On the iterations of the maps $ax^{2k} + b$ and $(ax^{2k} + b)^{-1}$ over finite fields of characteristic two

Simone Ugolini

Abstract. The maps $x \mapsto ax^{2k} + b$ defined over finite fields of characteristic two can be related to the duplication map over binary supersingular elliptic curves. Relying upon the structure of the group of rational points of such curves we can describe the possible cycle lengths of the maps. Then we extend our investigation to the maps $x \mapsto (ax^{2k} + b)^{-1}$. We also notice some relations between these latter maps and the polynomials $x^{2k+1} + x + a$, which have been extensively studied in literature.

Mathematics Subject Classification. 37P05, 37P25, 51E20.

Keywords. Arithmetic dynamical systems, finite fields, rational maps, supersingular elliptic curves.

1. Introduction

In a paper [1] appeared in 2004 Bluher studied the polynomials $x^{q+1} + ax + b$ defined over finite fields of characteristic $p$, with $q$ a power of $p$. The author studied the splitting field of such polynomials and other related problems, such as the number of roots in a given field. Later, other authors concentrated on such polynomials over finite fields of characteristic two.

Let $P_a(x) := x^{2k+1} + x + a$, where $k$ is a positive integer and $a \in \mathbb{F}_{2^n}^*$, for some positive integer $n$. In [1] the following result is proved.

Theorem 1.1. For any $a \in \mathbb{F}_{2^n}^*$ and a positive integer $k$, the polynomial $P_a(x)$ has either zero, one, two or $2^{\gcd(k,n)} + 1$ zeros in $\mathbb{F}_{2^n}$.

Helleseth and Kholosha [3,4] proved that when $\gcd(n, k) = 1$ the polynomial $P_a(x)$ has 0, 1 or 3 zeros in $\mathbb{F}_{2^n}$. Moreover, they provided criteria for $P_a(x)$
to have 0, 1 or 3 zeros depending upon the value of \(a\). In a paper appeared recently \([6]\) the authors calculated all possible roots of \(P_a(x)\) in \(\mathbb{F}_{2^n}\) and gave new criteria on \(a\) such that the equation \(P_a(x) = 0\) has 0, 1 or 3 solutions with the hypothesis that \(\gcd(k, n) = 1\).

Since \(x = 1\) is not a root of \(P_a(x)\), solving the equation \(P_a(x) = 0\) amounts to finding all \(x \in \mathbb{F}_{2^n}\) such that

\[
x = \frac{a}{x^{2^k} + 1}.
\]

From the point of view of dynamical systems, this latter problem is equivalent to finding all the fixed points in \(\mathbb{F}_{2^n}\) of the map \(x \mapsto \frac{1}{ax^{2^k} + a - 1}\). Such a map is an instance of the maps \(x \mapsto ax^{2^k} + b\) which can be written also as \(x \mapsto \frac{1}{a - 1}x^{2^k} + a - 1\). Such maps are involved in the definition of the duplication map of supersingular elliptic curves defined over finite fields of characteristic two.

In Sect. 5 we begin our investigation studying the iterations of the maps \(x \mapsto ax^4 + b\) over \(\mathbb{P}^1(\mathbb{F}_q)\). Such maps are involved in the definition of the duplication map of supersingular elliptic curves defined over finite fields of characteristic two. In Sect. 4 we extend our investigation to more general maps \(x \mapsto ax^{2^k} + b\) where \(k\) is a non-negative integer.

## 2. Preliminaries

In the paper we use the following notations.

- \(\mathbb{N}\) denotes the set of non-negative integers and \(\mathbb{N}^* := \mathbb{N}\setminus\{0\}\).
- If \(a, b \in \mathbb{N}\) with \(a \leq b\), then
  \[
  [a, b] := \{n \in \mathbb{N} : a \leq n \leq b\};
  \]
  \[
  ]a, +\infty[ := \{n \in \mathbb{N} : a < n\}.
  \]
- If \(x, y, n \in \mathbb{Z}\), then \(x \equiv y \mod n\) stands for
  \[
  x \equiv y \mod n \quad \text{or} \quad x \equiv -y \mod n.
  \]
- If \(f : A \to A\) is a map defined on a set \(A\) and \(m \in \mathbb{N}^*\) then we denote by \(f^m\) the \(m\)-fold composition of \(f\) with itself.
- If \(\mathbb{F}_q\) is a finite field with \(q\) elements, then \(\mathbb{P}^1(\mathbb{F}_q) := \mathbb{F}_q \cup \{\infty\}\). Moreover we denote by \(\overline{\mathbb{F}}_q\) the algebraic closure of \(\mathbb{F}_q\).

If \(f : \mathbb{P}^1(\mathbb{F}_q) \to \mathbb{P}^1(\mathbb{F}_q)\) is a map defined over \(\mathbb{P}^1(\mathbb{F}_q)\), then we denote by \(G_q(f)\) the digraph associated with \(f\) over \(\mathbb{P}^1(\mathbb{F}_q)\). The vertices of \(G_q(f)\) are the elements of \(\mathbb{P}^1(\mathbb{F}_q)\) and an arrow joins a vertex \(\alpha\) to a vertex \(\beta\) if \(f(\alpha) = \beta\).

If \(f : \mathbb{P}^1(\mathbb{F}_q) \to \mathbb{P}^1(\mathbb{F}_q)\) and \(x_0 \in \mathbb{P}^1(\mathbb{F}_q)\), then we denote the orbit of \(x_0\) by

\[
O(f, x_0) := \{f^i(x_0) : i \in \mathbb{N}\}.
\]

In case the map is not ambiguous, we use the shorter notation \(O(x_0)\). If \(f^j(x_0) = x_0\) for some \(j \in \mathbb{N}^*\), then we say that \(x_0\) is periodic with respect...
to $f$ or $f$-periodic (we also write that $x_0$ is periodic if the map $f$ is clear from the context). If $l \in \mathbb{N}^*$ is the smallest of the indices $j \in \mathbb{N}^*$ such that $f^j(x_0) = x_0$, then we say that $l$ is the period of $x_0$ or the length of the orbit $O(x_0)$. We notice that the length of the orbit is equal to the cardinality of the orbit itself, namely

$$l = |O(f, x_0)|.$$

We can prove that any $x_0 \in \mathbb{P}^1(\mathbb{F}_q)$ is periodic if $f$ is one-to-one.

**Lemma 2.1.** Let $f : \mathbb{P}^1(\mathbb{F}_q) \to \mathbb{P}^1(\mathbb{F}_q)$.

1. $f^i(x_0)$ is periodic for some $i \in \mathbb{N}$ if and only if $f^i(x_0) = f^k(x_0)$ for some $k \in [i, +\infty[$.
2. If $f : \mathbb{P}^1(\mathbb{F}_q) \to \mathbb{P}^1(\mathbb{F}_q)$ is one-to-one and $x_0 \in \mathbb{P}^1(\mathbb{F}_q)$, then $x_0$ is periodic.

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

1. If $f^i(x_0)$ is periodic then $f^j(f^i(x_0)) = f^i(x_0)$ for some $j \in \mathbb{N}^*$. Hence $f^i(x_0) = f^k(x_0)$ with $k = i + j$. Vice versa, if $f^i(x_0) = f^k(x_0)$ for some $k \in [i, +\infty[$ then $f^i(x_0)$ is periodic because $f^j(f^i(x_0)) = f^i(x_0)$ with $j := k - i$.

2. We consider the map $g : \mathbb{N} \to \mathbb{P}^1(\mathbb{F}_q)$ defined as

$$g(n) = f^n(x_0)$$

for any $n \in \mathbb{N}$. Since $\mathbb{P}^1(\mathbb{F}_q)$ is a finite set, the image set $g(\mathbb{N})$ is finite too. Hence there exist some $i, k \in \mathbb{N}$ with $i < k$ such that $f^i(x_0) = f^k(x_0)$. We define the set

$$I := \{i \in \mathbb{N} : f^i(x_0) \text{ is periodic}\}.$$

Let $m := \min(I)$. We have that $f^m(x_0) = f^j(x_0)$ for some $j \in ]m, +\infty[$. Suppose that $m > 0$. Since

$$f(f^{m-1}(x_0)) = f(f^{j-1}(x_0))$$

and $f$ is one-to-one, we have that $f^{m-1}(x_0) = f^{j-1}(x_0)$, in contradiction with the minimality of $m$. Hence $m = 0$, namely $x_0$ is periodic.

□

**Remark 2.2.** Since for a one-to-one map $f : \mathbb{P}^1(\mathbb{F}_q) \to \mathbb{P}^1(\mathbb{F}_q)$ every element $x_0 \in \mathbb{P}^1(\mathbb{F}_q)$ is periodic, the graph $G_q(f)$ is formed by a finite number of cycles, possibly of different lengths.

The lengths of the orbits of a map $f$ and its $m$-fold composition $f^m$ are related as described in the following lemma.

**Lemma 2.3.** Let $f$ be a map defined on $\mathbb{P}^1(\mathbb{F}_q)$ and $g := f^m$ for some $m \in \mathbb{N}^*$. If $x_0 \in \mathbb{P}^1(\mathbb{F}_q)$ is $f$-periodic and

$$l := |O(f, x_0)|,$$
then $x_0$ is $g$-periodic and
\[ |O(g, x_0)| = \frac{l}{\gcd(l, m)}. \]

**Proof.** If $g^h(x_0) = x_0$ for some $h \in \mathbb{N}^*$, then $f^{hm}(x_0) = x_0$. Therefore $l$ divides $hm$. The result follows because $\frac{l}{\gcd(l, m)}$ divides $h$. \hfill \Box

### 2.1. The maps $\vartheta_{a,b,k}$ and $\psi_{a,b,k}$

In this section we introduce some notations for the maps we investigate in this paper. First we recall the following results (see [5, Proposition 7.1.2] and [8, Theorem 1.68]).

**Proposition 2.4.** Let $\alpha \in \mathbb{F}_q^*$ and $n \in \mathbb{N}^*$. Then $x^n = \alpha$ has solutions if and only if $\alpha^{(q-1)/d} = 1$, where $d = \gcd(n, q-1)$. If there are solutions, then there are exactly $d$ solutions.

**Theorem 2.5.** Let $\mathbb{F}$ be a field. The element $b \in \mathbb{F}$ is a multiple root of $f \in \mathbb{F}[x]$ if and only if it is a root of both $f$ and $f'$.

Let $q := 2^n$ for some $n \in \mathbb{N}^*$. If $a \in \mathbb{F}_q^*$, $b \in \mathbb{F}_q$ and $k \in \mathbb{N}^*$ then we define the maps $\vartheta_{a,b,k}$ and $\psi_{a,b,k}$ on $\mathbb{P}^1(\mathbb{F}_q)$ as follows:

\[
\vartheta_{a,b,k}(x) := \begin{cases} 
  ax^{2^k} + b & \text{if } x \in \mathbb{F}_q, \\
  \infty & \text{if } x = \infty.
\end{cases}
\]

\[
\psi_{a,b,k}(x) := \begin{cases} 
  \infty & \text{if } ax^{2^k} + b = 0, \\
  0 & \text{if } x = \infty, \\
  \frac{1}{ax^{2^k} + b} & \text{otherwise}.
\end{cases}
\]

From Proposition 2.4 we get the following result.

**Lemma 2.6.** The maps $\vartheta_{a,b,k}$ and $\psi_{a,b,k}$ are one-to-one.

**Proof.** First we notice that $\vartheta_{a,b,k}(x) = \infty$ only if $x = \infty$. If $\vartheta_{a,b,k}(x_1) = \vartheta_{a,b,k}(x_2)$ for some $x_1, x_2 \in \mathbb{F}_q$ then $ax_1^{2^k} = ax_2^{2^k}$, namely $x_1^{2^k} = x_2^{2^k}$ because $a \neq 0$. Let $\alpha = x_1^{2^k} = x_2^{2^k}$. If $\alpha = 0$, then $x_1 = x_2 = 0$. If $\alpha \neq 0$, then $x_1 = x_2$ according to Proposition 2.4 since $\gcd(2^k, 2^n - 1) = 1$.

As regards the maps $\psi_{a,b,k}$, we have that $\psi_{a,b,k}(x) = \infty$ only if $x$ is a solution of the equation $ax^{2^k} + b = 0$. Since $\vartheta_{a,b,k}$ is one-to-one, this latter equation has only one solution. Moreover $\psi_{a,b,k}(x) = 0$ only for $x = \infty$. Finally, if $\frac{1}{ax_1^{2^k} + b} = \frac{1}{ax_2^{2^k} + b}$ then $\vartheta_{a,b,k}(x_1) = \vartheta_{a,b,k}(x_2).$ Hence $x_1 = x_2$. \hfill \Box
3. Dynamics of the map $x \mapsto ax^4 + b$

Let $q := 2^n$ for some $n \in \mathbb{N}^*$, $a \in \mathbb{F}_q^*$ and $b \in \mathbb{F}_q$. In the current section we investigate the map $\vartheta_{a,b,2}$, which we simply denote by $\vartheta$. The map $\vartheta$ is defined as follows over $\mathbb{P}^1(\mathbb{F}_q)$:

$$\vartheta(x) := \begin{cases} 
ax^4 + b & \text{if } x \in \mathbb{F}_q, \\
\infty & \text{if } x = \infty.
\end{cases}$$

The image of the map $\vartheta$ gives the $x$-component of the duplication map defined on a supersingular elliptic curve over a binary field (see for example [7, Chapter 6]). More precisely, consider the elliptic curve $E: y^2 + a_1 y = x^3 + a_2 x$ where $a_1, a_2 \in \mathbb{F}_q$. If $P := (x_0, y_0) \in E(\mathbb{F}_q)$, then $2P = (x_1, y_1)$, where

$$x_1 = \frac{x_0^4 + a_2^2}{a_1^2}.$$ 

Hence

$$\vartheta(x_0) = ax_0^4 + b = \frac{x_0^4 + a_2^2}{a_1^2},$$

with $a_1^2 := a^{-1}$ and $a_2^2 := a_1^2 b$.

We can describe the iterations of the map $\vartheta$ on $\mathbb{P}^1(\mathbb{F}_q)$ relying upon the group of rational points $E(\mathbb{F}_q)$ of $E$ over $\mathbb{F}_q$ or the group of rational points $E(\mathbb{F}_q^2)$ of $E$ over $\mathbb{F}_q^2$. In fact, for any $x_0 \in \mathbb{F}_q$ there exists some $y_0 \in \mathbb{F}_q^2$ such that $P := (x_0, y_0) \in E(\mathbb{F}_q^2)$. Hence $2^i P \in E(\mathbb{F}_q^2)$ for all $i \in \mathbb{N}^*$. Moreover, if $y_0 \in \mathbb{F}_q$ then $2^i P \in E(\mathbb{F}_q)$ for all $i \in \mathbb{N}^*$.

As recalled in [11, Remark 2.5], which indeed refers to [9], if $k \in \mathbb{N}^*$ and $E$ is an elliptic curve defined over $\mathbb{F}_{2^k}$, then there exist two positive integers $n_1, n_2$ such that

$$E(\mathbb{F}_{2^k}) \cong \mathbb{Z}/n_1 \mathbb{Z} \times \mathbb{Z}/n_2 \mathbb{Z}$$

with $n_1 \mid \gcd(n_2, 2^k - 1)$. Moreover, as recalled in [11, Section 4], the cardinality $|E(\mathbb{F}_{2^k})|$ is odd. Since the map $\vartheta$ is related to the duplication map over $E$, we are interested in studying the action of the pair of classes $([2], [2])$ on the elements belonging to $\mathbb{Z}/n_1 \mathbb{Z} \times \mathbb{Z}/n_2 \mathbb{Z}$.

3.1. Length of the cycles

Let $E(\mathbb{F}_{q^2})$ be isomorphic to

$$A := \mathbb{Z}/n_1 \mathbb{Z} \times \mathbb{Z}/n_2 \mathbb{Z}$$

for some $n_1, n_2 \in \mathbb{N}^*$. If $x_0 \in \mathbb{F}_q$, then $x_0$ is the $x$-coordinate of a point $P := ([a_1], [a_2])$ in $A$. Moreover $P$ and $-P$ are the only points whose $x$-coordinate is $x_0$. 

For $i \in \{1, 2\}$ we define
\[
d_i := \gcd(a_i, n_i);
m_i := \min\{k \in \mathbb{N}^* : 2^k a_i \approx a_i \mod n_i\}.
\]
Moreover we define
\[
m := \min\{k \in \mathbb{N}^* : 2^k P \approx P\};
l := \text{lcm}(m_1, m_2).
\]
In the next theorem we show what the length of the orbit $O(x_0)$ is.

**Theorem 3.1.** The following hold.

1. If $i \in \{1, 2\}$, then $m_i$ is the smallest of the positive integers $k$ such that $2^k \approx 1 \mod \frac{n_i}{d_i}$.
2. The length of $O(x_0)$ in $G_q(\vartheta)$ is $m$. Moreover we have that
\[
m = \begin{cases} l & \text{if } 2^l P \approx P, \\
2l & \text{otherwise}. \end{cases}
\]

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

1. We have that $2^k a_i \approx a_i \mod n_i$ for some $k \in \mathbb{N}^*$ if and only if $n_i$ divides $(2^k + 1)a_i$ or $(2^k - 1)a_i$. According to a well-known arithmetical lemma, this latter is equivalent to the fact that $\frac{n_i}{d_i}$ divides $(2^k + 1)$ or $(2^k - 1)$. Hence the claim for $m_i$ is proved.
2. We notice that $\vartheta^k(x_0) = x_0$ for some positive integer $k$ if and only if $2^k P \approx P$, namely if and only if
\[
([2^k a_1], [2^k a_2]) = ([a_1], [a_2]) \text{ or } ([2^k a_1], [2^k a_2]) = ([-a_1], [-a_2]).
\]

Therefore $\vartheta^m(x_0) = x_0$. Since $m$ must be a common multiple of $m_1$ and $m_2$, we have that $l := \text{lcm}(m_1, m_2)$ divides $m$. Moreover $2^l P \not\approx P$ only if $[2^l a_1] = [a_1]$ and $[2^l a_2] = [-a_2]$ or viceversa. In both cases we have that $2^{2l} P = P$.

\[ \square \]

**Remark 3.2.** We have proved that the length of $O(x_0)$ with $x_0 \in \mathbb{P}^1(\mathbb{F}_q)$ depends on $\gcd(a_1, n_1)$ and $\gcd(a_2, n_2)$, where $([a_1], [a_2])$ is a point in $E(\mathbb{F}_{q^2})$ whose $x$-coordinate is $x_0$. Therefore, the possible lengths of the cycles in $G_q(\vartheta)$ can be computed relying upon the pairs $(d_1, d_2)$, where $d_1$ and $d_2$ are (positive) divisors of $n_1$ and $n_2$ respectively and
\[
E(\mathbb{F}_{q^2}) \cong \mathbb{Z}/n_1 \mathbb{Z} \times \mathbb{Z}/n_2 \mathbb{Z}.
\]

If we focus on rational points of $E(\mathbb{F}_q)$, we can state a more precise result. With a little abuse of notation we suppose that $E(\mathbb{F}_q) \cong A$ where
\[
A := \mathbb{Z}/n_1 \mathbb{Z} \times \mathbb{Z}/n_2 \mathbb{Z}
\]
for some positive integers \(n_1\) and \(n_2\).

**Lemma 3.3.** The following hold.

1. If \(([a_1], [a_2]) \in A\), then \(\gcd(a_i, n_i) = \gcd(2a_i, n_i)\) for \(i \in \{1, 2\}\).
2. Let \(d_1\) and \(d_2\) be two positive integers such that 
   \[ d_1 \mid n_1 \quad \text{and} \quad d_2 \mid n_2. \]
   If \(m_1 := \frac{n_1}{d_1}\) and \(m_2 := \frac{n_2}{d_2}\), then there are \(\varphi(m_1) \cdot \varphi(m_2)\) points \(([a_1], [a_2])\) in \(A\) such that 
   \[ \gcd(a_1, n_1) = d_1 \quad \text{and} \quad \gcd(a_2, n_2) = d_2. \]

**Proof.** Let \(i \in \{1, 2\}\). We prove separately the statements.

1. The assertion follows from the fact that an integer \(m\) divides \(a_i\) and \(n_i\) if and only if \(m\) divides \(2a_i\) and \(n_i\) because \(n_i\) is odd.
2. Let \([a_i] \in \mathbb{Z}/n_i\mathbb{Z}\) with \(a_i \in [1, n_i]\). Then \(\gcd(a_i, n_i) = d_i\) if and only if 
   \(a_i = d_i k\) and \(n_i = d_i k'\) for some integers \(k, k'\) with \(\gcd(k, k') = 1\) and \(1 \leq k \leq \frac{n_i}{d_i}\). Since \(m_i = \frac{n_i}{d_i}\), this latter is equivalent to saying that 
   \(\gcd(k, m_i) = 1\) and \(k \in [1, m_i]\). Hence there are \(\varphi(m_i)\) classes \([a_i]\) in 
   \(\mathbb{Z}/n_i\mathbb{Z}\) such that \(\gcd(a_i, n_i) = d_i\).

\[ \square \]

**Example 3.4.** Let \(\mathbb{F}_q\) be the field with \(q := 2^5\) elements. We denote by \(g\) a generator of \(\mathbb{F}_q^*\). We construct the graph \(G_q(\vartheta)\), where \(\vartheta\) is defined on \(\mathbf{P}^1(\mathbb{F}_q)\) as follows:

\[
\vartheta(x) := \begin{cases} 
gx^4 + g^3 & \text{if } x \in \mathbb{F}_q, \\
\infty & \text{if } x = \infty.
\end{cases}
\]

The map \(\vartheta\) is related to the duplication map defined over the curve

\[ E : y^2 + g^{15} y = x^3 + gx. \]

The vertices of \(G_q(\vartheta)\) are labelled by the exponents of \(g^i\) for \(i \in [0, 30]\). The remaining two vertices are labelled by \(\infty\) and ‘0’ (the zero of \(\mathbb{F}_q\)).
Using Sage [10] we get that $E(\mathbb{F}_q) \cong \mathbb{Z}/41\mathbb{Z}$. Adopting the notations of the current section and Lemma 3.3 we have that $n_1 = 1$ and $n_2 = 41$. The set of (positive) divisors of $n_2$ is

$$D = \{1, 41\}.$$

Let $d_2 := 1$ and $m_2 := 41$. Then 10 is the smallest $k \in \mathbb{N}^*$ such that

$$2^k \approx 1 \mod 41.$$

Therefore there are $\varphi(m_2) = 40$ points in $E(\mathbb{F}_q)$ whose $x$-coordinates belong to cycles of length 10. Since exactly two points have the same $x$-coordinate, these 40 points form 2 cycles of length 10. We notice in passing that the two cycles are the orbits $O(g^0)$ and $O(g^2)$.

Let $d_2 := 41$ and $m_2 := 1$. This case corresponds to the element $\infty$, which forms a cycle of length 1.

Now we consider the group $E(\mathbb{F}_{q^2})$. We have that $E(\mathbb{F}_{q^2}) \cong \mathbb{Z}/1025\mathbb{Z}$. Since $1025 = 5^2 \cdot 41$, the set of divisors of 1025 is

$$D = \{1, 5, 25, 41, 205, 1025\}.$$

We notice in particular that for $d_2 := 205$ we have $m_2 := \frac{1025}{205} = 5$. Then 2 is the smallest $k \in \mathbb{N}^*$ such that $2^k \approx 1 \mod 5$. Hence there are two rational points in $E(\mathbb{F}_{q^2})$ whose $x$-coordinates form the cycle of length 2 in $G_q(\vartheta)$. We get the remaining cycle of length 10 setting $d_2 := 25$ and correspondingly $m_2 := \frac{1025}{25} = 41$. 

4. Dynamics of the maps $ax^{2^k} + b$

Let $n \in \mathbb{N}^*$. In this section we study the maps $\vartheta_{a,b,k}$, where $a, b \in \mathbb{F}_{2^n}$ with $a \neq 0$ and $k \in \mathbb{N}$, defined on $\mathbb{P}^1(\mathbb{F}_{2^n})$ as in Sect. 2.1. We adopt the shorter notation $\vartheta_{a,b}$ for the map $\vartheta_{a,b,2}$. In Lemmas 4.1 and 4.2 we show how the dynamics of the map $\vartheta_{a,b,k}$ can be related to the dynamics of the map $\vartheta_{c,d}$ for suitable coefficients $c$ and $d$ in $\mathbb{F}_{2^n}$.

For any $q \in \mathbb{N}^*$ and any $t \in \mathbb{N}$ we define

$$s_t^q := \begin{cases} 0 & \text{if } t = 0, \\ \sum_{i=0}^{t-1} q^i & \text{if } t > 0. \end{cases}$$

**Lemma 4.1.** Let $q := 2^k$ for some $k \in \mathbb{N}$. Let $m \in \mathbb{N}^*$ and $a, b \in \mathbb{F}_{2^n}$ with $a \neq 0$. Let $\tau(x) := ax^q + b$ for any $x \in \mathbb{F}_{2^n}$, then

$$\tau^m(x) = a^{s_m}x^{q^m} + b_m,$$

where $b_m := \sum_{i=0}^{m-1} a^{s_i}b^i$ with $s_t := s_t^q$ for any $t \in [0, m - 1]$.

**Proof.** We prove the claim by induction on $m \in \mathbb{N}^*$.

If $m = 1$, then

$$\tau^1(x) = \tau(x) = ax^q + b = a^{s_1}x^{q^1} + b_1.$$  

Now we prove the inductive step. If $m \geq 1$, then

$$\tau^{m+1}(x) = \tau(\tau^m(x)) = a(a^{s_m}x^{q^m} + b_m)^q + b = a^{1+qs_m}x^{q^{m+1}} + ab_m^q + b.$$  

We notice that

$$1 + qs_m = 1 + \sum_{i=0}^{m-1} q^{i+1} = 1 + \sum_{i=1}^{m} q^i = \sum_{i=0}^{m} q^i = s_{m+1},$$

while

$$ab_m^q + b = a \sum_{t=0}^{m-1} a^{qs_t}b^{q^{t+1}} + b = \sum_{t=0}^{m-1} a^{qs_t+1}b^{q^{t+1}} + b = \sum_{t=0}^{m-1} a^{s_{t+1}}b^{q^{t+1}} + b = b_{m+1}.$$  

Therefore $\tau^{m+1}(x) = a^{s_{m+1}}x^{q^{m+1}} + b_{m+1}$.

**Lemma 4.2.** Let $k$ be an integer with $k \geq 2$ and $a, b \in \mathbb{F}_{2^n}$ with $a \neq 0$. Then there exist some $c, d \in \mathbb{F}_{2^n}$ such that for any $x \in \mathbb{P}^1(\mathbb{F}_{2^n})$ we have that

$$\vartheta_{c,d}^k(x) = \vartheta_{a,b,k}(x) \quad \text{if } k \text{ is even},$$  

$$\vartheta_{c,d}^k(x) = \vartheta_{a,b,k}^2(x) \quad \text{if } k \text{ is odd}.$$
Proof. If \( c, d \in \mathbb{F}_{2^n} \) and \( j \in \mathbb{N}^* \), then from Lemma 4.1 we get that
\[
\vartheta_{c,d}^j(x) = c^{s_j} x^{4^j} + d_j
\]
with \( s_j := s_j^4 \) and \( d_j := \sum_{i=0}^{j-1} c^{s_i} d^{4^i} \).

For any \( k \in \mathbb{N}^* \) we have that
\[
\vartheta_{a,b,k}(x) = a x^{2^k} + b,
\]
\[
\vartheta_{a,b,k}^2(x) = a^{2^k+1} x^{2^{2k}} + ab^{2^k} + b.
\]
If \( k \) is even, then we set \( j := \frac{k}{2} \) and we find \( c, d \in \mathbb{F}_{2^n} \) solving the equations
\[
c^{s_j} = a \quad \text{and} \quad \sum_{i=0}^{j-1} c^{s_i} d^{4^i} = b.
\]
If \( k \) is odd, then we set \( j := k \) and we find \( c, d \in \mathbb{F}_{2^n} \) solving the equations
\[
c^{s_j} = a^{2^k+1} \quad \text{and} \quad \sum_{i=0}^{j-1} c^{s_i} d^{4^i} = ab^{2^k} + b.
\]
\[\square\]

Remark 4.3. One of the hypotheses of Lemma 4.2 is that \( k \geq 2 \). Indeed, if we consider \( n \geq 2 \), we have that
\[
\vartheta_{a,b,0}(x) = \vartheta_{a,b,n}(x),
\]
\[
\vartheta_{a,b,1}(x) = \vartheta_{a,b,n+1}(x),
\]
because \( x^{2^n} = x \) and \( x^{2^{n+1}} = (x^{2^n})^2 = x^2 \).

Under the same hypotheses (and using the same notations) of Lemma 4.2 we define the map \( \psi \) on \( \mathbb{P}^1(\mathbb{F}_{2^n}) \) as follows:
\[
\psi(x) := \begin{cases} 
\vartheta_{a,b,k}(x) & \text{if } k \text{ is even}, \\
\vartheta_{a,b,k}^2(x) & \text{if } k \text{ is odd}.
\end{cases}
\]
Moreover we define the integer
\[
m := \begin{cases} 
\frac{k}{2} & \text{if } k \text{ is even}, \\
k & \text{if } k \text{ is odd}.
\end{cases}
\]
The following holds.

Lemma 4.4. Let \( x_0 \in \mathbb{P}^1(\mathbb{F}_{2^n}) \) and
\[
l_1 := |O(\vartheta_{c,d}, x_0)|,
\]
\[
l_2 := |O(\vartheta_{a,b,k}, x_0)|,
\]
\[
l_3 := |O(\psi, x_0)|.
\]
Then $l_3 = \frac{l_1}{\gcd(l_1, m)}$. Moreover $l_2 = l_3$ if $k$ is even, while $l_2 \in \{l_3, 2l_3\}$ if $k$ is odd.

**Proof.** From Lemma 2.3 we get immediately that $l_3 = \frac{l_1}{\gcd(l_1, m)}$ because $\psi = \vartheta_{c,d}^m$. If $k$ is even, then $l_2 = l_3$ because $\vartheta_{a,b,k} = \psi$. If $k$ is odd, then from Lemma 2.3 we get that

$$l_2 = l_3 \cdot \gcd(l_2, 2).$$

Hence $l_2 = l_3$ if $l_2$ is odd, while $l_2 = 2l_3$ if $l_2$ is even. \(\square\)

**Example 4.5.** Let $g$ be a generator of $\mathbb{F}_q^*$, where $q := 2^5$. In this example we consider the map $\sigma := \vartheta_{g^7, g^3, 3}$, which is defined for all $x \in \mathbb{F}_q$ as

$$\sigma(x) = g^7x^8 + g^3.$$

Since $k = 3$, we define $\psi(x) := \sigma^2(x)$ for all $x \in \mathbb{P}^1(\mathbb{F}_q)$. We want to find $c, d \in \mathbb{F}_q$ such that

$$\vartheta_{c,d}^3(x) = \psi(x)$$

for all $x \in \mathbb{P}^1(\mathbb{F}_q)$. More explicitly, we have to solve the equations

$$c^{3^3} = (g^7)^9,$$

$$\sum_{i=0}^{2} c^{s_i} d^{4^i} = g^7(g^3)^8 + g^3,$$

namely

$$c^{21} = g^{63},$$

$$d + cd^4 + c^5d^{16} = g^{31} + g^3.$$

The first equation is satisfied for $c = g^3$, while one solution of the second equation is $d = g^{15}$. We define the map

$$\vartheta(x) := \vartheta_{c,d}(x) = \begin{cases} g^3x^4 + g^{15} & \text{if } x \in \mathbb{F}_q, \\ \infty & \text{if } x = \infty. \end{cases}$$

The map $\vartheta$ is related to the duplication map defined over the curve

$$E : y^2 + g^{14}y = x^3 + g^6x.$$

We consider the group

$$E(\mathbb{F}_q) \cong \mathbb{Z}/33\mathbb{Z}.$$

Using the notations of Sect. 3.1 we have that $n_2 = 33$. The set of positive divisors of 33 is

$$D := \{1, 3, 11, 33\}.$$
For each $d \in D$ we can find the smallest $k \in \mathbb{N}^*$ such that $2^k \equiv 1 \mod d$. Such a $k$ corresponds to a possible length of an orbit in $G_q(\vartheta)$. We collect the values of $k$ in the set

$$K := \{1, 5\}.$$ 

According to the notations of Lemma 4.4 we have that $l_1 \in K$ and $l_3 = l_1$. Since $k$ is odd, the possible length of an orbit $O(\sigma, x_0)$, where $x_0$ is the $x$-coordinate of a point in $E(\mathbb{F}_q)$, is 1, 2, 5 or 10.

We can extend our investigation to the group

$$E(\mathbb{F}_{q^2}) \cong \mathbb{Z}/33\mathbb{Z} \times \mathbb{Z}/33\mathbb{Z}.$$ 

We have $n_1 = n_2 = 33$. Moreover, the pairs of divisors of $(n_1, n_2)$ are $(d_1, d_2)$ with $d_1, d_2 \in D$. For any such a pair we can compute the smallest $k \in \mathbb{N}^*$ such that

$$2^k \equiv 1 \mod d_1 \quad \text{and} \quad 2^k \equiv 1 \mod d_2$$

$$\text{or}$$

$$2^k \equiv -1 \mod d_1 \quad \text{and} \quad 2^k \equiv -1 \mod d_2$$

The values of $k$ we get are the elements of

$$K := \{1, 2, 5, 10\}.$$ 

Correspondingly, the possible length of an orbit $O(\sigma, x_0)$ with $x_0 \in \mathbb{P}^1(\mathbb{F}_q)$ is 1, 2, 4, 5, 10 or 20.

Below we represent the graph $G_q(\sigma)$. 
5. Dynamics of the maps $\left( ax^{2^k} + b \right)^{-1}$

In this section we study the dynamics of the maps $\left( ax^{2^k} + b \right)^{-1}$, namely the maps $\psi_{a,b,k}$ defined in Sect. 2.1, where $a, b \in \mathbb{F}_{2^n}$ with $a \neq 0$ and $k \in \mathbb{N}^*$.

We can find an invertible map $\tau$ defined on $\mathbb{P}^1(\overline{\mathbb{F}_{2^n}})$ such that $\psi_{a,b,k}$ is conjugated to $\vartheta_{c,0,k}$ through $\tau$ for some $c \in \mathbb{F}_{2^n}$, namely

$$(\tau^{-1} \circ \psi_{a,b,k} \circ \tau)(x) = \vartheta_{c,0,k}(x)$$

or equivalently

$$(\psi_{a,b,k} \circ \tau)(x) = (\tau \circ \vartheta_{c,0,k})(x)$$

for all $x \in \mathbb{P}^1(\overline{\mathbb{F}_{2^n}})$. 

We construct the map $\tau$ as follows, for some $c_1, c_2, c_3 \in \mathbb{F}_{2^n}$ with $c_3+c_1c_2 \neq 0$:

$$
\tau(x) := \begin{cases} 
\frac{1}{c_2} & \text{if } x = \infty, \\
\infty & \text{if } c_2x + c_3 = 0, \\
0 & \text{if } x = c_1, \\
x + c_1 & \text{if } c_2x + c_3 \neq 0.
\end{cases}
$$

Now we find the values of $c_1, c_2, c_3$ and $c$. Let $x \in \mathbb{F}_{2^n}$ be an element such that $x \neq c_1$ and $c_2x + c_3 \neq 0$. If $q := 2^k$, then

$$(\psi_{a,b,k} \circ \tau)(x) = (\tau \circ \vartheta_{c,0,k})(x)$$

if and only if

$$
\frac{1}{a \left(\frac{x + c_1}{c_2x + c_3}\right)^q} + b = \frac{cx^q + c_1}{c_2cx^q + c_3}.
$$

Unravelling the left-hand-side of this latter equation we get

$$
\frac{c_2^q x^q + c_3^q}{(a + bc_2^q)x^q + (ac_1^q + bc_3^q)} = \frac{cx^q + c_1}{c_2cx^q + c_3}.
$$

The two rational functions above are equal if we find $c, c_1, c_2, c_3$ in $\mathbb{F}_{2^n}$ such that

$$
\begin{cases} 
c = c_2^q \\
c_1 = c_3^q \\
c_2c = a + bc_2^q \\
c_3 = ac_1^q + bc_3^q
\end{cases} \quad (5.1)
$$

If we plug $c := c_2^q$ in $c_2c = a + bc_2^q$ we get the equation

$$
c_2^{q+1} + bc_2^q + a = 0
$$

which is satisfied for some $c_2 \in \mathbb{F}_{2^n}$ with $c_2 \neq 0$. We notice in passing that $c_3 + c_1c_2 = 0$ if and only if $c_3 + c_2c_3^q = 0$, namely if and only if $c_3$ is a root of the polynomial

$$
u(x) := x + c_2x^q \in \mathbb{F}_{2^n}[x].
$$

If we plug $c_1 := c_3^q$ in $c_3 = ac_1^q + bc_3^q$ we get the equation

$$
a c_3^q + bc_3^q + c_3 = 0,
$$

which is satisfied if and only if $c_3$ is a root of the polynomial

$$
v(x) := ax^q^2 + bx^q + x \in \mathbb{F}_{2^n}[x].
$$

Since $u(x)$ and $v(x)$ are $q$-polynomials and $u'(x) = v'(x) \neq 0$, they have respectively $q$ and $q^2$ distinct roots in $\mathbb{F}_{2^n}$ (see [8, Theorem 3.50]). Therefore

$$
c_3 + c_1c_2 \neq 0
$$
for some $c_3 \in \mathbb{F}_{2^m}$. We also notice that, if the equations (5.1) are satisfied, then $c_2, c_3 \neq 0$.

We should also check that
\[
\psi_{a,b,k}(\tau(x)) = \tau(\vartheta_{c,0,k}(x))
\]
for $x \in \{c_1, c_2 c_3\}$. We discuss separately some cases.

- If $b \neq 0$ and $x = c_1$, then
  \[
  \psi_{a,b,k}(\tau(x)) = \psi_{a,b,k}(0) = \frac{1}{b},
  \]
  \[
  \tau(\vartheta_{c,0,k}(x)) = \tau(cc^q) = \frac{cc^q + c_1}{c_2cc^q + c_3} = \frac{c_2c_1 + c_3}{ac_1 + bc_2c_1 + ac_1 + bc_3} = \frac{c_2c_1 + c_3}{b(c_2c_1 + c_3)} = \frac{1}{b}.
  \]

- If $b = 0$ and $x = c_1$, then $c_2 = \frac{a}{c}, c_3 = ac^q$ and $c_2 c_3 = cc^q$. Therefore
  \[
  \psi_{a,b,k}(\tau(x)) = \psi_{a,b,k}(0) = \infty,
  \]
  \[
  \tau(\vartheta_{c,0,k}(x)) = \tau(cc^q) = \infty.
  \]

- If $x = \frac{c_1}{c_2}$, then
  \[
  \psi_{a,b,k}(\tau(x)) = \psi_{a,b,k}(\infty) = 0,
  \]
  \[
  \tau(\vartheta_{c,0,k}(x)) = \tau(c_1) = 0.
  \]

5.1. Fixed points

If $m \in \mathbb{N}^*$ and $c \in \mathbb{F}_{2^m}^*$, then the map $\vartheta := \vartheta_{c,0,k}$ has at least two fixed points in $\mathbb{P}^1(\mathbb{F}_{2^m})$ since
\[
\vartheta(0) = 0 \quad \text{and} \quad \vartheta(\infty) = \infty.
\]

Now we consider a map $\psi := \psi_{a,b,k}$, defined over $\mathbb{P}^1(\mathbb{F}_{2^m})$ and conjugated to $\vartheta$ through a suitable map $\tau$ with $c_1, c_2, c_3 \in \mathbb{F}_{2^m}$. We can compute the number of fixed points of $\psi$, or equivalently the number of cycles of length 1 in $G_{2^m}(\psi)$.

**Theorem 5.1.** Let $d := \gcd(2^k - 1, 2^m - 1)$.

1. The elements $\frac{c_1}{c_3}$ and $\frac{1}{c_2}$ are fixed points for the map $\psi$.
2. If $(c^{-1})^{\frac{2^m-1}{2^k-1}} \neq 1$, then $\psi$ has exactly two fixed points in $\mathbb{P}^1(\mathbb{F}_{2^m})$.
3. If $(c^{-1})^{\frac{2^m-1}{2^k-1}} = 1$, then $\psi$ has $d + 2$ fixed points in $\mathbb{P}^1(\mathbb{F}_{2^m})$.

**Proof.** We notice that the map $\tau$ establishes a one-to-one correspondence between the fixed points of $\psi$ and $\vartheta$. Now we prove separately the statements.

1. Since $\tau(0) = \frac{c_1}{c_3}$ and $\tau(\infty) = \frac{1}{c_2}$, we have that $\frac{c_1}{c_3}$ and $\frac{1}{c_2}$ are fixed points for $\psi_{a,b,k}$. Moreover $\frac{c_1}{c_3} \neq \frac{1}{c_2}$ because $c_1 c_2 + c_3 \neq 0$. 

2. If \( x \in \mathbb{F}_{2^m}^* \), then
\[
c x^{2^k} = x \iff x^{2^k - 1} = c^{-1}.
\]

According to Proposition 2.4, this latter equation has no solution in \( \mathbb{F}_{2^m} \).
Hence the only fixed points of \( \psi \) are \( \frac{c_1}{c_3} \) and \( \frac{1}{c_2} \).

3. Similarly to the previous item, in this case the equation \( x^{2^k - 1} = c^{-1} \) has \( d \) distinct solutions in \( \mathbb{F}_{2^m} \). Since 0 and \( \infty \) are fixed points of \( \vartheta \), we get the result. \( \square \)

**Example 5.2.** Let \( g \) be a generator of \( \mathbb{F}_{2^5}^* \). We consider the map \( \psi := \psi_{g,g^2,2} \), whose image for all but two points of \( \mathbb{P}^1(\mathbb{F}_{2^5}) \) is
\[
\psi(x) = \frac{1}{gx^4 + g^2}.
\]

Using GAP [2] we find the following values for \( c_1, c_2, c_3 \) and \( c \):
\[
c_1 := g; \quad c_2 := g^3; \quad c_3 := g^8; \quad c := g^{12}.
\]

We notice that \( m = 5 \) and \( k = 2 \) according to the notations of Theorem 5.1.
Since \( 2^k - 1 \) and \( 2^m - 1 \) are coprime and \((c^{-1})2^m-1 = 1\), the map \( \psi \) has 3 fixed points in \( \mathbb{P}^1(\mathbb{F}_{2^m}) \).

The graph \( G_{2^5}(\psi) \) is represented in the following figure.
The map \( \psi \) is conjugated to the map \( \vartheta := \vartheta_{c,0,2} \) defined over \( \mathbb{P}^1(\mathbb{F}_{25}) \). The map \( \vartheta \) describes the \( x \)-coordinate of the duplication map defined over the elliptic curve

\[
E : y^2 + g^{25}y = x^3.
\]

Since \( E(\mathbb{F}_{25}) \cong \mathbb{Z}/33\mathbb{Z} \) and the positive divisors of 33 are 1, 3, 11 and 33, the rational points of \( E(\mathbb{F}_{25}) \) give rise to cycles of lengths 1 and 5.

Moreover \( E(\mathbb{F}_{210}) \cong \mathbb{Z}/33\mathbb{Z} \times \mathbb{Z}/33\mathbb{Z} \). We have that \( n_1 = n_2 = 33 \). Consider the pairs of positive divisors \( (d_1, d_2) \) of \( (n_1, n_2) \). We still get that the possible cycle lengths of elements which are \( x \)-coordinates (in \( \mathbb{F}_{25} \)) of rational points in \( E(\mathbb{F}_{210}) \) are 1, 2, 5 and 10 (see Example 4.5).
Acknowledgements

The author is grateful to the anonymous Reviewer for reading the manuscript.

Publisher’s Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

References

[1] Bluher, A.W.: On $x^q+1 + ax + b$. Finite Fields Appl. 10(3), 285–305 (2004)
[2] The GAP Group, GAP - Groups, Algorithms and Programming, version 4.9.1, http://www.gap-system.org, (2018)
[3] Helleseth, T., Kholosha, A.: On the equation $x^{2^l+1} + x + a$ over $GF(2^k)$. Finite Fields Appl. 14(1), 159–176 (2008)
[4] Helleseth, T., Kholosha, A.: $x^{2^l+1} + x + a$ and related affine polynomials over $GF(2^k)$. Cryptogr. Commun. 2(1), 85–109 (2010)
[5] Ireland, K., Rosen, M.: A Classical Introduction to Modern Number Theory. Springer, New York (1990)
[6] Kim, K.H., Mesnager, S.: Solving $x^{2^k+1} + x + a = 0$ in $F_{2^n}$ with $\gcd(n, k) = 1$. Finite Fields Appl. 63, 1–15 (2020)
[7] Koblitz, N.: Algebraic Aspects of Cryptography. Springer, New York (1998)
[8] Lidl, R., Niederreiter, H.: Finite Fields. Cambridge University Press, Cambridge (1997)
[9] Silverman, J.H.: The Arithmetic of Elliptic Curves. Springer, New York (1986)
[10] The Sage Developers, SageMath, the Sage Mathematics Software System (Version 9.0), (2020) https://www.sagemath.org
[11] Wittmann, C.: Group structure of elliptic curves over finite fields. J. Number Theory 88, 335–344 (2001)

Simone Ugolini
Università di Trento
Trento
Italy
e-mail: s.ugolini@unitn.it

Received: September 15, 2020.
Accepted: January 5, 2021.