

\[ N(\pi_p^n + 1) \equiv 4 \cdot (1 + a) \neq 0 \pmod{8} \]

and consequently \(\nu_2(N(\pi_p^n + 1)) = 2\).

Set \(n := 2^{r-1}m\). Then,

\[ \nu_2(N(\pi_p^{2m} - 1)) = \nu_2(N(\pi_p^{2m} - 1)) = \nu_2(N(\pi_p^n - 1)) + \nu_2(N(\pi_p^n + 1)). \]

From (1), (2) and (3) we get that \(\nu_2(N(\pi_p^n - 1)) + \nu_2(N(\pi_p^n + 1)) \geq 5\). Hence, \(\nu_2(N(\pi_p^{2m} - 1)) \geq 5\).

Set now \(n := 2^m m\). Then,

\[ \nu_2(N(\pi_p^{2m} - 1)) = \nu_2(N(\pi_p^n - 1)) + \nu_2(N(\pi_p^n + 1)). \]

Since \(\nu_2(N(\pi_p^{2m} - 1)) \geq 5\), from (3) we get that \(\nu_2(N(\pi_p^n + 1)) = 2\). All considered,

\[ \nu_2(N(\pi_p^{2m} - 1)) = \nu_2(N(\pi_p^{2m} - 1)) + 2. \]

\(\square\)

2.2. Case \(k \in C_3\). In this section we fix an odd prime \(p \equiv 1, 2, \text{ or } 4 \pmod{7}\) and a root \(k\) of \(x^2 + \frac{3}{2}x + \frac{1}{2}\) in \(\mathbb{F}_p\).

The notations of the current section are the same as in [4, Section 4], except for the symbol \(\nu_r\), which we introduce in the present paper. For the reader’s convenience we review all the relevant notations:

- \(R = \mathbb{Z}[\alpha]\), where \(\alpha = \frac{1 + \sqrt{-7}}{2}\);
- \(N\) is the norm function on \(R\), which takes any element \(a + b\alpha \in \mathbb{Z}[\alpha]\) to \((a + b\alpha) \cdot (a + b\alpha)\);
- \(E\) is the elliptic curve of equation \(y^2 = x^3 - 35x + 98\) over \(\mathbb{F}_p\);
- \(\pi_p\) is the representation in \(R\) of the Frobenius endomorphism of \(E\) over \(\mathbb{F}_p\);
- \(\sigma \equiv 2k + 1 \pmod{p}\), while \(\overline{\sigma} \equiv -2k \pmod{p}\);
Proof.

Lemma 2.10. Let

\[ E(\mathbf{F}_{p^n}) = \{0, (-7, 0), (\sigma + 3, 0), (\bar{\sigma} + 3, 0)\} \subseteq E(\mathbf{F}_{p^n}), \]

\[ E(\mathbf{F}_{p^n})^* = \{\infty, -7, \sigma + 3, \bar{\sigma} + 3\} \subseteq \mathbf{P}^1(\mathbf{F}_{p^n}), \]

being \( O \) the point at infinity of \( E \);

- \( \rho_0 \) is the element of \( R \) defined as

\[ \rho_0 = \begin{cases} \alpha, & \text{if } \alpha \equiv \sigma \pmod{\pi_p}, \\ \bar{\sigma}, & \text{if } \bar{\sigma} \equiv \sigma \pmod{\pi_p}; \end{cases} \]

- \( \mathbf{P}^1(\mathbf{F}_{p^n}) = A_n \cup B_n \), where \( A_n \) and \( B_n \) are two disjoint subsets of \( \mathbf{P}^1(\mathbf{F}_{p^n}) \) for any positive integer \( n \);

- for any \( r \in R \) such that \( r = r_0^{e_0} \cdot r_1 \), where \( r_0 \) and \( r_1 \) are two coprime elements of \( R \) and \( e_0 \) is a nonnegative integer, we denote by \( \nu_{r_0}(r) \) the exponent of the greatest power of \( r_0 \) which divides \( r \), namely \( \nu_{r_0}(r) = e_0 \).

In [4] Section 4 we introduced the rational maps \( \eta_k \) and \( \chi_k \), defined on \( \mathbf{P}^1(\mathbf{F}_{p^n}) \) in such a way that

\[ \nu_k(x) = \chi_k^{-1} \circ \eta_k \circ \chi_k(x) \]

for any \( x \in \mathbf{P}^1(\mathbf{F}_{p^n}) \). In virtue of this fact, the graphs \( G_{\phi_k}^{p^n} \) and \( G_{\psi_k}^{p^n} \) are isomorphic.

According to [4] Lemma 4.4], either all the elements belonging to a connected component of \( G_{\phi_k}^{p^n} \) are in \( A_n \) or they are in \( B_n \). As in Section 2.1 we define the sets \( E(\mathbf{F}_{p^n})_{A_n} \) and \( E(\mathbf{F}_{p^n})_{B_n} \) and the isomorphisms \( \psi_n \) and \( \tilde{\psi}_n \).

The dynamics of the map \( \eta_k \) on \( A_n \) (resp. \( B_n \)) can be studied relying upon the iterations of \( |\rho_0| \) in \( R/(\pi_p^n - 1)R \) (resp. \( R/(\pi_p^n + 1)R \)). In particular, according to [4] Theorem 4.6], the depth of the trees in a connected component formed by elements of \( A_n \) (resp. \( B_n \)) is equal to \( e_0 \), being \( \rho_0^{e_0} \) the greatest power of \( \rho_0 \) which divides \( \pi_p^n - 1 \) (resp. \( \pi_p^n + 1 \)), namely \( e_0 \) is equal to \( \nu_{\rho_0}(\pi_p^n - 1) \) (resp. \( \nu_{\rho_0}(\pi_p^n + 1) \)).

We prove a technical lemma, which provides some useful results for the construction of the sequences of irreducible polynomials.

Lemma 2.10. Let \( n \) be a positive integer. Then, the following hold:

1. \( \nu_{\rho_0}(\pi_p^n - 1) \geq 1 \);
2. if \( \nu_{\rho_0}(\pi_p^n - 1) = 1 \), then \( \nu_{\rho_0}(\pi_p^n + 1) \geq 2 \);
3. if \( \nu_{\rho_0}(\pi_p^n + 1) \geq 2 \), then \( \nu_{\rho_0}(\pi_p^n + 1) = 1 \);
4. \( \nu_{\rho_0}(\pi_p^{2^n + i - 1}) = \nu_{\rho_0}(\pi_p^{2^n - 1}) + 1 \), for any positive integer \( i \).

Proof. Let

\[ S = R/\rho_0^{e_0} R \times R/\rho_1^{e_1} R \cong R/(\pi_p^n - 1)R, \]

\[ \tilde{S} = R/\rho_0^{e_0} R \times R/\rho_1^{e_1} R \cong R/(\pi_p^n + 1)R, \]

for some elements \( \rho_1 \) and \( \rho_1 \) in \( R \) coprime to \( \rho_0 \) and some nonnegative integers \( e_0, e_1, e_0 \), and \( e_1 \). Moreover, define \( x_P = \pi + 3 \) and \( x_Q = 2\pi - 1 \). Then, denote by \( y_Q \) and \( -y_Q \) the \( y \)-coordinates of the two rational points \( E(\mathbf{F}_{p^n}) \) having \( x_Q \) as \( x \)-coordinate. We remind the reader that, according to [4] Lemma 4.3],

\[ \eta_k(x_Q) = x_P; \]
\[ \eta_k(x_P) = \infty. \]
Consider the points 0, P in S and the points Œ, Œ in Ŝ defined as follows:

\[ O = (0, 0) = \psi_n(O); \]
\[ \hat{O} = (0, 0) = \varphi_n(O); \]
\[ P = (P_0, P_1) = \psi_n(x_P, 0); \]
\[ \hat{P} = (\hat{P}_0, \hat{P}_1) = \varphi_n(x_P, 0). \]

(1) Since \( \eta_k(x_P) = \infty \), we have that \( [\rho_0]P = ([\rho_0]P_0, [\rho_0]P_1) = 0 \). Indeed, \( P_1 = 0 \), because \( \rho_0 \) and \( \rho_1 \) are coprime. Moreover, \( P \not= 0 \) and consequently \( P_0 \not= 0 \). Therefore, \( e_0 = \nu_\rho_0(\pi_p^n - 1) \geq 1 \).

(2) Since \( x_Q \in F_{p^n} \), either \( x_Q \) belongs to \( A_n \) or \( x_Q \) belongs to \( B_n \).

Suppose that \( x_Q \in A_n \) and define \( Q = (Q_0, Q_1) = \psi_n(x_Q, y_Q) \). Then, \( [\rho_0]Q = P \) and \( [\rho_0]^2Q = 0 \). In particular, \( Q_1 = 0 \), because \( \rho_0 \) and \( \rho_1 \) are coprime. Moreover, since \( e_0 = 1 \) by hypothesis, \( [\rho_0]Q_0 = 0 \) and consequently \( P_0 = 0 \). This latter is absurd and we deduce that \( x_Q \in B_n \).

Define now \( \tilde{Q} = (\hat{Q}_0, \hat{Q}_1) = \varphi_n(x_Q, y_Q) \). Since \( [\rho_0]\tilde{Q} = \hat{P} \not= \hat{O} \), we conclude that \( e_0 = \nu_\rho_0(\pi_p^n + 1) \geq 2 \).

(3) Since \( \hat{P} \in \hat{S} \) and \( \hat{P} \not= \hat{O} \), we deduce that \( \nu_\rho_0(\pi_p^n + 1) = 1 \). Indeed, \( \nu_\rho_0(\pi_p^n + 1) = 1 \). Suppose, on the contrary, that \( \nu_\rho_0(\pi_p^n + 1) \geq 2 \). Consider the point \( \tilde{R} = ([\rho_0]^{r_0-2}, 0) \in \tilde{S} \). Since \( [\rho_0]^2\tilde{R} = \tilde{O} \), we have that \( [\rho_0]\tilde{R} = \tilde{P} \). In particular, \( \tilde{R} \in \{ \varphi_n(x_Q, y_Q), \psi_n(x_Q, -y_Q) \} \). As a consequence, \( x_Q \in B_n \). Since by hypothesis \( e_0 \geq 2 \), any tree rooted in an element of \( A_n \) has depth at least 2. Therefore, \( x_Q \in A_n \), because it belongs to the level 2 of the tree of \( G_{p^n} \) rooted in \( \infty \).

All considered, we get a contradiction due to the fact that \( A_n \cap B_n = \emptyset \) by definition.

(4) From (1), (2) and (3) we deduce that
\[ \nu_0(\pi_p^n - 1) = \nu_0(\pi_p^{n-1} - 1) + \nu_0(\pi_p^{n-1} + 1) \geq 3. \]

Finally, according to (3),
\[ \nu_0(\pi_p^{n+1} - 1) = \nu_0(\pi_p^n - 1) + \nu_0(\pi_p^n + 1) = \nu_0(\pi_p^n - 1) + 1. \]

\[ \square \]

2.3. Case \( k \in C_3^- \). According to Lemma 2.11, if \( k \in C_3^- \) and \( n \) is a positive integer, then the dynamics of \( \vartheta_k \) on \( P^1(F_{p^n}) \) is strictly related to the dynamics of \( \vartheta_{-k} \), a map which belongs to the family of maps investigated in [4] Section 4. Indeed, an element \( \tilde{x} \in P^1(F_{p^n}) \) is \( \vartheta_k \)-periodic if and only if it is \( \vartheta_{-k} \)-periodic. In the case that \( \tilde{x} \) is not \( \vartheta_k \)-periodic, \( \tilde{x} \) belongs to a certain level \( t \) of some tree both in \( G_{\vartheta_k}^{p^n} \) and in \( G_{\vartheta_{-k}}^{p^n} \).

3. CONSTRUCTING IRREDUCIBLE POLYNOMIALS VIA THE \( Q_k \)-TRANSFORMS

The following theorem describes how the iterative procedure for constructing irreducible polynomials via the \( Q_k \)-transforms works, when \( k \in C_2 \cup C_3 \cup C_5^- \).

**Theorem 3.1.** Let \( f_0 \in \text{Irr}_p(n) \), for some odd prime \( p \) and some positive integer \( n \), and \( k \in C_2 \cup C_3 \cup C_5^- \).

Define two nonnegative integers \( e_0 \) and \( e_1 \) as follows:
Theorem 3.1.\[ \text{Proof.} \]

Let \( G \) be a non-empty tree in \( \mathbb{Z} \) with depth \( e \), such that, for any \( i \in G \), there exists a positive integer \( t \) such that there exists a non-negative integer \( s \) while \( f \in F \) has degree \( n \) over \( F \). Moreover, the following hold:

- If \( k \in C_2 \), then
  
  \[
  \begin{align*}
  e_0 &= \nu_2(N(p^n - 1)), \\
  e_1 &= \nu_2(N(p^n + 1)), 
  \end{align*}
  \]
  
  where \( \nu_2, N \) and \( p \) are defined as in Section \ref{section: preliminaries}.

- If \( k \in C_3 \cup C_5 \), then
  
  \[
  \begin{align*}
  e_0 &= \nu_{p_0}(p^n - 1), \\
  e_1 &= \nu_{p_0}(p^n + 1), 
  \end{align*}
  \]
  
  where \( p_0, \nu_{p_0} \) and \( p \) are defined as in Section \ref{section: preliminaries}.

If \( f_0^{Q_k} \) is irreducible, define \( f_1 := f_0^{Q_k} \). Otherwise, as stated in Theorem \ref{theorem: factorization}, factor \( f_0^{Q_k} \) into the product of two monic irreducible polynomials \( g_1, g_2 \) of the same degree \( n \), where \( g_1 \) has a non-\( \partial_k \)-periodic root in \( F_{p^n} \). In this latter case we set \( f_1 := g_1 \).

For \( i \geq 2 \) define inductively a sequence \( \{f_i\}_{i \geq 2} \) in such a way:

- If \( f_{i-1}^{Q_k} \) is irreducible, then set \( f_i := f_{i-1}^{Q_k} \).
- If \( f_{i-1}^{Q_k} \) is not irreducible, then factor \( f_{i-1}^{Q_k} \) into the product of two monic irreducible polynomials \( g_1, g_2 \) of the same degree and set \( f_i := g_1 \).

Then, there exist a non-negative integer \( s \) and a positive integer \( t \) such that:

- \( s \leq \max\{e_0, e_1\} \)
- \( s + t \leq e_0 + e_1 \)
- \( \{f_0, \ldots, f_s\} \subseteq \text{Irr}_p(n) \)
- \( \{f_{s+1}, \ldots, f_{s+t}\} \subseteq \text{Irr}_p(2n) \)

Moreover, the following hold:

- If \( k \in C_2 \), then \( \{f_{s+t+1}, f_{s+t+2}\} \subseteq \text{Irr}_p(2^{j+1} \cdot n) \) for any \( j \geq 1 \).
- If \( k \in C_3 \cup C_5 \), then \( f_{s+t+j} \in \text{Irr}_p(2^{j+1} \cdot n) \) for any \( j \geq 1 \).

\textbf{Proof.} The proof of the present theorem follows the same lines of the proof of \textbf{[5]} Theorem 3.1.

First, we denote by \( \beta_0 \in F_{p^n} \) a root of \( f_0 \). Then, we construct inductively a sequence \( \{\beta_i\}_{i \geq 0} \) of elements belonging to \( F_{p^n} \) or to appropriate extensions of \( F_{p^n} \) such that, for any \( i \geq 0 \), the following hold:

- \( f_i(\beta_i) = 0 \)
- \( \partial_k(\beta_{i+1}) = \beta_i \)

We notice that, being the roots of \( f_1 \) not \( \partial_k \)-periodic, \( \beta_0 \) is a vertex of some tree in \( G_{\theta_k}^{\alpha} \). Since the depth of a tree in \( G_{\theta_k}^{\alpha} \) is either equal to \( e_0 \) or to \( e_1 \), we conclude that there exists a non-negative integer \( s \leq \max\{e_0, e_1\} \) such that \( \beta_s \) has degree \( n \) over \( F_p \), while \( \beta_{s+1} \) has degree \( 2n \) over \( F_p \), implying that \( \{f_0, \ldots, f_s\} \subseteq \text{Irr}_p(n) \), while \( f_{s+1} \in \text{Irr}_p(2n) \).

We notice that \( \beta_0 \) is the root of a tree in \( G_{\theta_k}^{\alpha} \) which has depth \( e_0 + e_1 \). Therefore, there exists a positive integer \( t \), with \( s+t \leq e_0 + e_1 \), such that \( \beta_{s+t} \) has degree \( 2n \) over \( F_p \), while \( \beta_{s+t+1} \) has degree \( 4n \) over \( F_p \), implying that \( \{f_{s+1}, \ldots, f_{s+t}\} \subseteq \text{Irr}_p(2n) \).

The last two statements regarding the polynomials \( f_i \), for \( i > s + t \), follow respectively from Lemma \ref{lemma: factorization} and Lemma \ref{lemma: inductive}. \qed

\textbf{Remark 3.2.} One of the hypotheses of Theorem \ref{theorem: existence} is that the polynomial \( f_1 \) has no \( \partial_k \)-periodic roots. While this is true if \( f_0^{Q_k} \in \text{Irr}_p(2n) \), the same does not always hold.
hold if \( f^Q_k(x) = g_1(x) \cdot g_2(x) \), for some monic irreducible polynomials \( g_1, g_2 \) of equal degree \( n \). More precisely, at least one of \( g_1 \) and \( g_2 \) has no \( \vartheta_k \)-periodic roots. If one of them, say \( g_1 \), has \( \vartheta_k \)-periodic roots and we set \( f := g_1 \), it can happen that \( f \in \text{Irr}_p(n) \), where \( \hat{e} = \max\{e_0, e_1\} \). If this is the case, then we break the iterative procedure and set \( f_1 := g_2 \). Doing that, the hypotheses of the theorem are satisfied and we can proceed with the iterative construction.

Example 3.3. Consider the prime \( p = 53 \). We notice that \( p \equiv 1 \pmod{4} \) and \( p \equiv 4 \pmod{7} \).

First, we fix a root \( k \) of \( x^2 + \frac{1}{4} \) in \( \mathbb{F}_p \), namely \( k = 15 \), and construct a sequence of monic irreducible polynomials from the polynomial \( f_0(x) = x^5 + 3x + 51 \in \text{Irr}_{53}(5) \) via the transform \( Q_{15} \). Proceeding as explained in Theorem 3.1 using a computational tool as [2], we get that \( f_1, f_2 \) and \( f_3 \) belong to \( \text{Irr}_{53}(10) \), while \( f_4 \in \text{Irr}_{53}(20) \). Therefore, in accordance with the notations and the claims of Theorem 3.1 in this example \( s = 1, t = 2 \) and \( \{f_{3+2j-1}, f_{3+2j}\} \subseteq \text{Irr}_{53}(2^{j+1} \cdot 5) \) for any \( j \geq 1 \).

We notice in passing that, while \( f_{3+2j-1} = f_{3+2j-2}^{Q_{15}} \) for any \( j \geq 1 \), any polynomial \( f_{3+2j} \) is equal to one of the two irreducible factors of \( f_{3+2j-1}^{Q_{15}} \). This latter is equivalent to saying that every two steps in our construction the factorization of a polynomial is required. While efficient algorithms for the factorization of a polynomial into two equal-degree polynomials are known, one can reduce this burden taking \( k \in \text{C}_3 \cup \text{C}_3^{-} \).

Consider now \( k = 7 \in \text{C}_3 \) and \( f_0 \) as before. Constructing a sequence of monic irreducible polynomials via the transform \( Q_7 \) starting from \( f_0 \) we get that \( f_1 \in \text{Irr}_{53}(10) \), while \( f_2 \in \text{Irr}_{53}(20) \). Therefore, in accordance with Theorem 3.1 in this example \( s = 0, t = 1 \) and \( f_{1+j} \in \text{Irr}_{53}(2^{j+1} \cdot 5) \) for any \( j \geq 1 \). In particular, \( f_{j+1} = f_{j}^{Q_7} \) for \( j \geq 1 \) and no factorization is required.

References

1. S. D. Cohen, The explicit construction of irreducible polynomials over finite fields, Des. Codes Cryptogr. 2 (1992), no. 2, 169–174.
2. The GAP Group, GAP - Groups, Algorithms and Programming, http://www.gap-system.org
3. H. Meyn, On the construction of irreducible self-reciprocal polynomials over finite fields, Appl. Algebra Engrg. Comm. Comput. 1 (1990), no. 1, 43–53.
4. S. Ugolini, On the iterations of certain maps \( x \mapsto k \cdot (x + x^{-1}) \) over finite fields of odd characteristic, J. Number Theory (2014).
5. S. Ugolini, Sequences of irreducible polynomials without prescribed coefficients over odd prime fields, Des. Codes Cryptogr. (November 2013).

E-mail address: sugolini@gmail.com