Proceedings of the Edinburgh Mathematical Society (2000) **43**, 113–128 ©

THE DYNAMICS OF LINEARIZED POLYNOMIALS

STEPHEN D. COHEN[1] AND DIRK HACHENBERGER[2]

[1]*Department of Mathematics, University of Glasgow,*
Glasgow G12 8QW, UK (sdc@maths.gla.ac.uk)
[2]*Institut für Mathematik, Universität Augsburg, 86159 Augsburg,*
Germany (dirk.hachenberger@math.uni-augsburg.de)

(Received 11 March 1998; revised 18 October 1998)

Abstract Let $F = \mathrm{GF}(q)$. To any polynomial $G \in F[x]$ there is associated a mapping $\hat{G}$ on the set I_F of monic irreducible polynomials over F. We present a natural and effective theory of the dynamics of $\hat{G}$ for the case in which G is a monic q-linearized polynomial. The main outcome is the following theorem.

Assume that G is not of the form x^{q^l}, where $l \geqslant 0$ (in which event the dynamics is trivial). Then, for every integer $n \geqslant 1$ and for every integer $k \geqslant 0$, there exist infinitely many $\mu \in I_F$ having preperiod k and primitive period n with respect to $\hat{G}$.

Previously, Morton, by somewhat different means, had studied the primitive periods of $\hat{G}$ when $G = x^q - ax$, a a non-zero element of F. Our theorem extends and generalizes Morton's result. Moreover, it establishes a conjecture of Morton for the class of q-linearized polynomials.

Keywords: finite field; polynomial dynamics; linearized polynomial; period

AMS 1991 *Mathematics subject classification:* Primary 11T99, 39B12, 58F08

1. Introduction

We start very generally and give the fundamental definitions needed to study the *dynamics of mappings*. Let $\gamma : S \to S$ be a mapping defined on a non-empty set S and let $a \in S$. Then a is called *periodic* (*with respect to* γ) if there exist non-negative integers k and l such that $k < l$ and

$$\gamma^k(a) = \gamma^l(a). \tag{1.1}$$

Here, γ^k denotes the kth iterate of the mapping γ and γ^0 is defined to be the identity on S. If every $a \in S$ is periodic, then γ is called *periodic* (*on* S). Let $a \in S$ be periodic with respect to γ and $k < l$ be such that (1.1) holds. Then $l - k$ is called a *period of* a (*with respect to* γ). If k is minimal such that (1.1) holds for some $l > k$, then k is called the *preperiod of* a. If both k and l are minimal such that $k < l$ and (1.1) holds, then $l - k$ is called the *primitive period of* a. Of course, the primitive period of a divides every period of a. If the preperiod of a is equal to zero, then a is called *purely periodic*. (In the literature, the term 'periodic' often refers to what we call 'purely' periodic.) Generally, the set

$$\{\gamma^n(a) \mid n \geqslant 0\} \tag{1.2}$$

is called the *orbit of* a. The term *dynamics of* γ (*on* S) embraces all that pertains to the nature of the orbits of γ on S. Typical questions are 'what lengths of (primitive) periods are realized' and 'how long can the preperiods be?'

We turn to the particular situation which we are interested in. Let $F = \mathrm{GF}(q)$ be the Galois field of order q and $\bar{F}$ be an algebraic closure of F. If $G \in F[x]$ is a polynomial with coefficients in F, then, via evaluation, G can be regarded as a mapping on $\bar{F}$ that leaves every intermediate field of $\bar{F}$ over F invariant. Let $\alpha \in \bar{F}$ and $F(\alpha)$ be the subfield of $\bar{F}$ obtained by adjoining the element α to F. Since $F(\alpha)$ is a finite field (in particular a finite set), we have that α is periodic with respect to G and, as this holds for all $\alpha \in \bar{F}$, G is periodic on $\bar{F}$.

Let I_F denote the set of monic irreducible polynomials over F and again let $G \in F[x]$. Then G also induces a mapping $\hat{G}$ on I_F as follows. Let $f \in I_F$ and $\alpha \in \bar{F}$ be a root of f. Then $\hat{G}(f)$ is defined to be the minimal polynomial of $G(\alpha)$. Of course this is well defined. Moreover, since every $\alpha \in \bar{F}$ is periodic with respect to G, we have that, for every $\alpha \in \bar{F}$, μ_α is periodic with respect to $\hat{G}$, where μ_α denotes the minimal polynomial of α over F (μ_α is irreducible). Since every $\mu \in I_F$ is of the form μ_α for some $\alpha \in \bar{F}$, we obtain that $\hat{G}$ is periodic on I_F.

The study of the dynamics of a mapping $\hat{G}$ on I_F was initiated by Vivaldi [**13**], Batra and Morton [**1**, **2**] and Morton [**9**]. In the latter three papers, the main emphasis is laid on the case in which $G = x^q - ax$ ($a \in F$). The main result in [**9**] (Theorem 1) states that, for every $n \geqslant 0$, there exist infinitely many $\mu \in I_F$, which are purely periodic and have primitive period n with respect to $\hat{G}$ (where $G = x^q - ax$, $a \neq 0$).

In the present paper, we shall extend and generalize this result considerably. In order to accomplish this we present a natural and effective formulation of the dynamics of $\hat{G}$ for the case in which G is a *q-linearized* (*additive*) *polynomial* (of which class $G = x^q - ax$ presents the simplest example). As a consequence, we obtain the following theorem.

Theorem 1.1. *Let $G \neq 0$ be a q-linearized polynomial over F. Assume that G is not of the form x^{q^l}, $l \geqslant 0$. Then, for every integer $n \geqslant 1$ and for every integer $k \geqslant 0$, there exist infinitely many irreducible monic polynomials over F, which, with respect to $\hat{G}$, have primitive period n and preperiod k.*

In particular, this theorem establishes the conjecture in [**9**, p. 12] for the class of q-linearized polynomials. This class comprises polynomials having the shape

$$\sum_i g_i x^{q^i} \in F[x].$$

In § 2, we amplify this definition of a q-linearized polynomial and give a formulation of the main problem in terms of *additive orders.* These are fundamental when studying $\bar{F}$

as an F-vector space together with the Frobenius automorphism σ_F over F. Moreover, we will show that Theorem 1.1 is already true provided that, for every $n \geqslant 1$, there exists *one* irreducible polynomial over F having primitive period n. In § 3, we use character sums in order to prove Theorem 1.1 for primitive periods n which are not divisible by the characteristic of F. In § 4, we deal with periods divisible by the characteristic of F and complete the proof of Theorem 1.1.

Some remarks are in order on the relationship of this work to Morton [**9**], which was our starting point. In his paper, Morton similarly divides the investigation into three parts, which correspond loosely to our §§ 2–4, respectively. He works with the Carlitz module rather than mere considerations of orders (as in § 2): the Carlitz module, however, is neither necessary nor even convenient for general q-linearized polynomials. Instead of the precise formulation using character sums (§ 3), he employs less effective 'Cebotarev' notions. Finally, his treatment of primitive periods divisible by the characteristic differs substantially from ours (§ 4).

2. Linearized polynomials and additive orders

The notion of a q-linearized polynomial goes back to the work of Ore [**10**] (see also [**11**, ch. 3, § 4]). It has proved to be very useful when considering the additive structure of a (finite) extension of $F = \mathrm{GF}(q)$. Let $c = \sum_i c_i x^i \in F[x]$. Then the polynomial

$$A_q(c) := \sum_i c_i x^{q^i} \tag{2.1}$$

is called the *associated q-linearized polynomial of c*, or, more simply, the *associated q-polynomial of c*. For example, $x^q - ax$ is the associated q-linearized polynomial of $x - a$.

Let σ_F be the Frobenius automorphism of $\bar{F}$ over F. Then, for $c \in F[x]$ and $\alpha \in \bar{F}$,

$$A_q(c)(\alpha) = c(\sigma_F)(\alpha). \tag{2.2}$$

In particular, (2.2) imparts a module structure of $\bar{F}$ over the ring $F[x]$ with respect to σ_F (see, for example, [**6**, **7**]). For an integer $n \geqslant 0$ let $[c]^n$ denote the nth iterate of the polynomial c, i.e. $[c]^0 := 1$, $[c]^1 := c$ and, inductively, $[c]^n := [c]^{n-1}(c)$. Thus, again for $\alpha \in \bar{F}$,

$$[A_q(c)]^n(\alpha) = c^n(\sigma_F)(\alpha). \tag{2.3}$$

If $F(\alpha)$ has degree d over F then $(x^d - 1)(\sigma_F)(\alpha) = 0$. Thus, there exists a monic polynomial $f \in F[x]$ of least degree such that $f(\sigma_F)(\alpha) = 0$. This polynomial is uniquely determined. It is called the *F-order of* α and is denoted by $\mathrm{Ord}_F(\alpha)$. It is the monic polynomial f of least degree such that α is a root of the associated q-polynomial $A_q(f)$ of f.

If U is a σ_F-invariant F-subspace of $\bar{F}$, then U will simply be called a *submodule of* $\bar{F}$. Let $\mathcal{P}_F$ be the set of monic polynomials in $F[x]$ that are not divisible by x. Then the following gives the connection between finite submodules of $\bar{F}$, q-linearized polynomials and members of $\mathcal{P}_F$, again see [**6**, **7**].

Proposition 2.1. *The set $\mathcal{P}_F$ corresponds bijectively to the finite submodules of $\bar{F}$. More precisely, if $f \in \mathcal{P}_F$, then the submodule $U_{F,f}$ belonging to f is exactly the set of roots of $A_q(f)$ (in $\bar{F}$), i.e. the kernel of the mapping $f(\sigma_F)$.*

Moreover, every finite submodule of $\bar{F}$ is cyclic (i.e. free on one generator). The generators of $U_{F,f}$ are exactly the elements of $\bar{F}$ whose F-order is equal to f.

Finally, f is the minimal polynomial of the F-vector space $U_{F,f}$ when considered with respect to σ_F.

Next, let g be a monic polynomial in $F[x]$, let x^k be the largest power of x dividing g, and let h be the cofactor of x^k in g. Let G and H, respectively, be the associated q-polynomials of g and h. Since $A_q(x^k) = x^{q^k}$ induces the identity mapping on I_F, the dynamics of $\hat{G}$ and $\hat{H}$ on I_F are the same. We therefore restrict our attention to the case in which g is not divisible by x, i.e. we assume from now on that $g \in \mathcal{P}_F$, $g \neq 1$. We study the dynamics of $\hat{G}$ on the set I_F, where $G := A_q(g)$ is the associated q-linearized polynomial corresponding to g. We therefore refer to g as the *dynamic polynomial.*

The following basic result is [**6**, Lemma 7.4]. It is crucial for studying the preperiods and the periods of $\hat{G}$ on I_F.

Lemma 2.2. *Let $\alpha \in \bar{F}$ have F-order f. Let $g \in F[x]$ be monic. Then $g(\sigma_F)(\alpha)$ has F-order $f/\gcd(g, f)$ (where* gcd *denotes the greatest common divisor).*

In particular, $g(\sigma_F)(\alpha)$ has the same F-order as α if and only if g and $\mathrm{Ord}_F(\alpha)$ are relatively prime.

Since the F-order of each $\alpha \in \bar{F}$ is not divisible by x (see Proposition 2.1), we see that the conjugates of α under σ_F, namely the elements of the set

$$\{\alpha^{q^k} \mid k \geqslant 0\}$$

(i.e. the roots of μ_α), all have the same F-order. Consequently, μ_α is purely periodic with respect to $\hat{G}$ provided that g and $\mathrm{Ord}_F(\alpha)$ are relatively prime.

Assume that μ_α is purely periodic with respect to $\hat{G}$. Let n be the primitive period of μ_α. By definition, $n \geqslant 1$ is the minimum number such that $\hat{G}^n(\mu_\alpha) = \mu_\alpha$. Thus, $n \geqslant 1$ is the minimum number such that there exists an $l \geqslant 0$ such that

$$[G]^n(\alpha) = \alpha^{q^l} = \sigma_F^l(\alpha) = [x^q]^l(\alpha). \tag{2.4}$$

The latter is equivalent to the fact that the F-order of α, say f, is a divisor of

$$g^n - x^l. \tag{2.5}$$

Moreover, there exists an integer $m \geqslant 1$ such that

$$[G]^m(\alpha) = \alpha = \sigma_F^0(\alpha) = [x](\alpha). \tag{2.6}$$

The latter means that f is a divisor of

$$g^m - 1. \tag{2.7}$$

Thus, (2.6) implies the following result, which can be interpreted as meaning that g is a unit modulo f.

Lemma 2.3. *Let $\alpha \in \bar{F}$ and $\mu_\alpha \in I_F$ be the minimal polynomial of α. Then μ_α is purely periodic with respect to $\hat{G}$ if and only if g and $\mathrm{Ord}_F(\alpha)$ are relatively prime.*

If $m \geqslant 1$ is the least integer satisfying (2.6), then m is the multiplicative order of g in the group of units modulo f. This number will be denoted by $\mathrm{ord}_f(g)$. Since, by the definition of $\mathcal{P}_F$, x and f are relatively prime, x is likewise a unit modulo f. Now, letting $[g + (f)]$ and $[x + (f)]$ be the subgroups of units modulo f that are generated by $g \bmod f$ and $x \bmod f$, respectively, we have established the following characterization of the primitive period of μ_α with respect to $\hat{G}$.

Proposition 2.4. *Let f be the F-order of $\alpha \in \bar{F}$. Assume that f is relatively prime to g. Then μ_α is purely periodic with respect to $\hat{G}$ and the primitive period of μ_α with respect to $\hat{G}$ is equal to*

$$\min\{k \geqslant 1 \mid g^k + (f) \in [x + (f)]\}.$$

This number is equal to the index of the group C in $[g + (f)]$, where C is the intersection of $[x + (f)]$ with $[g + (f)]$.

Let $\alpha \in \bar{F}$. Then Lemma 2.3 and Proposition 2.4 show, furthermore, that the fundamental parameters of μ_α with respect to $\hat{G}$, i.e. the preperiod and the primitive period, depend only on the F-order of α. Therefore (essentially by Lemma 2.2), g likewise induces a mapping $\hat{g}$ on the set $\mathcal{P}_F$. In fact, as will emerge from the proof of Proposition 2.7 below, the preperiodic structure of $\hat{g}$ on $\mathcal{P}_F$ is essentially connected to the preperiodic structure of $\hat{G}$ on I_F. On the other hand, by Lemmas 2.2 and 2.3, μ_α is purely periodic with respect to $\hat{G}$ if and only if $\mathrm{Ord}_F(\alpha)$ is purely periodic with respect to $\hat{g}$. Moreover, again by Lemma 2.2 and the remark thereafter, $\hat{g}$ only admits primitive periods of length 1.

We now introduce some notation as follows. If $f \in \mathcal{P}_F$ is relatively prime to g, then

$$\pi_g(f) \tag{2.8}$$

denotes the primitive period of μ_α with respect to $\hat{G}$, where α is *any* element having F-order f. For convenience, we sometimes also write $\pi_g\{\mu_\alpha\}$ for $\pi_g(f)$, noting that, because f and μ_α are both members of $F[x]$, some distinction of notation is expedient.

For $n \geqslant 1$ let

$$\mathcal{P}_g(n) := \{f \in \mathcal{P}_F \mid \gcd(g, f) = 1,\ \pi_g(f) = n\}, \tag{2.9}$$

and

$$I_g(n) := \{\mu_\alpha \in I_F \mid \gcd(g, \mathrm{Ord}_F(\alpha)) = 1,\ \pi_g\{\mu_\alpha\} = n\}. \tag{2.10}$$

The first part of the following proposition is a reformulation of what has been said above.

Proposition 2.5. *Let $\alpha \in \bar{F}$ have F-order f. Assume that f is relatively prime to g. Then*

(1) *$\mu_\alpha \in I_g(n)$ if and only if $f \in \mathcal{P}_g(n)$;*

(2) *$I_g(n)$ is empty if and only if $\mathcal{P}_g(n)$ is empty; and*

(3) *$I_g(n)$ is finite if and only if $\mathcal{P}_g(n)$ is finite.*

Proof. It remains to prove parts (2) and (3).

(2) If $\mu \in I_g(n)$, then $\mathrm{Ord}_F(\alpha) \in \mathcal{P}_g(n)$ for every root α of μ. If $f \in \mathcal{P}_g(n)$, then, by Proposition 2.1, a generator α of $U_{F,f}$ has F-order f. Thus, $\mu_\alpha \in I_g(n)$.

(3) Clearly, if $\mathcal{P}_g(n)$ is infinite, then $I_g(n)$ is infinite. Assume, therefore, that $I_g(n)$ is infinite. If $f \in \mathcal{P}_g(n)$, then $A_q(f)$ has only a finite number of roots. Thus, there exist only a finite number of elements $\alpha \in \bar{F}$ such that μ_α divides $A_q(f)$ and this is equivalent to the fact that $\mathrm{Ord}_F(\alpha)$ divides f. Thus, $\mathcal{P}_g(n)$ has infinite cardinality as well. □

The goal of the remainder of this section is the following reduction of Theorem 1.1.

Theorem 2.6. *Let $g \in \mathcal{P}_F$, $g \neq 1$. Then the following assertions are equivalent.*

(i) *$I_g(n)$ is not empty for all $n \geqslant 1$.*

(ii) *$\mathcal{P}_g(n)$ is not empty for all $n \geqslant 1$.*

(iii) *Theorem 1.1 is valid.*

In order to prove this we first deal with the preperiodic structure of $\hat{G}$. Let $\alpha \in \bar{F}$ and let h_0 be the F-order of α. For $n \geqslant 1$ let h_n be the F-order of $[G]^n(\alpha) = g^n(\sigma_F)(\alpha)$. Using Lemma 2.2 we see that the series (h_n) is ultimately constant, say after k steps. Then k is minimal such that h_k and g are relatively prime. Moreover, k is equal to the preperiod of μ_α. Altogether, this already gives a concrete description of the preperiodic behaviour of $\hat{G}$. In particular, we can show the following.

Proposition 2.7. *Given a polynomial $g \in \mathcal{P}_F$, $g \neq 1$, let $f \in \mathcal{P}_g(n)$. Then, for every $k \geqslant 0$, there exists a $\mu \in I_F$ such that the preperiod of μ is equal to k and every root of $\hat{G}^k(\mu)$ has F-order f (whence the primitive period $\pi_g\{\mu\}$ of μ is equal to n).*

In particular, the preperiods of the mapping $\hat{G}$ on I_F can be arbitrarily long.

Proof. Let a be an irreducible divisor of g and a^m be the maximal power of a dividing g. Let f be relatively prime to g and consider the polynomial $h = a^{km}f$. Then, using Lemma 2.2, the preperiod of $\hat{G}$ on the minimal polynomial of an element having F-order h has length k. The rest also follows from Lemma 2.2. □

Observe that for different f_1 and f_2 in $\mathcal{P}_g(n)$, the construction in the above proof leads to different μ_1 and μ_2. Therefore, the part of Theorem 1.1 concerning the preperiods follows from the part concerning the primitive periods.

We next give a fundamental lemma that will also be very useful in § 4.

Lemma 2.8. *Assume that $f, h \in \mathcal{P}_F$ are relatively prime to g. Let $\alpha \in \bar{F}$ have F-order f. Then the following conditions hold.*

(1) *If $n \geqslant 1$ is such that $\hat{G}^n(\mu_\alpha) = \mu_\alpha$, then $\pi_g(f)$ is a divisor of n.*

(2) *If $n \geqslant 1$ and $l \geqslant 0$ are such that f divides $g^n - x^l$, then $\pi_g(f)$ divides n.*

(3) *If f divides h, then $\pi_g(f)$ divides $\pi_g(h)$.*

Proof. Observe first that μ_α is purely periodic by our assumption. (1) follows since n is a period of μ_α and thus is divisible by $\pi_g(f)$.

(2) is a reformulation of (1).

(3) is an application of (2). □

The final ingredient in the proof of Theorem 2.6 is the following result.

Proposition 2.9. *Given a polynomial $g \in \mathcal{P}_F$, $g \neq 1$. Assume that $f \in \mathcal{P}_F$ is relatively prime to g. Let $n = \pi_g(f)$ be the period of μ_α, where $\alpha \in \bar{F}$ has F-order f. Then $\mathcal{P}_g(n)$ is infinite.*

Proof. There exists $l \geqslant 0$ such that f divides $f_0 := g^n - x^l$. Let α_0 be an element having F-order f_0. An application of Lemma 2.8 shows that $\pi_g(f_0) = n = \pi_g(f)$.

Next, let d be the multiplicative order of x modulo f, i.e. $d \geqslant 1$ is the least integer such that f divides $x^d - 1$ (recall that x does not divide f, whence x is a unit modulo f). For $k \geqslant 0$ let $f_k := g^n - x^{l+kd}$ and let α_k be an element having F-order f_k: the existence of α_k is guaranteed by Proposition 2.1. Since f divides f_0 and f divides $x^d - 1$, we have that f divides f_k, which is equal to

$$g^n - x^l - x^l \cdot (x^{dk} - 1).$$

Thus, again by using Lemma 2.8, we have that $\pi_g(f_k) = n$ for all $k \geqslant 0$. Consequently, $\mathcal{P}_g(n)$ has infinite cardinality. □

Proposition 2.9 can be summarized by saying that, for any $n \geqslant 1$, $\mathcal{P}_g(n)$ is either empty or infinite. Thus, Theorem 2.6 follows immediately from part (2) of Proposition 2.5, Proposition 2.9 and Proposition 2.7. The conclusion we can distil from this section is that the obstacle that remains for the proof of Theorem 1.1 is to establish unconditionally assertion (ii) of Theorem 2.6. This will require further ideas.

3. Primitive periods coprime to the characteristic

As we have just seen, in order to prove the validity of Theorem 1.1 for a given n and a given dynamic polynomial g, it suffices to show that $\mathcal{P}_g(n)$, say, is non-empty. In the present section, we settle directly the assertion of Theorem 1.1 concerning primitive periods n that are coprime to the characteristic p of F. Our method mainly involves character sums and ideas of Cohen [**4**] (see also [**5**]). In fact, these techniques are strong enough even to prove the following theorem: its focus is on *irreducible* polynomials in $\mathcal{P}_g(n)$.

Theorem 3.1. *Let $n \geqslant 1$ be relatively prime to the characteristic p of F. Then $I_F \cap \mathcal{P}_g(n)$ has infinite cardinality.*

We start by giving a brief motivation for assuming at this point that n is not divisible by p and for studying the set $I_F \cap \mathcal{P}_g(n)$.

Let $f \in \mathcal{P}_F$ be relatively prime to g. Recall that $\pi_g(f)$ is the least integer $k \geqslant 1$ such that g^k modulo f is contained in the subgroup generated by x modulo f. Now, assume additionally that f is irreducible, i.e. $f \in I_F$. Let θ be a root of f. Then

$$\pi_g(f) = \min\{k \geqslant 1 \mid g(\theta)^k = \theta^i \text{ for some } i \geqslant 0\}. \tag{3.1}$$

Let $n := \pi_g(f)$. Then, necessarily, n divides $\operatorname{ord}(g(\theta))$, the multiplicative order of $g(\theta)$, which itself is a divisor of $q^d - 1$, where d is the degree of f. Thus, in the above situation, n is relatively prime to p and $F(\theta)$ contains the nth roots of unity. Hence, for a given n, relatively prime to p, we consider extension fields of $F(\zeta_n)$, ζ_n a primitive nth root of unity, and try to find irreducible $f \in \mathcal{P}_F$ such that n is equal to the right-hand side of equation (3.1).

The following conditions, (3.2 *a*) and (3.2 *b*) on an integer n and any integer d such that n divides $q^d - 1$, guarantee that n is the minimum given by the right-hand side of (3.1) and, therefore, is consistent with its designation as $\pi_g(f)$:

$$\operatorname{ord}(\theta) = \frac{q^d - 1}{n}, \tag{3.2 a}$$

$$\gcd\left(\frac{q^d - 1}{\operatorname{ord}(g(\theta))}, n\right) = 1, \quad g(\theta) \neq 0. \tag{3.2 b}$$

By way of explanation, note that (3.2 *a*) implies that $\theta \in E := \mathrm{GF}(q^d)$. Moreover, (3.2 *b*) means that $g(\theta) = \beta^r$, $\beta \in E^*$ (the multiplicative group of E), is false for any divisor $r > 1$ of n, i.e. $g(\theta)$ is not *any kind of nth power in E* (see [**5**]). Furthermore, (3.2 *a*) implies that any non-zero nth power in E is a power of θ. Note also that, if θ is an element of $\bar{F}$ satisfying (3.2), then its minimal polynomial f is an element of $\mathcal{P}_F$ and has degree d. For then, $\operatorname{ord}(g(\theta))$ divides $q^d - 1$ and, if $\operatorname{ord}(\theta)$ divides $q^{d_0} - 1$, where d_0 divides d, then $\operatorname{ord}(g(\theta))$ divides $q^{d_0} - 1$. Moreover, from (3.2 *a*), n is a multiple of $(q^d - 1)/(q^{d_0} - 1)$ whereas, from (3.2 *b*), n and $(q^d - 1)/(q^{d_0} - 1)$ are relatively prime. Thus $d_0 = d$.

Now the main idea for the proof of Theorem 3.1 is the following. Given $n \geqslant 1$, let $\delta := \operatorname{ord}_n(q)$. We show that there exists a positive integer a_0 such that for all $a \geqslant a_0$ there exists an element θ_a satisfying (3.2) with $d = \delta a$, i.e. $\mu_{\theta_a} \in I_F \cap \mathcal{P}_g(n)$.

We introduce some further notation. Given g, let $N_n^*(d)$ be the number of $f \in \mathcal{P}_F$ having degree d such that (3.1) holds. It follows from the above that

$$N_n^*(d) \geqslant (1/d) \cdot N_n(d), \tag{3.3}$$

where $N_n(d)$ is the number of elements $\theta \in E = \mathrm{GF}(q^d)$ such that (3.2) holds. Given n, d with n dividing $q^d - 1$, write $n = n_1 n_2$, where n_1 and n_2 are relatively prime, the square-free part $\nu(n_1)$ of n_1 is equal to the square-free part of

$$\gcd\left(\frac{q^d-1}{n}, n\right)$$

and

$$\gcd\left(\frac{q^d-1}{n}, n_2\right) = 1.$$

Moreover, let φ be the Euler totient function, μ denote the Möbius function, $\omega(k)$ the number of different prime divisors of k, and $W(k) := 2^{\omega(k)}$ be the number of square-free divisors of k.

Proposition 3.2. *Under the above assumptions we have (except in the trivial case in which* $\deg(g)q^d = 2$*)*

$$N_n(d) = \frac{\varphi((q^d-1)/n_1)\varphi(n_1)}{(q^d-1)n} \cdot (q^d + R), \tag{3.4}$$

where

$$|R| \leqslant n \deg(g) q^{d/2} W(q^d - 1) W(n_1). \tag{3.5}$$

Proof. With the exclusion of the case mentioned in the statement, observe first that (3.5) is weaker than the trivial estimate $|R| \leqslant q^d$ unless

$$q^{d/2} > n \deg(g) W(q^d - 1) W(n_1) \geqslant 2, \tag{3.6}$$

which we henceforth assume.

The proof is along lines such as those of [**4**, Theorem 2.4]. We obtain an expression for $N_n(d)$ by employing the appropriate characteristic functions for the subsets of E satisfying (3.2 a) and (3.2 b), respectively. To describe such functions in generality, temporarily replace E by $F = \mathrm{GF}(q)$ and let e be any divisor of $q - 1$. Then (as used, for example, in [**4**]), for $\beta \in F$,

$$\frac{\varphi(e)}{e} \sum_{r \mid e} \frac{\mu(r)}{\varphi(r)} \sum_{\mathrm{ord}(\chi) = r} \chi(\beta) = \begin{cases} 1, & \text{if } \beta \neq 0 \text{ and } \gcd\left(\dfrac{q-1}{\mathrm{ord}(\beta)}, e\right) = 1, \\ 0, & \text{otherwise,} \end{cases} \tag{3.7}$$

where the sum over χ is over all $\varphi(r)$ multiplicative characters of F of order r. Further, as established in [**3**, Lemma 2], for $\beta \in F$,

$$\frac{\varphi(e)}{q-1} \sum_{s \mid q-1} \frac{\mu(s^*)}{\varphi(s^*)} \sum_{\mathrm{ord}(\eta) = s} \eta(\beta) = \begin{cases} 1, & \text{if } \beta \neq 0 \text{ and } \mathrm{ord}(\beta) = e, \\ 0, & \text{otherwise,} \end{cases} \tag{3.8}$$

where the sum over η is over all multiplicative characters of order s and

$$s^* = s \Big/ \gcd\left(s, \frac{q-1}{e}\right).$$

Returning to the present context, we replace q by q^d in the previous paragraph and set $e = n$ in (3.7) and $e = (q^d - 1)/n$ in (3.8) to yield

$$N_n(d) = \frac{\varphi(n)}{n} \frac{\varphi((q^d-1)/n)}{(q^d-1)} \sum_{r|n} \sum_{s|q^d-1} \frac{\mu(r)}{\varphi(r)} \frac{\mu(s^*)}{\varphi(s^*)} \sum_{\operatorname{ord}(\chi)=r} \sum_{\operatorname{ord}(\eta)=s} S(\chi,\eta), \tag{3.9}$$

where the sums over χ and η are over all multiplicative characters of indicated order, where

$$S(\chi,\eta) = \sum_{\alpha \in E} \chi(g(\alpha))\eta(\alpha), \tag{3.10}$$

and (now)

$$s^* := \frac{s}{\gcd(s,n)}.$$

Since n_2 and $(q^d-1)/n$ are relatively prime, it is easy to see that, in (3.9), $\varphi(n)\varphi((q^d - 1)/n)$ can be replaced with $\varphi(n_1)\varphi((q^d-1)/n_1)$. Furthermore, it is obvious that

$$S(\chi_0,\eta_0) = q^d - m_0 - 1, \tag{3.11}$$

where $m_0 \leqslant m := \deg(g)$ is the number of zeros of g in E, and χ_0, η_0 denote the trivial characters. Otherwise, for characters χ, η not both trivial, we use the consequence of Weil's theorem given in [**4**, Lemma 2.3], namely

$$|S(\chi,\eta)| \leqslant mq^{d/2}. \tag{3.12}$$

(Of course, depending on circumstances, this may be improved.) It follows that $N_n(d)$ has the form (3.4), where

$$q^{-d/2}|R| \leqslant m \sum_{r|n} \sum_{s|q^d-1} \frac{\lambda(r)}{\varphi(r)} \frac{\lambda(s^*)}{\varphi(s^*)} \varphi(r)\varphi(s) =: T_1, \tag{3.13}$$

where $\lambda = \mu^2$, and m is the degree of g. (In particular, the use of (3.13) to bound $|R|$ allows for a contribution of $mq^{d/2}$ from $S(\chi_0,\eta_0)$, which, by (3.6), certainly exceeds the deficiency $m_0 + 1$ in (3.11).) Then, evidently,

$$T_1 = mW(n)T_2,$$

where

$$T_2 := \sum_{s|q^d-1} \frac{\lambda(s^*)\varphi(s)}{\varphi(s^*)}. \tag{3.14}$$

Now, let Q be the part of $q^d - 1$ prime to n. Then, by the multiplicativity of the functions involved, T_2 can be expressed as

$$T_2 = \sum_{t|Q} \lambda(t) \cdot \sum_{u|q^d-1,\ \nu(u)|\nu(n)} \frac{\lambda(u^*)\varphi(u)}{\varphi(u^*)} = W(Q)T_3, \tag{3.15}$$

where the definition of u^* is analogous to that of s^* and, since $\lambda(u^*) = 0$ unless u divides $n\nu(n_1)$,

$$T_3 = \sum_{u|n\nu(n_1)} \frac{\lambda(u^*)\varphi(u)}{\varphi(u^*)}. \tag{3.16}$$

If u divides $n\nu(n_1)$, then u^* divides $\nu(n_1)$. For each divisor v of $\nu(n_1)$ we consider the contribution to T_3 of those divisors u for which $u^* = v$. For this purpose, given the divisor v of $\nu(n_1)$, write $n = l_v m_v$, where $\gcd(l_v, m_v) = 1$, v divides l_v, and $\gcd(v, m_v) = 1$. Then the set of *distinct* divisors u of $n\nu(n_1)$ with $u^* = v$ is the set

$$\{vl_v r \mid r \text{ divides } m_v\}.$$

Moreover, if $u = vl_v r$ is in this set, then

$$\frac{\varphi(u)}{\varphi(u^*)} = l_v\varphi(r).$$

Hence, from (3.16),

$$T_3 = \sum_{v|\nu(n_1)} l_v \sum_{r|m_v} \varphi(r) = \sum_{v|\nu(n_1)} l_v m_v = n \cdot \sum_{v|\nu(n_1)} 1 = nW(n_1). \tag{3.17}$$

Since, by definition of Q, $W(n)W(Q) = W(q^d - 1)$, the result now follows by combining (3.13)–(3.17). This completes the proof. □

We now use Proposition 3.2 to show that $N_n(d)$ and, therefore, $N_n^*(d)$ are generally positive. For this we need some bound on the function $W(N)$. In fact, from [**8**, § 22.10], for any $\varepsilon > 0$,

$$W(N) < N^{(1+\varepsilon)\log(2)\log(\log(N))}, \quad N > N_0(\varepsilon), \tag{3.18}$$

and a form of this bound with an explicit function $N_0(\varepsilon)$ could be derived, for example, from [**12**]. To give an indication of the magnitudes involved we use the following simple result.

Lemma 3.3. *For any positive integer N, we have*

$$W(N) < 5N^{1/4}. \tag{3.19}$$

Proof. The function $V(N) := W(N)/N^{1/4}$ is multiplicative. If $N = l^b$, $b \geqslant 1$, where $l > 16$ is a prime, then $V(N) = 2/N^{1/4} < 1$, whereas if

$$N = 2^{b_2} \cdot 3^{b_3} \cdot 5^{b_5} \cdot 7^{b_7} \cdot 11^{b_{11}} \cdot 13^{b_{13}}$$

with each $b_j \geqslant 0$, then, clearly,

$$V(N) \leqslant V(2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13) < 4.9.$$

Thus everything is proved. □

We are now able to prove the following theorem, from which the assertion of Theorem 3.1 follows immediately.

Theorem 3.4. *Let $g \in \mathcal{P}_F$ and let $n \geqslant 1$ be an integer relatively prime to the characteristic p of $F = \mathrm{GF}(q)$. Suppose that*

$$d \geqslant \frac{4\log(25n\deg(g))}{\log(q)} \tag{3.20}$$

is an integer such that $q^d - 1$ is divisible by n. Then $N_n(d)$ and $N_n^*(d)$ are positive.

Proof. Suppose that $N_n(d) = 0$. Then, from (3.4) and (3.5), using the same notation as in the proof of Proposition 3.2, we have

$$q^{d/2} \leqslant mnW(q^d - 1)W(n_1), \tag{3.21}$$

where $m := \deg(g)$. Let $n_1' = \nu(n_1)$. Then $\omega(n_1) = \omega(n_1')$ and, by the definition of n_1, $(n_1')^2$ divides $q^d - 1$, so that

$$W(q^d - 1) = W\left(\frac{q^d - 1}{n_1'}\right).$$

Hence, by Lemma 3.3, using the multiplicativity of W,

$$q^{d/2} \leqslant mnW\left(\frac{q^d - 1}{n_1'}\right)W(n_1') < 25mnq^{d/4}.$$

This implies that $N_n(d) = 0$ only if $q^{d/4} < 25mn$, i.e. (3.20) does not hold. This is a contradiction. Thus, $N_n(d) > 0$, and the result follows with the aid of (3.3). □

We finally remark that, replacing (3.19) with a more general inequality of the form

$$W(N) < c(\varepsilon)N^{\varepsilon}, \quad \varepsilon > 0,$$

we could replace the factor 4 in (3.20) with $2+\varepsilon$ (at the cost of increasing other constants involved).

4. Primitive periods divisible by the characteristic

Let again $g \in \mathcal{P}_F$, $g \neq 1$, be the dynamic polynomial. In the present section, we consider the additive orders of elements of $\bar{F}$ whose periods are divisible by the characteristic p of F. We use the same notation throughout as in § 2. For $f \in \mathcal{P}_F$, let d_f be the multiplicative order of x modulo f.

Lemma 4.1. *Assume that f is relatively prime to g and that f is square free. Then $\pi_g(f)$ is not divisible by p.*

Proof. Let $n := \pi_g(f)$. From the proof of Proposition 2.9, it is evident that there exists a unique $m < d_f$ such that f divides $g^n - x^m$. Assume that n is divisible by p. Let N be the multiplicative order of g modulo f. By Lemma 2.8 we have that n divides N. Consequently, N is divisible by p and, therefore,

$$g^N - 1 = (g^{N/p} - 1)^p.$$

Since f is assumed to be square free, we deduce that f divides $g^{N/p} - 1$, but this contradicts the definition of N. Consequently, n is prime to p, and the result is proved. □

The converse of Lemma 4.1 is not true. Take, for example, $q = 3 = p$, $g = x^2 + 1$ and $f = x - 1$ or $f = x + 1$. Then $g^2 - x^2 = (x^2 - 1)^2$ is divisible by f^2, whence $\pi_g(f^2)$ divides 2.

Throughout, for $f \in F[x]$, let $\nu(f)$ be the square-free part of f.

Proposition 4.2. *Let $f \in \mathcal{P}_F$ be relatively prime to g. Assume that $\pi_g(f)$ is not divisible by p. Then*

$$\pi_g(\nu(f)) = \pi_g(f). \tag{4.1}$$

Proof. Let $k := \pi_g(\nu(f))$ and $n := \pi_g(f)$. Then $\nu(f)$ divides $g^k - x^m$ for a unique $m < d_{\nu(f)}$. For every $l \geqslant 0$ we have that $\nu(f)^{p^l}$ divides

$$(g^k - x^m)^{p^l} = g^{kp^l} - x^{mp^l},$$

whence, by Lemma 2.8, $\pi_g(\nu(f)^{p^l})$ divides kp^l. Now, choose l such that f divides $\nu(f)^{p^l}$. Then $n = \pi_g(f)$ divides $\pi_g(\nu(f)^{p^l})$. We deduce that n divides kp^l. Since, by assumption, p does not divide n, we conclude that n divides k. But, again by Lemma 2.8, k divides n. Hence $k = n$ and everything is proved. □

The proof of the last result also yields the following.

Lemma 4.3. *Let $f \in \mathcal{P}_F$ be relatively prime to g. Then, for every $k \geqslant 0$, there exists $l \geqslant 0$ such that*

$$\pi_g(f^{p^k}) = \pi_g(f) \cdot p^l.$$

Lemma 4.4. *Let $f \in \mathcal{P}_F$ be relatively prime to g. Assume that $\pi_g(f) = n$ is divisible by p. Let $m < d_f$ be the unique non-negative integer such that f divides $g^n - x^m$. Then m is divisible by p.*

Proof. Assume that m is not divisible by p. Then the derivative of $g^n - x^m$ is equal to mx^{m-1} and is therefore non-zero. Since, by assumption, g is not divisible by x, we see that $g^n - x^m$ and mx^{m-1} are relatively prime. Thus, $g^n - x^m$ is square free. Consequently, f, which is a divisor of $g^n - x^m$ likewise is square free. But, by Lemma 4.1, this is a contradiction to the assumption that n is divisible by p. The lemma is proved. □

We employ a final lemma whose scope, for convenience, extends to polynomials $g \in F[x]$ outside $\mathcal{P}_F$.

Lemma 4.5. *Let $f \in \mathcal{P}_F$ and $g \in F[x]$ be non-constant monic polynomials. Suppose that for every positive integer j, there is an integer m_j such that $g - x^{m_j}$ is divisible by f^{p^j}. Then $g = x^r$ for some $r \geqslant 1$.*

Proof. Let r be the degree of g. For $j \geqslant 2$, we have that

$$x^{m_j} \equiv x^{m_{j-1}} \pmod{f^{p^{j-1}}},$$

and so, since $f^{p^{j-1}} = f_0^{p^{j-2}}(x^p)$, say, then

$$m_j \equiv m_{j-1} \pmod{p}, \quad j \geqslant 2.$$

Let i be such that $0 \leqslant i \leqslant p-1$ and $m_1 + i$ is divisible by p. Then

$$m_j + i \equiv 0 \pmod{p}, \quad j \geqslant 1.$$

Replacing g by gx^i and m_j by $m_j + i$, we may assume that, for all $j \geqslant 1$, p divides m_j. Now there exist monic polynomials h_j in $F[x]$ such that

$$g - x^{m_j} = h_j f^{p^j}, \quad j \geqslant 1. \tag{4.2}$$

Differentiate this expression to yield

$$g' = h_j' f^{p^j} = h_j' f_0^{p^{j-1}}(x^p), \quad j \geqslant 1. \tag{4.3}$$

Now suppose that $p^j > r$. Then (4.3) can hold only if $g' = h_j' = 0$. Thus $h_j' = 0$ for all $j \geqslant 1$. We conclude that $g = g_0(x^p)$, say, and that, for all $j \geqslant 1$, $h_j = \hat{h}_j(x^p)$. It follows that

$$g_0 \equiv x^{\hat{m}_j} \pmod{f_0^{p^j}}, \quad j \geqslant 1,$$

where $\hat{m}_j = m_{j+1}/p$ for $j \geqslant 1$. Moreover, $r_0 := \deg(g_0) = (r+i)/p \geqslant r$ implies that $r(p-1) \leqslant i$, which can only happen if $r = r_0 = 1$ and $i = p-1$. Furthermore, if $r = 1$ and g is the original polynomial (before replacement by $x^i g$), then $x^{p-1}g = g_0(x^p)$ only if $g = x$. Hence, if $r = 1$, the result holds. Otherwise, carry out the above procedure with repetition, as necessary to obtain a sequence of polynomials $g, g_0, g_1, \dots, g_s = x$ of strictly decreasing degree all possessing the same property. Reversing this process, we obtain

$$g_s = x, \quad g_{s-1} = x^{p-i_s} = x^{r_{s-1}} \quad (r_{s-1} \geqslant 1,\ i_s \geqslant 0), \quad \dots,$$

until we reach

$$g_0 = x^{pr_1 - i_1} = x^{r_0}, \quad g = x^{pr_0 - i} = x^r,$$

whence everything is proved. □

In the corollary to Lemma 4.5 which follows, g resumes its role as the dynamic polynomial (in $\mathcal{P}_F$).

Proposition 4.6. *Let $f \in \mathcal{P}_F$ be relatively prime to g. Assume that $\pi_g(f) =: n$ is not divisible by p. Then there exists $k \geqslant 1$ such that $\pi_g(f^{p^k}) \neq n$.*

Proof. Suppose the contrary. Then, for every $j \geqslant 1$, $\pi_g(f^{p^j}) = n$ and, accordingly, for some $m_j \geqslant 0$, $g^n - x^{m_j}$ is divisible by f^{p^j}. We conclude from Lemma 4.5 that $g = x^r$, which contradicts the fact that $g \in \mathcal{P}_F$. This completes the proof. □

By Proposition 4.6, given $f \in \mathcal{P}_F$ we may define $k(f)$, *the p-index of f*, as the least non-negative integer for which $\pi_g(f^{p^k})$ is divisible by p. Of course, $k(f) \geqslant 1$ whenever p does not divide $\pi_g(f)$.

Proposition 4.7. *Let $f \in \mathcal{P}_F$ be relatively prime to g. Assume that $\pi_g(f)$ is not divisible by p. Set $k := k(f)$. Then*

$$\pi_g(f^{p^{k+l}}) = \pi_g(f) \cdot p^{l+1}, \quad \textit{for all } l \geqslant 0. \tag{4.4}$$

Proof. Let $n := \pi_g(f)$ and assume that $\pi_g(f^{p^j}) = np^l$, where $l \geqslant 1$. Define i by $\pi_g(f^{p^{j-1}}) = np^i$.

Consider the unique $m < d_{f^{p^j}} := \operatorname{ord}_{f^{p^j}}(x)$ such that f^{p^j} divides $g^{np^l} - x^m$. By Lemma 4.4, m is divisible by p. Hence,

$$g^{np^l} - x^m = (g^{np^{l-1}} - x^{m/p})^p.$$

Thus, $f^{p^{j-1}}$ divides $g^{np^{l-1}} - x^{m/p}$, whence $\pi_g(f^{p^{j-1}})$ divides np^{l-1} (Lemma 2.8), and, therefore, $i \leqslant l-1$. Conversely, by the definition of i, $f^{p^{j-1}}$ divides $g^{np^i} - x^{m'}$ for some unique $m' < d_{f^{p^{j-1}}}$. Therefore f^{p^j} divides

$$g^{np^{i+1}} - x^{m'p}.$$

Again by Lemma 2.8, $\pi_g(f^{p^j}) = np^l$ divides np^{i+1}. Hence, $i \geqslant l-1$. Consequently, we have proved that

$$\pi_g(f^{p^{j-1}}) = np^{l-1}. \tag{4.5}$$

A similar argument shows that

$$\pi_g(f^{p^{j+1}}) = np^{l+1}. \tag{4.6}$$

The statement now follows by induction. □

Evidently, Proposition 4.7 taken, for example, with Theorem 3.1 and Proposition 2.7 yields the truth of Theorem 1.1 in full generality.

We have, throughout, focused our attention on the latter without discussing details that would surely come within the scope of the theory. These would include an analysis of the p-index $k(f)$ and of square-free non-irreducible f in $\mathcal{P}_g(n)$.

Acknowledgements. During the time of this research, D.H. was a visitor at the University of Glasgow. He thanks the Deutsche Forschungsgemeinschaft for supporting this visit through a Forschungsstipendium. He also thanks the Department of Mathematics of the University of Glasgow for its kind hospitality.

References

1. A. Batra and P. Morton, Algebraic dynamics of polynomial maps on the algebraic closure of a finite field, I, *Rocky Mountain J. Math.* **24** (1994), 453–481.
2. A. Batra and P. Morton, Algebraic dynamics of polynomial maps on the algebraic closure of a finite field, II, *Rocky Mountain J. Math.* **24** (1994), 905–932.
3. L. Carlitz, Sets of primitive roots, *Compos. Math.* **13** (1956), 65–70.
4. S. D. Cohen, Primitive roots and powers among values of polynomials over finite fields, *J. Reine Angew. Math.* **350** (1984), 137–151.
5. S. D. Cohen, Primitive elements and polynomials: existence results, in *Proc. 1st Int. Conf. on Finite Fields and Applications* (ed. G. L. Mullen and P. J.-S. Shiue), Lecture Notes in Pure and Applied Mathematics, vol. 141, pp. 43–55 (Dekker, 1993).
6. D. Hachenberger, *Finite fields: normal bases and completely free elements* (Kluwer, Boston, 1997).
7. D. Hachenberger, *Finite fields: algebraic closure and module structures* (Forschungsbericht, Deutsche Forschungsgemeinschaft, 1997).
8. G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, 5th edn (Oxford University Press, 1979).
9. P. Morton, Periods of maps on irreducible polynomials over finite fields, *Finite Fields Applic.* **3** (1997), 11–24.
10. O. Ore, Contributions to the theory of finite fields, *Trans. Am. Math. Soc.* **36** (1934), 243–274.
11. R. Lidl and H. Niederreiter, *Finite fields* (Addison-Wesley, Reading, MA, 1983).
12. J. B. Rosser and L. Schoenfeld, Approximate formulas for some functions of prime numbers, *Illinois J. Math.* **6** (1962), 64–94.
13. F. Vivaldi, Dynamics over irreducible polynomials, *Nonlinearity* **5** (1992), 941–960.