Functional graphs of rational maps induced by endomorphisms of ordinary elliptic curves over finite fields

S. Ugolini

Abstract In this paper we study the dynamics of rational maps induced by endomorphisms of ordinary elliptic curves defined over finite fields. For any such map we describe the cycle and the tree structures of the associated graphs.

Keywords Dynamical systems · Finite fields · Arithmetic dynamics · Endomorphisms of elliptic curves

Mathematics Subject Classification 37P55 · 37P05 · 11G20

1 Introduction

The study of the dynamics of polynomial and rational maps over finite fields has attracted the attention of many investigators. Motivated also by Pollard’s rho algorithm, Rogers [9] and Vasiga and Shallit [16] dealt with certain quadratic maps. Later other studies on monomial, polynomial and rational maps appeared (see for example [1,2,5,8,10]).

In two different articles [13,14] we studied the dynamics of the maps $x \mapsto x + x^{-1}$ over finite fields of characteristic 2, 3 and 5. Later [15] we extended such results to certain maps of the form $x \mapsto k \cdot (x + x^{-1})$, which are related to some endomorphisms of ordinary elliptic curves defined over finite fields.

The idea behind the current work is to generalize the studies of our three aforementioned papers in an unified frame. More precisely, we aim at studying the functional graphs of rational maps induced by endomorphisms of ordinary elliptic curves defined over finite fields.

Consider an ordinary elliptic curve $E$ defined over the field $\mathbb{F}_q$ with $q$ elements, where $q$ is a power of a prime $p$, and an endomorphism $\alpha$ of $E$ defined as

$$\alpha(x, y) := (\alpha_1(x), y \cdot \alpha_2(x))$$

(1.1)
for some rational functions $\alpha_1$ and $\alpha_2$ in $\mathbb{F}_q(x)$, where $\alpha_1(x) = \frac{a(x)}{b(x)}$ for some polynomials $a(x)$ and $b(x)$ in $\mathbb{F}_q[x]$ with $\gcd(a(x), b(x)) = 1$.

Let $n$ be a positive integer and consider the map $r$ defined over $\mathbb{P}^1(\mathbb{F}_{q^n}) := \mathbb{F}_{q^n} \cup \{\infty\}$ as

$$r(x) := \begin{cases} \infty & \text{if } x = \infty \text{ or } b(x) = 0; \\ \alpha_1(x) & \text{otherwise.} \end{cases}$$

We want to study the properties of the digraph $G^{q^n}$ whose vertices are the elements of $\mathbb{P}^1(\mathbb{F}_{q^n})$ and where an arrow connects two elements $x_1$ and $x_2$ provided that $x_2 = r(x_1)$.

A detailed description of the structure of $G^{q^n}$ is given in Sect. 3. Very briefly, $G^{q^n}$ is formed by a finite number of connected components. Each component consists of a cycle, whose vertices are roots of reversed trees. We say that an element $\tilde{x} \in \mathbb{P}^1(\mathbb{F}_{q^n})$ is $r$-periodic if $r^m(\tilde{x}) = \tilde{x}$ for some positive integer $m$ (here $r^m$ denotes the $m$-fold composition of $r$ with itself).

### 1.1 General settings of the paper

In the paper $E$ is an ordinary elliptic curve defined by an equation of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad (1.2)$$

for some coefficients $a_i \in \mathbb{F}_q$, where $q$ is a power of a prime.

The endomorphism ring $\text{End}(E)$ of $E$ over $\mathbb{F}_q$ is isomorphic to an order in an imaginary quadratic number field $\mathbb{Q}(\sqrt{d})$ for some square-free negative integer $d$ (see [6]). In particular, the unique maximal order in $K := \mathbb{Q}(\sqrt{d})$ is the ring of integers $\mathcal{O}_K$ of $K$. In this paper we assume that $\text{End}(E) = \mathcal{O}_K$.

### 1.2 Structure of the paper

The paper is organized as follows.

- In Sect. 2 we recall some general facts on the ring $R$ of the endomorphisms of $E$ over $\mathbb{F}_q$ and its quotients with respect to ideals.
- Section 3 contains the main results of the paper. In Sect. 3.1 we describe the cycles of the graph $G^{q^n}$, while in Sect. 3.2 we describe the structure of the trees.
- In Sect. 4 we analyse the structure of $G^{q^n}$ choosing three different elliptic curves and endomorphisms.

### 1.3 Notation

For the sake of brevity, if $i$ and $j$ are two non-negative integers such that $i < j$ we define

$$[i, j] := \{x \in \mathbb{N} : i \leq x \leq j\}.$$

### 2 Background

Let $R$ be the endomorphism ring of $E$ over $\mathbb{F}_q$. According to the assumptions made in the introduction $R = \mathbb{Z}[\omega_d]$, where

$$\omega_d := \begin{cases} \frac{1 + \sqrt{d}}{2} & \text{if } d \equiv 1 \pmod{4}, \\ \frac{\sqrt{d}}{2} & \text{otherwise.} \end{cases}$$
For any ideal \( I \) in \( R \) we denote by \( N(I) \) the absolute norm of \( I \), namely

\[
N(I) := |R/I|.
\]

Let \( m := |E(\mathbb{F}_q)| \) and \( d' := (q + 1 - m)^2 - 4q \).

As proved by Wittmann [18], \( d' < 0 \) and the \( q \)-Frobenius endomorphism \( \pi_q \) which takes an element \( (x, y) \in \mathbb{F}_q^2 \) to \( (x^q, y^q) \) is represented in \( R \) by

\[
\pi_q = \frac{q + 1 - m + f_0 \sqrt{d}}{2}
\]

for some positive integer \( f_0 \) such that \( f_0^2 d = d' \).

## 2.1 Dedekind domains and ideal factorization

Since \( R \) is a Dedekind domain, any ideal \( I \) in \( R \) factors into prime ideals and \( R/I \) is isomorphic to

\[
\left( \prod_{i=1}^{j} R/\mathfrak{P}_i^{e_i} \right) \times \left( \prod_{i=j+1}^{k} R/\mathfrak{P}_i^{e_i} \right) \times \left( \prod_{i=k+1}^{l} R/\mathfrak{P}_i^{e_i} \right),
\]

(2.1)

where

- \( j, k \) and \( l \) are non-negative integers;
- any \( e_i \) is a positive integer for \( i \in [1, l] \);
- \( \mathfrak{P}_i \) is a prime ideal above a splitting rational prime \( p_i \) for any \( i \in [1, j] \);
- \( \mathfrak{P}_i \) is a prime ideal above an inert rational prime \( p_i \) for any \( i \in [j + 1, k] \);
- \( \mathfrak{P}_i \) is a prime ideal above a ramified rational prime \( p_i \) for any \( i \in [k + 1, l] \).

Moreover we adopt the following conventions for the integers \( j, k \) and \( l \):

- if no prime ideal above a splitting (resp. inert, ramified) rational prime appears in the factorization of \( I \), then \( j := 0 \) (resp. \( k := j, l := k \));
- if \( k \neq j \) (resp. \( l \neq k \)), then \( k > j \) (resp. \( l > k \) and \( l > j \)).

## 2.2 Galois rings

The main source for the definitions and the results presented in this section is [17].

A Galois ring is defined to be a finite ring with identity 1 such that the set of its zero divisors with 0 added forms a principal ideal \( \langle 1 \rangle \) for some prime number \( p \) ([17, Definition 14.1]).

In the following \( p \) is a rational prime, while \( s \) and \( m \) are two positive integers. Moreover, for any positive integer \( a \), we denote the ring \( \mathbb{Z}/p^a\mathbb{Z} \) by \( \mathbb{Z}_{p^a} \).

Let \( h \) be a monic polynomial in \( \mathbb{Z}_{p^s}[x] \). We say that \( h \) is basic irreducible (resp. basic primitive) in \( \mathbb{Z}_{p^s}[x] \) if the polynomial \( \overline{h} \) obtained reducing the coefficients of \( h \) modulo \( p \) is irreducible (resp. primitive) in \( \mathbb{Z}_p[x] \).

If \( h \) is a monic basic irreducible polynomial of positive degree \( m \) over \( \mathbb{Z}_{p^s} \), then \( \mathbb{Z}_{p^s}[x]/\langle h(x) \rangle \) is a Galois ring of characteristic \( p^s \) and cardinality \( p^{sm} \) ([17, Example 14.2]), which we denote by \( GR(p^s, p^{sm}) \). Indeed, as explained in [17, Section 14.2], any Galois ring has characteristic a power of a prime and the following holds.

**Theorem 2.1** Let \( G \) be a Galois ring of characteristic \( p^s \) and cardinality \( p^{sm} \). Then \( G \) is isomorphic to the ring \( \mathbb{Z}_{p^s}[x]/\langle h(x) \rangle \) for any monic basic irreducible polynomial \( h(x) \) of degree \( m \) over \( \mathbb{Z}_{p^s} \).
Theorem 2.2 (1) In the Galois ring $GR(p^s, p^{sm})$ there exists a nonzero element $\xi$ of order $p^m - 1$, which is a root of a monic basic primitive polynomial $h(x)$ of degree $m$ over $\mathbb{Z}_{ps}$ and dividing $x^{p^m - 1} - 1$ in $\mathbb{Z}_{ps}[x]$.

(2) Any element $c \in GR(p^s, p^{sm})$ can be written uniquely as
\[ c = c_0 + c_1 p + \cdots + c_{s-1} p^{s-1}, \]
where $c_0, c_1, \ldots, c_{s-1} \in \Gamma := \{0, 1, \xi, \xi^2, \ldots, \xi^{p^m-2}\}$.

(3) All the elements $c$ with $c_0 = 0$ are either zero divisors or zero, and they form the ideal $\langle p \rangle$ of $GR(p^s, p^{sm})$.

(4) Every nonzero element $c \in GR(p^s, p^{sm})$ can be expressed uniquely in the form $c = up^r$, where $u$ is a unit and $0 \leq r < s$.

Remark 2.3 We notice in passing that $\mathbb{Z}_{ps}$ is a Galois ring on its own. Indeed $\mathbb{Z}_{ps} \cong GR(p^s, p^s)$.

2.3 Structure of the quotient rings $R/\mathfrak{M}_i^{e_i}$

The main references for this section are [3, 4]. Still, the notation for Galois rings used in [3, 4] is slightly different from the notation adopted in this paper, which is the same as in [17].

We distinguish three cases.

Case 1: $i \in [1, j]$. According to [3, Theorem 5], there is an isomorphism
\[ R/\mathfrak{M}_i^{e_i} \cong \mathbb{Z}_{p_i^{e_i}} = GR(p_i^{e_i}, p_i^{e_i}). \]

Case 2: $i \in [j + 1, k]$. According to [3, Theorem 6] there is an isomorphism
\[ R/\mathfrak{M}_i^{e_i} \cong GR(p_i^{e_i}, p^{2e_i}). \]

Case 3: $i \in [k + 1, l]$. Let $x + c$ be a factor in $\mathbb{Q}(\sqrt{d})[x]$ of the minimal polynomial of $\sqrt{d}$ over $\mathbb{Q}$. The following hold in accordance with [4, Theorem 1].

- If $e_i = 1$, then the additive group of $R/\mathfrak{M}_i^{e_i}$ is isomorphic to a cyclic group of order $p_i$.
- If $e_i$ is even, then the additive group of $R/\mathfrak{M}_i^{e_i}$ is isomorphic to the direct sum of two cyclic groups and its elements can be represented as
\[ z_0 + z_1(c + d), \]
where $\langle c + d \rangle$ is a principal ideal in $\mathbb{Z}[\omega_d]$ and $z_0, z_1 \in \mathbb{Z}_{p_i^{e_i}/2}$.
- If $e_i$ is odd and $e_i \geq 3$, then the additive group of $R/\mathfrak{M}_i^{e_i}$ is isomorphic to the direct sum of two cyclic groups and its elements can be represented as
\[ x_0 + z_0(c + d), \]
where $x_0 \in \mathbb{Z}_{p_i^{(e_i+1)/2}}$ and $z_0 \in \mathbb{Z}_{p_i^{(e_i-1)/2}}$.

3 Structure of the graphs

According to [6, Theorem 1] there is an isomorphism
\[ E(\mathbb{F}_{q^n}) \cong R/(\pi_q^n - 1) R \]
of $R$-modules.
The following trivially holds because the Eq. (1.2) has degree two.

**Lemma 3.1** Let \( \tilde{x} \in \mathbb{F}_{q^n} \). Then there exist two different or coincident points in \( E(\mathbb{F}_{q^{2n}}) \) having such an \( x \)-coordinate.

Consider the sets

\[
E_0 := \{ x \in \mathbb{F}_{q^n} : (x, 0) \in E(\mathbb{F}_{q^n}) \} \cup \{ \infty \},
\]

\[
E_0(\mathbb{F}_{q^n}) := \{ (x, 0) : x \in \mathbb{F}_{q^n} \} \cup \{ O \},
\]

where \( O \) is the point at infinity of \( E \).

In analogy with [15] we introduce the sets

\[
A_n := \{ x \in \mathbb{F}_{q^n} : (x, y) \in E(\mathbb{F}_{q^n}) \text{ for some } y \in \mathbb{F}_{q^n} \} \cup \{ \infty \},
\]

\[
B_n := \{ x \in \mathbb{F}_{q^n} : (x, y) \in E(\mathbb{F}_{q^{2n}}) \text{ for some } y \in \mathbb{F}_{q^{2n}} \setminus \mathbb{F}_{q^n} \} \cup E_0,
\]

and correspondingly the set

\[
E(\mathbb{F}_{q^{2n}})_{B_n} := \{ (x, y) \in E(\mathbb{F}_{q^{2n}}) : x \in B_n \}.
\]

We notice that \( A_n \cap B_n = E_0 \) and the following holds in analogy with [15, Lemma 3.3].

**Lemma 3.2** Let \( P \) be a rational point of \( E(\mathbb{F}_{q^{2n}}) \) such that either \( P = O \) or \( P = (\tilde{x}, \tilde{y}) \) for some \( \tilde{x} \in \mathbb{F}_{q^n} \) and \( \tilde{y} \in \mathbb{F}_{q^{2n}} \). Then

\[
(\pi_q^n - 1) P = O \iff P \in E(\mathbb{F}_{q^n});
\]

\[
(\pi_q^n + 1) P = O \iff P \in E(\mathbb{F}_{q^{2n}})_{B_n}.
\]

In virtue of Lemma 3.2 we can say that there is an isomorphism

\[
E(\mathbb{F}_{q^{2n}})_{B_n} \cong R/(\pi_q^n + 1) R.
\]

We set \( S := A_n \) (resp. \( \tilde{x} \in B_n \)), then \( r(\tilde{x}) \in A_n \) (resp. \( r(\tilde{x}) \in B_n \)).

**Remark 3.4** While we can conveniently study the action of the map \( r \) separately on the elements of \( A_n \) and \( B_n \), we should take care of the fact that \( A_n \cap B_n = E_0 \).

The following holds for the action of \( r \) on \( E_0 \).

**Lemma 3.5** If \( \tilde{x} \in E_0 \), then \( r(\tilde{x}) \in E_0 \).

**Proof** The result follows from the fact that

\[
\alpha(\tilde{x}, 0) = (\alpha_1(\tilde{x}), 0)
\]

and \( r(\infty) = \infty \). \( \square \)

We set \( S := A_n \) or \( S := B_n \) and correspondingly \( \delta := \pi_q^n - 1 \) or \( \delta := \pi_q^n + 1 \).

The ring \( R/\langle \delta \rangle \) is isomorphic to

\[
R/I_c \times R/I_t,
\]

where \( I_c \) and \( I_t \) are two ideals such that \( \langle \alpha \rangle \not\subseteq \mathfrak{B}_c \) for any prime factor \( \mathfrak{B}_c \) of \( I_c \), while \( \langle \alpha \rangle \subseteq \mathfrak{B}_t \) for any prime factor \( \mathfrak{B}_t \) of \( I_t \).
3.1 Cycles of $S$

The following holds.

**Lemma 3.6** If $\tilde{x}$ is $r$-periodic in $S$, then $\tilde{x}$ is the $x$-coordinate of a point $(P, [0]) \in R/I_c \times R/I_t$.

**Proof** Let $(P, Q) \in R/I_c \times R/I_t$ be a point whose $x$-coordinate is $\tilde{x}$.

Since $\tilde{x}$ is $r$-periodic, there exists a positive integer $m$ such that $r^m(\tilde{x}) = \tilde{x}$. Hence

$$([\alpha]^m P, [\alpha]^m Q) \in \{(P, Q), (-P, -Q)\}. \quad (3.1)$$

According to the definition of $I_t$, we have that $\langle \alpha \rangle \subseteq \mathfrak{B}_t$ for any prime factor $\mathfrak{B}_t$ of $I_t$. Therefore there exists a positive integer $l$ such that

$$[\alpha]^l Q = [0] \quad (3.2)$$

in $R/I_t$. From (3.1) and (3.2) we deduce that

$$[\alpha]^{km} Q \in \{Q, -Q\} \text{ and } [\alpha]^{km} Q = [0] \quad (3.3)$$

for any integer $k$ such that $km \geq l$. This latter is possible only if $Q = [0]$. $\square$

Suppose that

$$R/I_c \cong \left( \prod_{i=1}^{j} R/\mathfrak{B}_{i}^{e_i} \right) \times \left( \prod_{i=j+1}^{k} R/\mathfrak{B}_{i}^{e_i} \right) \times \left( \prod_{i=k+1}^{l} R/\mathfrak{B}_{i}^{e_i} \right), \quad (3.4)$$

where the notations are as in Sect. 2.1. The description of the cycles formed by the elements of $S$ is similar to [14, Section 3.1].

For any $i \in [1, l]$ we define the interval $H_i$ as follows:

- $H_i := [0, e_i]$ if $i \in [1, k]$;
- $H_i := [0, (e_i + 1)/2]$ if $i \in [k + 1, l]$.

Moreover we define

$$H := \prod_{i=1}^{l} H_i.$$  

Let $h_i$ be an integer in $H_i$ for some $i \in [1, l]$. We introduce the notation $n_{h_i}$ distinguishing three cases.

1. If $i \in [1, j]$, then

$$n_{h_i} := \begin{cases} 1 & \text{if } h_i = 0, \\ p_i^{h_i} - p_i^{h_i - 1} & \text{otherwise.} \end{cases}$$

2. If $i \in [j + 1, k]$, or $i \in [k + 1, l]$ and $e_i$ is even, then

$$n_{h_i} := \begin{cases} 1 & \text{if } h_i = 0, \\ p_i^{2h_i} - p_i^{2(h_i - 1)} & \text{otherwise.} \end{cases}$$

\copyright Springer
(3) If $i \in [k + 1, l]$ and $e_i$ is odd, then

$$n_{h_i} := \begin{cases} 1 & \text{if } h_i = 0, \\ p_i^{2h_i} - p_i^{2(h_i-1)} & \text{if } 1 \leq h_i \leq (e_i - 1)/2, \\ p_i^{2h_i - 1} - p_i^{2(h_i-1)} & \text{if } h_i = (e_i + 1)/2. \end{cases}$$

Let $$s_{h_i} := \min\{v \in \mathbb{N} \setminus \{0\} : \alpha^v \pm 1 \in \mathcal{B}_{h_i}^0\},$$

where we adopt the convention that $\mathcal{B}_{h_i}^0 = R$. We notice in passing that $\alpha^v \pm 1 \in \mathcal{B}_{h_i}^{h_j}$ reads as $\alpha^v + 1 \in \mathcal{B}_{h_i}^{h_j}$ or $\alpha^v - 1 \in \mathcal{B}_{h_i}^{h_j}$.

A $r$-periodic element $\bar{x} \in S\setminus\{\infty\}$ is the $x$-coordinate of a rational point whose image in $R/I_e$ is $P = (P_i)^{l-1}$. Any $P_i$ has additive order $p_i^{h_i}$ in $R/\mathcal{B}_{i}^{e_i}$ for some $h_i \in H_i$. The $l$ integers $h_i$, for $i \in [1, l]$, form the $l$-tuple $h := (h_1, \ldots, h_l)$.

The following holds.

**Lemma 3.7** (1) Let $i \in [1, l]$. Then in $R/\mathcal{B}_{i}^{e_i}$ there are $n_{h_i}$ points of additive order $p_i^{h_i}$ for any $h_i \in H_i$.

(2) Let $P_i$ be a point of order $p_i^{h_i}$ in $R/\mathcal{B}_{i}^{e_i}$. Then the smallest of the positive integers $v$ such that $[\alpha]^v P_i \in \{\pm P_i\}$ is $s_{h_i}$.

**Proof** We prove separately the claims.

(1) Let $i \in [1, k]$. A point $P_i$ has additive order $p_i^{h_i}$ greater than 1 in $R/\mathcal{B}_{i}^{e_i}$ if and only if its representative in $GR(p_i^{e_i}, p_i^{m_{e_i}})$, where $m \in \{1, 2\}$, is

$$c_{e_i-h_i} p_i^{e_i-h_i} + \cdots + c_{e_i-1} p_i^{e_i-1}$$

for some coefficients $c_{e_i-h_i}, \ldots, c_{e_i-1} \in \{0, 1, \ldots, \xi^{p_i^{-2}}\}$ with $c_{e_i-h_i} \neq 0$. Therefore there are

$$(p_i^m - 1) \cdot p_i^{m(h_i-1)} = p_i^{m_{h_i}} - p_i^{m(h_i-1)}$$

points of additive order $p_i^{h_i}$ in $R/\mathcal{B}_{i}^{e_i}$.

If $i \in [k+1, l]$, then the result follows from the fact that $Z_{p_i} \cong GR(p_i^t, p_i^s)$ for any positive integer $s$.

(2) Suppose that $i \in [1, k]$. Let $v$ be a positive integer such that $[\alpha]^v P_i \in \{\pm P_i\}$, namely $[\alpha^v \pm 1] P_i = [0]$ in $R/\mathcal{B}_{i}^{e_i}$.

In $GR(p_i^{e_i}, p_i^{m_{e_i}})$, where $m \in \{1, 2\}$, we can represent $P_i$ in the form (3.5). Therefore, either $[\alpha^v \pm 1] = [0]$ or, according to Theorem 2.2 (4), $[\alpha^v \pm 1]$ can be written in $GR(p_i^{e_i}, p_i^{m_{e_i}})$ as

$$u p_i^{h_i}$$

for some unit $u$. Hence $[\alpha^v \pm 1] = [0]$ in $R/\mathcal{B}_{i}^{h_i}$, namely $\alpha^v \pm 1 \in \mathcal{B}_{i}^{h_i}$.

If $i \in [k+1, l]$, then the result follows in a similar way since $Z_{p_i} \cong GR(p_i^t, p_i^s)$ for any positive integer $s$.  

We define

$$s'_h := \text{lcm}(s_{h_1}, \ldots, s_{h_l}).$$
As a consequence of Lemma 3.7 the period of $\tilde{x}$ with respect to the action of $r$ is $s_h$, where

$$s_h := \begin{cases} s'_h & \text{if } [\alpha]^{s'_h} P \in \{\pm P\}; \\ 2s'_h & \text{otherwise.} \end{cases}$$

Consider an element $h := (h_i)_{i=1}^l$ in $H$. Let $s_h$ be defined as above.

We suppose that none of the following conditions is satisfied:

- $\prod_{i=1}^l p_i^{h_i} \in \{1, 2\}$;
- $\prod_{i=1}^l p_i^{h_i} = 4$ and $h_i \leq 1$ for any $i \in [1, l]$.

Indeed, we notice that the only point of order 1 is the point at infinity, while the rational points having order 2 have the $y$-coordinate equal to 0 and consequently their $x$-coordinate belongs to $E_0$.

The number of points $(P, [0])$ in $R/\langle \delta \rangle$ whose corresponding $x$-coordinate belongs to a cycle of length $s_h$ is $\prod_{i=1}^l n_{h_i}$.

If we denote by $C^S_h$ the set of all cycles in $G^{q^n}$ formed by such points, then the following holds in analogy with [14, Theorem 3.3].

**Theorem 3.8** If $h$ and $C^S_h$ are as above, then

$$|C^S_h| = \frac{1}{2s_h} \cdot \prod_{i=1}^l n_{h_i}.$$ 

### 3.2 Trees rooted in elements of $S$

If $x' \in \mathbb{P}^1(\mathbb{F}_{q^n})$ is not $r$-periodic, then it is preperiodic, namely some iterate of $x'$ is $r$-periodic. Therefore, if

$$Q = (Q_c, Q_t) \in R/I_c \times R/I_t$$

is a point in $E(\mathbb{F}_{q^n})$ whose $x$-coordinate is $x'$, then

$$[\alpha]^s Q = ([\alpha]^s Q_c, [0])$$

for some positive integer $s$.

Hence the trees rooted in elements of $S$ can be studied relying upon the structure of $R/I_t$, which we suppose to be isomorphic to

$$\left( \prod_{i=1}^{j} R/\mathfrak{B}_i^{e_i} \right) \times \left( \prod_{i=j+1}^{k} R/\mathfrak{B}_i^{e_i} \right) \times \left( \prod_{i=k+1}^{l} R/\mathfrak{B}_i^{e_i} \right),$$

where the notations are as in Sect. 2.1, but the indices $j, k$ and $l$, the ideals $\mathfrak{B}_i$ and the integers $e_i$ are not necessarily the same as in (3.4).

Let

$$\langle \alpha \rangle = \left( \prod_{i=1}^{l} \mathfrak{B}_i^{f_i} \right) \cdot J,$$

for some non-negative integers $f_i$, with $i \in [1, l]$, and some ideal $J$ such that no ideal $\mathfrak{B}_i$ appears in the factorization of $J$.

We define

$$d := \max_{i \in [1, l]} \left\{ \left\lfloor \frac{e_i}{f_i} \right\rfloor : f_i \neq 0 \right\},$$

for some non-negative integers $f_i$, with $i \in [1, l]$, and some ideal $J$ such that no ideal $\mathfrak{B}_i$ appears in the factorization of $J$.
provided that this latter set is non-empty.

If $\tilde{x} \in \mathbb{P}^1(\mathbb{F}_{q^n})$ is $r$-periodic, then

- $T^S(\tilde{x})$ denotes the tree rooted in $\tilde{x}$ and formed by elements of $S$;
- $T^S_h(\tilde{x})$ denotes the set of all vertices belonging to the level $h$ of $T^S(\tilde{x})$ for some $h \in [0, d]$;
- $T^{q^n}(\tilde{x})$ denotes the tree rooted in $\tilde{x}$ and formed by elements of $\mathbb{P}^1(\mathbb{F}_{q^n})$.

If $x' \in G^{q^n}$, then we denote by

$$\text{Pre}^S(x') := \{ x \in S : r(x) = x' \}$$

the preimage set of $x'$ in $S$ with respect to the map $r$.

**Remark 3.9** We notice that $T^S(\tilde{x}) \subseteq T^{q^n}(\tilde{x})$, namely $T^S(\tilde{x})$ is a subtree of $T^{q^n}(\tilde{x})$.

More in detail, we can distinguish the following cases.

- If $\tilde{x} \in S \setminus E_0$, then any predecessor of $\tilde{x}$ in $T^{q^n}(\tilde{x})$ belongs to $S \setminus E_0$ because of Lemmas 3.3 and 3.5. Therefore $T^S(\tilde{x}) = T^{q^n}(\tilde{x})$.
- If $\tilde{x} \in E_0$, then $T^{A_n}(\tilde{x})$ and $T^{B_n}(\tilde{x})$ can be proper subsets of $T^{q^n}(\tilde{x})$. Hence,

$$T^{q^n}(\tilde{x}) = T^{A_n}(\tilde{x}) \cup T^{B_n}(\tilde{x}),$$

with $T^{A_n}(\tilde{x}) \cap T^{B_n}(\tilde{x}) \subseteq E_0$.

**Remark 3.10** We notice that $|\text{Pre}^S(x')|$ is equal to the indegree of the vertex $x'$ in $G^{q^n}$, unless some element of $E_0$ is a preimage of $x'$ and is not contained in $S$.

We introduce some notations.

- For any $i \in [1, l]$ and any non-negative integer $s$ we define

$$m_i^s := \min\{e_i, f_is\}.$$

- For any $h \in [1, d]$ we define

$$v_h := \prod_{i=1}^l N\left(\mathfrak{B}_i^{m_i^h}\right) - \prod_{i=1}^l N\left(\mathfrak{B}_i^{m_i^{h-1}}\right),$$

$$\tilde{v}_h(\tilde{x}) := |T^S_h(\tilde{x}) \cap E_0|.$$  

- If $h \in [0, d - 1]$, then we define

$$v^h_i := N(\mathfrak{B}_i^{\min\{f_i, m_i^h\}})$$

for any $i \in [1, l]$ and

$$v^h := \prod_{i=1}^l v^h_i.$$  

- If $x_h \in T^S_h(\tilde{x})$ for some $h \in [0, d - 1]$, then we define

$$\tilde{v}(x_h) := |\text{Pre}^S(x_h) \cap E_0|.$$  

**Remark 3.11** We notice that $0 \leq \tilde{v}_h(\tilde{x}) \leq 3$ and $\tilde{v}_h(\tilde{x})$ can be non-zero only if $h \leq 2$, since the rational points (different from the point at infinity) having $x$-coordinate in $E_0$ have order 2.
Using the same notations as in Sect. 3.1 we get the following.

**Theorem 3.12** Let $f_i > 0$ for some $i \in [1, l]$.

1. The tree $T^S(\bar{x})$ has depth $d$ and, for any $h \in [1, d]$, we have that
   $$|T^S_h(\bar{x})| = \begin{cases} \frac{1}{2} \left[ v_h + \tilde{v}_h(\bar{x}) \right] & \text{if } \bar{x} \in E_0, \\ v_h & \text{if } \bar{x} \notin E_0. \end{cases}$$

2. If $x_h \in T^S_h(\bar{x})$ for some $h \in [0, d - 1]$ and $\text{Pre}^S(x_h) \setminus E_0 \neq \emptyset$, then
   $$|\text{Pre}^S(x_h) \setminus E_0| = \begin{cases} \frac{1}{2} \left( v^{h+1} - \tilde{v}(x_h) \right) & \text{if } x_h \in E_0, \\ v^{h+1} & \text{if } x_h \notin E_0. \end{cases}$$

**Proof** Let $(P, [0]) \in R/I_c \times R/I_t \cong R/\langle \delta \rangle$ be one of the points having $\bar{x}$ as $x$-coordinate in $E(F_{q^{2n}})$.

We prove separately the claims.

1. We notice that any vertex of $T^S(\bar{x})$ is the $x$-coordinate of a point of the form $\bar{V} = (\bar{P}, \bar{Q}) \in R/\langle \delta \rangle$ such that $[\alpha]^u \bar{V} \in \{(\pm \bar{P}, [0])\}$ for some non-negative integer $u \leq d$. According to the factorization (3.7) of $\langle \alpha \rangle$, we have that
   $$df_i \geq \frac{e_i}{f_i} f_i = e_i$$
   for any $i \in [1, l]$ with $f_i > 0$. Therefore the depth of $T^S(\bar{x})$ is at most $d$.

   Consider the $x$-coordinate $x'$ of the point $V := ([\alpha]^{-d} P, [1])$. As a consequence of the definition of $d$ we have that $[\alpha]^u V \notin \{ (\pm P, [0]) \}$ for any non-negative integer $u$ smaller than $d$, while $[\alpha]^d V \in \{ (\pm P, [0]) \}$. Hence we conclude that $T^S(\bar{x})$ has depth $d$.

   Now consider the $x$-coordinate $x'$ of a point $V := (P', Q)$ such that $x'$ belongs to $T^S_h(\bar{x})$ for some $h \geq 1$. Then $h$ is the smallest of the positive integers $u$ such that $[\alpha]^u V \in \{ (\pm P, [0]) \}$. In particular, $P' \in \{ (\pm [\alpha]^{-h} P) \}$, while
   $$Q \in (R/I_t)_h,$$
   where
   $$(R/I_t)_h := \left( \prod_{i=1}^{l} B_i^{e_i} / B_i^{m_i} \right) \setminus \left( \prod_{i=1}^{l} B_i^{e_i} / B_i^{m_i - 1} \right).$$
   We have that
   $$\prod_{i=1}^{l} B_i^{e_i - m_i^h} / B_i^{e_i} = \prod_{i=1}^{l} N \left( B_i^{m_i^h} \right),$$
   $$\prod_{i=1}^{l} B_i^{e_i - m_i^{h-1}} / B_i^{e_i} = \prod_{i=1}^{l} N \left( B_i^{m_i^{h-1}} \right).$$

   We deal separately with different cases.

   - **Case 1:** $(P, [0])$ has order $1$ or $2$.
     Then $\bar{x} \in E_0$ and $P = -P$. The result follows because $([\alpha]^{-h} P, Q)$ and $([\alpha]^{-h} P, -Q)$ have the same $x$-coordinate and $Q \neq -Q$, unless $([\alpha]^{-h} P, Q)$ has order $2$. 

\(\text{Springer}\)
• Case 2: \((P, [0])\) has order greater than 2.
  The result follows because \((\alpha)^{-b} P, Q)\) and \((-\alpha)^{-b} P, Q)\) have different \(x\)-coordinates, while \((\alpha)^{-b} P, Q)\) and \((-\alpha)^{-b} P, -Q)\) have the same \(x\)-coordinate.

(2) Let \(V_h := (\alpha)^{-b} P, Q\) be a point in \(R/\langle \delta \rangle\) whose \(x\)-coordinate is \(x_h\).

The endomorphism \(\alpha\) induces a \(v^{h+1-1}\) map on \(\mathfrak{B}_{i}^{e_i}/\mathfrak{B}_{i}^{e_i}\) for any \(i \in [1, l]\).

Let 
\[
[\alpha]^{-1} V_h := \left\{ \left( (\alpha)^{-(h+1)} P, \tilde{Q}_1 \right), \ldots, \left( (\alpha)^{-(h+1)} P, \tilde{Q}_{\nu^{h+1}} \right) \right\}
\]
be the set of preimages of \((\alpha)^{-h} P, Q)\) in \(R/\langle \delta \rangle\).

If \(Q \neq -Q\), then \(|[\alpha]^{-1} V_h| = \nu^{h+1}\), while \(|[\alpha]^{-1} V_h| = \frac{1}{2} \nu^{h+1}\) if \(Q = -Q\). \(\square\)

4 Examples

In this section we construct explicitly some graphs and show how their structure relates to the results previously proved.

We recall that, if \(q\) is a power of a prime and \(n\) is a positive integer, then
\[
\mathbb{P}^1(F_{q^n}) = \{g^m : m \in [0, q^n - 2] \} \cup \{0, \infty\}
\]
for some primitive element \(g \in F_{q^n}\).

In the examples we label the vertices of \(G_{q^n}\) using the exponents \(m \in [0, q^n - 2]\), the symbol \(\infty\) and the symbol ‘0’ for the zero of the field.

We notice that the computations for the construction of the graphs were carried out using GAP [11]. Moreover, the primitive element \(g\) used in each example is a root of a suitable primitive polynomial (more precisely, a Conway polynomial [7]).

| Example 4.1 | Primitive polynomial |
|-------------|---------------------|
| Example 4.2 | \(x - 5 \in \mathbb{F}_{73}[x]\) |
| Example 4.3 | \(x - 2 \in \mathbb{F}_{83}[x]\) |
| Example 4.3 | \(x^4 - x^2 - x + 2 \in \mathbb{F}_5[x]\) |

Along the way we made use of Sage [12] for the construction of the elliptic curves and for finding the endomorphisms.

**Example 4.1** Consider the ordinary elliptic curve
\[
E : y^2 = x^3 - x
\]
defined over \(\mathbb{F}_{73}\), whose endomorphism ring \(R\) is isomorphic to \(\mathbb{Z}[i]\).

Using Sage we find an isogeny \(\sigma\) of degree 10 from \(E\) to the curve
\[
E' : y^2 = x^3 + 8x
\]
defined over \(\mathbb{F}_{73}\) as
\[
\sigma(x, y) := (\sigma_1(x), y \cdot \sigma_2(x)),
\]
where
\[
\sigma_1(x) := \frac{x^{10} - 3x^8 + 5x^6 - 5x^4 + 3x^2 - 1}{x^9 + 28x^7 - 21x^5 + 28x^3 + x}.
\]

The curve \( E' \) is isomorphic to the curve \( E \) via the map
\[
\psi : E' \rightarrow E \quad (x, y) \mapsto (-3x, 22y).
\]

Therefore, there exists an endomorphism \( \alpha := \psi \circ \sigma \) of degree 10 of \( E \) defined as
\[
\alpha(x, y) := (\alpha_1(x), y \cdot \alpha_2(x)),
\]
where
\[
\alpha_1(x) := -3 \cdot \sigma_1(x).
\]

We define the map \( r \) as in the Introduction.
The graph associated with the action of \( r \) over \( \mathbb{P}^1(\mathbb{F}_{73}) \) is represented below.
The representations in $R$ of the Frobenius endomorphism $\pi_{73}$ and the endomorphism $\alpha$ are

$$\pi_{73} = -3 + 8i,$$
$$\alpha = 3 - i.$$  

If we set $\delta := \pi_{73} - 1$, then we have that

$$\langle \delta \rangle = (1 + i)^4 \cdot (1 - 2i),$$
$$\langle \alpha \rangle = (1 + i) \cdot (1 - 2i).$$

Given that $\langle \delta \rangle \subseteq \langle \alpha \rangle$, the only $r$-periodic element in $A_1$ is $\infty$.

We can study the structure of the tree $T^{A_1}(\infty)$ relying upon

$$R/I_I := R/\mathfrak{B}_1^4 \times R/\mathfrak{B}_2,$$

where

$$\mathfrak{B}_1 := (1 + i), \quad \mathfrak{B}_2 := (1 - 2i).$$

Using the notations of Sect. 3.2 we notice that

$$e_1 = 4, \ e_2 = 1,$$
$$f_1 = 1, \ f_2 = 1,$$

and $d = 4$. 
According to Theorem 3.12, $T^{A_{1}}(\infty)$ has depth 4. Moreover,
\[
|T_{1}^{A_{1}}(\infty)| = \frac{1}{2} \cdot [2 \cdot 5 - 1 + 1] = 5,
\]
\[
|T_{2}^{A_{1}}(\infty)| = \frac{1}{2} \cdot [4 \cdot 5 - 2 \cdot 5 + 2] = 6,
\]
\[
|T_{3}^{A_{1}}(\infty)| = \frac{1}{2} \cdot [8 \cdot 5 - 4 \cdot 5] = 10,
\]
\[
|T_{4}^{A_{1}}(\infty)| = \frac{1}{2} \cdot [16 \cdot 5 - 8 \cdot 5] = 20.
\]
As regards the indegrees of the vertices of $T^{A_{1}}(\infty)$, we notice that
\[
\nu^{1} = \nu^{2} = \nu^{3} = 10.
\]
Therefore
\[
|Pre^{A_{1}}(\infty)\setminus E_{0}| = 5.
\]
Moreover, for any vertex $x_{h} \in T^{A_{1}}(\infty)$ with $h \in [1, 3]$, we have that
\[
\bullet |Pre^{A_{1}}(x_{h})\setminus E_{0}| \in \{0, 5\} \text{ if } x_{h} \in E_{0};
\]
\[
\bullet |Pre^{A_{1}}(x_{h})\setminus E_{0}| \in \{0, 10\} \text{ if } x_{h} \notin E_{0}.
\]
Now we define $\delta := \pi_{73} + 1$. We have that
\[
\langle \delta \rangle = \langle 1 + i \rangle^{2} \cdot \langle -1 + 4i \rangle.
\]
Therefore, the cycles formed by the elements in $B_{1}$ can be studied relying upon
\[
R/I_{c} := R/B_{1},
\]
where
\[
B_{1} := \langle -1 + 4i \rangle.
\]
According to the notations of (3.4) we have that $j = 1$, $k = 1$ and $l = 1$, while
\[
H_{1} = [0, 1].
\]
Let $h_{1} \in H_{1}$. We have that
\[
sh_{1} = \begin{cases} 
1 & \text{if } h_{1} = 0, \\
8 & \text{if } h_{1} = 1.
\end{cases}
\]
Hence, according to Theorem 3.8, we have that
\[
|C_{B_{1}}^{1}(1)| = \frac{1}{2} \cdot 8 \cdot 16 = 1.
\]
Moreover the only cycle in $C_{B_{1}}^{1}(1)$ has length 8. There is also one cycle of length 1 formed by
\infty (notice in passing that the point at infinity $O$ has order 1).

Finally we notice that the structure of the tree $T^{B_{1}}(\tilde{x})$ rooted in some $\tilde{x} \in B_{1}$ can be studied relying upon
\[
R/B_{1}^{2},
\]
where $B_{1} := \langle 1 + i \rangle$. 

\(\text{Springer}\)
According to Theorem 3.12, the tree $T_{B_1}(\tilde{x})$ has depth 2 and

$$|T^1_{B_1}(\tilde{x})| = 1,$$
$$|T^2_{B_1}(\tilde{x})| = 2.$$ 

In particular, we notice that $T^1_{B_1}(\infty)$ is a subtree of $T^1_{A_1}(\infty)$ and that the elements of $E_0$ are vertices of both the trees. Hence $T^7_{B_1}(\infty) = T^1_{A_1}(\infty)$, while $T^1_{B_1}(\tilde{x}) = T^7_{B_1}(\tilde{x})$ for any other $r$-periodic element $\tilde{x}$.

Finally, since $N(\mathfrak{B}_1) = 2$, the indegree of any vertex of the tree is 0 or 2 in accordance with Theorem 3.12.

**Example 4.2** Consider the ordinary elliptic curve

$$E : y^2 = x^3 + 56x + 34$$

defined over $\mathbb{F}_{83}$.

Such an elliptic curve has endomorphism ring $R := \mathbb{Z}[\omega]$, where $\omega = \frac{1 + \sqrt{-19}}{2}$. We consider the endomorphism

$$\alpha(x, y) := (\alpha_1(x), y \cdot \alpha_2(x))$$

of degree 17, where $\alpha_1(x) := \frac{a(x)}{b(x)}$ with

$$a(x) := 4 \cdot \left( x^{17} - 32x^{16} + 13x^{15} + 12x^{14} - x^{13} - 32x^{12} + 32x^{11} - 10x^{10} + 8x^9 + 2x^8 - 8x^7 - x^6 + x^5 + 35x^4 + 41x^3 + 11x^2 + 29x + 22 \right);$$

$$b(x) := \left( x^{16} - 32x^{15} - 39x^{14} + 19x^{13} + 36x^{12} + 8x^{11} + 41x^{10} - 8x^9 - 32x^8 - 16x^7 - 41x^6 - 13x^5 - 3x^4 + 5x^3 + 3x^2 - 10x + 23 \right).$$

The following connected components of the graph $G^{83}$ are due to the elements belonging to $A_1$. 

![Diagram](image)
The structure of the 2 connected components above can be explained as follows.
In \( R \) we have that
\[
\pi_{83} = 7 + 2\omega, \\
\alpha = 3 + \omega.
\]
Let \( \delta := \pi_{83} - 1 \). Then
\[
\langle \delta \rangle = \langle 2 \rangle \cdot \langle 3 + \omega \rangle, \\
\langle \alpha \rangle = \langle 3 + \omega \rangle.
\]
The structure of the cycles formed by elements of \( A_1 \) can be determined relying upon
\[
R/I_c := R/\mathcal{B}_1,
\]
where \( \mathcal{B}_1 := \langle 2 \rangle \).
According to the notations of (3.4) we have that \( j = 0, k = 1 \) and \( l = 1 \), while
\[
H_1 = [0, 1].
\]
Let \( h_1 \in H_1 \). We have that
\[
s_{h_1} = \begin{cases} 
1 & \text{if } h_1 = 0, \\
3 & \text{if } h_1 = 1.
\end{cases}
\]
We notice that all points in \( R/\mathcal{B}_1 \) have order 1 or 2: the only point of order 1 is the point at infinity; the points of order 2 have \( x \)-coordinate in \( E_0 \). The cycle formed by \( \infty \) has length 1, while the other elements of \( E_0 \) form a cycle of length 3.
The structure of the trees can be studied relying upon

\[ R/I_t := R/\mathcal{B}_1, \]

where \( \mathcal{B}_1 := (3 + \omega) \).

Therefore \( T^{83}(\tilde{x}) \) has depth 1 for any \( \tilde{x} \in A_1 \). Moreover, according to Theorem 3.12, the number of vertices belonging to \( T^{83}_1(\tilde{x}) \) is

\[ |T^{83}_1(\tilde{x})| = \frac{1}{2} \cdot [17 - 1] = 8. \]

Now consider the remaining connected components of \( G^{83} \).

All the vertices in the connected components of length 1 and 3 above are due to elements belonging to \( B_1 \), which are the \( x \)-coordinates of the rational points contained in

\[ R/(\langle \delta \rangle), \]

where \( \delta := \pi_{83} + 1 \).

We have that

\[ \langle \delta \rangle = \langle 1 - \omega \rangle^2 \cdot (2). \]

Therefore the elements of \( B_1 \) are \( r \)-periodic.

Let

\[ R/I_c := R/\mathcal{B}_1^2 \times R/\mathcal{B}_2, \]

where

\[ \mathcal{B}_1 := \langle 1 - \omega \rangle, \mathcal{B}_2 := \langle 2 \rangle, \]

with \( N(\mathcal{B}_1) = 5 \).

According to the notations of (3.4) we have that \( j = 1, k = 2 \) and \( l = 2 \), while

\[ H_1 = [0, 2], \quad H_2 = [0, 1]. \]
Let $h_1 \in H_1$. We have that

$$s_{h_1} = \begin{cases} 
  1 & \text{if } h_1 = 0, \\
  1 & \text{if } h_1 = 1, \\
  1 & \text{if } h_1 = 2.
\end{cases}$$

Moreover $\alpha^{s_{h_1}} + 1 \in \mathcal{B}_1$ for $h_1 \in \{1, 2\}$.

Let $h_2 \in H_2$. We have that

$$s_{h_2} = \begin{cases} 
  1 & \text{if } h_2 = 0, \\
  3 & \text{if } h_2 = 1.
\end{cases}$$

Moreover $\alpha^{s_{h_2}} + 1 \in \mathcal{B}_2$ for $h_2 = 1$.

Hence, according to Theorem 3.8, we have that

$$|c_{B_1}^{(1,0)}| = \frac{1}{2 \cdot 1} \cdot 4 = 2,$$

$$|c_{B_1}^{(2,0)}| = \frac{1}{2 \cdot 1} \cdot 20 = 10,$$

and any cycle in $C_{B_1}^{(1,0)}$ and $C_{B_1}^{(2,0)}$ has length 1.

Moreover we have that

$$|c_{B_1}^{(1,1)}| = \frac{1}{2 \cdot 3} \cdot (4 \cdot 3) = 2,$$

$$|c_{B_1}^{(2,1)}| = \frac{1}{2 \cdot 3} \cdot (20 \cdot 3) = 10,$$

and any cycle in $C_{B_1}^{(1,1)}$ and $C_{B_1}^{(2,1)}$ has length 3.

In $\mathbb{R}/I_c$ we can find 1 point of order 1 and 3 points of order 2. Indeed, $\infty$ forms a cycle of length 1, while the $x$-coordinates of the points of order 2 form a cycle of length 3, namely the cycle whose vertices are labelled by 22, 23 and 53. We notice that such a cycle is formed by elements in $A_1$ too.

In conclusion, the elements of $B_1$ form 13 cycles of length 1 and 13 cycles of length 3. Two of these cycles are also formed by elements of $A_1$.

**Example 4.3** Consider the ordinary elliptic curve

$$E : y^2 = x^3 + x + \gamma$$

defined over $\mathbb{F}_{25}$, where $\gamma$ is a primitive element of $\mathbb{F}_{25}$.

The endomorphism ring of the curve $E$ is $R := \mathbb{Z}[\omega]$, where $\omega := \sqrt{-21}$.

We consider the endomorphism

$$\alpha(x, y) := (\alpha_1(x), y \cdot \alpha_2(x))$$
of degree 22, where \( \alpha_1(x) := \frac{a(x)}{b(x)} \) with

\[
\begin{align*}
  a(x) &:= x^{22} - \gamma x^{21} - 2\gamma x^{20} + (-\gamma + 1)x^{19} + (\gamma + 2)x^{18} + x^{17} - 2(\gamma + 1)x^{16} \\
  &
  - 2(\gamma - 1)x^{15} + x^{14} + \gamma x^{13} - (2\gamma + 1)x^{12} + 2\gamma x^{11} + (\gamma - 1)x^{10} + 2\gamma x^9 \\
  &- (\gamma + 2)x^8 - (\gamma - 2)x^7 - 2x^6 + (2\gamma + 1)x^5 - (\gamma - 1)x^4 + 2\gamma x^3 + 2\gamma x^2 \\
  &+ (2\gamma + 1)x + 2\gamma; \\
  b(x) &:= x^{21} - \gamma x^{20} - 2\gamma x^{19} - (\gamma - 1)x^{18} + (\gamma + 2)x^{17} + x^{16} - 2(\gamma + 1)x^{15} \\
  &- 2(\gamma - 1)x^{14} + x^{13} + \gamma x^{12} - (2\gamma + 1)x^{11} + 2\gamma x^{10} + (\gamma + 2)x^9 - \gamma x^8 \\
  &- 2(\gamma - 1)x^7 + \gamma x^6 + (\gamma + 1)x^5 - (\gamma + 1)x^4 + 2x^3 - (2\gamma - 1)x^2 - \gamma x \\
  &- 2\gamma - 1.
\end{align*}
\]

In this example we construct the graph associated with \( r \) over \( \mathbb{F}_{25^2} \).

According to the notations of the Introduction, we have

\[
g = 25, \quad n = 2.
\]

Using Sage we compute the minimal polynomial \( x^2 - 4x + 25 \) of the Frobenius endomorphism \( \pi_{25} \), whose representation as an element of \( R \) is

\[
\pi_{25} = 2 + \omega.
\]

The representation of \( \alpha \) as an endomorphism of \( R \) is

\[
\alpha = 1 + \omega.
\]

Since \( |\mathbb{P}^1(\mathbb{F}_{25^2})| = 626 \), we introduce some symbols with the aim to have a more compact representation of \( G_{25^2} \).

\[
\begin{align*}
  &\text{stands for} \\
  &\text{stands for } n \text{ vertices joined to the vertex } a
\end{align*}
\]
Here are the five connected components of $G^{25^2}$. 

![Graph of connected components]
Now we analyse the structure of the connected components of $G^{252}$ formed by the elements of $A_2$.

If $\delta := \pi_{25}^2 - 1$, then

$$\langle \delta \rangle = I_1 \cdot I_2 \cdot I_3^2 \cdot I_4,$$

$$\langle \alpha \rangle = I_2 \cdot I_3,$$

where

$$I_1 := \langle 5, \omega + 3 \rangle,$$

$$I_2 := \langle 11, \omega + 1 \rangle,$$

$$I_3 := \langle 2, \omega + 1 \rangle,$$

$$I_4 := \langle 3, \omega \rangle,$$

with $N(I_1) = 5$, $N(I_2) = 11$, $N(I_3) = 2$ and $N(I_4) = 3$.

The structure of the cycles formed by elements of $A_2$ can be determined relying upon

$$R/I_c := R/\mathcal{B}_1 \times R/\mathcal{B}_2,$$

where

$$\mathcal{B}_1 := I_1,$$

$$\mathcal{B}_2 := I_4.$$

According to the notations of (3.4) we have that $j = 1$, $k = 1$ and $l = 2$, while

$$H_1 = [0, 1], \quad H_2 = [0, 1].$$

Let $h_1 \in H_1$. We have that

$$s_{h_1} = \begin{cases} 1 & \text{if } h_1 = 0, \\ 2 & \text{if } h_1 = 1. \end{cases}$$
Moreover $\alpha + 1 \in \mathcal{B}_1$.

Let $h_2 \in H_2$. We have that

$$s_{h_2} = \begin{cases} 
1 & \text{if } h_2 = 0, \\
1 & \text{if } h_2 = 1.
\end{cases}$$

Moreover $\alpha - 1 \in \mathcal{B}_2$.

Hence, according to Theorem 3.8, we have that

$$|C_{A_2}^{A_2}((0,1))| = \frac{1}{2} \cdot 1 \cdot 1 = 1,$$

$$|C_{A_2}^{A_2}((1,0))| = \frac{1}{2} \cdot 2 \cdot 4 = 1,$$

$$|C_{A_2}^{A_2}((1,1))| = \frac{1}{2} \cdot 4 \cdot 2 = 1,$$

where the unique cycle in $C_{A_2}^{A_2}((0,1))$ (resp. $C_{A_2}^{A_2}((1,0))$, $C_{A_2}^{A_2}((1,1))$) has length 1 (resp. 2, 4). Such cycles can be found in the first three connected components of the graph. Finally, we notice that the point $([0], [0]) \in R/I_1$ has order 1. Indeed, $\infty$ forms a cycle of length 1.

Before proceeding we notice that

$$E_0 = \{ \infty, g^{287}, g^{311}, g^{364} \}.$$

Now we study the structure of the trees rooted in elements of $A_2$ relying upon

$$R/I_t := R/\mathcal{B}_1 \times R/\mathcal{B}_2,$$

where

$$\mathcal{B}_1 := I_2,$$

$$\mathcal{B}_2 := I_3.$$

If $\bar{x} \in A_2 \setminus E_0$, then

$$|T_{A_2}^{A_2}(\bar{x})| = 11 \cdot 2 - 1 = 21,$$

$$|T_{A_2}^{A_2}(\bar{x})| = 11 \cdot 4 - 11 \cdot 2 = 22,$$

while

$$|T_{A_2}^{A_2}(\infty)| = \frac{1}{2} \cdot [11 \cdot 2 - 1 + 1] = 11,$$

$$|T_{A_2}^{A_2}(\infty)| = \frac{1}{2} \cdot [11 \cdot 4 - 22 + 2] = 12.$$

We also notice that the indegree of any vertex belonging to a tree rooted in some element of the first three connected components is 22 since

$$\nu^1 = \nu^2 = 22$$

and no vertex in such components belongs to $E_0$.

Now we study the structure of the connected components formed by the elements of $B_2$.

If $\delta := \pi^2_{25} + 1$, then

$$\langle \delta \rangle = I_5 \cdot I_3^4.$$
where $I_3$ is as before, while

$$I_5 := (\omega - 4),$$

with $N(I_5) = 37$.

The structure of the cycles formed by the elements of $B_2$ can be determined relying upon

$$R/I_c := R/\mathcal{B}_1,$$

where $\mathcal{B}_1 := I_5$.

Following the notations of (3.4) we have that $j = 1$, $k = 1$ and $l = 1$, while

$$H_1 = [0, 1].$$

Let $h_1 \in H_1$. We have that

$$s_{h_1} = \begin{cases} 1 & \text{if } h_1 = 0, \\ 18 & \text{if } h_1 = 1. \end{cases}$$

Moreover $\alpha^{18} + 1 \in \mathcal{B}_1$.

Hence, according to Theorem 3.8, we have that

$$|C^{B_2}_{B_2}(\tilde{x})| = \frac{1}{2 \cdot 18} \cdot (36) = 1,$$

where the unique cycle in $C^{B_2}_{B_2}$ has length 18. Such a cycle can be found in the last connected component of the graph. As above, the point $([0]) \in R/I_c$ has order 1 and $\infty$ forms a cycle of length 1.

Now we study the structure of the trees rooted in elements of $B_2$ relying upon

$$R/I_t := R/\mathcal{B}_4^1,$$

where $\mathcal{B}_4 := I_3$.

Using the notations of Sect. 3.2 we have that

$$e_1 = 4,$$

$$f_1 = 1,$$

and $d = 4$.

If $\tilde{x} \in B_2 \setminus E_0$, then

$$|T_{B_2}^{B_2}(\tilde{x})| = 2 - 1 = 1,$$

$$|T_{B_2}^{B_2}(\tilde{x})| = 4 - 2 = 2,$$

$$|T_{B_2}^{B_2}(\tilde{x})| = 8 - 4 = 4,$$

$$|T_{B_2}^{B_2}(\tilde{x})| = 16 - 8 = 8,$$
while

\[ |T_1^{B_2}(\infty)| = \frac{1}{2} \cdot [2 - 1 + 1] = 1, \]

\[ |T_2^{B_2}(\infty)| = \frac{1}{2} \cdot [4 - 2 + 2] = 2, \]

\[ |T_3^{B_2}(\infty)| = \frac{1}{2} \cdot [8 - 4] = 2, \]

\[ |T_4^{B_2}(\infty)| = \frac{1}{2} \cdot [16 - 8] = 4. \]

**Acknowledgements** The author is grateful to the anonymous Reviewer for the careful reading of the manuscript and the valuable comments and suggestions.

**References**

1. W.-S. Chou, I. Shparlinski, On the cycle structure of repeated exponentiation modulo a prime. J. Number Theory 107(2), 345–356 (2004)
2. O. Colón-Reyes, A.S. Jarrah, R. Laubenbacher, B. Sturmfels, Monomial dynamical systems over finite fields. Complex Syst. 16(4), 333–342 (2006)
3. M. Elia, J.C. Interlando, R. Rosenbaum, On the structure of residue rings of prime ideals in algebraic number fields—PART I: unramified primes. Int. Math. Forum 5(56), 2795–2808 (2010)
4. M. Elia, J.C. Interlando, R. Rosenbaum, On the structure of residue rings of prime ideals in algebraic number fields—PART II: ramified primes. Int. Math. Forum 6(12), 565–589 (2011)
5. T. Gassert, Chebyshev action on finite fields. Discrete Math. 315, 83–94 (2014)
6. H.W. Lenstra, Complex multiplication structure of elliptic curves. J. Number Theory 56, 227–241 (1996)
7. F. Lübeck, Conway Polynomials for Finite Fields, http://www.math.rwth-aachen.de/~Frank.Luebeck/data/ConwayPol/index.html. Online; Accessed 25 Jan 2018
8. C. Qureshi, D. Panario, Rédei actions on finite fields and multiplication map in cyclic group. SIAM J. Discrete Math. 29(3), 1486–1503 (2015)
9. T. Rogers, The graph of the square mapping on the prime fields. Discrete Math. 148, 317–324 (1996)
10. M. Sha, S. Hu, Monomial dynamical systems of dimension one over finite fields. Acta Arith. 148(4), 309–331 (2011)
11. The GAP Group, GAP—Groups, Algorithms and Programming, http://www.gap-system.org
12. The Sage Developers, Sage Mathematics Software (Version 6.1.1) (2014), http://www.sagemath.org
13. S. Ugolini, Graphs associated with the map \( x \mapsto x + x^{-1} \) in finite fields of characteristic two, in Theory and Applications of Finite Fields, Contemp. Math., vol. 579, Amer. Math. Soc., Providence, RI (2012)
14. S. Ugolini, Graphs associated with the map \( X \mapsto X + X^{-1} \) in finite fields of characteristic three and five. J. Number Theory 133, 1207–1228 (2013)
15. S. Ugolini, On the iterations of certain maps \( X \mapsto K \cdot (X + X^{-1}) \) over finite fields of odd characteristic. J. Number Theory 142, 274–297 (2014)
16. T. Vasiga, J. Shallit, On the iteration of certain quadratic maps over \( GF(p) \). Discrete Math. 277, 219–240 (2004)
17. Z.-X. Wan, Finite Fields and Galois Rings (World Scientific Publishing, Singapore, 2012)
18. C. Wittmann, Group structure of elliptic curves over finite fields. J. Number Theory 88(2), 335–344 (2001)