Actions of Linearized Polynomials on the Algebraic Closure of a Finite Field

By *Stephen D. Cohen*[1]
and *Dirk Hachenberger*[2]

Abstract. Let g and h be monic polynomials in $F[x]$, where F is the finite field of order q. We define a dynamical system by letting the q-linearized polynomial associated with g act on equivalence classes of a certain F-subspace of the algebraic closure $\bar{F}$ of F in which related elements of $\bar{F}$ lie in the same orbit under the action of the q-linearized polynomial associated with h. When $h = x$, this is equivalent to the system in which the dynamic polynomial g acts on irreducible polynomials over F as discussed in [CH], where a conjecture of Morton [M] was proved as regards linearized polynomials. A generalization of that result is proved here. This states that when g and h are non-constant relatively prime polynomials, then there are infinitely many classes with prescribed preperiod and primitive period in the (g, h)-dynamical system.

Mathematics Subject Classification. 11T30, 11T99, 58F22.

Acknowledgements. Parts of this research were done while the second author was a visitor of the first author 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. This paper expands the invited talk of the first author at the 4th International Conference on Finite Fields and Applications at the University of Waterloo, Canada, 12-15 August, 1997. He gratefully acknowledges support from the conference.

[1]Department of Mathematics, University of Glasgow, Glasgow G12 8QW, Scotland, sdc@maths.gla.ac.uk

[2]Institut für Mathematik, Universität Augsburg, 86159 Augsburg, Germany, Hachenberger@math.uni-augsburg.de

1. Introduction

Let $F = \mathrm{GF}(q)$ and $\bar{F}$ be the algebraic closure of F. For any polynomial $f = \sum_i f_i x^i$ in $F[x]$, let $A_q(f)$ be the associated (additive) *q-linearized polynomial* (or simply *q-polynomial*) $\sum_i f_i x^{q^i}$ and set

$$x^f := A_q(f)(x). \tag{1.1}$$

By these means we obtain the set A_F of all q-polynomials. Moreover, A_F acquires a ring structure through addition and *polynomial composition.* Indeed, the association $f \to A_q(f)$ yields a ring isomorphism from $F[x]$ to A_F (see [O] or [LN]).

By the *dynamics* of a mapping γ on a set S is meant all that pertains to the orbits of elements of S under iterates of γ. For $i \geq 0$ let $\gamma^{(i)}$ denote the ith iterate of γ (with $\gamma^{(0)}$ being the identity on S). An element $s \in S$ is called *periodic*, if its orbit $\{\gamma^{(i)}(s) \mid i \geq 0\}$ is finite. If s is periodic and $k \geq 0$ and $n \geq 1$ are minimial such that $\gamma^{(k)}(s) = \gamma^{(k+n)}(s)$, then k is called the *preperiod of* s, while n is called the *primitive period* of s. A periodic element is called *purely periodic* if its preperiod is zero. The *backward orbit* of $s \in S$ is the set of all $t \in S$ for which there exists an $i \geq 0$ such that $\gamma^{(i)}(t) = s$, excluding the members of the orbit of s different from s, if s is purely periodic. We refer to (S, γ) as a *dynamical system.*

In this paper γ will be induced by a monic q-polynomial $A_q(g)$ in which event the above mentioned isomorphism reduces the study of iterates and composites of dynamical mappings to that of powers and products of ordinary polynomials, respectively. For the set S we may, in the first instance, choose $S = \bar{F}$. If $A_q(g)$ acts naturally on S (i.e., by evaluation), it is clear that every element is periodic. Moreover, if g is non-constant, then, given n, there are at most finitely many purely periodic elements of primitive period n: this is because $A_q(g^n - 1)$ is a nonzero polynomial and thus has only finitely many roots. Studies delineating those primitive periods (and preperiods) that can be realized in the dynamical system $(\bar{F}, A_q(g))$ and on other questions relating the dynamical structure to the polynomial and field structures have been undertaken by Batra and Morton [BM1, BM2] and Chou and Cohen [CC] and will not be discussed here in detail.

Nevertheless we elaborate on one aspect of the system just introduced. The subset V_g of $\bar{F}$ comprising the purely periodic elements of $(\bar{F}, A_q(g))$ can be partitioned into equivalence classes under the relation ρ_g defined by the rule that $(\alpha, \beta) \in \rho_g$ if and only if α and β lie in the same orbit under $A_q(g)$ (evidently, this can be done for every dynamical system (S, γ)). For example, if $g = x$ (so that $A_q(x)$ is the Frobenius automorphism $w \to w^q$

on $\bar{F}$), then $V_x = \bar{F}$ and $(\alpha, \beta) \in \rho_x$ if and only if α and β have the same minimal polynomial over F. In fact, if μ_α denotes the minimal polynomial of α over F, then $\alpha \to \mu_\alpha$ induces a bijection between the set V_x/ρ_x of equivalence classes of ρ_x and the set I_F of monic *irreducible* polynomials in $F[x]$. Observe that each $n \geq 1$ occurs as a primitive period. Another case in which $V_g = \bar{F}$ is the trivial one when $g = 1$, i.e., when $A_q(g)$ is the identity map: then V_1/ρ_1 essentially is the same as the set $\bar{F}$. Section 2 will include a more explicit description of the set V_g in general: it is always an F-subspace of $\bar{F}$ which is invariant under the Frobenius automorphism.

For a more general dynamical system, yet one that retains $A_q(g)$ as the dynamical polynomial, let h be another monic polynomial in $F[x]$ and take S to be the set V_h/ρ_h. Since $(\alpha^g)^h = (\alpha^h)^g$, there is a natural action of $A_q(g)$ on V_h/ρ_h: if $\rho_h(\alpha)$ denotes the equivalence class of α, then

$$A_q(g)(\rho_h(\alpha)) := \rho_h(A_q(g)(\alpha)) = \rho_h(\alpha^g) \tag{1.2}$$

is well-defined. In particular, if $h = 1$ we recover the situation discussed above and if $h = x$, then, from the previous paragraph we obtain a system equivalent to that in which the linearized polynomial $G := A_q(g)$ acts on I_F by defining

$$G(\mu_\alpha) := \mu_{\alpha^g}.$$

Such dynamical systems (I_F, G) (in a more general context in which the dynamic polynomial G need not be additive) were introduced by Vivaldi [V]. They were studied more intensively by Batra and Morton [BM1], [BM2], by Morton [M] and by Cohen and Hachenberger [CH]. For these systems the dynamics is richer because, potentially, there are *infinitely* many purely periodic elements of *any* given period. Indeed, in [CH], in establishing a conjecture of Morton [M] in the case of q-polynomials, it was shown that, for g not of the form x^l ($l \geq 0$ an integer), the system $(I_F, A_q(g))$, equivalently $(V_x/\rho_x, A_q(g))$, contains infinitely many elements having prescribed primitive period n (≥ 1) and preperiod k (≥ 0).

In the present paper we consider the general situation with arbitrary monic q-polynomials g and h. For simplicity, we refer to $(V_h/\rho_h, A_q(g))$ as the (g, h)*-(dynamical) system.* In order to extend the above mentioned result of [CH], necessarily, we except those polynomials satisfying a relation of the form $g^r = h^s$ where $r, s \geq 0$ are integers. In particular, we suppose that g and h are non-constant polynomials. In fact, since $A_q(h^i)$ ($i \geq 0$) induces the identity mapping on V_h/ρ_h, the (gh^i, h)-system has the same dynamics as the (g, h)-system. Consequently, we may assume that h does not divide g. Additionally, we impose the further constraint that g and h

are relatively prime, which however may not be altogether necessary. The result is as follows.

Theorem 1.1 *Let g and h be monic and relatively prime non-constant polynomials in $F[x]$. Let $n \geq 1$ and $k \geq 0$ be integers. Then there exist infinitely many classes $\lambda \in V_h/\rho_h$ which, with respect to the action of $A_q(g)$ definied in (1.2), have primitive period n and preperiod k.*

To complete this introduction we mention a simplification. If $g = g_0^l$ ($l \geq 2$), the existence of an element λ in V_h/ρ_h with primitive period ln and preperiod lk with respect to the (g_0, h)-system guarantees that λ has primitive period n and preperiod k in the (g, h)-system. Hence, we may assume that g is a *non-power*, i.e., g is different from g_0^l for $l \geq 2$, an integer.

2. Additive order and its uses

The notion of the additive order or F-order of an element $\alpha \in \bar{F}$ is fundamental to our study. References relevant to the present context are [H1], [CH].

By Section 1, $\bar{F}$ can be interpreted as an $F[x]$-module wherein the action of $f \in F[x]$ on $\alpha \in \bar{F}$ is given by $\alpha^f := A_q(f)(\alpha)$ (see (1.1)). Let $\mathcal{P}_F$ denote the set of all monic polynomials of $F[x]$ which are indivisible by x. The finite $F[x]$-submodules of $\bar{F}$ correspond bijectively to the members of $\mathcal{P}_F$: $f \in \mathcal{P}_F$ corresponds to the set of roots of $A_q(f)$ in $\bar{F}$. Moreover, every finite $F[x]$-submodule is cyclic, i.e., free on one generator. For any $\alpha \in \bar{F}$, the *F-order* or *additive order* of α (denoted by $\mathrm{Ord}_F(\alpha)$) is the polynomial $f \in \mathcal{P}_F$ of least degree for which $\alpha^f = 0$. In particular $\mathrm{Ord}_F(0) = 1$. The generators of the submodule corresponding to $f \in \mathcal{P}_F$ are exactly the elements $\alpha \in \bar{F}$ such that $\mathrm{Ord}_F(\alpha) = f$. There are precisely $\Phi_q(f)$ (> 0) such generators, where Φ_q denotes the finite field Euler function. For more details about $F[x]$-submodules, we refer to [H1, H2].

We state some simple properties of additive orders. For $\alpha, \beta \in \bar{F}$, $\mathrm{Ord}_F(\alpha + \beta)$ is a divisor of $\mathrm{Ord}_F(\alpha) \cdot \mathrm{Ord}_F(\beta)$ with equality if $\mathrm{Ord}_F(\alpha)$ and $\mathrm{Ord}_F(\beta)$ are coprime. A crucial result for the dynamics of linearized polynomials is the following.

Lemma 2.1 *Let $\alpha \in \bar{F}$. If $\mathrm{Ord}_F(\alpha) = f$ and $g \in F[x]$, then $\mathrm{Ord}_F(\alpha^g) = f/\gcd(g, f)$ (where $\gcd$ denotes the greatest common (monic) divisor).* □

Let $h \in F[x]$ be monic. We are now prepared to deduce a description of the subset V_h of $\bar{F}$ comprising exactly the purely periodic elements of the dynamical system $(\bar{F}, A_q(h))$ (see Section 1).

Proposition 2.2 *For any polynomial $h \in F[x]$,*

$$V_h = \{\alpha \in \bar{F} \mid \gcd(\mathrm{Ord}_F(\alpha), h) = 1\}. \tag{2.1}$$

Moreover, V_h is an $F[x]$- submodule of $\bar{F}$.

Proof. Let C_h be the right hand side of (2.1), i.e., the set of all elements $\alpha \in \bar{F}$ whose F-order is coprime to h. If $\alpha \in \bar{F}$ and $f \in F[x]$ then, by Lemma 2.1, the F-order of α^f is a divisor of $\mathrm{Ord}_F(\alpha)$. Thus, C_h is invariant under the action of $A_q(f)$ for all $f \in F[x]$. Now, if $\alpha \in V_h$, then $\alpha^{h^n} = \alpha$ for some integer $n \geq 1$. Thus, a further application of Lemma 2.1 shows that $\alpha \in C_h$. Conversely, if $\alpha \in C_h$, let l be the *multiplicative order of h modulo* $\mathrm{Ord}_F(\alpha)$, i.e., $l \geq 1$ is the least integer such that $h^l - 1$ is divisible by $\mathrm{Ord}_F(\alpha)$. Then $\alpha^{h^l} = \alpha$, whence $\alpha \in V_h$. □

For simplicity, throughout let $M_h := V_h/\rho_h$. As in the proof of Proposition 2.2, Lemma 2.1 shows that, for $\alpha, \beta \in V_h$, $\mathrm{Ord}_F(\alpha) = \mathrm{Ord}_F(\beta)$ whenever $\alpha \in \rho_h(\beta)$. Hence, for any $\lambda \in M_h$, we may define

$$\mathrm{Ord}_F(\lambda) := \mathrm{Ord}_F(\alpha), \text{ where } \alpha \in \lambda. \tag{2.2}$$

This shows that each member of M_h is periodic. We next proceed to demonstrate the pre-eminence of additive order for the preperiod and primitive periods of elements of M_h in the (g, h)-dynamical system for arbitrary polynomials g and h. Clearly, $\lambda = \rho_h(\alpha)$ $(\alpha \in V_h)$ is *purely periodic* if and only if $\alpha^{g^n} = \alpha^{h^l}$ for some integers $n \geq 1$ and $l \geq 0$. In this case the primitive period of λ is the minimal such value of n, denoted by $\pi_{g,h}\{\lambda\}$. Then, clearly,

$$\pi_{g,h}\{\lambda\} = \min\{n \mid \mathrm{Ord}_F(\lambda) \text{ divides } g^n - h^l \text{ for some } l \geq 0\}. \tag{2.3}$$

Combining (2.2) and Lemma 2.1, similarly to the proof of Proposition 2.2, we derive a description of the set $\mathcal{P}_{g,h}$ of purely periodic elements in the (g, h)-system.

Proposition 2.3 *Let $P_{g,h}$ be the set of purely periodic elements of M_h in the (g, h)-system and let $V_{g,h}$ be the union of all $\lambda \in P_{g,h}$ (regarding each such λ as a subset of V_h). Then $V_{g,h} = V_g \cap V_h = V_{gh}$, i.e., $V_{g,h}$ is the set of all $\alpha \in \bar{F}$ whose F-order is coprime to gh.* □

Following Proposition 2.3, for any $n \geq 1$, we define $P_{g,h}(n)$ as the subset of $P_{g,h}$ comprising all elements of primitive period n. From (2.3), if $\lambda \in$

(1) *If* $\nu(g)$ *divides* h, *then* $\mathcal{P}_{g,h} = M_h$.

(2) *If* $\nu(g)$ *does not divide* h, *then for each* $\lambda \in \mathcal{P}_{g,h}$ *and each integer* $k \geq 0$, *there exists an* $\eta \in M_h$ *which has preperiod* k *and satisfies* $A_q(g)^{(k)}(\eta) = \lambda$. □

From now on we shall only consider purely periodic elements and therefore assume that all additive orders f are co-prime to gh. Because of (2.4) we tend to work with F-orders rather than members of $P_{g,h}$.

We finally remark that for the $(g, 1)$-system (with $M_1 = \bar{F}$), Chou and Cohen [CC] further classify the preperiodic structure. Similar details can certainly be set down for the general (g, h)-system.

3. Infinitely many F-orders f with $\pi_{g,h}(f) = n$ from one

Consider a (g, h)-system, where g and h are non-constant monic polynomials over F. Following Section 2, define $\mathcal{P}_{g,h}(n)$ as the set of all F-orders $f \in \mathcal{P}_F$ prime to gh such that $\pi_{g,h}(f) = n$. The aim of this section is to show that, under the assumption of Theorem 1.1, $\mathcal{P}_{g,h}(n)$ is infinite provided it is non-empty.

Observe first that (2.3) and (2.4) can be recast to yield

$$\pi_{g,h}(f) = \min\{n |\, f \text{ divides } g^n - h^l \text{ for some } l \geq 0\,\}. \tag{3.1}$$

Thus, $\pi_{g,h}(f)$ can be interpreted as the group order of $g + fF[x]$ in the group of units $U_f^\times$ modulo f factorized by the subgroup $[h]$ generated by $h + fF[x]$. In fact, our main problem concerning the primitive periods in the (g, h)-system can be formulated as follows.

Given polynomials g, h over F and $n \geq 1$ an integer, do there exist infinitely many $f \in \mathcal{P}_F$, relatively prime to gh, such that the group order of $g + fF[x]$ in $U_f^\times/[h]$ is equal to n?

Lemma 3.1 *Assume that* $f, f^* \in \mathcal{P}_F$ *are relatively prime to* gh. *Let* $n \geq 1$ *and* $m \geq 0$ *be integers. Then the following hold.*

(1) f *divides* $g^n - h^l$ *if and only if* $\pi_{g,h}(f)$ *divides* n.

(2) *If* f *divides* f^*, *then* $\pi_{g,h}(f)$ *divides* $\pi_{g,h}(f^*)$. □

We are now prepared to prove the main result of this section. Note that it is convenient to assume that g and h are coprime.

Theorem 3.2 *Let* g, h *be monic non-constant polynomials in* $F[x]$ *which are relatively prime. Assume that* f *is a polynomial in* $\mathcal{P}_F$ *relatively prime to* gh. *If* $\pi_{g,h}(f) = n$, *then* $\mathcal{P}_{g,h}(n)$ *is infinite.*

Proof. Because $\pi_{g,h}(f) = n$, by (2.3) there exists $m \geq 0$ such that f divides $f_0 := g^n - h^m$. Since g and h are relatively prime, f_0 is prime to gh and therefore a member of $\mathcal{P}_{g,h}$. Moreover, from Lemma 3.1, $\pi_{g,h}(f_0) = n$. Let d be the multiplicative order of h modulo f. For $l \geq 0$, let $f_l := g^n - h^{m+ld}$ (relatively prime to gh). Since f divides both $g^n - h^m$ and $h^d - 1$, it also divides $f_l = g^n - h^m - h^m(h^{ld} - 1)$. Thus, again by Lemma 3.1, $\pi_{g,h}(f_l) = n$ for all l. Since the f_i are all distinct ($i \geq 0$), we conclude that $\mathcal{P}_{g,h}(n)$ is infinite. □

We remark that it follows from Theorem 3.2 that $\mathcal{P}_{g,h}(1)$ is infinite because $\{0\}$ is a member.

4. Irreducible F-orders with primitive period coprime to p

Let p be the characteristic of $F = \mathrm{GF}(q)$. In this section we consider again the (g, h)-system with g and h non-constant and relatively prime as in the statement of Theorem 1.1. Further, without loss of generality (as noted at the end of Section 1), we suppose that g is a *non-power.* The polynomial h, however, may be a power and we define m to be the maximal integer indivisible by p such that $h = h_0^m$ for some $h_0 \in F[x]$. Note that, additionally, h may be a p^eth power for some $e \geq 0$. If $m = 1$ we shall say that h is *at most a p-power.*

Given any n (≥ 1) indivisibe by p we prove directly that $\mathcal{P}_{g,h}(n)$ is infinite (and so certainly non-empty, cf. Theorem 3.2). To accomplish this goal, we seek to enumerate those F-orders f with $\pi_{g,h}(f) = n$ for which f is an *irreducible* polynomial over F of degree d, where n is a divisor of $q^d - 1$ and f is coprime to gh. Let $N_n^*(d)$ be the number of such f. We can take d to be any integer such that the least common multiple of m and n is a divisor of $q^d - 1$.

Suppose f is irreducible of degree d and θ is a root of f. Then $F(\theta) = \mathrm{GF}(q^d) =: F_d$, say. Moreover, by (3.1) we have

$$\pi_{g,h}(f) = \min\{n \mid g^n(\theta) = h^l(\theta) \text{ for some } l \geq 0\}. \tag{4.1}$$

Now, for the next part, suppose that h is at most a p-power. We shall indicate later modifications which treat the general case. Introducing yet one further notion of order - this time the multiplicative order $\mathrm{ord}(w)$ of non-zero elements w of $\bar{F}$ - we consider the relationship to (4.1) of the following conditions involving an element θ of F_d; namely

$$\mathrm{ord}(h(\theta)) = \frac{q^d - 1}{n}, \ h(\theta) \neq 0 \tag{4.2}$$

$$\gcd\left(\frac{q^d-1}{\operatorname{ord}(g(\theta))}, n\right) = 1, \ \ g(\theta) \neq 0. \tag{4.3}$$

Assume that (4.2) and (4.3) hold for $\theta \in F_d$. Suppose, in fact, that $\theta \in F_{d_0}$, where d_0 divides d. Then $g(\theta), h(\theta) \in F_{d_0}$ and $\operatorname{ord}(g(\theta))$ and $\operatorname{ord}(h(\theta))$ are divisors of $q^{d_0}-1$. Hence, from (4.2), n is a multiple of $\frac{q^d-1}{q^{d_0}-1}$, whereas, from (4.3), n is relatively prime to this number. Hence $d = d_0$ and $F_d = F(\theta)$. Consequently, f is irreducible of degree d. Furthermore, (4.2) implies that $h(\theta)$ is a generator of the (cyclic) group of nth powers in F_d^*. Hence $g^n(\theta) = h^l(\theta)$ for some $l \geq 0$. Moreover, (4.3) guarantees that $g(\theta)$ is *not any kind of nth power* in F_d, i.e., $g(\theta) = \beta^e$ for e dividing n implies $e = 1$. Thus, (4.1) holds and $\pi_{g,h}(f) = n$. We conclude that if $N_n(d)$ denotes the cardinality of the subset of F_d satisfying (4.2) and (4.3) then, clearly,

$$N_n^*(d) \geq \frac{1}{d} \cdot N_n(d),$$

and it suffices to show that $N_n(d)$ is positive.

To state our results we repeat some notation from [CH]. Define n_1 as the part of n involving primes common to n and $\frac{q^d-1}{n}$. More precisely, write $n = n_1 n_2$, where n_1 and n_2 are relatively prime, the squarefree part $\nu(n_1)$ of n_1 is equal to the squarefree part of $\gcd(\frac{q^d-1}{n}, n)$ and $\gcd(\frac{q^d-1}{n}, n_2) = 1$.

In this section φ and μ are the regular Euler and Möbius functions, respectively, and, if $\omega(k)$ is the number of distinct prime factors of k, then $W(k) := 2^{\omega(k)}$ is the number of squarefree factors of k.

The crucial result is the following.

Proposition 4.1 *Let g and h be non-constant monic polynomials in $F[x]$, where $F = \mathrm{GF}(q)$. Assume that g and h are relatively prime and that g is a non-power and h at most a p-power. Then, for any integers n (≥ 1) indivisible by the characteristic p of F and d such that n divides $q^d - 1$, we have*

$$N_n(d) = \frac{\varphi(\frac{q^d-1}{n_1})\varphi(n_1)}{(q^d-1)n} \cdot (q^d + R), \tag{4.4}$$

where

$$|R| \leq nMq^{d/2}W(q^d-1)W(n_1) \tag{4.5}$$

and $M = \deg(g) + \deg(h) - 1$. (The trivial case $Mq^d = 2$ is excluded.)

Proof. Employing the characteristic functions E_1 and E_2 for the sets of elements of F_d satisfying (4.3) and (4.2), respectively, we obtain

$$N_n(d) = \sum_{\alpha \in F_d} E_1(\alpha) E_2(\alpha).$$

Here, see e.g., [Co],

$$E_1(\alpha) = \frac{\varphi(n)}{n} \sum_{r|n} \frac{\mu(r)}{\varphi(r)} \sum_{\text{ord}(\chi)=r} \chi(g(\alpha)), \tag{4.6}$$

where the sum over χ is over all $\varphi(r)$ multiplicative characters of F_d of order r. The sum $E_2(\alpha)$ (associated with (4.2)) is rather more awkward but has the shape (taken from Lemma 2 of Carlitz [C]) given by

$$E_2(\alpha) = \frac{\varphi(\frac{q^d-1}{n})}{q^d - 1} \sum_{s|q-1} \frac{\mu(s^*)}{\varphi(s^*)} \sum_{\text{ord}(\eta)=s} \eta(h(\alpha)), \tag{4.7}$$

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

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

Accordingly,

$$N_n(d) = \frac{\varphi(n)}{n} \frac{\varphi(\frac{q^d-1}{n})}{(q^d-1)} \sum_{r|n} \sum_{s|q^d-1} \frac{\mu(r)}{\varphi(r)} \frac{\mu(s^*)}{\varphi(s^*)} \sum_{\text{ord}(\chi)=r} \sum_{\text{ord}(\eta)=s} S(\chi,\eta), \tag{4.8}$$

where $S(\chi, \eta)$ denotes the character sum

$$S(\chi,\eta) = \sum_{\alpha \in F_d} \chi(g(\alpha))\eta(h(\alpha)).$$

Because n_2 and $\frac{q^d-1}{n}$ are relatively prime, it is easy to see that, in (4.8), n_1 may replace n in $\varphi(n)\varphi(\frac{q^d-1}{n})$. But the important step is to estimate the character sums $S(\chi, \eta)$ for the characters which appear in (4.8). Clearly, if $\chi = \chi_0$ and $\eta = \eta_0$ are the trivial characters (of order 1), then

$$S(\chi,\eta) = q^d - M_0, \tag{4.9}$$

where $M_0 \leq M+1$ is the number of zeros of gh in F_d. Otherwise, by Weil's Theorem, see [L] (Chapter 6, Theorem 3, part (1)),

$$|S(\chi,\eta)| \leq Mq^{d/2}. \tag{4.10}$$

At this point it must be emphasized that (4.10) need not be valid for all relevant characters χ, η (not both trivial) if the conditions g, h relatively prime, or h at most a p-power, were to be relaxed and a discussion of the general situation has to overcome such difficulties.

We deduce from (4.8) to (4.10) that $N_n(d)$ has the form (4.4), where

$$q^{-d/2}|R| \leq M \sum_{r|n} \sum_{s|q^d-1} \frac{\lambda(r)}{\varphi(r)} \frac{\lambda(s^*)}{\varphi(s^*)} \varphi(r)\varphi(s) =: T_1 \tag{4.11}$$

and $\lambda = \mu^2$ here denotes Liouville's function. Evidently,

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

where

$$T_2 = \sum_{s|q^d-1} \frac{\lambda(s^*)\varphi(s)}{\varphi(s^*)}. \tag{4.12}$$

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

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

where the definition of u^* is analogous to that of s^* and where

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

since $\lambda(u^*) = 0$ unless u divides $n\nu(n_1)$. Somewhat surprisingly perhaps, T_3 can be evaluated exactly (see [CH]) as

$$T_3 = nW(n_1),$$

leading to a precise evaluation of T_1. Using the fact that $W(n)W(Q) = W(q^d - 1)$ we deduce the bound (4.5) for $|R|$. □

By means of Proposition 4.1 and the explicit bound $W(k) \leq 5k^{1/4}$ (see Lemma 3.3 of [CH]) we obtain the following result which establishes Theorem 1.1 for n indivisible by p and h at most a p-power (because we can choose any value of d larger than the stated bound to guarantee that $\mathcal{P}_{g,h}(n)$ is infinite).

Theorem 4.2 *Let g and h be non-constant monic polynomials in $F[x]$, where $F = \mathrm{GF}(q)$. Assume that g and h are relatively prime and that g is a non-power and h at most a p-power. Then, for any integer n (≥ 1)*

indivisible by the characteristic p of F and any integer d such that n divides $q^d - 1$ and

$$d \geq \frac{4\log(25n^{\frac{5}{4}}M)}{\log(q)}$$

(where $M = \deg(g) + \deg(h) - 1$), we have that $N_n(d)$ and $N_n^*(d)$ are positive. □

To complete this section we outline the modifications to the above discussion when h is a power. Assume $h = h_0^m$ with m indivisible by p as described at the beginning of the section. The other assumed conditions remain in force. In particular, we suppose that $q^d - 1$ is divisible by the least common multiple L of m and n. Let $l := \gcd(n, m)$, then $n' := n/l$ and $m' := m/l$ are relatively prime. We claim that the following extensions of (4.2) and (4.3) guarantee that $\theta \in F_d$ is the root of an irreducible polynomial f of degree d such that (4.1) holds (so that $\pi_{g,h}(f) = n$), they are

$$\operatorname{ord}(h_0(\theta)) = \frac{q^d - 1}{n'}, \ h_0(\theta) \neq 0, \tag{4.13}$$

$$\operatorname{ord}(g(\theta)) \text{ divides } \tfrac{q^d-1}{m'}, \ \gcd(\tfrac{q^d-1}{m'\operatorname{ord}(g(\theta))}, m'n') = 1, \ g(\theta) \neq 0. \tag{4.14}$$

Observe that (4.13) means that $h(\theta)$ generates the Lth powers of F_d^*. Further, (4.14) implies that $g(\theta)$ is an m'th power but no higher power which is a divisor of L. Note that h_0 is at most a p-power and we could carry out a calculation similar to that of Proposition 4.1 to yield a satisfactory estimate for the cardinality of the subset of F_d satisfying (4.13) and (4.14).

An alternative to the above procedure is to replace (4.14) by the more stringent condition

$$\operatorname{ord}(g(\theta)) = \frac{q^d - 1}{m'} \tag{4.15}$$

and employ some of the estimates used in Proposition 4.1.

To illustrate the above, take $n = 12$ and $m = 8$; thus $q^d - 1$ is divisible by $L = 24$. Further $n' = 3$ and $m' = 2$. Also (4.13) means that $h_0(\theta)$ is the cube of a primitive element of F_d. On the other hand, (4.14) implies that $g(\theta)$ is a square but neither a cube nor a 4th power, whereas (4.15) simply means that $g(\theta)$ is the square of a primitive element.

Denote by $N_n'(d)$ the cardinality of the subset of F_d satisfying (4.13) and (4.15). Then, by following the proof of Proposition 4.1, but using a further analogue of (4.12) for T_1 as well as T_2, we obtain an expression for $N_n'(d)$ of the form

$$N_n'(d) = c(q^d + R),\ c > 0,$$

where

$$|R| \leq mnMq^{d/2}W(\frac{q^d-1}{n})W(\frac{q^d-1}{m}).$$

Though this is not the best possible lower bound for $N_n(d)$, it leads to a satisfactory extension of Theorem 4.2 that suffices to establish that $\mathcal{P}_{g,h}(n)$ is infinite for n indivisible by p.

5. Generating F-orders with primitive period divisible by p

Once more consider the (g,h)-system where g and h are non-constant and relatively prime. We know from Sections 3 and 4 that $\mathcal{P}_{g,h}(n)$ is infinite whenever n is indivisible by the characteristic p of $F = \mathrm{GF}(q)$. Given n not divisible by p, we shall show in this section that from any $f \in \mathcal{P}_{g,h}(n)$ can be derived a distinct F-order f_l in $\mathcal{P}_{g,h}(np^l)$ for each $l \geq 1$. As a consequence of this, Theorem 1.1 is completely proved. Assume throughout that f and gh are relatively prime.

First, some remarks are offered on where to look for F-orders with primitive periods divisible by p. In Section 4, for any n indivisible by p, we found *irreducible* polynomials f in $\mathcal{P}_{g,h}(n)$. Although this is far from a comprehensive treatment, it is the case that, in broad terms, such periods are associated with square-free F-orders f.

On the one hand, $\pi_{g,h}(f) = n$ is indivisible by p whenever f is square-free. To justify this, suppose p divides n. Let N be the multiplicative order of g modulo f. Then f divides $g^N - 1$ and so, by the definition of n and Lemma 3.1 (1), n divides N. Consequently, p divides N and f divides $g^{N/p} - 1$ (since f is square-free). This contradicts the definition of N.

On the other hand, if p does not divide n and $f \in \mathcal{P}_{g,h}(n)$, we claim that the square-free part $\nu(f)$ of f also lies in $\mathcal{P}_{g,h}(n)$. To justify this, let $\pi_{g,h}(\nu(f)) = k$ and let f divide $\nu(f)^{p^l}$, where $l \geq 0$. Then $\nu(f)$ divides $g^k - h^m$, say, and so $\nu(f)^{p^l}$ divides $g^{kp^l} - h^{mp^l}$. It follows from Lemma 3.1 that $n = \pi_{g,h}(f)$ divides $\pi_{g,h}(\nu(f)^{p^l})$ and the latter divides kp^l. Since n is indivisible by p we conclude that $k = n$.

The above argument also reveals that, if $f \in \mathcal{P}_{g,h}(n)$ and $j \geq 0$ is an integer, then $\pi_{g,h}(f^{p^j})$ is of the form np^{l_j} with $(l_j)_{j \geq 0}$ being an increasing sequence of nonnegative integers. Thus it is sensible to search for members of $\mathcal{P}_{g,h}(np^l)$ of the form f^{p^j}. The key result is as follows.

Proposition 5.1 *Let g and h be relatively prime and monic polynomials in $F[x]$ of degree at least 1. Let $n \geq 1$ be an integer and assume that $\pi_{g,h}(f)$ divides n where $f \in \mathcal{P}_f$ is relatively prime to gh. Then there exists a power $P > 1$ of the characteristic p of F such that $\pi_{g,h}(f^P)$ does not divide n.*

Proof. Observe first that by (1) of Lemma 3.1, if $k = \pi_{g,h}(f)$ divides n, then f divides $g^n - h^m$ for some $m \geq 0$. Now assume by way of contradiction that $\pi_{g,h}(f^P)$ divides n for each power $P \geq 1$ of p. Let $h^m = h_0^{m_0}$, where h_0 is a divisor of h which is not a pth power and analogously let $g^n = g_0^{n_0}$, where g_0 divides g and is not a pth power. Then $\pi_{g_0,h_0}(f^P)$ divides n_0 for each power $P \geq 1$ of p, and therefore the assumption of the proposition is satisfied for the (g_0, h_0)-system, f and $n_0 \geq 1$. From now on, we assume that g and h are not pth powers and shall derive a contradiction.

For a power $P \geq 1$ of p, let $m(P)$ be the unique nonnegative integer bounded by the multiplicative order of h modulo f^P such that $g^n - h^{m(P)}$ is divisible by f^P. Let $r = r(P)$ be the largest power of p dividing $\gcd(n, m(P))$ and write $N := N(P) = n/r$, $M(P) := m(P)/r$. Observe that r is bounded since n is fixed. Moreover, N or $M(P)$ is not divisible by p. We assume that r divides P and let $Q := P/r$. Then f^Q divides $g^N - h^{M(P)}$ as well as $g^{nQ} - h^{m(1)Q}$. Consequently, letting for simplicity $M = M(P)$ and $m = m(1)$, f^Q divides

$$A = A(P) := -(g^N - h^M)g^{nQ-N} + g^{nQ} - h^{mQ} = h^M g^{nQ-N} - h^{mQ}.$$

If $a \in F[x]$ is such that $A = af^Q$ and Q is larger than 1, then the formal derivative A' of A is equal to

$$A' = a'f^Q = h^{M-1}g^{nQ-N-1}(Mh'g - Ng'h).$$

If $B(P) := Mh'g - Ng'h \neq 0$ then $A' \neq 0$, whence the relative primeness of f and gh implies that f^Q divides $B(P)$. Since the degree of $B(P)$ is bounded for all P, this gives a contradiction for sufficiently large P (and Q). Thus, $B(P) = 0$ for large P, which we now assume. If $M \equiv 0 \bmod p$ then p does not divide N and therefore $g'h = 0$, whence $g' = 0$. This is a contradiction to the assumptions that $\deg(g) \geq 1$ and that g is not a pth power. Similarly, if $N \equiv 0 \bmod p$, then p does not divide M and therefore $h'g = 0$, whence $h' = 0$. Again, this is a contradiction. We deduce that p does not divide NM and therefore $h'g = \gamma g'h$ for some nonzero $\gamma \in F$. But this cannot happen, as g and h are assumed to be relatively prime and neither g' nor h' is zero. This completes the proof of Proposition 5.1. □

We now resume the discussion of the (g, h)-system described at the beginning of the section. Assume from now on that $f \in \mathcal{P}_{g,h}(n)$ for a given $n \geq 1$

(we know the existence of f when n is indivisible by p). An application of Proposition 5.1 shows that there exists an integer $j \geq 1$ such that $\pi_{g,h}(f^{p^j})$ does not divide n. In fact, $\pi_{g,h}(f^{p^j}) = np^l$ for some $l \geq 1$. Now let $\kappa(f)$ be the *p-index of* f, i.e., the least integer $k \geq 1$ such that np divides $\pi_{g,h}(f^{p^k})$. Then it is clear that $f_1 := f^{\kappa(f)} \in \mathcal{P}_{g,h}(np)$. If, by induction, $f_i \in \mathcal{P}_{g,h}(np^i)$ for some $i \geq 1$, then $f_{i+1} := f_i^{\kappa(f_i)} \in \mathcal{P}_{g,h}(np^{i+1})$. This finally completes the proof of Theorem 1.1, since $\mathcal{P}_{g,h}(n)$ is known to be nonempty (in fact infinite) if p does not divide n.

Nevertheless for h not a pth power, we give a final result representing a more precise version of the above. There is also a small restriction of f, namely that its degree be at least that of h.

Theorem 5.2 *Let g and h be monic non-constant polynomials over F which are relatively prime. Assume that h is not a pth power. Assume further that, for a given n, $f \in \mathcal{P}_{g,h}(n)$ and $\deg(f) \geq \deg(h)$. Let $\kappa := \kappa(f)$ be the p-index of f. Then*

$$\pi_{g,h}(f^{p^{\kappa+l}}) = np^{l+1} \text{ for all } l \geq 0. \tag{5.1}$$

Proof. The condition on h means that h' is non-zero. By the definition of κ, (5.1) is valid for $l = 0$. Assume by induction that the assertion holds for all $j \leq l$ and some $l \geq 0$. Assume further that, for some $c \in F[x]$ and some $m \geq 0$,

$$cf^{p^{\kappa+l+1}} = g^{np^{l+1}} - h^m.$$

Differentiating, we obtain that $f^{p^{\kappa+l}}$ divides $mh^{m-1}h'$. Using the facts that f and h are relatively prime and $\deg(f) \geq \deg(h)$, we deduce that m is divisible by p. Thus, $f^{p^{\kappa+l}}$ divides $g^{np^l} - h^{m/p}$, a contradiction to $\pi_{g,h}(f^{\kappa+l}) = np^{l+1}$. This completes the proof. □

References

[BM1] *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.

[BM2] *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.

[C] *L. Carlitz*, Sets of primitive roots, Compos. Math. **13** (1956), 65-70.

[CC] *W. S. Chou* and *S. D. Cohen*, The dynamics of linearized and sublinearized polynomials on finite fields, Preprint 97/47, University of Glasgow (1997).

[Co] *S. D. Cohen*, Primitive roots and powers among values of polynomials over finite fields, J. reine angew. Math. **350** (1984), 137-151.

[CH] *S. D. Cohen* and *D. Hachenberger*, The dynamics of linearized polynomials, Preprint 97/21, University of Glasgow (1997).

[H1] *D. Hachenberger*, "Finite Fields: Normal Bases and Completely Free Elements", Kluwer Academic Publishers, Boston, 1997.

[H2] *D. Hachenberger*, Finite fields: algebraic closure and module structures, Forschungsbericht, Deutsche Forschungsgemeinschaft (1997).

[L] *W. C. W. Li*, "Number Theory with Applications", World Scientific, 1996.

[LN] *R. Lidl* and *H. Niederreiter*, "Finite Fields", Addison-Wesley, Reading, Massachusetts, 1983.

[M] *P. Morton*, Periods of maps on irreducible polynomials over finite fields, Finite Fields and Their Applications **3** (1997), 11-24.

[O] *O. Ore*, Contributions to the theory of finite fields, Trans. Amer. Math. Soc. **36** (1934), 243-274.

[V] *F. Vivaldi*, Dynamics over irreducible polynomials, Nonlinearity **5** (1992), 941-960.