Proceedings of the Edinburgh Mathematical Society (2025) **68**, 795–810
doi:10.1017/S0013091525000173

ITERATING ADDITIVE POLYNOMIALS OVER FINITE FIELDS

LUCAS REIS

Departamento de Matemática, Universidade Federal de Minas Gerais, Belo Horizonte, MG, Brazil

Email: lucasreismat@gmail.com

(Received 3 September 2023)

Abstract Let q be a power of a prime p, let $\mathbb{F}_q$ be the finite field with q elements and, for each nonconstant polynomial $F \in \mathbb{F}_q[X]$ and each integer $n \geq 1$, let $s_F(n)$ be the degree of the splitting field (over $\mathbb{F}_q$) of the iterated polynomial $F^{(n)}(X)$. In 1999, Odoni proved that $s_A(n)$ grows linearly with respect to n if $A \in \mathbb{F}_q[X]$ is an additive polynomial not of the form aX^{p^h}; moreover, if $q = p$ and $B(X) = X^p - X$, he obtained the formula $s_B(n) = p^{\lceil \log_p n \rceil}$. In this paper we note that $s_F(n)$ grows at least linearly unless $F \in \mathbb{F}_q[X]$ has an exceptional form and we obtain a stronger form of Odoni's result, extending it to affine polynomials. In particular, we prove that if A is additive, then $s_A(n)$ resembles the step function $p^{\lceil \log_p n \rceil}$ and we indeed have the identity $s_A(n) = \alpha p^{\lceil \log_p \beta n \rceil}$ for some $\alpha, \beta \in \mathbb{Q}$, unless A presents a special irregularity of dynamical flavour. As applications of our main result, we obtain statistics for periodic points of linear maps over $\mathbb{F}_{q^i}$ as $i \to +\infty$ and for the factorization of iterates of affine polynomials over finite fields.

Keywords: dynamics over finite fields; additive polynomials; factorization of polynomials

2020 Mathematics subject classification: Primary 11T55
Secondary 37P05

1. Introduction

Given a field K, a polynomial $F \in K[X]$ and a positive integer n, let $F^{(n)}(X)$ be the n-th fold composition of F with itself. Some past works have dealt with polynomials F in which the iterates $F^{(n)}(X)$ present special factorization over K: see [2, 3, 18]. The main case of study is when all the iterates $F^{(n)}(X), n \geq 1$ are irreducible over K: such polynomials are called *stable*. There are a few constructions of stable polynomials [7, 19], where the field of coefficients K is a number field or a function field. In [19], Odoni proves the stability of 'generic' additive polynomials with coefficients in a function field and compute the Galois group of the iterates of such polynomials. Recall that a polynomial $f \in K[X]$ is additive if the identity $f(X+Y) = f(X) + f(Y)$ holds in the polynomial ring $K[X, Y]$. If K has positive characteristic p, the additive polynomials in $K[X]$ are precisely those of the form $\sum_{i=0}^{h} a_i X^{p^i}$ with $a_i \in K$. However, in the case where K is finite, such polynomials are usually not stable. In fact, no *affine polynomial* (i.e., $A(X) + b$ with $A(X)$ additive and

© The Author(s), 2025. Published by Cambridge University Press on Behalf of The Edinburgh Mathematical Society

https://doi.org/10.1017/S0013091525000173 Published online by Cambridge University Press

$b \in K$) of degree at least 2 can be stable if K is finite: see Theorem 10 in [1] for more details.

The stability of polynomials over finite fields has been explored primarily in the case of quadratic polynomials. A relaxation of stable polynomials is considered in [13], yielding the so-called *settled polynomials*. A more general problem on the factorization of $F^{(n)}(X)$ is proposed in [5] in the case where K is finite. In particular, the problem suggests to explore some arithmetic functions associated with $F^{(n)}(X)$ such as the degrees of the irreducible factors (largest, average) and the number of irreducible factors. For more details, see Question 18.9 in [5]. Many issues related to Question 18.9 were eariler discussed in [9] and, more recently, in [24].

Still in the finite field setting, an arithmetic function that can be considered is $s_F(n)$, the smallest positive integer such that $F^{(n)}(X)$ splits completely over $\mathbb{F}_{q^{s_F(n)}}$. For instance, F is stable if and only if $s_F(n) = \deg(F)^n$ for every $n \geq 1$. As previously mentioned, in [1] the authors prove that no affine polynomial of degree at least 2 and with coefficients in a finite field can be stable. In [20], Odoni proved something much stronger for additive polynomials: if $A \in \mathbb{F}_q[X]$ is an additive polynomial not of the form aX^{p^h}, then $s_A(n)$ grows linearly with respect to n. More precisely, he proved that the sequence $\{s_A(n) \cdot n^{-1}\}_{n\geq 1}$ is bounded and its set of limit points equals $[\alpha_A, p\alpha_A]$ for some $\alpha_A > 0$. For more details, see Theorem 2 in [20]. Odoni's result implies a refined information on the factorization of iterated additive polynomials: the iterates of additive polynomials typically split into many distinct irreducible factors, all of small degree. He ends the paper with an interesting example, where the constant α_A is explicitly computed: if $q = p$, then $s_{X^p-X}(n) = p^{\lceil \log_p n \rceil}$ for every $n \geq 1$ and, in particular, $\alpha_{X^p-X} = 1$.

Odoni's proof on the growth of $s_A(n)$ with A additive relies on transferring the problem to the skew polynomial ring $\mathbb{F}_q[X, \sigma]$: this is a natural model for the ring of additive polynomials (with respect to the ordinary sum and composition of polynomials). In this approach, the problem of computing $s_A(n)$ translates into computing valuations of elements in $\mathbb{F}_q[X, \sigma]$ with respect to some ideals of the same ring. However, the latter is quite nontrivial: since the ring $\mathbb{F}_q[X, \sigma]$ is not commutative, we no longer have many useful factorization properties of elements and ideals. In particular, the computations in the paper are involved and technical. Moreover, in his approach, he only deals with a subsequence $\{s_A(n\nu) \cdot (n\nu)^{-1}\}_{n\geq 1}$ with fixed $\nu \in \mathbb{N}$, noticing that such subsequence controls the oscilation of the whole sequence. We actually believe that he was trying to derive a simple closed formula like the one $s_{X^p-X}(n) = p^{\lceil \log_p n \rceil}$ for $q = p$. For more details, see sections 3–5 of [20].

In this paper, we study the function $s_A(n)$ in more detail and recover Odoni's results in a richer form. In particular, we prove that in many cases we have $s_A(n) = \alpha p^{\lceil \log_p \beta n \rceil}$ if n is sufficiently large, where $\alpha, \beta \in \mathbb{Q}$ do not depend on n and can explicitly be obtained from some initial values $s_A(1), \ldots, s_A(s_0)$. We also derive a weaker result for affine polynomials $A(X) + b$ and, in particular, we prove that the degree of the splitting fields of the iterates of such polynomials also presents linear growth. The latter is a major obstruction in Odoni's approach: there is no identification of affine polynomials in the polynomial ring $\mathbb{F}_q[X, \sigma]$. Before we state our main results, we comment that the linear growth is the slowest possible growth for the the degree of the splitting field of 'generic' iterated polynomials.

https://doi.org/10.1017/S0013091525000173 Published online by Cambridge University Press

Remark 1.1. Let $\mathbb{F}_q$ be a finite field of characteristic p and assume that $F \in \mathbb{F}_q[X]$ is not of the form $aX^s + b$, where $a \in \mathbb{F}_q^*$ and either $b = 0$ or $b \neq 0$ and $s = p^h$ with $h \geq 0$. According to Corollary 2.5 of [24], there exists an absolute constant $c_F > 0$ such that, for every positive integer n, the polynomial $F^{(n)}(X)$ contains an irreducible factor over $\mathbb{F}_q$ with degree at least $c_F \cdot n$. The latter readily implies that $\frac{s_F(n)}{n} \geq c_F$ for every $n \geq 1$. If $F(X) = aX^s + b$ with $a \in \mathbb{F}_q^*$ and either $b = 0$ or $b \neq 0$ and $s = p^h$ with $h \geq 0$, it is direct to verify that $s_F(n) = 1$ for every $n \geq 1$. In particular, these polynomials are genuine exceptions.

Our main result goes as follows.

Theorem 1.2. *Let q be a power of a prime p, let $A(X) \in \mathbb{F}_q[X]$ be an additive polynomial not of the form aX^{p^h} and, for each $b \in \mathbb{F}_q^*$, set $A_b(X) = A(X) + b$. Then the following hold:*

(i) *for every $n \geq 1$, we have $s_A(np) \in \{s_A(n), p \cdot s_A(n)\}$ and, in particular, there exists $0 \leq i < \log_p n + 1$ such that*

$$s_A(n) = s_A(1) \cdot p^i. \tag{1}$$

(ii) *for every $b \in \mathbb{F}_q^*$ and every $n \geq 1$, we have $s_{A_b}(n) \in \{s_A(n), p \cdot s_A(n)\}$;*

(iii) *the sequence $\left\{\frac{s_A(n)}{n}\right\}_{n\geq 1}$ is bounded and its set of limit points equals $[c_A, pc_A]$ for some $c_A > 0$;*

(iv) *if c_A is as in the previous item, the sequence $\left\{\frac{s_{A_b}(n)}{n}\right\}_{n\geq 1}$ is bounded and its set of limit points is contained in the interval $[c_A, p^2 c_A]$;*

(v) *$c_{A^{(k)}} = k \cdot c_A$ for every $k \geq 1$.*

Moreover, for $s_0 = \max\{j > 0 : s_A(j) = s_A(1)\}$, there exists $A_* \in \mathbb{F}_q[X]$ of the form R^q with $R \in \mathbb{F}_q[x]$ additive and an integer $r \geq 1$ such that

$$(X^{q^{s_A(1)}} - X)^{q^r} = X^{q^{s_A(1)+r}} - X^{q^r} = A_*(A^{(s_0)}(X)).$$

In particular, $c_A \leq \frac{s_A(1)}{s_0}$ with equality if and only if the $\mathbb{F}_p$-linear map $z \mapsto A_*(z)$ is not nilpotent over $\mathbb{F}_{q^{s_A(1)}}$. In the case of equality, we also have

$$s_A(n) = s_A(1) p^{\left\lceil \log_p \frac{n}{s_0} \right\rceil}, \; n > s_0. \tag{2}$$

Next we provide one numerical example, showing the applicability of Theorem 1.2.

Example 1.3. Let $\alpha \in \mathbb{F}_4$ be such that $\alpha^2 = \alpha + 1$ and set $A(X) = X^8 + \alpha X \in \mathbb{F}_4[X]$. A direct computation yields $s_A(1) = 3$ and $s_A(2) = 6$, hence $s_0 = 1$. Moreover, the polynomial $A_*(X) = X^{32} + \alpha^2 X^4 = (X^8 + \alpha^2 X)^4$ satisfies

https://doi.org/10.1017/S0013091525000173 Published online by Cambridge University Press

$$A_*(A(X)) = X^{256} - X^4.$$

It is direct to verify that, in this case, the map $z \mapsto A_*(z)$ is not nilpotent over $\mathbb{F}_{4^3}$. Theorem 1.2 implies $c_A = 3$ and

$$s_A(n) = 3p^{\lceil \log_p n \rceil}, n \geq 2.$$

Remark 1.4. In the context of Theorem 1.2 we see that Eq. (2) provides a simple closed formula for $s_A(n)$ whenever the companion polynomial $A_*(X)$ does not induce a nilpotent linear map over the splitting field of $A(X)$. Additive polynomials yielding nilpotent linear maps over extensions of finite fields were previously introduced and explored by the author in [22]. However, we discuss other issues there, namely, the construction and cycle decomposition of permutation polynomials arising from nilpotent additive polynomials. Nevertheless, such polynomials yield very special dynamical systems over finite fields: if $N \in \mathbb{F}_q[X]$ is additive such that $z \mapsto N(z)$ is nilpotent over $\mathbb{F}_{q^M}$, then $0 \in \mathbb{F}_{q^M}$ is the only periodic point under this map. In particular, the corresponding directed graph representation of the map $z \mapsto N(z)$ over $\mathbb{F}_{q^M}$ (called *functional graph*) contains only one connected component. In the proof of Theorem 1.2 we prove that the condition on $A_*(X)$ being nilpotent is also equivalent to the following: for each positive integer n, there exists $k = k(n)$ such that $A_*^{(k(n))}(X)$ is divisible by $A^{(n)}(X)$. Since A, A_* are additive, we have that $A_*(0) = A(0) = 0$ and so the latter implies that $A^{-\infty}(0) \subseteq A_*^{-\infty}(0)$. Here, for a polynomial $F \in \mathbb{F}_q[X]$, the set

$$F^{-\infty}(0) = \bigcup_{j \geq 0} \{y \in \overline{\mathbb{F}}_q \, : \, F^{(j)}(y) = 0\}$$

is just the *reversed orbit* of 0 under the map $z \mapsto F(z)$ over $\overline{\mathbb{F}}_q$.

If we assume that $A(X) \in \mathbb{F}_q[X]$ is of the form $\sum_{i=0}^{m} a_i X^{q^i}$, we directly obtain an explicit formula for $s_A(n)$ like the one given in equation (2): in particular, we can compute the constant c_A. The latter generalizes the case $A(X) = X^p - X$ given by Odoni and, in fact, it covers the class of additive polynomials A with coefficients in $\mathbb{F}_p[X]$ (i.e., we are simply considering the case $q = p$). For more details, see Theorem 4.1.

As applications of Theorem 1.2, we also provide statistics for the factorization of iterated affine polynomials and for the number of periodic points under maps $z \mapsto A(z)$ with A additive. First, we need the following definition.

Definition 1.5. *For each nonconstant polynomial $F \in \mathbb{F}_q[X]$ and each positive integer n, let $N_F(n)$ be the number of distinct irreducible factors of $F^{(n)}(X)$ over $\mathbb{F}_q$. Moreover, if $f_{1,n}, \ldots, f_{N_F(n),n} \in \mathbb{F}_q[X]$ are the distinct irreducible factors of $F^{(n)}(X)$ over $\mathbb{F}_q$, we set*

$$\rho_F(n) = \frac{1}{N_F(n)} \sum_{i=1}^{N_F(n)} \deg(f_{i,n}),$$

the average degree of the $f_{i,n}$s.

https://doi.org/10.1017/S0013091525000173 Published online by Cambridge University Press

In the following theorem, we prove that $\rho_B(n)$ also grows linearly with respect to n if B is a generic affine polynomial.

Theorem 1.6. *Let $A \in \mathbb{F}_q[X]$ be an additive polynomial that is not of the form aX^{p^h}, fix $b \in \mathbb{F}_q$ and set $B(X) = A(X) + b$. Then there exists $\alpha_B, \beta_B > 0$ such that $\frac{\rho_B(n)}{n} \in [\alpha_B, \beta_B]$ for every $n \geq 1$.*

Proposition 5.18 in [24] essentially proves Theorem 1.6 in the case where $A(X)$ is of the form $\sum_{i=0}^{m} a_i X^{q^i}$. However, this case is much simpler since we can even describe the degree distribution of the irreducible factors of $A^{(n)}(X)$ over $\mathbb{F}_q$. In particular, the techniques employed there cannot be extended to arbitrary additive polynomials. See § 5.2 in [24] for more details.

The following theorem entails that the proportion of periodic points under additive polynomial maps is, in general, irregular through the finite extensions of $\mathbb{F}_q$.

Theorem 1.7. *Let $A \in \mathbb{F}_q[X]$ be an additive polynomial, and for each integer n, let $\pi_A(n)$ be the number of elements in $\mathbb{F}_{q^n}$ that are periodic under the map $z \mapsto A(z)$. Then the limit*

$$\lim_{n\to\infty} \frac{\pi_A(n)}{q^n}$$

does not exist unless $A(X) = aX^{p^h}$ for some $a \in \mathbb{F}_q$ and some $h \geq 0$. In the latter case, the limit equals 0 if $a = 0$ and equals 1 if $a \neq 0$.

Observe that $\frac{\pi_A(n)}{q^n}$ is just the *proportion* of points in $\mathbb{F}_{q^n}$ that are periodic with respect to the map $z \mapsto A(z)$. The latter can be considered in a more general context, where A is replaced by a generic polynomial $F \in \mathbb{F}_q[X]$. Very little is known on the behaviour of $\frac{\pi_F(n)}{q^n}$: some related problems are considered in [10, 12]. More recently, in [6] the proportion of periodic points is explored in the case of quadratic maps over the projective space $\mathbb{P}^1(\mathbb{F}_{q^n})$, where the analogue limit equals zero (up to some exceptional cases). An earlier work [16] explored the proportion of periodic points for the case of monomials and Chebyshev polynomials. In particular, for these two classes of polynomials, the corresponding limit does not exist in general. Along with monomials and Chebyshev polynomials, additive polynomials have *wild* dynamical behaviour. For instance, these three families of polynomials cover most of the known *exceptional polynomials* (i.e., polynomials whose induced map permute infinitely many finite extensions of $\mathbb{F}_q$). For more details on exceptional polynomials, see § 8.4 of [17].

It is worth mentioning that the dynamics of Chebyshev polynomials and monomials are well understood by means of their *functional graphs* (a directed graph representation of the iteration of maps). In fact, the results in [21] imply a simple description of the graphs for such polynomials and also for some special additive polynomials. On the other hand, the dynamics of arbitrary additive polynomials over finite fields is only well understood from the Linear Algebra point of view: see [4, 8, 11, 14, 25]. Our proof for Theorem 1.7 relies on finding finite extensions of $\mathbb{F}_q$ containing a small/large number of roots of the iterates of A. However, we do not obtain a complete description of the

https://doi.org/10.1017/S0013091525000173 Published online by Cambridge University Press

dynamics of the map $z \mapsto A(z)$. Instead, those extensions are detected by employing item (i) of Theorem 1.2, combined with Theorem 4.2, a general basic result on the structure of periodic points of linear maps over finite fields. In particular, we prove that, as $n \to \infty$, the quotient $\frac{\pi_A(n)}{q^n}$ must oscilate between zero and a positive constant unless $A(X) = aX^{p^h}$ for some $a \in \mathbb{F}_q$ and some $h \geq 0$.

In the proof of our results we employ many arithmetic properties of additive polynomials, regarding them not only as elements of the polynomial ring $\mathbb{F}_q[X]$ but also as maps over the algebraic closure $\overline{\mathbb{F}}_q$ of $\mathbb{F}_q$. A crucial tool is lemma 2.1, where we compile many elementary results on the composition of additive polynomials over finite fields, including some commuting properties.

We end this section with the structure of the paper. In § 2, we provide basic machinery, and in § 3, we prove our main result, Theorem 1.2. Finally, in § 3.1, we provide an enhanced version of Theorem 1.2 that applies to a subclass of additive polynomials, along with some applications of the same theorem.

2. Preparation

For the rest of this paper, we fix q a power of a prime p. In this short section we provide two technical lemmas that will be frequently employed.

Lemma 2.1. *Let $A, B \in \mathbb{F}_q[X]$ be additive polynomials with $A(X)$ nonzero. Then $A(X)$ divides $B(X)$ if and only if there exists another additive polynomial $C \in \mathbb{F}_q[X]$ such that $B(X) = C(A(X))$. Moreover, if $B(X) = C(A(X))$ and $B(X) = \sum_{i=0}^{s} a_i X^{q^i}$ for some $a_i \in \mathbb{F}_p$, then the following holds:*

(i) *$A(C(X)) = B(X)$, i.e., $A(C(X)) = C(A(X))$;*
(ii) *if $A(X) = A_0^{(k)}(X)$ for some $k \geq 1$ and some additive $A_0 \in \mathbb{F}_q[X]$, then $A_0(C(X)) = C(A_0(X))$.*

Proof. The first statement is a routine exercise and can be proved, for instance, by induction on the degree of B; see also Exercise 3.68 in [15]. For the proof of item (i), it suffices to prove that $A(X)$ and $B(X)$ commute. In fact, in this case, the equality $B(X) = C(A(X))$ implies that

$$B(A(X)) = A(B(X)) = A(C(A(X))),$$

and so by setting $Y = A(X)$, we obtain the polynomial identity $B(Y) = A(C(Y))$. The fact that $A(X)$ and $B(X)$ commute follows by induction on the number of nonzero coefficients in $A(X)$, so we omit details. Item (ii) follows in a similar way, noticing that the polynomials $A_0(X)$ and $B(X)$ commute. □

Given a polynomial $f(X) = \sum_{i=0}^{r} a_i X^i \in \mathbb{F}_q[X]$, set $L_f(X) = \sum_{i=0}^{r} a_i X^{q^i}$. The polynomial $L_f(X)$ is commonly known as the *q-linearized associate* with $f(X)$. The following lemma is easily verified.

https://doi.org/10.1017/S0013091525000173 Published online by Cambridge University Press

Lemma 2.2. *For $f, g \in \mathbb{F}_q[X]$, the following holds:*

(a) $L_{f+g}(X) = L_f(X) + L_g(X)$;
(b) $L_{fg}(X) = L_f(L_g(X))$. *In particular, for every $n \geq 1$, we have $L_f^{(n)}(X) = L_{f^n}(X)$.*
(c) $L_c(X) = cX$ *for every $c \in \mathbb{F}_q$.*

3. Proof of Theorem 1.2

In this section we prove our main result. We fix the following important notation: for integers $r, s \geq 0$ with $s > 0$, set

$$\mathcal{S}_{s,r}(X) = X^{q^{s+r}} - X^{q^r} = (X^{q^s} - X)^{q^r}.$$

Lemma 2.2 implies the following important identity that will be further used: for every integer $i \geq 0$,

$$\mathcal{S}_{s,r}^{(p^i)}(X) = \mathcal{S}_{sp^i, rp^i}(X). \tag{3}$$

We have the following auxiliary result.

Lemma 3.1. *Let $A \in \mathbb{F}_q[X]$ be a nonzero additive polynomial, and let j be a positive integer. Then the following are equivalent:*

(i) *$A(X)$ splits completely in $\mathbb{F}_{q^j}$;*
(ii) *$A(X)$ divides $\mathcal{S}_{j,r}(X)$ for some $r \geq 0$;*
(iii) *there exist $r \geq 0$ and an additive polynomial $B \in \mathbb{F}_q[X]$ such that $B(A(X)) = \mathcal{S}_{j,r}(X)$.*

Moreover, if A is separable, we can assume that $r = 0$.

Proof. For the implication (i)→(ii), assume that $A(X)$ splits completely in $\mathbb{F}_{q^j}$. Hence every irreducible divisor of $A(X)$ over $\mathbb{F}_q$ divides $X^{q^j} - X$. Take r large enough so that, in the factorization of $A(X)$ over $\mathbb{F}_q$, no irreducible factor has multiplicity greater than q^r. Hence $A(X)$ divides $(X^{q^j} - X)^{q^r} = \mathcal{S}_{j,r}(X)$. The implication (ii)→(iii) follows directly by lemma 2.1. For the implication (iii)→(i), assume that $B(A(X)) = \mathcal{S}_{j,r}(X)$. Again, from lemma 2.1, it follows that $A(X)$ divides $\mathcal{S}_{j,r}(X) = (X^{q^j} - X)^{q^r}$ and so the roots of $A(X)$ are also roots of $X^{q^j} - X$. In other words, $A(X)$ splits completely in $\mathbb{F}_{q^j}$. Finally, if $A(X)$ is separable, then $A(X)$ divides $\mathcal{S}_{j,r}(X) = (\mathcal{S}_{j,0}(X))^{q^r}$ if and only if it divides $S_{j,0}(X)$. □

We end this part with an important remark that is used along the way without further mention. If $A \in \mathbb{F}_q[X]$ is nonzero and additive, then $A(0) = 0$ and so the splitting field of $A^{(n)}(X)$ contains the splitting field of $A^{(j)}(X)$ whenever $1 \leq j \leq n$. In particular, for every $1 \leq j < n$, the number $s_A(j)$ divides $s_A(n)$.

https://doi.org/10.1017/S0013091525000173 Published online by Cambridge University Press

3.1. Proof of Theorem 1.2

We prove the items separately.

(i) Fix $n \geq 1$, and let $\mathbb{F}_{q^K}$ be the splitting field of $A^{(n)}(X)$ over $\mathbb{F}_q$, that is, $s_A(n) = K$. From lemma 2.1, there exist an additive polynomial $B \in \mathbb{F}_q[X]$ and an integer $r \geq 0$ such that

$$B(A^{(n)}(X)) = \mathcal{S}_{K,r}(X), \tag{4}$$

and the polynomials A, B commute. In particular, taking the p-th iterate on both sides of Eq. (4), we obtain

$$B^{(p)}(A^{(np)}(X)) = \mathcal{S}^{(p)}_{K,r}(X) = \mathcal{S}_{pK,pr}(X).$$

From lemma 3.1, the polynomial $A^{(np)}(X)$ splits completely in $\mathbb{F}_{q^{pK}}$. Therefore, $s_A(np)$ divides pK. Recall that, as $np > n$, the number $s_A(np)$ is divisible by $s_A(n) = K$. In particular, we obtain

$$s_A(np) \in \{K, pK\} = \{s_A(n), p \cdot s_A(n)\}.$$

The latter readily implies that $s_A(p^j) \leq s_A(1) \cdot p^j$ for every $j \geq 0$. Recall that $s_A(m)$ divides $s_A(n)$ if $m < n$. In particular, it is clear that for every $n \geq 1$, we have $s_A(n) = s_A(1)p^i$ for some $i \geq 0$. Moreover, if $n \geq 1$ and $j = \lceil \log_p n \rceil < 1 + \log_p n$, we have $n \leq p^j$ and so

$$s_A(n) \leq s_A(p^j) \leq s_A(1) \cdot p^j.$$

(ii) It is direct to verify that there exists a sequence $\{\beta_\ell\}_{\ell \geq 1}$ of elements in $\mathbb{F}_q$ such that $A_b^{(\ell)}(X) = A^{(\ell)}(X) + \beta_\ell$ for every $\ell \geq 1$. Now fix $n \geq 1$, and let $\mathbb{F}_{q^S}$ and $\mathbb{F}_{q^T}$ be the splitting fields of $A_b^{(n)}(X)$ and $A^{(n)}(X)$, respectively. In particular, the roots of $A_b^{(n)}(X)$ comprise an $\mathbb{F}_p$-affine space $\mathcal{L} \subseteq \mathbb{F}_{q^S}$ whose difference set $\mathcal{L} - \mathcal{L} = \{y - z : y, z \in \mathcal{L}\}$ coincides with the set of the roots of $A^{(n)}(X)$. Therefore, the roots of $A^{(n)}(X)$ lie in $\mathbb{F}_{q^S}$ and so T divides S. Conversely, since $A^{(n)}(X)$ splits completely in $\mathbb{F}_{q^T}$, lemma 3.1 entails that $\mathcal{S}_{T,r}(X) = B(A^{(n)}(X))$ for some additive polynomial $B \in \mathbb{F}_q[X]$ and some $r \geq 0$. In particular,

$$\mathcal{S}_{T,r}(X) \equiv -B(\beta_n) \pmod{A_b^{(n)}(X)}.$$

However, recall that $\beta_n \in \mathbb{F}_q$ and $B \in \mathbb{F}_q[X]$, hence $B(\beta_n) \in \mathbb{F}_q$ and so $\mathcal{S}_{T,r}(X)$ vanishes at $-B(\beta_n)$. In conclusion,

$$\mathcal{S}^{(2)}_{T,r}(X) \equiv \mathcal{S}_{T,r}(-B(\beta_n)) \equiv 0 \pmod{A_b^{(n)}(X)}.$$

https://doi.org/10.1017/S0013091525000173 Published online by Cambridge University Press

Since $p \geq 2$, we obtain

$$\mathcal{S}_{Tp,rp}(X) = \mathcal{S}_{T,r}^{(p)}(X) \equiv \mathcal{S}_{T,r}^{(p-2)}(0) \equiv 0 \pmod{A_b^{(n)}(X)}.$$

Observe that, for $y \in \overline{\mathbb{F}}_q$, we have $S_{Tp,rp}(y) = 0$ if and only if $y \in \mathbb{F}_{q^{Tp}}$. Hence $A_b^{(n)}(X)$ splits completely in $\mathbb{F}_{q^{pT}}$ and so S divides pT. Since T divides S, we conclude that $S \in \{T, pT\}$. In other words,

$$s_{A_b}(n) \in \{s_A(n), p \cdot s_A(n)\}.$$

(iii) For simplicity, we write $M = s_A(1)$ and $\gamma_A(n) = \frac{s_A(n)}{n}$. Item (i) entails that $s_A(n) < Mp^{1+\log_p n} = Mpn$ for every $n \geq 1$. In particular, the sequence $\{\gamma_A(n)\}_{n\geq 1}$ is bounded. For each integer $i \geq 0$, item (i) and Remark 1.1 entail that

$$s_i = \max\{j > 0 \,:\, s_A(j) = Mp^i\}$$

is a well defined positive integer. Since $ps_i > s_i$, we obtain $s_A(ps_i) \geq Mp^{i+1}$. Item (i) implies $s_A(ps_i) \leq Mp^{i+1}$ and so $s_A(ps_i) = Mp^{i+1}$. In particular, it follows by the definition that $s_{i+1} \geq ps_i$. The latter combined with the identity $s_A(s_{i+1}) = ps_A(s_i)$ implies that the sequence $\mathbf{\Gamma} := \{\gamma_A(s_i)\}_{i\geq 0}$ is not increasing. Since $A(X)$ is not of the form aX^{p^j}, Remark 1.1 entails that $\mathbf{\Gamma}$ is bounded below by a positive real number. Hence there exists $c_A > 0$ such that

$$\lim_{i\to+\infty} \gamma_A(s_i) = c_A.$$

If n is an integer with $s_i < n \leq s_{i+1}$, then $s_A(n) = Mp^{i+1}$ and so

$$\gamma_A(s_{i+1}) = \frac{Mp^{i+1}}{s_{i+1}} \leq \gamma_A(n) = \frac{Mp^{i+1}}{n} < \frac{Mp^{i+1}}{s_i} = p\gamma_A(s_i).$$

In particular,

$$c_A = \liminf_{n\to+\infty} \gamma_A(n) \leq \limsup_{n\to+\infty} \gamma_A(n) \leq pc_A.$$

The latter implies that the set of limit points of $\{\gamma_A(n)\}_{n\geq 0}$ is contained in the interval $[c_A, pc_A]$. Since such a set of limit points must be closed, it suffices to prove that the sequence $\{\gamma_A(n)\}_{n\geq 1}$ is dense in the open interval (c_A, pc_A). For each real number $\alpha \in (1, p)$ and each integer $i \geq 0$, set $t_i = \lceil \frac{ps_i}{\alpha} \rceil$. In particular, $t_i = \frac{ps_i}{\alpha} + \kappa_i$ for some $\kappa_i \in [0, 1)$. It follows by the definition that $s_i < t_i \leq ps_i$. Recall that

https://doi.org/10.1017/S0013091525000173 Published online by Cambridge University Press

$s_{i+1} \geq ps_i$, hence $s_A(t_i) = Mp^{i+1} = ps_A(s_i)$. Since $\{s_i\}_{i\geq 0}$ is unbounded, the sequence

$$\gamma_A(t_i) = \frac{ps_A(s_i)}{t_i} = \frac{\alpha s_A(s_i)}{s_i + \frac{\alpha}{p}\kappa_i},\ i \geq 0$$

converges to αc_A.

(iv) This item follows by item (iii) and the following restatement of item (ii):

$$\frac{s_{A_b}(n)}{n} \in \left\{ \frac{s_A(n)}{n}, \frac{ps_A(n)}{n} \right\},\ n \geq 1.$$

(v) Fix k a positive integer. We employ the notation of the previous items. Observe that $s_{A^{(k)}}(n) = s_A(nk)$ for every $n \geq 1$ and so $\gamma_{A^{(k)}}(n) = k\gamma_A(nk)$. From this fact and item (iii), we conclude that the set of limit points of $\{\gamma_{A^{(k)}}(n)\}_{n\geq 1}$ is contained in the interval $[kc_A, pkc_A]$. Hence $c_{A^{(k)}} \geq kc_A$ and $pc_{A^{(k)}} \leq pkc_A$. In conclusion, $c_{A^{(k)}} = kc_A$.

We proceed to the proof of the remaining statements in Theorem 1.2. From hypothesis, the polynomial $A^{(s_0)}(X)$ splits completely in $\mathbb{F}_{q^M}$, and hence lemma 3.1 entails that there exist $r \geq 0$ and $A_* \in \mathbb{F}_q[X]$ such that

$$A_*(A^{(s_0)}(X)) = X^{q^{s_A(1)+r}} - X^{q^r}.$$

Replacing r by $r+1$ and A_* by A_*^q if necessary, we can always assume that $r \geq 1$ and that the polynomial A_* is of the form R^q with $R \in \mathbb{F}_q[x]$ additive. As before, for each integer $i \geq 0$, set $s_i = \max\{j > 0 : s_A(j) = Mp^i\}$, where $M = s_A(1)$. From lemma 2.1, the polynomials A and A_* commute. In particular, as in the proof of item (i), we obtain

$$A_*^{(p^i)}(A^{(s_0p^i)}(X)) = X^{q^{Mp^i+rp^i}} - X^{q^{rp^i}} = \mathcal{S}_{Mp^i,rp^i}(X).$$

Hence $s_i \geq s_0p^i$ with equality if and only if $A_*^{(p^i)}(X)$ is not of the form $E(A(X))$ for some additive $E \in \mathbb{F}_q[X]$. In particular, $\frac{s_A(s_i)}{s_i} \leq \frac{M}{s_0}$ with equality if and only if $s_i = s_0p^i$. Recall that the sequence $\left\{\frac{s_A(s_i)}{s_i}\right\}_{i\geq 0}$ is not increasing and, by the definition, it converges to c_A. Hence $c_A \leq \frac{M}{s_0}$ with equality if and only if $\frac{s_A(s_i)}{s_i} = \frac{M}{s_0}$ for every $i \geq 0$, that is, $s_i = s_0p^i$ for every $i \geq 0$. As we have seen, the latter is equivalent to $A_*^{(p^i)}(X)$ not being of the form $E(A(X))$ with $E \in \mathbb{F}_q[X]$ additive, for every $i \geq 0$. Since A_* is of the form R^q with $R \in \mathbb{F}_q[x]$ additive, we see that $A_*^{(n)}(X)$ is divisible by $X^{q^M} - X$ for some $n \geq 1$ if and only if $A_*^{(m)}(X)$ is divisible by $(X^{q^M} - X)^{q^r}$ for some $m \geq 1$. Taking $i \to +\infty$, and using the fact that A_* and A commute, we see that the following statements are equivalent.

https://doi.org/10.1017/S0013091525000173 Published online by Cambridge University Press

- There do not exist $i \geq 0$ such that $A_*^{(p^i)}(X)$ is of the form $E(A(X))$ with $E \in \mathbb{F}_q[X]$ additive.
- There do not exist $n \geq 1$ such that $A_*^{(n)}(X)$ is of the form $E(A^{(s_0)}(X))$ with $E \in \mathbb{F}_q[X]$ additive.
- There do not exist $n \geq 1$ such that $A_*^{(n)}(X)$ is of the form

$$E(A_*(A^{(s_0)}(X))) = E((X^{q^M} - X)^{q^r}),$$

  with $E \in \mathbb{F}_q[X]$ additive.
- There do not exist $n \geq 1$ such that $A_*^{(n)}(X)$ is divisible by

$$(X^{q^M} - X)^{q^r}.$$

- There do not exist $n \geq 1$ such that $A_*^{(n)}(X)$ is divisible by $X^{q^M} - X$;
- There do not exist $n \geq 1$ such that $A_*^{(n)}(y) = 0$ for every $y \in \mathbb{F}_{q^M}$.
- The $\mathbb{F}_p$-linear map $z \mapsto A_*(z)$ is not nilpotent over $\mathbb{F}_{q^M}$.

Now, if we assume that $z \mapsto A_*(z)$ is not nilpotent over $\mathbb{F}_{q^M}$, we proved that $s_i = s_0 p^i$ for every $i \geq 0$. Take $n > s_0$ and let $j \geq 0$ be the unique integer such that

$$s_0 p^j = s_j < n \leq s_{j+1} = s_0 p^{j+1},$$

hence $s_A(n) = M p^{j+1}$. A direct computation yields $j + 1 = \left\lceil \log_p \frac{n}{s_0} \right\rceil$, from where the result follows.

3.1.1. Comments on Theorem 1.2

Observe that, for real numbers $\alpha, \beta > 0$, the function $f : \mathbb{N} \to \mathbb{R}_{>0}$ given by $f(n) = \alpha p^{\lceil \log_p \beta n \rceil}$ has the following properties: it is an increasing step function such that $f(\mathbb{N}) = \{\alpha p^j \ : \ j \geq 0\}$ and, for

$$a_j := \#f^{-1}((0, \alpha p^j]) = \left\lfloor \frac{p^j}{\beta} \right\rfloor,$$

we have that $\lim_{j\to\infty} \frac{a_j}{a_{j+1}} = \frac{1}{p}$. In particular, we may conclude that the graph of $f(n)$ resembles a fractal.

Although Theorem 1.2 does not guarantee that the function $s_A(n)$ has the form $\alpha p^{\lceil \log_p \beta n \rceil}$ for generic A, we comment that its graph shares some of the forementioned features. Item (i) in Theorem 1.2 readily implies that $s_A(n)$ is a step function with the image set of the form $\{\alpha p^j \ : \ j \geq 0\}$. Finally, looking at the proof of item (iii) of Theorem 1.2, we see that $\{a_j\}_{j\geq 0}$ coincides with the sequence $\{s_j\}_{j\geq 0}$, and we proved that $s_{j+1} \geq p s_j$ for every $j \geq 0$. In particular, we conclude that $\limsup_{j\to\infty} \frac{a_j}{a_{j+1}} \leq \frac{1}{p}$. However, our results are not sufficient to obtain any conclusion on the existence of the limit $\lim_{j\to\infty} \frac{a_{j+1}}{a_j}$.

https://doi.org/10.1017/S0013091525000173 Published online by Cambridge University Press

We believe that in [19], Odoni was trying to explore a similar issue. In fact, in his results on the behaviour of the function $s_A(n)$, he proves that $s_A(n+r_n) \in \{s_A(n), ps_A(n)\}$ whenever n is sufficiently large and $\{r_n\}_{n\geq 1}$ satisfies $\lim_{n\to\infty} \frac{r_n}{n} = 0$: see Lemma 5.2 of [19] for more details. As $p \geq 2$, item (i) in Theorem 1.2 provides a much stronger result in this direction: we only require that $r_n \leq (p-1)n$.

4. Miscellaneous results

In this section, we discuss some applications and improvements on Theorem 1.2.

4.1. Iterating special additive polynomials

Here we obtain an enhanced version of Theorem 1.2 in the special case where A is q-linearized, i.e., $A(X)$ is of the form $\sum_{i=0}^{m} a_i X^{q^i}$. The latter is equivalent to $A(X) = L_f(X)$ for some $f \in \mathbb{F}_q[X]$. For simplicity, we assume that A is separable, i.e., $f(X)$ is not divisible by X. The general case follows easily: indeed, if $f(X) = X^r F(X)$ with $\gcd(F(X), X) = 1$, then

$$L_f^{(n)}(X) = L_F^{(n)}(X)^{q^{rn}}.$$

In particular, $s_A(n) = s_B(n)$ for every $n \geq 0$, where $B(X) = L_F(X)$. For a polynomial $g \in \mathbb{F}_q[X]$ that is not divisible by X, it is direct to verify that there exists $i \geq 1$ such that $g(X)$ divides $X^i - 1$. The smallest positive integer with this property is the *order* of g, which we denote by $\mathrm{ord}(g)$. By a simple calculation, we verify that $g(X)$ divides $X^s - 1$ if and only if s is divisible by $\mathrm{ord}(g)$. From these facts, we obtain the following explicit result that generalizes the observation given by Odoni in the case $A(X) = X^p - X$.

Theorem 4.1. *Let $f \in \mathbb{F}_q[X]$ be a polynomial not divisible by X, let f_0 be its squarefree part and let e be the least positive integer such that $f(X)$ divides $f_0(X)^e$. If $E = \mathrm{ord}(f_0)$, then for $A = L_f(X)$ and every $n \geq 0$, we have*

$$s_A(n) = E \cdot p^{\lceil \log_p ne \rceil}.$$

In particular, if c_A is as in Theorem 1.2, then $c_A = Ee$.

Proof. By employing a Euclidean division and the properties presented in lemma 2.2, we see that for nonzero $g, h \in \mathbb{F}_q[X]$, the polynomial $g(X)$ divides $h(X)$ if and only if $L_g(X)$ divides $L_h(X)$. In particular, since $A = L_f(X)$ is separable and $Y^{q^j} - Y = L_{X^j-1}(Y)$, we observe that for every $s \geq 1$ the following are equivalent:

- $L_f^{(n)}(X) = L_{f^n}(X)$ splits completely in $\mathbb{F}_{q^s}$;
- $f(X)^n$ divides $X^s - 1$;
- s is divisible by $\mathrm{ord}(f^n)$.

Hence, $s_A(n) = \mathrm{ord}(f^n)$. The equality $\mathrm{ord}(f^n) = E \cdot p^{\lceil \log_p ne \rceil}$ follows by item (ii) of Lemma 5 in [23]. The equality $c_A = Ee$ follows by direct computation. □

https://doi.org/10.1017/S0013091525000173 Published online by Cambridge University Press

4.2. Proof of Theorem 1.6

From items (iii) and (iv) of Theorem 1.2, there exists $\beta_B > 0$ such that, for every $n \geq 1$, the irreducible factors of $B^{(n)}(X)$ have all degrees at most $\beta_B n$ and hence $\frac{\rho_B(n)}{n} \leq \beta_B$ for every $n \geq 1$. It remains to provide an absolute lower bound on $\frac{\rho_B(n)}{n}$. We observe that the formal derivative of an affine polynomial is a constant, which is nonzero if and only if the polynomial is separable. The latter is also equivalent to the affine polynomial not being a perfect p-th power. Write $B(X) = B_0(X)^{p^m}$, where $m \geq 0$ and $B_0(X)$ is not of the form $S(X)^p$. From hypothesis, $\deg(B_0) = p^d$ for some $d \geq 1$. From the initial observation, it follows by induction on $n \geq 1$ that $B^{(n)}(X) = \tilde{B}_n(X)^{p^{mn}}$ for some affine separable polynomial $\tilde{B}_n$ of degree p^{dn}. In particular, the set $\mathcal{Z}_n$ of the distinct roots of $B^{(n)}(X)$ has cardinality p^{dn} and so it follows by the definition that

$$\rho_B(n) = \frac{p^{dn}}{N_B(n)}. \tag{5}$$

Our aim is to provide a non-trivial bound for $N_B(n)$. Let $\mathbb{F}_{q^M}$ be the splitting field of $B(X)$ over $\mathbb{F}_q$, and let n be a positive integer which we will assume to be sufficiently large. From items (i) and (ii) in Theorem 1.2, we have that $s_B(n) = Mp^t$ for some $t = t(n)$ such that $0 \leq t < \log_p n + 2$. Hence, $B^{(n)}(X)$ splits completely in $\mathbb{F}_{q^{Mp^t}}$, i.e., $\mathcal{Z}_n \subseteq \mathbb{F}_{q^{Mp^t}}$. Moreover, from items (iii) and (iv) in Theorem 1.2, we have that $t \to +\infty$ as $n \to +\infty$, so we can assume that t is sufficiently large.

As B is affine, for each $0 \leq j \leq t$, the set $\mathcal{U}_j := \mathcal{Z}_n \cap \mathbb{F}_{q^{Mp^j}}$ is an $\mathbb{F}_p$-affine space. For each $0 \leq j \leq t$, let δ_j be the dimension of $\mathcal{U}_j$. From the inclusions $\mathbb{F}_{q^M} \subset \mathbb{F}_{q^{Mp}} \subset \cdots \subset \mathbb{F}_{q^{Mp^t}}$ we obtain $\delta_0 \leq \cdots \leq \delta_t = dn$. Set $\mathcal{Y}_0 = \mathcal{U}_0$, and for each $1 \leq j \leq t$, set $\mathcal{Y}_j = \mathcal{U}_j \setminus \mathcal{U}_{j-1}$. Therefore, $\#\mathcal{Y}_j = p^{\delta_j} - p^{\delta_{j-1}}$ for every $1 \leq j \leq t$. Moreover, if $1 \leq j \leq t$ and $\alpha \in \mathcal{Y}_j$, then $\alpha \in \mathbb{F}_{q^{Mp^j}} \setminus \mathbb{F}_{q^{Mp^{j-1}}}$, and so the degree D_α of the minimal polynomial of α over $\mathbb{F}_q$ divides Mp^j, but it does not divide Mp^{j-1}. The latter implies that D_α is divisible by p^j and so $D_\alpha \geq p^j$. Therefore, for every $1 \leq j \leq t$, the set $\mathcal{Y}_j$ produces at most $\frac{p^{\delta_j} - p^{\delta_{j-1}}}{p^j}$ distinct irreducible factors of $B^{(n)}(X)$. As $\mathcal{Z}_n = \bigcup_{i=0}^{t} \mathcal{Y}_j$, we obtain

$$N_B(n) \leq p^{\delta_0} + \sum_{j=1}^{t} \frac{p^{\delta_j} - p^{\delta_{j-1}}}{p^j} \leq \sum_{j=0}^{t} p^{\delta_j - j}. \tag{6}$$

We now provide nontrivial bounds for δ_j. Set

$$\mathcal{W}_j = \{u - v \,:\, u, v \in \mathcal{U}_j\}.$$

Observe that $B^{(n)}(X) = A^{(n)}(X) + \beta_n$ for some $\beta_n \in \mathbb{F}_q$. Therefore, $\mathcal{W}_j \subseteq \mathbb{F}_{q^{Mp^j}}$ is an $\mathbb{F}_p$-vector space of dimension δ_j, whose elements are roots of $A^{(n)}(X)$. Moreover, the roots of $A^{(n)}(X)$ comprise the set $\mathcal{S} = \cup_{i=0}^{t} \mathcal{W}_j$. As A is additive, it follows that $A(0) = 0$ and so $\mathcal{S}$ also contains the roots of $A^{(r)}(X)$ for $1 \leq r \leq n$. As $pr \geq r + 1$, from item (i) in Theorem 1.2, we obtain that $s_A(r+1) \in \{s_A(r), ps_A(r)\}$ for every $r \geq 1$. In

https://doi.org/10.1017/S0013091525000173 Published online by Cambridge University Press

other words, the degree of the splitting field of consecutive iterates of A increases by a factor p each time it increases. The latter implies that we must have the strict inclusions $\mathcal{W}_0 \subsetneq \cdots \subsetneq \mathcal{W}_t$ and so we obtain $\delta_0 < \cdots < \delta_t$. Therefore, $\delta_j \leq \delta_t - (t-j) = dn + j - t$ and so $\delta_j - j \leq dn - t$ for every $0 \leq j \leq t$. Since $\mathcal{U}_j \subseteq \mathbb{F}_{q^{Mp^j}}$, if $q = p^R$, we also have the trivial bound $\#\mathcal{U}_j \leq \#\mathbb{F}_{q^{Mp^j}}$, i.e., $\delta_j - j \leq \delta_j \leq RMp^j$. Let $k = k(t)$ be the smallest positive integer such that $RMp^{t-k} \leq dn - t$, i.e.,

$$p^{-k} \leq \frac{dn-t}{RMp^t} = \frac{dn-t}{Rs_B(n)} = \frac{d}{R} \cdot \frac{n}{s_B(n)} \left(1 - \frac{t}{dn}\right).$$

From items (iii) and (iv) in Theorem 1.2, the number $\frac{n}{s_B(n)}$ lies in an interval $[a,b]$ with $0 < a < b < +\infty$. Moreover, as $0 \leq t < \log_p n + 2$ we obtain $\lim_{n\to\infty} \frac{t}{n} = 0$ and so we conclude that there exists $c > 0$ such that $k(t) \leq c$ whenever n (hence t) is sufficiently large. In particular, taking n large enough, we have $k(t) < t$ and so from Ineq. (6) we obtain

$$\begin{aligned} N_B(n) \leq \sum_{j=0}^{t-k(t)} p^{RMp^j} + \sum_{j=t-k(t)+1}^{t} p^{dn-t} &\leq 2p^{RMp^{t-k(t)}} + k(t)p^{dn-t} \\ &\leq (k(t)+2)p^{dn-t}. \end{aligned}$$

The latter combined with Eq. (5) yields

$$\rho_B(n) \geq \frac{p^t}{k(t)+2} = \frac{s_B(n)}{M(k(t)+2)} \geq \frac{s_B(n)}{M(c+2)} = n \cdot \frac{s_B(n)}{n} \cdot \frac{1}{M(c+2)},$$

and so the result follows by items (iii) and (iv) in Theorem 1.2.

4.3. Dynamics of linear maps over finite fields

Here, we provide statistics on the periodic points under the iteration of linear maps over finite fields. We start with a general structural theorem.

Theorem 4.2. *Let $A \in \mathbb{F}_q[X]$ be an additive polynomial, and let $n \geq 1$. Then we have a direct sum of $\mathbb{F}_p$-vector spaces $\mathbb{F}_{q^n} = \mathcal{W}_0 \oplus \mathcal{W}_1$, where $\mathcal{W}_0 = \bigcup_{t\geq 0}\{y \in \mathbb{F}_{q^n} : A^{(t)}(y) = 0\}$ and $\mathcal{W}_1$ comprises the elements of $\mathbb{F}_{q^n}$ that are periodic under A. In particular, the number $\pi_A(n)$ of periodic points of $\mathbb{F}_{q^n}$ under the map $z \mapsto A(z)$ satisfies*

$$\pi_A(n) = \#\mathcal{W}_1 = \frac{q^n}{\#\mathcal{W}_0}.$$

Proof. Observe that, as A is additive, the map $z \mapsto A(z)$ is an $\mathbb{F}_p$-linear map over $\mathbb{F}_{q^n}$. Let $P(X)$ be its characteristic polynomial, and write $P(X) = X^r Q(X)$, where $r \geq 0$ and $\gcd(Q(X), X) = 1$. We now employ a classical linear algebra result: we have $\mathbb{F}_{q^n} = V_0 \oplus V_1$, where V_0 (respectively, V_1) is the A-invariant subspace of $\mathbb{F}_{q^n}$ associated

https://doi.org/10.1017/S0013091525000173 Published online by Cambridge University Press

with the factor X^r (respectively, $Q(X)$). Moreover, V_1 is the largest A-invariant subspace where A restricts to a bijection. We clearly have $V_0 = \mathcal{W}_0$. As $\mathbb{F}_{q^n}$ is finite, A restricts to a bijection on an A-invariant subspace if and only if the elements of this subspace are periodic under the map $z \mapsto A(z)$. We directly verify that $\mathcal{W}_1$ is an A-invariant subspace, hence $V_1 = \mathcal{W}_1$, and the result follows. □

4.3.1. Proof of Theorem 1.7

The case where $A(X) = aX^{p^h}$ follows by direct computations since $z \mapsto A(z)$ is the zero map for $a = 0$ and, if $a \neq 0$, such a map is a permutation of the whole field $\overline{\mathbb{F}}_q$. We now assume that $A(X)$ is not of this form. As in the proof of Theorem 1.6, for every integer $n \geq 1$, we verify that there exist integers $r \geq 0$ and $d \geq 1$ such that $A^{(n)}(X) = \tilde{A}_n(X)^{p^{nr}}$ for some additive separable polynomial $\tilde{A}_n(X) \in \mathbb{F}_q[X]$ of degree p^{dn}.

For each positive integer n, set $\Delta(n) = \#\bigcup_{t\geq 0}\{y \in \mathbb{F}_{q^n} : A^{(t)}(y) = 0\}$. Theorem 4.2 implies the identity $\frac{\pi_A(n)}{q^n} = \Delta(n)^{-1}$, so we only need to find values of n, where $\Delta(n)$ is relatively small/sufficiently large. Let $\mathbb{F}_{q^M}$ be the splitting field of $A(X)$ over $\mathbb{F}_q$, and let N be the largest positive integer such that $\mathbb{F}_{q^M}$ contains a root of $A^{(N)}(X)$ that is not a root of $A^{(N-1)}(X)$ (under the convention that $A^{(0)}(X) = X$). From item (i) in Theorem 1.2, the roots of $A^{(j)}(X)$ that are not in $\mathbb{F}_{q^M}$ must be contained in $\mathbb{F}_{q^{Mp^s}}$ for some $s \geq 1$. In particular, we obtain $\Delta(Mt) \leq p^{\mathrm{d}N}$ whenever $\gcd(t, p) = 1$. Therefore,

$$\limsup_{n\to\infty} \frac{\pi_A(n)}{n} \geq \limsup_{t\to\infty} \frac{\pi_A(Mt)}{q^{Mt}} \geq p^{-\mathrm{d}N} > 0.$$

On the other hand, from item (i) in Theorem 1.2, we have that $A^{(p^i)}(X)$ splits completely in $\mathbb{F}_{q^{Mp^i}}$ and so $\Delta(Mp^i) \geq p^{dp^i}$ for every integer $i \geq 0$. Therefore,

$$\liminf_{n\to\infty} \frac{\pi_A(n)}{n} \leq \liminf_{i\to\infty} \frac{\pi(Mp^i)}{q^{Mp^i}} \leq \liminf_{i\to\infty} p^{-\mathrm{d}p^i} = 0.$$

Acknowledgements. This work was conducted during a pleasant visit of the author at the Mathematics Department of Carleton University, Canada, supported by Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES) – Finance Code 001. We would like to thank the reviewer for her/his thoughtful comments and efforts towards improving the manuscript.

References

[1] O. Ahmadi, F. Luca, A. Ostafe and I. Shparlisnki, On stable quadratic polynomials, *Glasgow Math. J.* **54**(2) (2012), 359–369.

[2] N. Ali, Stabilité des polynômes, *Acta Arith.* **119**(1) (2005), 53–63.

[3] M. Ayad and D. L. McQuillan, Irreducibility of the iterates of a quadratic polynomial over a field., *Acta Arith.* **93**(1) (2000), 87–97. Corrigendum: Acta Arith 99 (2001), 1, 97.

[4] E. Bach and A. Bridy, On the number of distinct functional graphs of affine-linear transformations over finite fields, *Linear Algebra Appl.* **439**(5) (2013), 1312–1320.

https://doi.org/10.1017/S0013091525000173 Published online by Cambridge University Press

[5] R. Benedetto, P. Ingram, R. Jones, M. Manes, J. H. Silverman and T. Tucker, Current trends and open problems in arithmetic dynamics, *Bull. Am. Math. Soc.* **56**(4) (2019), 611–685.

[6] A. Bridy, R. Jones, G. Kelsey and R. Lodge, Iterated monodromy groups of rational functions and periodic points over finite fields, *Math. Ann.* **390** (2023), 439–475.

[7] L. Danielson and B. Fein, On the irreducibility of the iterates of $x^n - b$, *Proc. Am. Math. Soc.* **130**(6) (2001), 1589–1596.

[8] B. Elspas, The theory of autonomous linear sequential networks, *IRE Trans. Circ. Theory CT* **6**(1) (1959), 45–60.

[9] D. Gómez-Pérez, A. Ostafe and I. Shparlinski, On irreducible divisors of iterated polynomials, *Rev. Mat. Iberoam.* **30**(4) (2014), 1123–1134.

[10] D. Garton, Periodic points of polynomials over finite fields, *Trans. Am. Math. Soc.* **375**(7) (2022), 4849–4871.

[11] R. A. Hernandez-Toledo, Linear finite dynamical systems, *Commun. Algebra* **33**(9) (2005), 2977–2989.

[12] J. Juul, The Image size of iterated rational maps over finite fields, *Int. Math. Res. Not.* **5** (2021), 3362–3388.

[13] R. Jones and N. Boston, Settled polynomials over finite fields, *Proc. Am. Math. Soc.* **140**(6) (2012), 1849–1863.

[14] H. -C. Li, Periodic points of a linear transformation, *Linear Algebra Appl.* **437**(10) (2012), 2489–2497.

[15] R. Lidl and H. Niederreiter, *Introduction to Finite Fields and Their applications* (Cambridge University Press, New York, NY, USA, 1986).

[16] M. Manes and B. Thompson, Periodic points in towers of finite fields for polynomials associated to algebraic groups, *Rocky Mountain J. Math.* **49**(1) (2019), 171–197.

[17] G. L. Mullen and D. Panario, *Handbook of Finite Fields*, (Taylor and Francis, Boca Raton, 2013).

[18] R. W. K. Odoni, The Galois theory of iterates and composites of polynomials, *Proc. London Math. Soc.* **51**(3) (1985), 385–414.

[19] R. W. K. Odoni, On the Galois groups of iterated generic additive polynomials, *Math. Proc. Camb. Phil. Soc.* **121**(1) (1997), 1–6.

[20] R. W. K. Odoni, On additive polynomials over finite fields, *Proc. Edinb. Math. Soc.* **42**(1) (1999), 1–16.

[21] C. Qureshi and L. Reis, Dynamics of the a-map over residually finite Dedekind domains, *J. Num. Theory* **204** (2019), 134–154.

[22] L. Reis, Nilpotent linearized polynomials over finite fields and applications, *Finite Fields Appl.* **50** (2018), 279–292.

[23] L. Reis, Factorization of a class of composed polynomials, *Des. Codes Cryptogr.* **87**(7) (2018), 1657–1671.

[24] L. Reis, On the factorization of iterated polynomials, *Rev. Mat. Iberoam.* **36**(7) (2020), 1957–1978.

[25] L. Reis, Counting distinct functional graphs from linear finite dynamical systems, *Linear Algebra Appl.* **656** (2023), 409–420.

https://doi.org/10.1017/S0013091525000173 Published online by Cambridge University Press