DISTRIBUTION OF CYCLE LENGTHS OF A QUADRATIC MAP OVER FINITE FIELDS OF CHARACTERISTIC 2

ATSANON WADSANTHAT AND CHATCHAWAN PANRAKSA

Abstract. The map $x \mapsto x^2+x$ defined on a fixed finite field of characteristic 2 is investigated as a dynamical system. The map is known to be a linear map. Its nilpotent points form a subfield, and periodic cycles are somewhat uniform. A general upper bound for the cycle lengths is given in terms of the Carmichael function of the field degree.

1. Introduction

This work stems from our earlier study of maps of the form $x \mapsto x^2 + bx$ defined over finite fields of characteristic 2 for general b in the field [12]. It was found that the case $b = 1$ is an exception compared with others. For instance, because the map looks simpler than others, an explicit formula for its iterations can always be given. The iteration formula provides a convenient ground for the description of orbits of points, and hence the behavior of the map. It turns out that binary expansion and primality play a large role in determining the orbits.

The map is an example of a finite linear dynamical system, which has been studied before. The set of periodic points of such a dynamical system is fully described in [4]. The crucial property used is that the given system preserves an algebraic operation, which is the addition of vectors in a vector space in that case. Other operation-preserving maps were studied, such as the squaring map $x \mapsto x^2$ over finite rings in [1], [8], and [10], and the more general $x \mapsto x^n$ in [7]. Because basic algebraic structures can be realized as modules, and that the given map is linear, the previous studies used Fitting's lemma and our discussion will do the same.

Fitting's lemma states that, for a given module endomorphism, a simultaneously Artinian and Noetherian module can be written as a direct sum of two certain submodules. These two submodules, within respective contexts, are the sets of nilpotent and periodic points. This decomposition allows for describing the maps with ease; the sets can be investigated separately. Within our context, however, more can be said on the sets. The set of nilpotent points can be identified quickly. Moreover, the set of periodic points is found to be largely uniform, especially if the degree of the field is prime or a power of 2.

Before proceeding, let us establish some notations and recall a few definitions. Unless stated otherwise, N will denote a positive integer, possibly with some conditions, and $q = 2^N$. The symbol $\mathbb{F}_q$ represents the finite field of q elements, so it will be of characteristic 2 and degree N. The function $f : \mathbb{F}_q \to \mathbb{F}_q$ is given by $f(x) = x^2 + x$. For any positive integer n and any $x \in \mathbb{F}_q$, $f^n(x)$ is the nth iteration of x. A given point $x \in \mathbb{F}_q$ is termed *nilpotent* (respectively, *periodic*) if there exists an n such that $f^n(x) = 0$ (respectively, $f^n(x) = x$).

We make a few observations as well. The function f is a linear one because for all $x, y \in \mathbb{F}_q$,

$$f(x+y) = (x+y)^2 + (x+y) = f(x) + f(y) . \tag{1.1}$$

Thus, by Fitting's lemma [5], there exists a positive integer n such that

$$\mathbb{F}_q = \text{Ker } f^n \oplus \text{Im } f^n, \tag{1.2}$$

where the first and second summands can be proved to be the sets of nilpotent and periodic points, respectively. Hence, nilpotent points form an additive subgroup of $\mathbb{F}_q$, and periodic points form another one.

The two main results of this paper are to characterize the set of nilpotent points of f, and primes in terms of its cycle lengths. First, if $N = 2^k M$ is the degree of the field, and M is odd, then the nilpotent points form a subfield of degree 2^k. Second, if N is odd, then N is prime if and only if the nonzero cycles of $x \mapsto x^2 + x$ are equal in length. These statements are provided here, and proved later near the end of Sections 3 and 4, respectively.

Theorem 1.1. *Let $N = 2^k M$, where k is nonnegative and M is odd. Then, the set of nilpotent points of f is a subfield of $\mathbb{F}_q$ of degree 2^k.*

Theorem 1.2. *Suppose that N is an odd number. The nonzero periodic cycles of $x \mapsto x^2 + x$ on $\mathbb{F}_q$ are of equal length if and only if N is prime.*

2. General Iteration Identities

In this section, a closed form for $f^n(x)$ in terms of powers of x is given. It is shown that the formula involves, in large part, the binary expansion of the number n of iterations. One of these formulas can be used in obtaining an upper bound for periodic cycle lengths.

Lemma 2.1. *Let $n = 2^k$ be a positive integer. Then for all $x \in \mathbb{F}_q$,*

$$f^n(x) = x^{2^n} + x. \tag{2.1}$$

Proof. The idea is to use induction on the exponent k. If $n = 2^0 = 1$, then for all $x \in \mathbb{F}_q$,

$$f^1(x) = x^{2^{2^0}} + x = x^2 + x,$$

which holds by definition of f.

Suppose that the formula holds for a fixed k and all $x \in \mathbb{F}_q$. Then for $n = 2^{k+1}$ and all $x \in \mathbb{F}_q$,

$$\begin{aligned} f^{2^{k+1}}(x) &= f^{2^k}\left(f^{2^k}(x)\right) \\ &= f^{2^k}\left(x^{2^{2^k}} + x\right) \\ &= \left(x^{2^{2^k}} + x\right)^{2^{2^k}} + \left(x^{2^{2^k}} + x\right) \\ &= x^{2^{2^{k+1}}} + x. \end{aligned}$$

By induction, it is concluded that (2.1) holds for all powers of 2 and all $x \in \mathbb{F}_q$. □

Proposition 2.2. *Let $n = 2^r + 2^s$ for some different $r, s \in \mathbb{N}$. Then for all $x \in \mathbb{F}_q$,*

$$f^n(x) = x^{2^{2^r+2^s}} + x^{2^{2^r}} + x^{2^{2^s}} + x. \tag{2.2}$$

Proof. Let $r, s \in \mathbb{N}$ be given different integers, and let $x \in \mathbb{F}_q$ be arbitrary. Consider

$$\begin{aligned} f^{2^r+2^s}(x) &= f^{2^r}\left(f^{2^s}(x)\right) \\ &= f^{2^r}\left(x^{2^{2^s}} + x\right) \\ &= \left(x^{2^{2^s}} + x\right)^{2^{2^r}} + \left(x^{2^{2^s}} + x\right) \\ &= x^{2^{2^r+2^s}} + x^{2^{2^r}} + x^{2^{2^s}} + x. \end{aligned}$$

Since r, s, and x are arbitrary, the proof is complete. □

Proposition 2.3. *Let $n \in \mathbb{N}$ have the binary expansion*

$$n = \sum_{k=1}^{m} 2^{r_k} \tag{2.3}$$

where $r_k \in \mathbb{N}$ for $k = 1, 2, \ldots, m$. Then for all $x \in \mathbb{F}_q$,

$$f^n(x) = \sum x^{2^c}, \tag{2.4}$$

where c ranges over $\{0,1\}$-linear combinations from $\{2^{r_1}, 2^{r_2}, \ldots, 2^{r_m}\}$.

Proof. Suppose that (2.4) holds for every $x \in \mathbb{F}_q$ and for positive integers with at most m terms in the right side of (2.3). Let $x \in \mathbb{F}_q$ be arbitrary and consider when n has $m+1$ terms in its binary expansion, say

$$n = \sum_{k=1}^{m+1} 2^{r_k} = 2^{r_{m+1}} + \sum_{k=1}^{m} 2^{r_k}. \tag{2.5}$$

Let $n' = n - 2^{r_{m+1}}$. Then n' has m terms in its binary expansion, and

$$\begin{aligned} f^{2^{m+1}}\left(f^{n'}(x)\right) &= f^{2^{m+1}}\left(\sum x^{2^c}\right) \\ &= \sum x^{2^{c+2^{m+1}}} + \sum x^{2^c}, \end{aligned}$$

where c runs through all $\{0,1\}$-linear combinations from $\{2^{r_1}, 2^{r_2}, \ldots, 2^{r_m}\}$. Any $\{0,1\}$-linear combination d from $\{2^{r_1}, 2^{r_2}, \ldots, 2^{r_m}, 2^{r_{m+1}}\}$ either contains the term $2^{r_{m+1}}$ or not. If it does, then x^{2^d} is found in the first sum. Otherwise, it is in the second sum. Hence, the sums can be written as one sum

$$\sum x^{2^d}$$

where d runs through all $\{0,1\}$-linear combinations from $\{2^{r_1}, 2^{r_2}, \ldots, 2^{r_{m+1}}\}$. The proof is complete. □

3. Nilpotent Points

Recall that a point $x \in \mathbb{F}_q$ is *nilpotent* if there exists an $n \in \mathbb{N}$ such that $f^n(x) = 0$. The set of nilpotent points is known to be a subspace of the vector space $\mathbb{F}_q$, which means that the sum of two nilpotent points is again nilpotent. For the map f, however, nilpotent points are more limited in choice, as we shall show that they form a subfield of $\mathbb{F}_q$. If $N = 2^k M$, where M is odd and k is nonnegative, the subfield of nilpotent points has degree 2^k.

Lemma 3.1. *Let $x, y \in \mathbb{F}_q$ be nilpotent points of f. Then, xy is a nilpotent point of f.*

Proof. Let $x, y \in \mathbb{F}_q$ be nilpotent points of f. By definition, there exists an $n \in \mathbb{N}$ such that $f^n(x) = f^n(y) = 0$. Let m be such that $2^m \geq n$. Taking iterations of f yields $f^{2^m}(x) = f^{2^m}(y) = 0$. By Lemma 2.1,

$$x^{2^{2^m}} = x, \tag{3.1}$$

$$y^{2^{2^m}} = y. \tag{3.2}$$

Multiplying both equations yields

$$\begin{aligned} (xy)^{2^{2^m}} &= xy \\ f^{2^m}(xy) &= 0. \end{aligned}$$

By definition, xy is nilpotent. □

Proof of Theorem 1.1. Let F be the subfield of $\mathbb{F}_q$ of degree 2^k. Then for every $x \in F$,

$$x^{2^{2^k}} = x. \tag{3.3}$$

This implies that $f^{2^k}(x) = 0$, so x is a nilpotent point of f. Conversely, let x be a nilpotent point of f. By definition, there exists an $n \in \mathbb{N}$ such that $f^n(x) = 0$. Let $m \in \mathbb{N}$ be such that $2^m \geq n$. On the one hand, if $m \leq k$, then $f^{2^k}(x) = 0$, and immediately $x \in F$. On the other hand, if $m > k$, then x satisfies $x^{2^N} = x$ and $x^{2^{2^m}} = x$. By the division algorithm, there exist unique d_1 and r_1 such that $2^m = Nd_1 + r_1$ and $0 \leq r_1 < N$. It must be the case that

$$\begin{aligned} x^{2^{2^m}} &= x \\ x^{2^{Nd_1+r_1}} &= x \\ x^{2^{r_1}} &= x. \end{aligned}$$

By the Euclidean algorithm, the process can be applied until an equation of the form

$$x^{2^r} = x, \tag{3.4}$$

where $r = \gcd(2^m, N) = 2^k$ is derived. Therefore, $x^{2^{2^k}} = x$, and $x \in F$. □

As a corollary, we identify N for which f is a *fixed point system.* A mapping is termed as such when all its periodic points are fixed ones.

Corollary 3.2. *The map f is a fixed point system if and only if $N = 2^k$ for some nonnegative integer k.*

Proof. Suppose that $N = 2^k$ for some nonnegative integer k. Theorem 1.1 dictates that the subfield of nilpotent points of f must be of degree 2^k, implying that every point $x \in \mathbb{F}_q$ is nilpotent. Hence, every point is eventually mapped to 0, which is the sole fixed point of f, and f is a fixed point system.

Conversely, suppose that f is a fixed point system. Since the field $\mathbb{F}_q$ being finite, there exist an n such that $f^n(x) = 0$ for all $x \in \mathbb{F}_q$. There exists an $m \in \mathbb{N}$ such that $2^m \geq n$. This implies $f^{2^m}(x) = 0$ for all $x \in \mathbb{F}_q$, so $x^{2^{2^m}} = x$. Choosing k to be the least possible such m yields the assertion. □

Corollary 3.3. *If N is odd, then f has only two nilpotent points, namely 0 and 1.*

Theorem 1.1 and its corollaries intuitively suggest that if $N = 2^k M$ is the degree of the given field, then the orbits are largely unaffected by its subfield of degree 2^k. In this sense, N can be assumed to be odd, which corresponds to $k = 0$.

4. Periodic Cycles

In this section, we investigate the cycle structure of f by giving a crude upper bound for the maximal cycle length of f, and show how the primality of N plays a part in determining cycles. To be specific, assuming that N is odd, all periodic cycles of f except one are of the same length if and only if N is a prime.

A few observations are in order. The map f has exactly one fixed point, namely 0, which is obtained from solving $f(x) = x$. Thus, no other points are fixed points of f, and we call a periodic cycle *nonzero* if it is not that fixed point.

We also recall that the Carmichael function $\lambda(N)$ is the least positive integer such that for all a relatively prime to N, $a^{\lambda(N)} - 1$ is divisible by N. For odd prime power $P = p^r$, $\lambda(p^r) = p^r - p^{r-1}$.

Lemma 4.1. *Let $N = 2^k M$, where k is nonnegative and M is odd. For all x in $\mathbb{F}_q$,*

$$f^{2^{\lambda(M)+k}}(x) = f^{2^k}(x), \tag{4.1}$$

where $\lambda(M)$ is the Carmichael function of M.

Proof. Let $x \in \mathbb{F}_q$ be arbitrary. By the definition of λ, $2^{\lambda(M)} = Mc + 1$ for some positive integer c. This implies

$$2^{\lambda(M)+k} = 2^k Mc + 2^k = Nc + 2^k. \tag{4.2}$$

Consider

$$\begin{aligned} f^{2^{\lambda(M)+k}}(x) &= x^{2^{2^{\lambda(M)+k}}} + x \\ &= x^{2^{Nc+2^k}} + x \\ &= x^{2^{2^k}} + x \\ &= f^{2^k}(x). \end{aligned}$$

The proof is complete. □

Thus, if $N = 2^k M$ and M is odd, Lemma 4.1 shows that the trees attached to each periodic point are of height 2^k, and the cycles are of length $2^{\lambda(N)+k} - 2^k$. Since these facts are crucial to the overall description of f as a dynamical system, they are recorded as a corollary.

Corollary 4.2. *Let $N = 2^k M$, where k is a nonnegative integer and M is an odd number. Then, the following conditions hold.*

1. *For every $x \in \mathbb{F}_q$, there exists a nonnegative integer m such that $m \leq 2^k$ and $f^m(x)$ is a periodic point.*
2. *Every periodic point $x \in \mathbb{F}_q$ of f has period $2^{\lambda(N)+k} - 2^k$.*

The bound in Corollary 4.2, however, might be ineffective in some cases, one of which is highlighted below. It concerns different powers of 2, and Mersenne numbers in particular.

Proposition 4.3. *Suppose that the binary expansion of N is a geometric series, namely*

$$N = 2^a + 2^{a+r} + 2^{a+2r} + \ldots + 2^{a+(k-1)r}. \tag{4.3}$$

Then for all $x \in \mathbb{F}_q$,

$$f^{2^{a+kr}}(x) = f^{2^a}(x). \tag{4.4}$$

Proof. Let $x \in \mathbb{F}_q$ be arbitrary. Note that $(2^r - 1)\,N = 2^{a+kr} - 2^a$. Consider

$$\begin{aligned} f^{2^{a+kr}}(x) &= x^{2^{2^{a+kr}}} + x \\ &= x^{2^{(2^r-1)N+2^a}} + x \\ &= x^{2^{2^a}} + x \\ &= f^{2^a}(x)\,. \end{aligned}$$

Noticing that x is arbitrary completes the proof. □

In particular, Proposition 4.3 applies to numbers N of the form $2^m + 1$ and $2^m - 1$, which include Mersenne and Fermat primes. Noticing that their binary expansions are geometric series proves the following corollaries.

Corollary 4.4. *Let $N = 2^r - 2^s$ for some nonnegative integers r, s with $r > s+1$. Then for all $x \in \mathbb{F}_q$,*

$$f^{2^r}(x) = f^{2^s}(x)\,. \tag{4.5}$$

Corollary 4.5. *Let $N = 2^r + 2^s$ for some nonnegative integers r, s with $r > s+1$. Then for all $x \in \mathbb{F}_q$,*

$$f^{2^{2r}}(x) = f^{2^{2s}}(x)\,. \tag{4.6}$$

Lemma 4.1, Proposition 4.3, and its two corollaries, give an upper bound for cycle lengths. In general, the map f on a finite field of degree $N = 2^k M$, where k is nonnegative and M is odd, has cycle lengths not longer than $2^{\lambda(M)+k} - 2^k$. If N has a binary expansion which is a geometric series, the cycle length is a multiple of N, likely between N and $N^2 - 2N$.

In case of $N = 2^r - 2^s = 2^s\,(2^{r-s} - 1)$ and $r > s+1$, it is inferred from Corollary 4.4 that the lengths of periodic cycles cannot be greater than $2^r - 2^s = N$. Theorem 1.1 indicates that the subspace of nilpotent points is of dimension 2^s. Consequently, the subspace of periodic points must be of dimension $k = N - 2^s$. Periodic cycles of maximal length must be at least k iterations long by virtue of linear independence. Thus, the length of such cycles must be N. It is stressed that, for $N = 2^r - 2^s$ with $r > s+1$, the bound from Corollary 4.4 is exact for maximal cycles.

It remains to prove Theorem 1.2, which demonstrates how primality of an odd N affects the cycle lengths. Specifically, if the degree N of the field is an odd prime, then all periodic cycles, except the sole fixed point, have the same length. The converse also holds.

Proof of Theorem 1.2. Assume that N is odd. Let $\{C_1, C_2, \ldots, C_k\}$ be the enumeration of non-fixed periodic cycles of the map, with lengths c_1, c_2, …, c_k, respectively. The sum of these lengths is equal to the number of nonzero periodic points, which is $2^{N-1} - 1$. By Lemma 4.1, for each $i = 1, 2, \ldots, k$, there exists an integer d_i such that $c_i d_i = 2^{\lambda(N)} - 1$. Counting the number of periodic points and considering the definition of d_i yield

$$\sum_{j=1}^{k} \frac{1}{d_j} = \frac{2^{N-1} - 1}{2^{\lambda(N)} - 1}. \tag{4.7}$$

Dividing $N - 1$ by $\lambda(N)$ gives positive integers s and t such that $N - 1 = s\lambda(N) + t$ and $0 \leq \lambda(N)$. If N is prime, then $\lambda(N) = N - 1$ and the right side of (4.7) is 1. If N is composite, then $\lambda(N) \leq N - 3$ and the right side of (4.7) is at least 4. Note that $\lambda(N) = N - 2$ is impossible because $N - 2$ is odd but $\lambda(N)$ is always even.

Define

$$\mu = \sum_{j=1}^{k} \frac{c_j}{d_j} = \frac{1}{2^{\lambda(N)} - 1} \sum_{j=1}^{k} c_j^2. \tag{4.8}$$

The Cauchy-Schwarz inequality implies

$$\mu^2 \leq \left(\sum_{j=1}^{k} \frac{1}{d_j} \right) \left(\sum_{j=1}^{k} \frac{c_j^2}{d_j} \right). \tag{4.9}$$

Consider the expression

$$s = \sum_{j=1}^{k} \frac{(c_j - \mu)^2}{d_j} = \sum_{j=1}^{k} \frac{c_j^2}{d_j} - \left(2 - \sum_{j=1}^{k} \frac{1}{d_j} \right) \mu^2. \tag{4.10}$$

Preparations are done at this point. On the one hand, suppose that $c_j = \mu$ for all j. Then $s = 0$, and equality holds in (4.9). An appropriate substitution yields

$$\mu^2 = \left(\sum_{j=1}^{k} \frac{1}{d_j} \right) \left(2 - \sum_{j=1}^{k} \frac{1}{d_j} \right) \mu^2.$$

This implies $\sum_{j=1}^{k} \frac{1}{d_j} = 1$, so $\lambda(N) = N - 1$. Therefore, N is prime.

On the other hand, suppose that N is prime. Then $\lambda(N) = N - 1$, so from $2^{N-1} - 1 = c_1 d_1 = c_1 + c_2 + \ldots + c_k$,

$$d_1 = 1 + \frac{c_2}{c_1} + \frac{c_3}{c_1} + \ldots + \frac{c_k}{c_1}.$$

To interpret this, if the nonzero periodic points are grouped into cycles of length c_1, then all those points are exhausted. In this way, there are $\frac{c_2}{c_1}$ cycles of length c_2, $\frac{c_3}{c_1}$ cycles of length c_3, and so on. Thus, c_1 divides each of c_2, c_3, …, c_k. More generally, for any $i, j \in \{1, 2, 3, \ldots, k\}$, c_i divides c_j. It follows that $c_i = c_j$ for any pair $i, j \in \{1, 2, 3, \ldots, k\}$. As an implication, $d_i = k$ for all i. Hence, for each i,

$$c_i = \frac{2^{N-1} - 1}{k} = \sum_{j=1}^{k} \frac{c_j}{k} = \mu.$$

□

The cycle lengths of f for $N = 2, 3, 4, \ldots, 15$ are enumerated in Table 1 below. It shows how the primality and binary expansion of N regulate the existence and uniformity of cycles. In particular, it verifies our theorems in Sections 3 and 4, and illustrates how they apply for each N. For $N = 3, 5, 7, 11, 13$, there is only one cycle length. In contrast, for $N = 9, 15$, there are at least two different lengths.

N	Upper bound	Obtained from corollary	Nonzero cycles
2	1	3.2	None
3	3	4.4	1 cycle of length 3
4	1	3.2	None
5	15	4.5	1 cycle of length 15
6	6	4.4	1 cycle of length 3 2 cycles of length 6
7	7	4.4	9 cycles of length 7
8	1	3.2	None
9	63	4.5	1 cycle of length 3 4 cycles of length 63
10	30	4.2	1 cycle of length 15 8 cycles of length 30
11	1023	4.2	3 cycles of length 341
12	12	4.4	1 cycle of length 3 2 cycles of length 6 20 cycles of length 12
13	4095	4.2	5 cycles of length 819
14	14	4.4	9 cycles of length 7 288 cycles of length 14
15	15	4.4	1 cycle of length 3 3 cycles of length 5 1091 cycles of length 15

TABLE 1. Cycle lengths of f on $\mathbb{F}_q$ as N ranges from 2 to 15.

All examples in Table 1 are calculated using Sage computer algebra software, version 6.4.1 [9]. The code for each N, ran case-by-case, is given in Figure 1.

```
sage: #Set degree N and order q, vary N on each run
sage: N=6; q=2^N
sage: #Build finite field
sage: a=var(‘a’); F=GF(q,‘a’)
sage: #Create digraph of f
sage: C=F.list()
sage: G=DiGraph([C, lambda i,j: F(i^2+i)==F(j)])
sage: #List cycles and count lengths
sage: l1=G.all_simple_cycles()
sage: l2=[len(l)-1 for l in l1]
sage: #Count cycles
sage: from itertools import groupby
sage: [(len(list(m)),l) for l,m in groupby(l2)]
```

FIGURE 1. Code for finding cycle lengths of f for each N.

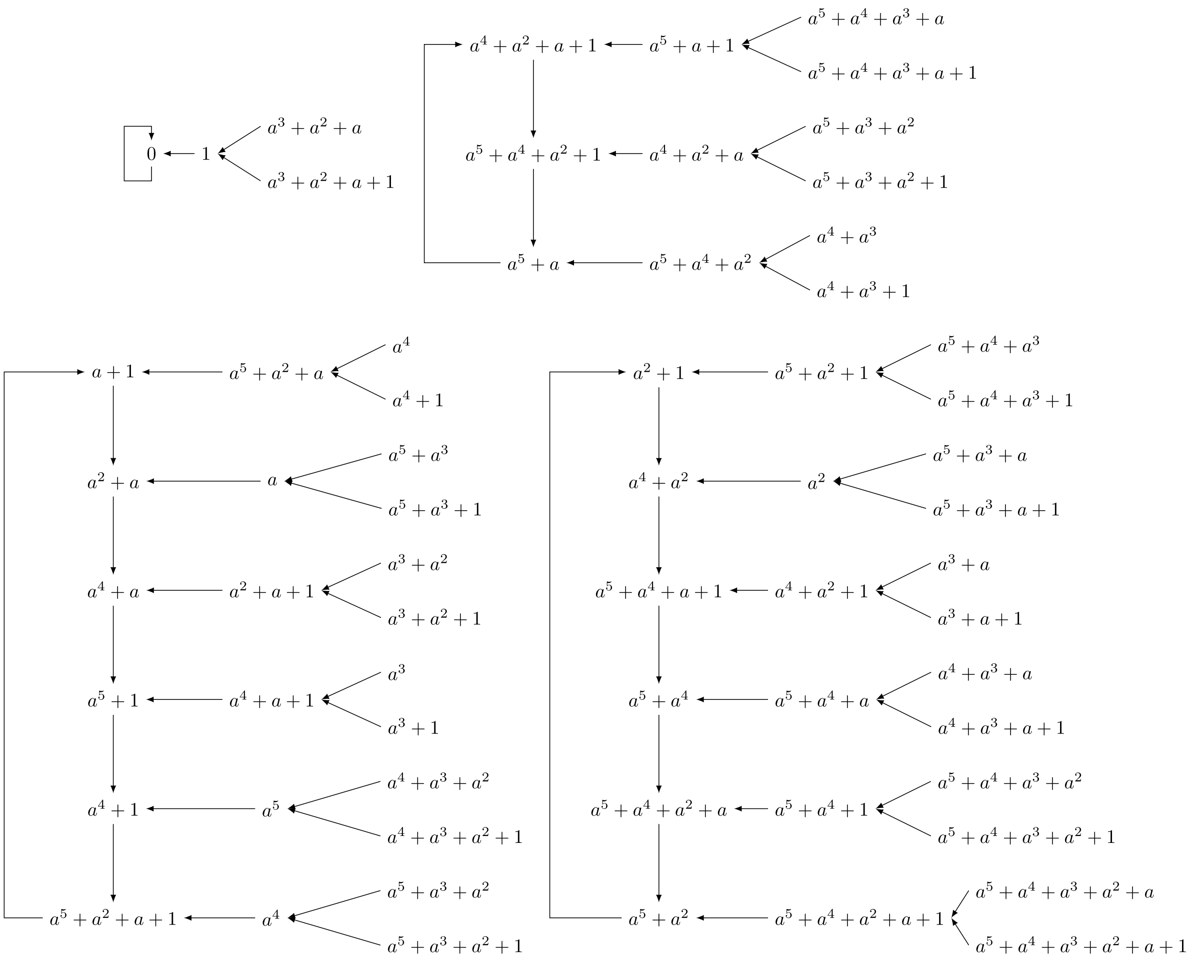

FIGURE 2. Direct graph of f on $\mathbb{F}_{64} \cong \mathbb{F}_2[a]/\left\langle a^6+a^4+a^3+a+1\right\rangle$.

5. Conclusion and Discussion

For the specific map $x \mapsto x^2+x$ defined on finite fields of characteristic 2, the nilpotent and cycle structure are obtained in terms of degree of the field. By Theorem 1.1, the set of nilpotent points is the maximal subfield of degree 2^k. The degree N characterizes the uniformity of cycle lengths. By Theorem 1.2, except the fixed point, periodic cycles are of the same length if and only if N is prime.

It is likely that the bound from Corollary 4.2 can be made sharper by considering the order of 2 in the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$ or considering a geometric sum.

It might be possible to use Corollary 4.4 and Theorem 1.2 in conjunction to derive a test for Mersenne primes, or Lemma 4.1 to estimate $\lambda(N)$, using only bitwise operations. With a so-called normal basis for $\mathbb{F}_q$, the map $x \mapsto x^2+x$ is a cyclic permutation of bits, followed by an exclusive or.

References

[1] E. L. Blanton Jr., S. P. Hurd, and J. S. McCranie, *On a digraph defined by squaring modulo n*, The Fibonacci Quarterly, **30.4** (1992), 322–334.

[2] R. Burton, *Elementary Number Theory*, 7th ed., McGraw-Hill, New York, 2011.

[3] H. Griffin, *Elementary Theory of Numbers*, McGraw-Hill, New York, 1954.

[4] R. A. Hernández Toledo, *Linear finite dynamical systems*, Comm. Algebra, **33.9** (2005), 2977–2989.

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

[6] R. Lidl and H. Niederreiter, *Finite Fields*, 2nd ed., Cambridge University Press, Cambridge, England, UK, 1997.

[7] C. Lucheta, E. Miller, and C. Reiter, *Digraph from powers modulo p*, The Fibonacci Quarterly, **34.3** (1996), 226–239.

[8] T. D. Rogers, *The graph of the square mapping on the prime fields*, Discrete Math., **148** (1996), 317–324.

[9] SageMath, the Sage Mathematics Software System (Version 6.4.1), The Sage Developers, 2014, `http://www.sagemath.org`.

[10] T. Vasiga and J. Shallit, *On the iteration of certain quadratic maps over GF(p)*, Discrete Math., **277** (2004), 219–240.

[11] W. R. Wade, *An Introduction to Analysis*, 4th ed., Pearson, New Jersey, 2010.

[12] A. Wadsanthat, C. Panraksa, and W. Kositwattanarerk, *Linear maps given by quadratic polynomials*, East-West J. Math., preprint.

MSC2010: 11B39, 33C05

Department of Mathematics, Faculty of Science, Mahidol University, Ratchathewi, Bangkok, 10240 Thailand

E-mail address: `atsanon.wad@student.mahidol.ac.th`

Mahidol University International College, Mahidol University, Salaya, Nakhon Pathom, 73170 Thailand

E-mail address: `chatchawan.pan@mahidol.edu`