East-West J. of Mathematics: Vol. 21, No 1 (2019) pp. 70-84
https://doi.org/10.36853/ewjm0356

LINEAR MAPS GIVEN BY QUADRATIC POLYNOMIALS

Atsanon Wadsanthat[1], **Chatchawan Panraksa**[2], and **Wittawat Kositwattanarerk**[3]

[1] *Department of Mathematics, Faculty of Science,*
Mahidol University
Ratchathewi, Bangkok 10400
email: atsanon.wad@student.mahidol.ac.th

[2] *Mahidol University International College*
Mahidol University
Salaya, Nakhon Pathom 73170
email: chatchawan.pan@mahidol.edu

[3] *Department of Mathematics, Faculty of Science,*
Mahidol University
Ratchathewi, Bangkok 10400
email: wittawat.kos@mahidol.edu

Abstract

Quadratic maps of a specific type, defined on finite fields of characteristic two, are studied in terms of conjugacy maps, tree structures, and periodic points. In terms of conjugacy, it is found that conjugate field elements yield conjugate maps. Convenient bases for the sets of nilpotent and periodic points are determined separately. From these bases, various previous results are obtained with little reliance on matrix-based methods, allowing more efficient methods to be implemented as they arise.

1 Introduction

Some theoretical phenomena can be seen as dynamical systems defined over finite sets, possibly endowed with some algebraic structure. For example, the Lucas-Lehmer test for Mersenne primes can be viewed as the map $x \mapsto x^2 - 2$

Key words: conjugate dynamical systems, conjugate elements, nilpotent points, periodic points
(2010) Mathematics Subject Classification: 37C20, 37C25

over a finite ring of interest [9]. In this light, investigation of such systems leads to an insight of the phenomena in question.

Quadratic maps over fields of characteristic different from 2 are polynomials of low degree, yet they exhibit interesting dynamical properties, especially in terms of periodicity. Non-periodic trees and periodic cycles behave irregularly, as indicated in [14]. Over finite fields of characteristic greater than 2, only two maps, namely $x \mapsto x^2$ and $x \mapsto x^2 - 2$, are exceptions to such irregularities.

The squaring map $x \mapsto x^2$ on finite fields $\mathbb{F}_p$, for p prime, was studied in several works, such as [1], [12], [14], and [16]. It is shown in [1] that primitive roots form long orbits. More concretely, if $p = 2^\omega q + 1$ and g is a primitive root of p, then g is a source, and its orbit contains a long periodic cycle. The number of periodic cycles is given by [14], using a few number-theoretic conjectures, such as Artin's Conjecture on Primitive Roots.

The map $x \mapsto x^2 - 2$ was also studied as well. Small examples computed by Kravitz in [9] pointed out the map's regularity, at least for a few Mersenne primes. In that article, it is indicated that if $p = 2^k - 1$ is a Mersenne prime, then the periodic cycle lengths are divisors of k. A solid and general proof is given in [6], which shows that its cycles and trees are adequately uniform, and that the number of periodic and non-periodic points can be found systematically.

Description of periodic cycles remain an open question, except in some cases, such as linear transformations on arbitrary finite fields and quadratic maps. As proved in [7], the cycle structure of a linear transformation can be found from its minimal polynomial, and that the maximal cycle length is the order of that polynomial. For general quadratic maps, upper bounds are given in [13], which shows that cycle lengths cannot exceed 0.375 of the field size plus a small number.

Inspired by the mentioned studies, quadratic maps of the form $x \mapsto x^2 + bx$ defined over finite fields $\mathbb{F}_q$, for $q = 2^N$, are investigated using only elementary principles. This article shows that, compared to quadratic maps over other fields, the maps over finite fields of characteristic 2 behave uniformly and consistently, allowing their basic dynamical properties to be deduced. Furthermore, our methods will rely less on matrices and more on bases.

Besides from the introduction and conclusion, this article is divided into four sections, namely Preliminary Results, Tree Structure, Periodic Cycles, and Conjugate Maps, covering basic descriptions of maps of the form $x \mapsto x^2 + bx$ defined over finite fields of characteristic 2. Preliminary Results establishes a formula for iterations of such maps, as well as one for finding pre-images of any given point $x \in \mathbb{F}_q$. Tree Structure describes how non-periodic points can be found via an algebraic basis. Periodic Cycles uses the information on non-periodic points to deduce periodic points and cycle lengths, and a parametrization of cycles of period 3. Finally, Conjugate Maps shows how field automorphisms may act as conjugacies between two maps $x \mapsto x^2 + bx$ and $x \mapsto x^2 + cx$.

To begin with, some definitions are provided here. The symbol $\mathbb{F}_q$ always denotes a fixed finite field of size $q = 2^N$, where N is a positive integer.

2 Preliminary Results

A quadratic map is one defined by a quadratic polynomial $f(x) = ax^2 + bx + c$ on $\mathbb{F}_q$, where $a, b, c \in \mathbb{F}_q$ are constants. It can be shown via Hilbert's Theorem 90 that an arbitrary quadratic map $x \mapsto ax^2 + bx + c$ is conjugate to either $x \mapsto x^2 + bx$ or $x \mapsto x^2 + bx + \left(b^2 + 1\right)\zeta$, where $\zeta \in \mathbb{F}_q$ is a fixed element with absolute trace 1. In this study, maps of the first type are investigated.

In this section, a few simple formulas for the map $x \mapsto x^2 + bx$ are proved in Lemmas 2.1 and 2.2. They concern with iterations and the least periods of periodic points. Also, auxiliary formulas for solving $f_b(x) = y$, given $y \in \mathbb{F}_q$, are provided in Lemmas 2.3 and 2.4.

Henceforth, unless stated to the contrary, some notations are fixed as follows. N and q denote a fixed positive integer and the number 2^N, respectively. Also, for each $b \in \mathbb{F}_q$, $f_b : \mathbb{F}_q \to \mathbb{F}_q$ is the function given by $f_b(x) = x^2 + bx$ for each $x \in \mathbb{F}_q$. For any positive integer n, f_b^n refers to the n-th iteration of f, i.e., the composition of f_b with itself n times. In addition, f^0 is taken to be the identity map on $\mathbb{F}_q$.

The first lemma asserts that f_b is a linear map, and it relates the iterations of any two points $x, y \in \mathbb{F}_q$ and the iteration of their sum. The proof is a routine argument by induction on the number of iterations, so it will be skipped. The second one is a special case, where only periodic points are considered.

Lemma 2.1. *Fix a $b \in \mathbb{F}_q$. Then for each $n \in \mathbb{N}$ and $x, y \in \mathbb{F}_q$,*

$$f_b^n(x + y) = f_b^n(x) + f_b^n(y). \tag{2.1}$$

Lemma 2.2. *Fix a $b \in \mathbb{F}_q$. If $x, y \in \mathbb{F}_q$ are periodic points of f_b and $x \neq y$, so is $x + y$, with a period equal to the least common multiple of x and y.*

Proof. Only the second statement needs to be proved, for the first immediately follows. Let $x, y \in \mathbb{F}_q$ be periodic points of f_b, and call m and n the least period of x and y, respectively. Set l to be the least common multiple of m and n. By periodicity of x and y, $f_b^m(x) = x$ and $f_b^n(y) = y$.

Since l is a common multiple of m and n, it follows that $f_b^l(x) = x$ and $f_b^l(y) = y$. Lemma 2.1 implies

$$f_b^l(x + y) = x + y.$$

Thus, $x + y$ is also a periodic point, with period l. □

Lemma 2.2 states that the set of periodic points is closed under addition. A consequence of this observation is that it forms a group and, by Lagrange's Theorem, the number of periodic points must be a power of 2. A slightly more insightful proof is provided later.

Given $y \in \mathbb{F}_q$, the existence of solutions of the equation $f_b\left(x\right) = y$ depends on the *trace* of a related element of the field. The definition of the trace to be used is borrowed from Lidl and Niederreiter [11], but only a special case is needed here. For a fixed $\alpha \in F = \mathbb{F}_q$, its *trace* (or *absolute trace*) is the sum of all its Galois conjugates; that is,

$$\mathrm{Tr}\left(\alpha\right) = \alpha + \alpha^2 + \alpha^4 + \ldots + \alpha^{2^{N-1}}. \tag{2.2}$$

As $\mathbb{F}_q$ has characteristic 2, the trace can assume only two values, namely 0 and 1.

Later sections require solving equations of the form $f_b\left(x\right) = y$ for x, given $y \in \mathbb{F}_q$. If $b = 0$, a unique solution always exists. If $b = 1$, the next lemma furnishes a sufficient condition and an explicit formula for x.

Lemma 2.3. *[2] Let $\delta \in \mathbb{F}_q$, and $Tr(\delta) = 0$. Then the equation $x^2 + x = \delta$ has the explicit root*

$$x = 1 + \sum_{j=1}^{N-1} \delta^{2^j} \left(\sum_{k=0}^{j-1} u^{2^k} \right), \tag{2.3}$$

where $u \in \mathbb{F}_q$ and $Tr(u) = 1$. The other root is $x + 1$.

If b is neither 0 nor 1, then a change of variables can be done so that Lemma 2.3 is applicable. Given a fixed $\zeta \in \mathbb{F}_q$, the equation $t^2 + bt = \zeta$ can be solved for t by setting $t = bx$, yielding

$$\begin{aligned} b^2x^2 + b^2x &= \zeta \\ x^2 + x &= \frac{\zeta}{b^{-2}}. \end{aligned}$$

The last equation can be solved for x, and hence t, using Lemma 2.3 if its hypothesis is fulfilled; i.e., the trace of ζb^{-2} is 0.

The condition $\mathrm{Tr}\left(\delta\right) = 0$ is not only sufficient, but also necessary, as the next lemma indicates. Again, only the case where $K = \mathbb{F}_2$ is of particular interest.

Lemma 2.4. *[11] Let F be a finite extension of $K = \mathbb{F}_q$. Then for $\alpha \in F$ we have $Tr_{F/K}\left(\delta\right) = 0$ if and only if $\delta = \beta^q - \beta$ for some $\beta \in F$.*

3 Main Results

3.1 Tree Structure

Since f_b is a linear transformation, Fitting's lemma indicates the simplest structure for the set of non-periodic points of f_b. It is composed of trees, all of which are isomorphic in the graph-theoretic sense. When $\mathbb{F}_q$ is viewed as a vector space, as required by that lemma, the set of nilpotent points of f_b is known to be a subspace. A basis for that subspace can be constructed in a natural way without much need for a preexisting one.

Recall that Fitting's lemma states that if $f : M \to M$ is a module endomorphism, and M is both Artinian and Noetherian, then it can be decomposed into a certain direct sum. Its formal statement is stated here so that it can be used later.

Following Lang [10], the submodules Im u^∞ and Ker u^∞ are defined by stationarity of the chains

$$\text{Ker } u \subset \text{Ker } u^2 \subset \text{Ker } u^3 \subset \ldots$$

and

$$\text{Im } u \supset \text{Im } u^2 \supset \text{Im } u^3 \supset \ldots,$$

respectively. There exists a sufficiently large n such that Im $u^n =$ Im u^{n+1} and Ker $u^n =$ Ker u^{n+1}. Define Im u^∞ (respectively Ker u^∞) to be Im u^n (respectively Ker u^n).

Lemma 3.1 (Fitting's Lemma). *[10] Assume that the module M is Noetherian and Artinian. Let u be an endomorphism in M. Then M has a direct sum decomposition*

$$M = Im\ u^\infty \oplus Ker\ u^\infty. \tag{3.1}$$

Furthermore, the restriction of u to Im u^∞ is an automorphism, and the restriction of u to Ker u^∞ is nilpotent; i.e., there exists an n such that $u^n(x) = 0$ for all $x \in$ Ker u^∞.

The finite field $\mathbb{F}_q$ can be viewed as a vector space over the field $\mathbb{F}_2$ of dimension N, and hence a module. The fact that it is Noetherian and Artinian should be obvious; it is a finite set. Lemma 2.1 shows that $f_b : \mathbb{F}_q \to \mathbb{F}_q$ is indeed a module endomorphism, so Fitting's lemma can be applied, yielding the following observation, which a majority of results are based on.

Theorem 3.2. *Let $b \in \mathbb{F}_q$ be fixed. Then there exist subspaces K and P of $\mathbb{F}_q$ such that*

$$\mathbb{F}_q = K \oplus P. \tag{3.2}$$

The subspaces K and P are the sets of nilpotent and periodic points, respectively. In other words,

$$K = \{x \in \mathbb{F}_q \mid f_b^n(x) = 0 \text{ for some } n\},$$
$$P = \{x \in \mathbb{F}_q \mid x \text{ is a periodic point of } f_b\}.$$

Proof. By applying Fitting's lemma to f_b, $\mathbb{F}_q$ can be written as a direct sum

$$\mathbb{F}_q = \text{Ker } f_b^{\infty} \oplus \text{Im } f_b^{\infty}.$$

Set $K = \text{Ker } f_b^{\infty}$ and $P = \text{Im } f_b^{\infty}$. By definition of K, there exists an n such that $f_b^n(x) = 0$ for all $x \in K$.

According to Fitting's lemma, the restriction of f_b to P is an automorphism, and hence a bijective map. Pick any $x \in P$ and consider the orbit of x, namely

$$\mathcal{O}(x) = \left\{x, f_b(x), f_b^2(x), \ldots\right\}.$$

By the pigeonhole principle, the list must repeat after some m iterations. If $f_b^m(x) = f_b^i(x)$ for some i between 0 and m, then, by taking inverse of f_b for i times, $x = f_b^{m-i}(x)$. That is, x is a periodic point of f_b. Conversely, if x is periodic, then for some positive integer m, $x = f_b^n(x) = f_b^n\left(f_b^{m-n}(x)\right)$. It follows that $x \in P$. □

For each periodic point p of f_b, define V_p to be the set of points $x \in \mathbb{F}_q$ such that $f_b^n(x) = p$ for some n, and that no prior iteration of x is periodic, that is, $f_b^k(x)$ is not periodic for any $k = 0, 1, 2, \ldots, n-1$. The next lemma establishes a bijection between V_0 and V_p for any periodic point p, and that bijection preserves successive iterations.

Before proceeding, notice $f_b(0) = 0^2 + b(0) = 0$, so 0 is a fixed, hence periodic, point of f_b. Also note that $f_b(b) = b^2 + b(b) = 0$, so V_0 is well-defined and nonempty unless $b = 0$. The following observation is an immediate consequence of Theorem 3.2 and the definition of V_0.

Corollary 3.3. *Suppose that $b \in \mathbb{F}_q \setminus \{0\}$. Let K be as in Theorem 3.2. Then $K = V_0 \cup \{0\}$.*

Lemma 3.4. *Suppose that $b \neq 0$. Let p be any periodic point, and V_p be defined as above. Then there exists a map $\phi : V_p \to V_0$ such that*

1. *ϕ is bijective;*
2. *if $x, y \in V_0$ such that $y = f_b(x)$, then $\phi(y) = f_b(\phi(x))$.*

Proof. Let p be any periodic point of f_b, and consider the set V_0. From Theorem 3.2,

$$\mathbb{F}_q = K \oplus P, \tag{3.3}$$

where $K = V_0 \cup \{0\}$ by Corollary 3.3, and P is the set of periodic points of f_b.

To construct ϕ, let $x \in \mathbb{F}_q$ be arbitrary. Then x can be expressed as a unique sum

$$x = \dot{x} + \tilde{x},$$

where $\dot{x} \in K$ and $\tilde{x} \in P$. Define $\phi : V_p \to V_0$ by

$$\phi(x) = \dot{x}.$$

Due to the uniqueness of the sum, the map is well-defined and injective.

To see that ϕ is surjective, let $y \in V_0$ be arbitrary. By construction, there exists n_3 such that $f_b^{n_3}(y) = 0$ and $f_b^l(y)$ is non-periodic for $l = 0, 1, 2, \ldots, n_3 - 1$. Since p is periodic, there exists a periodic point $\tilde{p}$ such that $f_b^{n_3}(\tilde{p}) = p$. Choose $x_0 = y + \tilde{p}$. It can be seen that $y \in \ker f_b^n$ and $\tilde{p} \in \operatorname{im} f_b^n$, so there is only one such x_0. It follows that $\phi(x_0) = y$.

It remains to show that the chosen x_0 is indeed in V_p. Note that for each $k \in \{0, 1, 2, \ldots, n_3 - 1\}$,

$$f_b^k(x_0) = f_b^k(y) + f_b^k(\tilde{p}).$$

For these values of k, it is impossible for $f_b^k(y)$ to be zero, and consequently $f_b^k(x_0)$ cannot be periodic. Also consider

$$f_b^{n_3}(x_0) = f_b^{n_3}(y) + f_b^{n_3}(\tilde{p}) = f_b^{n_3}(\tilde{p}) = p.$$

By construction, $x_0 \in V_p$. It follows that the map ϕ is surjective, and hence bijective.

Finally, to see that ϕ preserves successive iterations, take any s, t of V_p and suppose that $t = f_b(s)$. We need to show that $\phi(t) = f_b(\phi(s))$. Write $s = \dot{s} + \tilde{s}$ and $t = \dot{t} + \tilde{t}$ for some uniquely determined $\dot{s}, \dot{t} \in K$ and $\tilde{s}, \tilde{t} \in P$. Then

$$\dot{t} + \tilde{t} = f_b(\dot{s}) + f_b(\tilde{s}).$$

Since $\dot{s} \in K$, $f_b(\dot{s}) \in K$ as well. Similarly, $\tilde{s} \in P$ implies $f_b(\tilde{s}) \in P$. By uniqueness of the sum, $\dot{t} = f_b(\dot{s})$. By construction, $\phi(t) = \dot{t}$. It follows that

$$\phi(t) = \dot{t} = f_b(\phi(s)).$$

Therefore, the second assertion is proved, and the proof is complete. □

From Lemma 3.4, the problem of studying V_p for each p is reduced to determining V_0. It is somewhat easier to study the related set K as the latter is a vector subspace. It must possess a basis if $b \notin \{0, 1\}$. A natural basis for K is built in the next lemma. In it, a *source* is a point $x \in \mathbb{F}_q$ without a pre-image under f_b.

Lemma 3.5. *Suppose that $b \in \mathbb{F}_q \setminus \{0, 1\}$. Let K be as in Theorem 3.2. Then*

$$B_K = \left\{x_0, f_b(x_0), f_b^2(x_0), \ldots, f_b^{h-1}(x_0)\right\}$$

forms a basis of K, where x_0 is a source, and h is the least positive integer such that $f_b^h(x_0) = 0$.

Proof. Suppose that $b \in \mathbb{F}_q \setminus \{0, 1\}$. Consider the map f_b and let K be as in the theorem. Let $b_1 = b$. For each $i = 2, 3, 4, \ldots$, if b_{i-1} has at least one pre-image under f_b, let that be b_i. So, $f_b(b_i) = b_{i-1}$. Note that the process must terminate after finitely many steps due to finiteness of K. Choose x_0 to be the last b_i found from the process. The fact that x_0 is a source follows by design.

Suppose that h is the least positive integer satisfying $f_b^h(x_0) = 0$. Let

$$B_K = \left\{x_0, f_b(x_0), f_b^2(x_0), \ldots, f_b^{h-1}(x_0)\right\}.$$

The goal is to show that B_K is linearly independent, and that its span is the whole K. Suppose that

$$\alpha_0 x_0 + \alpha_1 f_b(x_0) + \alpha_2 f_b^2(x_0) + \ldots + \alpha_{h-1} f_b^{h-1}(x_0) = 0$$

for some $\alpha_0, \alpha_1, \alpha_2, \ldots, \alpha_{h-1}$ in $\mathbb{F}_2$. Taking f_b^{h-i}, $i = 1, 2, 3, \ldots, h-1$ on both sides, we successively obtain $\alpha_0 f_b^{h-i}(x_0) = 0$ for $i = 1, 2, 3, \ldots, h-1$. Since $f_b^{h-1}(x_0) = b \neq 0$, it follows that $\alpha_i = 0$. Hence, B_K is a linearly independent set.

To show that B_K spans K, suppose that there exists a $y \in K$ not in the span of B_K. Since $y \in K$, $f_b^n(y) = 0$ for some n. Since 0 is in the span, there must be a positive integer n' such that $z = f_b^{n'}(y) \in \text{Span } B_K$ but $z' = f_b^{n'-1}(y) \notin \text{Span } B_K$. Now, $z \in \text{Span } B_K$ implies

$$z = \beta_0 x_0 + \beta_1 f_b(x_0) + \beta_2 f_b^2(x_0) + \ldots + \beta_{h-1} f_b^{h-1}(x_0).$$

Substituting $z = f_b^{n'}(y)$ yields,

$$f_b^{n'}(y) = \beta_0 x_0 + \beta_1 f_b(x_0) + \ldots + \beta_{h-1} f_b^{h-1}(x_0).$$

It follows that $\beta_{n'} = 1$ and $\beta_i = 0$ for all $i < n'$ from linear independence. There are two cases to consider, namely when $n' = 0$ and $n' > 0$. It will be shown that neither case is possible.

Suppose that $n' > 0$. Then $\beta_0 = 0$. Either

$$z' = \beta_1 x_0 + \beta_2 f_b(x_0) + \ldots + \beta_{h-1} f_b^{h-2}(x_0)$$

or

$$z' = \beta_1 x_0 + \beta_2 f_b(x_0) + \ldots + \beta_{h-1} f_b^{h-2}(x_0) + b$$

must hold. Since $b = f_b^{h-1}(x_0)$, either case means $z' \in \text{Span } B_K$, contradicting the choice of z'.

On the other hand, suppose that $n' = 0$. Then

$$y = \beta_0 x_0 + \beta_1 f_b(x_0) + \ldots + \beta_{h-1} f_b^{h-1}(x_0).$$

Clearly, $y \in \text{Span } B_K$, contradicting the choice of y.

Therefore, every $y \in K$ can be written as a linear combination of elements in B_K, and B_K is a basis of K. □

From the lemma and its proof, one can construct a basis for K by finding successive pre-images of 0 under f_b until a source is reached. It is reminded that pre-images of any given $x \in K$ are exactly the solutions of

$$t^2 + bt = x,$$

the solution of which is given by

$$t = b + b \sum_{j=1}^{N-1} x^{2^j} \left(\sum_{k=0}^{j-1} u^{2^k} \right),$$

where $u \in \mathbb{F}_q$ is a fixed element with trace 1.

Since K is a vector subspace of $\mathbb{F}_q$, and its basis has exactly h elements, and coefficients in any linear combination of elements from that basis has only two choices, it is evident that there are exactly 2^h nilpotent points.

An inspection of the basis so constructed reveals that V_0 has a simple shape; it is a perfect binary tree. This stems from the fact that every nilpotent point of f_b has precisely two pre-images if one exists.

Proposition 3.6. *Suppose that $b \in \mathbb{F}_q \setminus \{0,1\}$. Let $x, y \in V_0$, and suppose that there exists a positive integer l such that $f_b^l(x) = f_b^l(y) = b$. Then x is a source if and only if y is a source.*

Proof. Let $x, y \in V_0$ and suppose that the l-th iterates of x and y are both equal to b. Assume that x is a source but y is not. Due to symmetry, only one implication is proved.

Let K be as in Theorem 3.2, and h be the dimension of K as in Lemma 3.5. Since x is a source, x and its successive iterations $f_b(x), f_b^2(x), f_b^3(x), \ldots, f_b^{h-1}(x)$ form a basis B for K. Write

$$y = \alpha_0 x + \alpha_1 f_b(x) + \alpha_2 f_b^2(x) + \ldots + \alpha_{h-1} f_b^{h-1}(x). \tag{3.4}$$

Recall that $f_b^{h-1}(x) = b$. By taking f_b^l on both sides of (3.4),

$$b = f_b^l(y) = \alpha_0 b.$$

Since $b \neq 0$, it follows that $\alpha_0 = 1$.

If, on the contrary, $f_b(t) = y$ for some $t \in \mathbb{F}_q$, then $t \in V_0$. Write

$$t = \beta_0 x + \beta_1 f_b(x) + \beta_2 f_b^2(x) + \ldots + \beta_{h-1} f_b^{h-1}(x).$$

Taking f_b on both sides,

$$y = \beta_0 f_b(x) + \beta_1 f_b^2(x) + \beta_2 f_b^3(x) + \ldots + \beta_{h-2} f_b^{h-1}(x). \tag{3.5}$$

Equating (3.4) and (3.5) gives $\alpha_0 = 0$, which is absurd. Therefore, y is also a source. □

The proof of Proposition 3.6 can be imitated to reveal another phenomenon. The sum of two points in V_0 is a source when one is a source and the other is not.

Proposition 3.7. *Suppose that $b \in \mathbb{F}_q \{0,1\}$. Let $x, y \in V_0$ and suppose that x is a source. Then $x+y$ is a source if and only if y is not a source.*

Proof. Let $x, y \in V_0$ be given and suppose that x is a source. Assume further that y is a source.

Just as in the proof of Lemma 3.5, build a basis B out of iterates of x. Write

$$y = \alpha_0 x + \alpha_1 f_b(x) + \alpha_2 f_b^2(x) + \ldots + \alpha_{h-1} f_b^{h-1}(x). \tag{3.6}$$

It is already seen in the previous proof that $\alpha_0 = 1$. It must be the case that

$$\begin{aligned} x+y &= \alpha_1 f_b(x) + \alpha_2 f_b^2(x) + \ldots + \alpha_{h-1} f_b^{h-1}(x) \\ &= f_b\left(\alpha_1 x + \alpha_2 f_b(x) + \ldots + \alpha_{h-1} f_b^{h-2}(x)\right). \end{aligned}$$

Thus, $x+y$ has a pre-image, namely z. Therefore, $x+y$ is not a source.

Assume instead that y is not a source. Write

$$y = \beta_0 x + \beta_1 f_b(x) + \beta_2 f_b^2(x) + \ldots + \beta_{h-1} f_b^{h-1}(x). \tag{3.7}$$

If $\beta_0 = 1$, then taking f^{h-1} on both sides of (3.7) implies $b = 0$. This contradicts the assumption that y is not a source. It follows that $\beta_0 = 0$, and

$$x+y = x + \beta_1 f_b(x) + \beta_2 f_b^2(x) + \ldots + \beta_{h-1} f_b^{h-1}(x). \tag{3.8}$$

As seen in the proof of Proposition 3.6, if $x+y$ is not a source, then x cannot be one, contradicting with the hypothesis. Therefore, $x+y$ is a source. □

From Propositions 3.6 and 3.7, each $x \in K$ has exactly two pre-images if one exists, and all sources are on the same "level." This is possible only if V_0, and hence V_p for any periodic point p, forms a perfect binary tree.

3.2 Periodic Cycles

Next, the periodic structure of f_b is investigated. It is established that the set of periodic points forms a vector subspace of $\mathbb{F}_q$. It must possess a basis, of which the construction is the final aim. It is also shown that cycles can be categorized according to the sum of points in them.

Since periodic cycles are formed from periodic points, the number of periodic points should be counted first. It is established that the field $\mathbb{F}_q$ is a direct sum of the sets of nilpotent and periodic points, so the dimensions of both sets add up to the degree N of the field. If h denotes the dimension of the subspace of nilpotent points as before, then the subspace of periodic points has dimension $N-h$. Therefore, there are 2^{N-h} periodic points. It is also expected that a basis for the subspace of periodic points has $N-h$ elements.

By solving the equation $f_b(x) = x$, two fixed points are obtained, namely 0 and $b+1$. The sum of points in a given periodic cycle can only assume these two values. Also, for periodic cycles of odd length, if the points add up to 0, then another cycle can be constructed to make the points add up to $b+1$.

Lemma 3.8. *Let $b \in \mathbb{F}_q$ be arbitrary. Let C be a periodic cycle of f_b. Then the following hold.*

1. *The sum of all points in C is either 0 or $b+1$.*
2. *If C has odd length, there exists a periodic cycle D such that D has the same length as C, but the sum of points in D is different.*

Proof. Let C be a periodic cycle of f_b. Pick a point $x_0 \in C$. Every $x \in C$ is clearly of the form $f_b^i(x_0)$ for some nonnegative integer i less than the length of C. Consider the sum of points in C, namely

$$s = \sum_{i=0}^{|C|-1} f_b^i(x_0).$$

Then s is a fixed point of f_b. To see this, consider

$$\begin{aligned} f_b(s) &= \sum_{i=0}^{|C|-1} f_b^{i+1}(x_0) \\ &= \sum_{i=0}^{|C|-1} f_b^i(x_0) \\ &= s. \end{aligned}$$

Since s is a fixed point of f_b, it must be either 0 or $b+1$. This proves the first assertion.

To prove the second statement, assume that C has odd length. Let $y_0 = x_0 + b + 1$, and D be the set of iterations of y_0 under f_b. According to Lemma 2.2, y_0 is a periodic point with least period equal to that of x_0, hence $|D| = |C|$. However, consider the sum of points s' in D.

$$\begin{aligned} s' &= \sum_{i=0}^{|D|-1} f_b^i(x_0 + b + 1) \\ &= \sum_{i=0}^{|C|-1} f_b^i(x_0) + \sum_{i=0}^{|C|-1} (b+1) \\ &= s + b + 1. \end{aligned}$$

If $s = 0$, then $s' = b+1$, but if $s = b+1$, on the other hand, then $s' = 0$. Therefore, the sum of points in D is different from that in C. This proves the second assertion. □

Now a basis for the subspace of periodic points can be constructed. There must be a periodic cycle whose length is the longest. If one is found, then a periodic point can be picked from it, and its $N-h$ iterates form such a basis. It remains to show that the candidate basis is linearly independent, and that every periodic point can be written as a linear combination from it.

Theorem 3.9. *Let $b \in \mathbb{F}_q \setminus \{1\}$ be given, and let C be the periodic cycle of f_b satisfying the two following conditions.*

1. *Its length is the greatest among all cycle lengths.*
2. *All points in it add up to $b+1$.*

Let $x_0 \in C$, and let h be the dimension of the set of nilpotent points of f_b. Then

$$B_P = \left\{ f_b^k\left(x_0\right) \mid k = 0, 1, 2, \ldots, N-h-1 \right\}$$

is a basis for the set of periodic points of f_b.

Proof. Let x_0 denote such a periodic point. Let P denote the set of periodic points of f_b, and let c be the least period of x_0. For convenience, let $x_i = f_b^i\left(x_0\right)$ for $i = 1, 2, 3, \ldots, c-1$, and $x_c = x_0$. To prove the linear independence of B_P, consider the equation

$$\delta_0 x_0 + \delta_1 x_1 + \ldots + \delta_{N-h-1} x_{N-h-1} = 0. \tag{3.9}$$

By iterating (3.9) $|C|$ times, these equations are obtained and added to yield

$$\left(\delta_0 + \ldots + \delta_{N-h-1}\right)(b+1) = 0.$$

Since $b \neq 1$, it follows that

$$\begin{gathered} \delta_0 + \delta_1 + \ldots + \delta_{N-h-1} = 0 \\ \left(\delta_0 + \delta_1 + \ldots + \delta_{N-h-2}\right) x_{N-h-1} = \delta_{N-h-1} x_{N-h-1}. \end{gathered}$$

Set $y_i = x_0 + x_{N-h-1}$ for $i = 0, 1, \ldots, N-h-2$. Substituting in (3.9) gives

$$\delta_0 y_0 + \delta_1 y_1 + \ldots + \delta_{N-h-2}\left(y_{N-h-2}\right) = 0. \tag{3.10}$$

The above process can be performed on 3.10 to yield

$$\left(\delta_0 + \ldots + \delta_{N-h-2}\right) y = 0,$$

where $y = y_1 + \ldots + y_{N-h-2}$. On the one hand, if $N-h$ is odd, then $y = b+1 \neq 0$. On the other hand, if $N-h$ is even, then $y = x_{N-h-1} + b + 1 \neq 0$. In either case, $\delta_0 + \ldots + \delta_{N-h-2} = 0$, so $\delta_{N-h-1} = 0$. The whole argument can be repeated again to obtain

$$\delta_{N-h-1} = \delta_{N-h-2} = \delta_{N-h-3} = \ldots = \delta_0 = 0.$$

Therefore, B_P is linearly independent. It is also the case that x_{N-h} is linearly dependent on B_P, so it must be a linear combination from elements in B_P as well.

It is clear from Lemma 2.2 that linear combinations from elements in B_P are points of period c. To see that points of smaller periods can be written as such a linear combination as well, let d be a proper divisor of c, and consider

$$y = x_0 + x_d + x_{2d} + \ldots + x_{kd}, \tag{3.11}$$

where k is a positive integer such that $(k+1)\,d = c$. Then y is a point of period d because

$$\begin{aligned} f_b^d\,(y) &= x_d + x_{2d} + x_{3d} + \ldots + x_c \\ &= x_0 + x_d + x_{2d} + \ldots + x_{kd} = y. \end{aligned}$$

All iterations of x_0 after $N - h - 1$ is a linear combination of elements in B_P, so y is also in the span of B_P as well. Therefore, B_P is a basis of the set P. □

3.3 Conjugate Maps

Recall that two dynamical systems f and g are *conjugate* if there exists a bijective map ϕ such that $\phi \circ f \circ \phi^{-1} = g$. The definition is taken from [8], although it is not required here that ϕ be continuous. Conjugate systems share key dynamical properties, as ϕ preserves iterations, orbits, and periodicity. Conjugacy is also an equivalence relation among dynamical systems. In this section, it will be shown that field automorphisms act as conjugacy maps between maps within the family $\{f_b \mid b \in \mathbb{F}_q\}$. Since field automorphisms are well-studied in the context of Galois theory, this moderately limits the number of similar systems.

Proposition 3.10. *Let $b \in \mathbb{F}_q$. Then the maps f_b and f_{b^2} are conjugate.*

Proof. Let $\phi : \mathbb{F}_q \to \mathbb{F}_q$ be given by the Frobenius automorphism; i.e. $\phi\,(x) = x^2$ for each $x \in \mathbb{F}_q$. The map is well-known to be bijective. Let $x \in \mathbb{F}_q$ be arbitrary. Consider

$$\begin{aligned} (\phi \circ f_b)\,(x) &= \phi\left(x^2 + bx\right) \\ &= x^4 + b^2 x^2 \\ &= (\phi\,(x))^2 + b^2 \phi\,(x) \\ &= f_{b^2}\,(\phi\,(x)) \\ &= (f_{b^2} \circ \phi)\,(x)\,. \end{aligned}$$

Therefore, f_b and f_{b^2} are conjugate. □

The following corollary is not surprising due to the fact that conjugacy is an equivalence relation, and that the Frobenius automorphism generates all automorphisms of the field. The latter fact is proved, for example, in [4]. In loose terms, Galois conjugates from $\mathbb{F}_q$ yield maps with similar orbits. It is stated here without proof.

Corollary 3.11. *Let $b \in \mathbb{F}_q$ and $\sigma \in Gal(\mathbb{F}_q/\mathbb{F}_2)$. Then f_b and $f_{\sigma(b)}$ are conjugate.*

4 Conclusion and Discussion

In this article, basic descriptions of maps of the form $x \mapsto x^2 + bx$ are established, in terms of successive iterations, transient states, steady states, and conjugacy between such maps. It is seen that the maps exhibit a regularity not found in general quadratic maps. For example, if two periodic cycles of different lengths are found, then another one must exist, and can be calculated from the former two. Non-periodic points also form similarly shaped trees, so the determination of their structure can be restricted to the set of nilpotent points. A basis for the sets of nilpotent and periodic points are also constructed, which can be used for synthesis of the maps.

However, there is room for improvement. To synthesize the map in this manner, iterations of a random point are required, and not determined *a priori* from the parameter b. Several examples, found with the aid of Sage [15], point out a relationship between two ideas of minimal polynomials. If $b \in \mathbb{F}_q$ is a primitive element, then

$$m(x) = x^h \mu(x) + 1,$$

where h is the dimension of the set of nilpotent points of f_b, m is the minimal polynomial of b, and μ is the minimal polynomial of the restriction of f_b to its set of periodic points. If this conjecture holds, then the dynamics of f_b can be determined without using iterations of a random point, at least for primitive b. No counterexample is found so far, except when b is not primitive.

Acknowledgment The author Atsanon Wadsanthat is grateful of Assistant Professor Chaiwat Maneesawarng, from the Department of Mathematics, Faculty of Science, Mahidol University, and Dr. Pornrat Ruengrot, from Mahidol University International College, for their initial feedbacks and proofreading.

The authors would like to thank Dr. Igor Shparlinski and anonymous referees for their valuable reviews, suggestions, and improvements for a previous version of this article.

This work is funded by Sritangthong Scholarship, provided by Faculty of Science, Mahidol University.

References

[1] E. L. Blanton Jr., S. P. Hurd, and J. S. McCranie, On a digraph defined by squaring modulo n, Fibonacci Quarterly, 1992. 30(4), 322-334.

[2] J. Cherly, L. Gilliardo, L. Vaserstein, and E. Wheland, Solving quadratic equations over polynomial rings of characteristc two, Publicacions Matemàtiques, 1998. 42, 131-142.

[3] G. Deng, Cycles of linear dynamical systems over finite local rings, Journal of Algebra, 2015. 433, 243-261.

[4] D. S. Dummit and R. M. Foote, Abstract Algebra, John Wiley and Sons, 3rd ed., 2004.

[5] R. Flynn and D. Garton, Graph components and dynamics over finite fields, International Journal of Number Theory, 2014. 10:3, 779-792.

[6] C. L. Gilbert, J. D. Kolesar, C. A. Reiter, and J. D. Storey, Function digraphs of quadratic maps modulo p, Fibonacci Quarterly, 2001. 39, 32-49.

[7] R. A. Hernández Toledo, Linear finite dynamical systems, Communications in Algebra, 2005. 33:9, 2977-2989.

[8] R. A. Holmgren, A First Course in Discrete Dynamical Systems, Springer-Verlag, New York, 1994.

[9] S. Kravitz, The Lucas-Lehmer test for Mersenne numbers, Fibonacci Quarterly, 1970. 8:1, 1-3.

[10] S. Lang, Algebra, 3rd ed., Addison-Wesley Publishing Company, 1993.

[11] R. Lidl and H. Niederreiter, Finite Fields, 2nd ed., Cambridge University Press, 1997.

[12] C. Lucheta, E. Miller, and C. Reiter, Digraph from powers modulo p, Fibonacci Quarterly, 1996. 34:3, 226-239.

[13] A. Peinado, F. Montoya, J. Muñoz, and A. J. Yuste, Maximal Periods of $x^2 + c$ in $\mathbb{F}_q$, Lecture Notes in Computer Science, 2001. 2227, 219-228.

[14] T. D. Rogers, The graph of the square mapping on the prime fields, Discrete Mathematics, 1996. 148, 317-324.

[15] W. A. Stein et al., The Sage Development Team, Sage Mathematics Software (Version 6.4.1), 2014.

[16] T. Vasiga and J. Shallit, On the iteration of certain quadratic maps over $\mathrm{GF}(p)$, Discrete Mathematics, 2004. 277, 219-240.

[17] G. Xu and Y. M. Zou, Linear dynamical systems over finite rings, Journal of Algebra, 2009. 321:8, 2149-2155.