ON MULTIPLICATIVE INDEPENDENCE OF RATIONAL ITERATES

MARLEY YOUNG

Abstract. Lower bounds are given for the degree of multiplicative combinations of iterates of rational functions (with certain exceptions) over a general field, establishing the multiplicative independence of said functions. This leads to a generalisation of Gao’s method for constructing elements in $\mathbb{F}_q^n$ whose orders are larger than any polynomial in $n$ when $n$ becomes large. Additionally, for a field $\mathbb{F}$ of characteristic 0, an upper bound is given for the number of polynomials $u \in \mathbb{F}[X]$ such that $\{F_i(X, u(X))\}_{i=1}^n$ is multiplicatively dependent for given rational functions $F_1, \ldots, F_n \in \mathbb{F}(X, Y)$.

1. Introduction and Main Results

In light of the difficult open problem of giving an efficient algorithm for constructing primitive elements in finite fields, Gao [8] has given a method for the more modest task of constructing elements of “high order” in $\mathbb{F}_q^n$ when $q$ is fixed. That is, elements with order larger than any polynomial in $n$ when $n$ is large. In particular, if we define $\bar{n} = q^\lceil \log_q n \rceil$, and $g \in \mathbb{F}_q[X]$ is not a monomial or certain binomial, then it was shown that a root of an irreducible factor of degree $n$ of $X^{\bar{n}} - g(X)$ is an element in $\mathbb{F}_q^n$ of order at least

$$\frac{\log_q n}{n^{t-1} \left( \prod_{i=0}^{\log_q n} \frac{1}{d_i} \right)},$$

where $d = \lceil 2 \log_q n \rceil$ and $t = \lfloor \log_d n \rfloor$.

Gao, as a by-product of his method in [8], has also proved a theorem on the multiplicative independence of compositions of polynomials over finite fields, which we consider of independent interest. Our main task is to generalise these results to rational functions, and moreover to general fields, not necessarily finite.

Throughout the paper, $\mathbb{F}$ will denote a field of characteristic $p$ (zero or prime), and $f \in \mathbb{F}(X)$ a non-constant rational function in lowest terms over $\mathbb{F}$. That is, $f = g/h$ with $d := \deg f = \max \{ \deg g, \deg h \} \geq 1$. Being in “lowest terms” means $\gcd(g, h) = 1$, or equivalently, $g$ and $h$ share no roots in any extension field of $\mathbb{F}$. As such, when referring to zeros and poles of a rational function, we mean roots of its numerator and denominator respectively in an algebraic closure $\overline{\mathbb{F}}$ of $\mathbb{F}$. We define the iterates of $f$ by

$$f^{(0)}(X) = X; \quad f^{(k)}(X) = f \circ f^{(k-1)}(X) \text{ for } k \geq 1,$$
and say that they are multiplicatively independent, if for integers $n \geq 1$, $k_1, \ldots, k_n$, we have

$$(f^{(1)}(X))^{k_1} \cdots (f^{(n)}(X))^{k_n} = 1$$

if and only if $k_1 = \ldots = k_n = 0$. Otherwise, we say that they are multiplicatively dependent. In $[8]$, Gao proves that if $f \in \mathbb{F}_q[X]$ is not of the form $aX^d$, or $aX^{p^t} + b$, then the iterates of $f$ are multiplicatively independent.

In generalising this to rational functions, we encounter a few additional exceptional cases. Recall that two rational functions $\phi, \phi' \in \mathbb{F}(X)$ are linearly conjugate if there exists a rational function $\psi \in \mathbb{F}(X)$ of degree 1 such that $\phi' = \psi^{-1} \circ \phi \circ \psi$. We have the following.

**Theorem 1.1.** Suppose that $f = g/h \in \mathbb{F}(X)$ has degree $d \geq 2$, is not a monomial, nor a binomial of the form $aX^{p^t} + b$, and is not linearly conjugate to $1/X^d$. Let $n \geq 1$, and write

$$(1) \quad \Psi(n) = \min_{k_1, \ldots, k_n \in \mathbb{Z}} \deg \left( \left( (f^{(1)})^{k_1} \cdots (f^{(n)})^{k_n} \right) \right).$$

Let $e$ be the smallest positive integer $k$ such that 0 is a zero of $f^{(k)}$ (we say $e = \infty$ if $f^{(k)}(0) \neq 0$ for all $k \geq 1$). Then we have

(i) If $f \in \mathbb{F}[X]$, then $\Psi(n) \geq d^n$ if $n \leq e$, and $\Psi(n) \geq d^{n-e}$ otherwise.

(ii) If $\deg g > \deg h \geq 1$ or $1 \leq \deg g < \deg h$, then $\Psi(n) \geq d^{n-1}$.

(iii) If $\deg g = 0 < \deg h$, or $\deg g = \deg h$, and $f$ is separable, or not of the form $L(X^{p^t})$, where $L \in \mathbb{F}(X)$ has degree 1, then there exists an integer $j \geq 0$ such that $\Psi(n) \geq d^n$ if $n \leq j$, and $\Psi(n) \geq d^{n-j}$ otherwise.

It is easy to show that the above result implies the multiplicative independence of iterates of $f$.

**Corollary 1.2.** Suppose $f = g/h \in \mathbb{F}(X)$ has degree at least 2, is not a monomial nor a binomial of the form $aX^{p^t} + b$, and is not linearly conjugate to $1/X^d$. If $\deg g \neq \deg h$, or $f$ is separable, or not of the form $L(X^{p^t})$, where $L \in \mathbb{F}(X)$ has degree 1, then the iterates $f^{(1)}, \ldots, f^{(n)}$ are multiplicatively independent.

**Proof.** If $(f^{(1)}(X))^{k_1} \cdots (f^{(n)}(X))^{k_n} = 1$, then Theorem 1.1 ensures $k_n = 0$, as otherwise the degree would be positive. Then recursively we get $k_{n-1} = \ldots = k_1 = 0$. □

We use this in the following extension of the main theorem in $[8]$, with the improved bound from $[10]$.

**Theorem 1.3.** Let $g, h \in \mathbb{F}_q[X]$ be coprime with $\deg h, \deg g \leq d = \left[ 2 \log_q n \right]$ and suppose $f = g/h$ satisfies the conditions from Corollary 1.2. Suppose that $\alpha \in \mathbb{F}_{q^t}$ has degree $n$ and is a root of $X^m h(X) - g(X)$, where $m = \bar{n} = q \left[ \log_q n \right]$. Then for $t = \left[ \log_d n \right]$, $\alpha$ has order in $\mathbb{F}_{q^t}$ at least

$$\left( n + t - 1 \right)^{t-1} \prod_{i=0}^{t-1} \frac{1}{d^i}.$$  

As an aside we additionally ask, given rational functions $F_1, \ldots, F_n \in \mathbb{F}(X,Y)$ and polynomial $u \in \mathbb{F}[X]$, when $F_1(X,u(X)), \ldots, F_n(X,u(X))$ are multiplicatively
dependent. In particular, we find upper bounds on the degree of \( u \) such that this is possible, and the number of monic \( u \) for which this is the case.

**Theorem 1.4.** Suppose \( \mathbb{F} \) is a field of characteristic zero, and \( F_i = G_i/H_i \in \mathbb{F}(X,Y) \) are rational functions for \( 1 \leq i \leq n \), of respective degrees \( d_1 \leq \ldots \leq d_n \) in \( X \) and \( 1 \leq e_1 \leq \ldots \leq e_n \) in \( Y \). For \( 1 \leq i \neq j \leq n \), define

\[
R_{ij}(X) = \text{Res}_Y(G_i, G_j) \text{Res}_Y(H_i, H_j),
\]

where \( \text{Res}_Y(P, Q) \) is the resultant of \( P, Q \in \mathbb{F}[X,Y] \), considered as polynomials in \( Y \), and set

\[
E = \sum_{1 \leq i < j \leq n} \deg R_{ij}.
\]

If \( R_{ij} \neq 0 \) for all \( i \neq j \), then, where

\[
\alpha = \begin{cases} 
1, & \text{if at least one } F_i \text{ is a polynomial,} \\
2, & \text{otherwise,}
\end{cases}
\]

there are at most \( \left( e_n(E+2d_n-1)+E+d_n \right)^\alpha \) monic polynomials \( u \in \mathbb{F}[X] \) such that

\[
F_1(X, u(X)), \ldots, F_n(X, u(X))
\]

are multiplicatively dependent, and each has degree not exceeding \( E + 2d_n - 1 \).

Recalling that the resultant of two polynomials of respective degrees \( m \) and \( n \) is a polynomial in the coefficients of degree \( m + n \), and that each \( G_i \), written as a polynomial in \( Y \), has degree at most \( e_n \), with each coefficient having degree not exceeding \( d_n \), we have for \( i \neq j \), \( \deg \text{Res}_Y(G_i, G_j) \leq (e_n + e_n)d_n = 2d_ne_n \). Thus, counting \( \frac{n(n-1)}{2} \) distinct pairs \( \{i, j\} \), we obtain \( E \leq 4n(n-1)d_ne_n \).

Theorem 1.4 can be applied to the particular scenario of shifting a given set of polynomials by a polynomial \( u \), giving a analogue of results from [3] and [6], for algebraic numbers.

**Corollary 1.5.** Suppose \( \mathbb{F} \) has characteristic zero and \( f_1, \ldots, f_n \in \mathbb{F}[X] \) are distinct polynomials, not all constant, of respective degrees \( d_1 \leq \ldots \leq d_n \) and let

\[
C = d_n \frac{n(n-1)}{2}.
\]

Then there are at most \( \left( 3^{C+3d_n-1} \right)^C \) monic polynomials \( u \in \mathbb{F}[X] \) such that

\[
f_1 + u, \ldots, f_n + u
\]

are multiplicatively dependent, and each has degree not exceeding \( C + 2d_n - 1 \).

**Proof.** We have \( F_i(X, Y) = f_i(X) + Y \), giving, \( R_{ij}(X) = f_j(X) - f_i(X) \) and \( \deg R_{ij} \leq d_n \). Therefore \( E \leq \frac{n(n-1)}{2}d_n = C \), and the result follows, noting that \( e_n = 1 \).

\[ \square \]

2. **Proof of Theorem 1.1**

To prove Theorem 1.1 we need some facts about the composition of certain classes of rational functions. Let \( u = v/w, F = G/H \in \mathbb{F}(X) \) be in lowest terms over \( \mathbb{F} \), chosen so \( H \) is monic and \( G \) has leading coefficient \( A \), and write

\[
u(X) = \frac{v(X)}{w(X)} = \frac{a_lX^l + \ldots + a_sX^s}{b_mX^m + \ldots + b_lX^l}, \quad a_l, a_s, b_m, b_l \neq 0,
\]
with $D = \max \{l, m\} \geq 1$. Let $u \circ F = P/Q$. We have

$$\frac{P(X)}{Q(X)} = \frac{a_l \left( \frac{G(X)}{H(X)} \right)^l + \ldots + a_s \left( \frac{G(X)}{H(X)} \right)^s}{b_m \left( \frac{G(X)}{H(X)} \right)^m + \ldots + b_l \left( \frac{G(X)}{H(X)} \right)^l},$$

$$= H(X)^{m-l}G(X)^{s-l}q(X)r(X),$$

where

$$q(X) = \sum_{i=0}^{l-s} a_{l-i}G(X)^{l-s-i}H(X)^i \quad \text{and} \quad r(X) = \sum_{i=0}^{m-t} b_{m-i}G(X)^{m-t-i}H(X)^i.$$

Note that a composition of rational functions in lowest terms is itself in lowest terms (Lemma 2.2) is easily extended to our situation). In particular, $G, H, q$ and $r$ are pairwise relatively prime. This means we need not worry about the possibility of factors cancelling after composition. Hence, from (2), whenever $\deg G \neq \deg H$ we have

$$\deg P = \deg H(D-l) + (\deg G)s + \deg F(l-s),$$

$$\deg Q = \deg H(D-m) + (\deg G)t + \deg F(m-t).$$

Moreover, when $\deg G = \deg H$, the coefficient of $X^{lD}$ is $\nu(A)$ in $P$, and $\nu(A)$ in $Q$. These can’t both be zero as $\gcd(v, w) = 1$, so in all cases we have

$$\deg u \circ F = (\deg u)(\deg F).$$

We can use these facts to obtain results about which zeros and poles are common to different iterates of $f$, beginning by extending a result of Gao [8, Lemma 2.2].

**Lemma 2.1.** Write $f^{(k)} = g_k/h_k$ for the $k$-th iterate of $f$, and let $e$ be defined as in Theorem [7,1]. Additionally, let $\epsilon$, $\mu$ and $\nu$ be respectively the smallest positive integers $k$ such that $h_k(0) = 0$, $\deg g_k < \deg h_k$, and $\deg g_k > \deg h_k$ (again, these take the value $\infty$ if their respective conditions are not satisfied for any $k \geq 1$). Then, for all $k > l \geq 1$,

(i) A zero of $f^{(l)}$ is a zero of $f^{(k)}$ if and only if $\epsilon < \infty$ and $k \equiv l \pmod{e}$.

(ii) A pole of $f^{(l)}$ is a pole of $f^{(k)}$ if and only if $\deg g_{k-l} > \deg h_{k-l}$.

(iii) A pole of $f^{(l)}$ is a zero of $f^{(k)}$ if and only if $\deg g_{k-l} < \deg h_{k-l}$.

(iv) A zero of $f^{(l)}$ is a pole of $f^{(k)}$ if and only if $\mu, \epsilon < \infty$ and $k \equiv l - \mu \pmod{e}$. Note that here, $e = \epsilon + \mu$.

**Proof.** Let $k > l \geq 1$. For part (i), suppose that a zero $\beta$ of $f^{(l)}$ is a zero of $f^{(k)}$. Then $f^{(k)}(\beta) = f^{(l)}(\beta) = 0$. As $f^{(k)} = f^{(k-l)} \circ f^{(l)}$, we have

$$f^{(k-l)}(0) = f^{(k-l)}\left(f^{(l)}(\beta)\right) = f^{(k)}(\beta) = 0.$$

Thus we must have $\epsilon < \infty$, so assume this is the case. Write

$$f^{(e)}(X) = X^S \phi(X), \quad S \geq 1,$$

with 0 not a zero or pole of $\phi$. Then, for every $i \geq 1$, $f^{(ie)}(X) = X^{Si} \phi_i(X)$, for some $\phi_i \in \mathbb{F}(X)$, which does not have 0 as a zero or pole. If $k \equiv l \pmod{e}$, say

$$k = l + je \quad \text{where} \quad j \geq 1,$$

then

$$f^{(k)}(X) = f^{(je)}\left(f^{(l)}(X)\right) = \left(f^{(l)}(X)\right)^{Sj} \phi_j(X),$$
Hence any zero of \( f^{(\ell)} \) is a zero of \( f^{(k)} \). Now, suppose \( k \equiv \ell \pmod{e} \), say \( k = \ell + je + r \) where \( u \geq 0 \) and \( 1 \leq r < e \). If \( f^{(k)} \) and \( f^{(\ell)} \) have a zero in common then, by the above argument, \( f^{(j+e+r)}(0) = f^{(k-\ell)}(0) = 0 \). Noting that
\[
 f^{(j+e+r)}(X) = f^{(e)}(f^{(e)}(X)) = f^{(e)} \left( X^{\ell} \phi_j(X) \right),
\]
we have \( f^{(e)}(0) = 0 \), contradicting the choice of \( e \). Therefore \( f^{(k)} \) and \( f^{(\ell)} \) have no zero in common when \( k \not\equiv \ell \pmod{e} \).

Writing \( f^{(k)} = f^{(k-\ell)} \circ f^{(\ell)} \), the second and third parts follow immediately from (2).

Now, suppose that a zero \( \beta \) of \( f^{(\ell)} \) is a pole of \( f^{(k)} \). Again, writing \( f^{(k)} = f^{(k-\ell)} \circ f^{(\ell)} \), we must have \( \deg g_{k-\ell} < \deg h_{k-\ell} \) by (2), and so \( \mu \ll 0 \). Set \( u = f^{(\mu)} \), \( F = f^{(\mu)} \), so \( f^{(j+\mu)} = u \circ F = P/Q \) as in (2). If \( e, \epsilon > j \), then \( s = t = 0 \), and so (4) and (4) give \( \deg g_{j+\mu} = \deg h_{j+\mu} = d^{j+\mu} \). We thus note that
\[
(7) \quad \deg g_{k} = \deg h_{k} = d^{k} \quad \text{for all } 1 \leq k \neq \mu \leq \min\{\epsilon, e\}.
\]

Next, we have
\[
 f^{(k-\ell)}(0) = f^{(k-\ell)} \left( f^{(\ell)}(\beta) \right) = f^{(k)}(\beta),
\]
and so 0 is a pole of \( f^{(k-\ell)} \). That is, we indeed have \( \epsilon < \infty \). Furthermore, if \( e < \epsilon \), then \( f^{(r-\epsilon)}(0) = f^{(r-\epsilon)}(f^{(\epsilon)}(0)) = f^{(\epsilon)}(0) \), so 0 is a pole of \( f^{(r-\epsilon)} \), contradicting the choice of \( \epsilon \). Hence we have \( \epsilon < e \), and by setting \( u = f^{(j)} \), \( F = f^{(\epsilon)} \), (2) gives that 0 is a zero of \( f^{(j+\epsilon)} \) if and only if \( \deg g_{j} < \deg h_{j} \). Thus \( e = \epsilon + \mu \). Now write
\[
 f^{(\ell+\epsilon)}(X) = X^{-T} \psi(X), \quad T \geq 1,
\]
with 0 not a zero or pole of \( \psi \). If \( k \equiv \ell - \mu \pmod{e} \), say \( k = \ell + je - \mu = \ell + (j-1)e + \epsilon \), with \( j \geq 1 \), then
\[
 f^{(k)}(X) = f^{(j-1)e} \left( f^{(\ell)}(X) \right) = f^{(j-1)e} \left( \left( f^{(\ell)}(X) \right)^{-T} \psi \left( f^{(\ell)}(X) \right) \right)
 = \left( f^{(\ell)}(X) \right)^{-T} \psi \left( f^{(\ell)}(X) \right)^{S^{-1}} \phi_{j-1} \left( \left( f^{(\ell)}(X) \right)^{-T} \psi \left( f^{(\ell)}(X) \right) \right)
\]
and so any zero of \( f^{(\ell)} \) is a pole of \( f^{(k)} \). Suppose now that \( k = \ell + je + r - \mu \), with \( j \geq 1 \) and \( 1 \leq r < e \). If a zero \( \beta \) of \( f^{(\ell)} \) is a pole of \( f^{(k)} \), then \( f^{(k-\ell)}(0) = f^{(k)}(\beta) \), and so 0 is a pole of \( f^{(k-\ell)} = f^{((j-1)e+r)} \). Since
\[
 f^{((j-1)e+r)}(X) = X^{-T} \psi(X)^{S^{-1}} \phi_{j-1} \left( X^{-T} \psi(X) \right),
\]
0 is also a pole of \( f^{((j-1)e+r)} \) and hence, by part (ii), \( \deg g_{r} > \deg h_{r} \). This contradicts (7), so we are done.

We may also determine facts about the degrees of iterates of \( f \).

**Lemma 2.2.** Throughout, if \( \min\{\mu, \nu\} < \infty \), define
\[
\delta = \left| \deg g_{\min\{\mu, \nu\}} - \deg h_{\min\{\mu, \nu\}} \right|
\]
and let \( S_{k} \) and \( T_{k} \) be respectively the degrees of the lowest order term in \( g_{k} \) and \( h_{k} \).

We have
(i) If \( \nu < \mu \), then for integer \( i \geq 1 \), \( \deg g_{i\nu} = d^{i\nu} \), and \( \deg h_{i\nu} = d^{i\nu} - \delta^{i} \).
Moreover, \( \deg g_{k} = \deg h_{k} = d^{k} \) whenever \( k \not\equiv 0 \pmod{\nu} \).

(ii) If \( \mu < \nu \) and \( \epsilon = \epsilon = \infty \), then \( \deg g_{k} = \deg h_{k} = d^{k} \) for all \( k \neq \mu \).
Proof. Throughout the proof, we will write a given iterate \( F_i \) and infer the degrees of its numerator and denominator via the equations \((3)\) and \((4)\). For the first part, we use induction on \( i \). By definition and from \((5)\), we have 
\[
\deg g_k = \deg h_k = d^k \quad \text{for } 1 \leq k < \nu.
\]
The case \( i = 1 \) is thus trivial. Writing \( u = f^{(k)} \) and \( F = f^{(\nu)} \), we obtain \( \deg g_{\nu + j} = \deg h_{\nu + k} = d^{\nu + k} \) when \( 1 \leq k < \nu \), and when \( k = \nu \), we get \( \deg g_{(\nu + 1)\nu} = d^{(\nu + 1)\nu} \) and
\[
\deg h_{(\nu + 1)\nu} = (d^\nu - \delta)(d^{(i - 1)\nu} - \delta^{i - 1}) + d^{\nu}(d^\nu - \delta) = d^{\nu^2} - \delta^i,
\]
as required.

The second part follows from \((7)\). For the third and fourth parts, setting \( u = f^{(k)} \) and \( F = f^{(\mu)} \) gives \( \deg g_{k + \mu} = d^\nu(D - \ell) + (d^\nu - \delta)S_k + d^\nu(l - S_k) = d^{k + \mu} - \delta S_k \) and likewise \( \deg h_{k + \mu} = d^{k + \mu} - \delta T_k \). If we put \( u = f^{(e)} \), \( F = f^{((i - 1)\nu - \delta)} \), induction on \( i \) with \((2)\) then shows that \( S_{ie} = S_e \). By Lemma \(2.1\) (i), \( S_k = 0 \) for all \( k \not\equiv 0 \) (mod \( e \)). Then, for part (iii), we have \( e < \epsilon \), and so \( T_k = 0 \) for all \( k \) by Lemma \(2.4\) (iv).

For part (iv), we set \( u = f^{(\mu)} \) and \( F = f^{(\epsilon)} \) so that \((4)\) implies \( S_e = \delta T \). Thus \( S_{ie} = \delta T^i \). We similarly obtain \( T_{ie + \epsilon} = \delta^i T^{i + 1} \). Now, suppose \( ie < k < (i + 1)e \). By Lemma \(2.1\) (iv), we have \( T_k \neq 0 \) if and only if \( k \equiv ie - \mu \equiv \epsilon \) (mod \( e \)). The results follow. 

We hence obtain the following result.

**Lemma 2.3.**

(i) If \( \nu < \mu \), then for \( 1 \leq \ell < k \), a pole of \( f^{(\ell)} \) is a pole of \( f^{(k)} \) if and only if \( k \equiv \ell \) (mod \( \nu \)).

(ii) If \( \mu < \nu \) and \( \epsilon < \infty \), then for \( 1 \leq \ell < k \), a zero or pole of \( f^{(\ell)} \) is a zero of \( f^{(k)} \) if and only if \( k - \ell - \mu \geq 1 \), and it is a pole of \( f^{(k - \mu)} \).

(iii) If \( \mu < \nu \) and \( \epsilon < \infty \), then for \( 1 \leq \ell < k \), a zero or pole of \( f^{(\ell)} \) is a pole of \( f^{(k)} \) if and only if \( k - \ell - \epsilon \geq 1 \), and it is a zero of \( f^{(k - \epsilon)} \).

**Proof.** Let \( 1 \leq \ell < k \). If \( \nu < \mu \), a pole of \( f^{(\ell)} \) is a pole of \( f^{(k)} \) if and only if \( \deg g_{k - \ell} > \deg h_{k - \ell} \) by Lemma \(2.1\) (ii). This occurs precisely when \( k \equiv \ell \) (mod \( \nu \)) by Lemma \(2.2\) (i).

For the second part, by Lemma \(2.1\) (i) we have that a zero of \( f^{(\ell)} \) is a zero of \( f^{(k)} \) if and only if \( k \equiv \ell \) (mod \( e \)). Note that this implies that \( k - \ell \geq \epsilon = \mu + \epsilon \), and so \( k - \ell - \mu \geq 1 \). Then, by Lemma \(2.1\) (iv), a zero of \( f^{(\ell)} \) is a pole of \( f^{(k - \mu)} \) if and only if \( k - \mu \equiv \ell - \mu \) (mod \( e \)), which is an equivalent condition. From Lemma \(2.1\) (iii), a pole of \( f^{(\ell)} \) is a zero of \( f^{(k)} \) if and only if \( \deg g_{k - \ell} < \deg h_{k - \ell} \). This occurs precisely when \( k \equiv \ell + \mu \) (mod \( e \)) by Lemma \(2.2\) (iv). On the other hand, a pole of \( f^{(\ell)} \) is a pole of \( f^{(k - \mu)} \) if and only if \( \deg g_{k - \ell - \mu} > \deg h_{k - \ell - \mu} \). By Lemma \(2.2\) (iv), this happens exactly when \( k - \mu \equiv \ell \) (mod \( e \)), which is again equivalent.
Finally, for part (iii), by Lemma 2.1 (iv), a zero of \( f^{(k)} \) is a pole of \( f^{(k-\ell)} \) if and only if \( k \equiv \ell - \mu \pmod{\epsilon} \). Since \( e = \mu + \epsilon \), this is equivalent to \( k - \epsilon \equiv \ell \pmod{\epsilon} \), which is the precise condition for a zero of \( f^{(k)} \) to be a zero of \( f^{(k-\ell)} \), by Lemma 2.1 (i).

Furthermore, from Lemma 2.1 (ii), a pole of \( f^{(k)} \) is a pole of \( f^{(k+\mu)} \) if and only if \( \deg y_k - \ell > \deg h_k - \ell \). According to Lemma 2.2 (iv), this is equivalent to \( k - \ell - e \equiv \mu + ie \), which equates to \( k - \ell = t \equiv \mu + ie \). Again by Lemma 2.2 (iv), this is equivalent to having \( \deg g_{k-\ell} < \deg h_{k-\ell} \), which is in turn equivalent to the given pole of \( f^{(k)} \) being a zero of \( f^{(k+\mu)} \), by Lemma 2.1 (iii).

\[ \Box \]

In order to prove multiplicative independence for the iterates of \( f \), it is clearly necessary to show that no iterate of \( f \) is a monomial. We first look to a result of Silverman [18].

**Lemma 2.4.** Suppose there exists an integer \( n \) such that \( f^{(n)} \in \mathbb{F}[X] \). Then either \( f \in \mathbb{F}[X] \), \( f \) is linearly conjugate to \( 1/X^d \), or \( f \) is inseparable, and \( f(X) = L(X^{p^s}) \) for some \( L \in \mathbb{F}(X) \) of degree 1.

Indeed, if no iterate of \( f \) is a polynomial, then certainly none can be a monomial. In particular, in the case where \( f \) is separable, we have that if \( f^{(n)} \) is a polynomial for some \( n \geq 1 \), then already \( f^{(2)} \) is a polynomial. This makes it easy to check whether a given rational function becomes a polynomial under iteration. This is not true however, when \( f \) is inseparable. For example, if \( \mathbb{F} \) has characteristic 2, then \( f(X) = 1 + 1/X^2 \) satisfies \( f^{(2)}(X) = \frac{1}{X^4+1} \) and \( f^{(3)}(X) = X^8 \). Nevertheless, exceptional cases of this type are described completely in the above result.

Now, we treat the case where \( f \) is a polynomial separately. Note that in the case of characteristic 0, the following can actually be viewed as a corollary of the stronger result [21, Theorem 1], which concerns the number of terms (monomials) of composite polynomials. The results of [21] are further extended to rational functions in [27].

**Lemma 2.5.** If \( f \in \mathbb{F}[x] \) is not a monomial or binomial of the form \( aX^{p^s} + b \), with \( a \neq 0, b \in \mathbb{F}, \ell \in \mathbb{N} \), then \( f^{(k)} \) is not a monomial for any \( k \geq 1 \).

**Proof.** Beginning with the case where \( \mathbb{F} \) has zero characteristic, we proceed by induction on \( k \). That is, suppose \( \deg f \geq 2 \), and that \( f \) is not a monomial. Then the case where \( k = 1 \) is trivial. If \( f^{(k-1)} \) is not a monomial, we can write

\[
\begin{align*}
    f(X) &= a_1X^{d_1} + \ldots + a_sX^{d_s}; \\
    s &> 1, \quad d = d_1 > \ldots > d_s \geq 0, \quad a_1, \ldots, a_s \in \mathbb{F} \setminus \{0\},
\end{align*}
\]

and

\[
\begin{align*}
    f^{(k-1)}(X) &= b_1X^{e_1} + \ldots + b_tX^{e_t}; \\
    t &> 1, \quad d^{k-1} = e_1 > \ldots > e_t \geq 0, \quad b_1, \ldots, b_t \in \mathbb{F} \setminus \{0\}.
\end{align*}
\]

Hence we have the following cases:

If \( d_s = 0, e_t \neq 0 \), we have that

\[
\begin{align*}
    f^{(k)}(X) &= f(f^{(k-1)}(X)) \\
    &= a_1(b_1X^{e_1} + \ldots + b_tX^{e_t})^{d_1} + \ldots + a_s
\end{align*}
\]
has constant term \(a_s \neq 0\). Similarly, if \(d_s \neq 0\), \(e_t = 0\),
\[
f^{(k)}(X) = f^{(k-1)}(f(X)) = b_1(a_1X^{d_1} + \ldots + a_sX^{d_s})^e + \ldots + b_t
\]
has constant term \(b_t \neq 0\). If \(d_s \neq 0\), \(e_t \neq 0\), then
\[
f^{(k)}(X) = f(f^{(k-1)}(X)) = a_1(b_1X^{e_1} + \ldots + b_tX^{e_t})^{d_1} + \ldots + a_s(b_1X^{e_1} + \ldots + b_tX^{e_t})^{d_s}
\]
has lowest order term \(a_1b_1^{d_1}X^{e_1} \neq 0\), since \(a_s \neq 0\), \(b_t \neq 0\). Finally, when \(d_s = e_t = 0\), if \(e_2 > 0\), we have
\[
f^{(k)}(X) = f(f^{(k-1)}(X)) = a_1(b_1X^{e_1} + b_2X^{e_2} + \ldots + b_t)^{d_1} + \ldots + a_s.
\]
In this case, the term in \(X^{(d_1-1)e_1+e_2}\) has coefficient \(d_1a_1b_1^{d_1-1}b_2 \neq 0\), since we have \(a_1, b_1, b_2 \neq 0\), and \(F\) has 0 characteristic. Otherwise, \(e_2 = 0\) and
\[
f^{(k)}(X) = f^{(k-1)}(f(X)) = b_1(a_1X^{d_1} + a_2X^{d_2} + \ldots + a_s)^{e_1} + b_2.
\]
Similarly, the term in \(X^{(e_1-1)d_1+d_2}\) has coefficient \(e_1b_1a_1^{e_1-1}a_2 \neq 0\). That is, in all cases \(f^{(k)}\) is not a monomial, and we are done.

Now, suppose \(F\) has positive characteristic \(p\), and that \(f^{(k)}\) is monomial, say of the form \(cX^{d^k}\) with \(c \in F \setminus \{0\}\), for some \(k > 1\). We can write
\[
f(X) = a_1X^{d_1p^t} + \ldots + a_1X^{d_1p^\ell} + b,
\]
where \(a_1, \ldots, a_s \in F \setminus \{0\}\), \(b \in F\), \(t \geq 1\), \(\ell \geq 0\), \(d_1 > \ldots > d_s \geq 1\), and \(p \nmid \gcd(d_1, \ldots, d_s)\).

Here, the degree of \(f\) is \(d = d_1p^\ell\). Denote \(r = p^\ell\) and let
\[
v(X) = a_1X^{d_1} + \ldots + a_1X^{d_1} + b,
\]
\[
w_i(X) = a_1^{r^{-i}}X^{d_1} + \ldots + a_1^{r^{-i}}X^{d_1} + b^{-i}, \ i \geq 1.
\]
Since \(r^i\) is a power of \(p\), we have for any \(i \geq 1\)
\[
(w_i(X))^{r^i} = a_1X^{d_1r^i} + \ldots + a_1X^{d_1r^i} + b = v(X^{r^i}).
\]
Hence
\[
f(X) = v(X^r),
\]
\[
f^{(2)}(X) = v(v(X^r)) = v \left( (w_1(X))^{r^2} \right) = (w_2 \circ w_1(X))^{r^2}.
\]
\[
: \quad f^{(k)}(X) = (w_k \circ w_{k-1} \circ \ldots \circ w_1(X))^{r^k}, \ k \geq 1.
\]
Hence we have
\[
w_k \circ w_{k-1} \circ \ldots \circ w_1(X) = c_0X^{d_1},
\]
From (6), since $k_n$ found in previous iterates will contribute to the value of $\Psi(n)$, where $\Psi(n)$ is a monomial. Since $d_{aX^p}$, we must have $p | d_i$ for $2 \leq i \leq t$. Hence

$$w'_i(X) = d_1a_1^{-r}X^{d_1-1}, \quad i \geq 1.$$ 

From (6), $w'_2(w_1(X)) = d_1a_1^{-r^2}(w_1(X))^{d_1-1}$ is also a factor of $x^{s_{k-n}}$. If $d_1 > 1$, then $w_1$ is a monomial and hence $f$ must also be a monomial. If $d_1 = 1$, then $d_1 > \ldots > d_t \geq 1$ implies that $t = 1$. Therefore $f$ is a binomial of the form $aX^{r^t} + b$. &

We can now prove Theorem 1.1. Recall that we write $f^{(k)} = g_k/h_k$, and define $\delta$, $S_k$, and $T_k$ as in Lemma 2.2. Now, where $\Psi(n)$ is defined as in (11), noting that $F(X)$ is a unique factorisation domain, any zeros or poles of $f^{(n)}$ which cannot be found in previous iterates will contribute to the value of $\Psi(n)$ counting multiplicity, since $k_n \neq 0$.

We first consider part (i), where $f \in F[X]$. If $n \leq e$, then by Lemma 2.4 (i), $\gcd(f(n), f^{(k)}) = 1$ for all $1 \leq k < n$. Hence, $\Psi(n) \geq \deg f(n) = d^n$. Otherwise, let $f^{(e)}$ be as in (9). Then, setting $u = f^{(e)}$, and $F = f^{(n-e)}$, from (2) we have $f(n) = (f^{(n-e)})^{S/q}$, with $\gcd(q, f^{(n-e)}) = 1$. Since $f^{(e)}$ is not a monomial by Lemma 2.3, $S < d^e$, and so $\deg q = d^n - Sd^{n-e} \geq d^{n-e}$. By Lemma 2.3 (i), $f^{(k)} | f^{(n-e)}$ for all $1 \leq k < n$ with $k \equiv n \pmod{e}$, and by Lemma 2.4 (i), $\gcd(f^{(n)}, f^{(k)}) = 1$ for all $1 \leq k < n$ with $k \neq n \pmod{e}$. Thus $\Psi(n) \geq \deg q \geq d^{n-e}$, as required.

Now, if $n < \min\{\mu, \nu\}$, then by Lemma 2.1 parts (ii) and (iv), we have that $\gcd(h_n, g_k) = \gcd(h_n, h_k) = 1$ for all $1 \leq k < n$, and so $\Psi(n) \geq \deg h_n = d^n$. If $\nu < \mu = \infty$, then by Lemma 2.4 (iv), we have $\gcd(h_n, g_k) = 1$ for all $1 \leq k < n$. Hence, setting $u = f^{(\nu)}$ and $F = f^{(n-\nu)}$, so that $f^{(n)} = h_{n-\nu}g_{n-\nu}/q'$ by (2), we must have $s \geq t$. Then, by Lemma 2.2 (i),

$$\Psi(n) \geq \deg r = \deg h_n - \delta \deg h_{n-\nu} = d^{n-\nu}(d^\nu - \delta) \geq d^{n-\nu},$$

provided $f^{(\nu)} \notin F[X]$, which is the case under our assumptions, due to Lemma 2.4. This in particular gives part (ii), where $\deg g > \deg h \geq 1$, as in that case $\nu = 1$.

For the case where $\mu < \nu$ and $n > \mu$, if $e < \epsilon$, then by Lemma 2.2 (ii) and (iii), $\deg h_k = d^k \geq \deg g_k$ for all $k \geq 1$. Moreover, if $n \leq \epsilon$, then $\deg h_k = d^k \geq \deg g_k$ for all $1 \leq k < n$ by (7). So, by Lemma 2.1 (ii) and (iv), $\gcd(g_k, h_n) = \gcd(h_k, h_n) = 1$ for all $1 \leq k < n$, giving $\Psi(n) \geq \deg h_n = d^n$. Hence we assume that $\epsilon < n < \infty$. Suppose now that $\deg g_x > 0$. Since $\epsilon = \mu + \epsilon > \mu$, we do not have $\mu = ie$, and so $S_\mu = 0$, by Lemma 2.2 (iv). Hence, where $u = f^{(\mu)}$ and $F = f^{(n-\mu)}$, (2) gives $g_n = h_{n-\mu}^\delta$. If $n = \mu + ie$, then $n - \mu = \mu + (i-1)e + \epsilon$, and so by Lemma 2.2 (iv),

$$\delta \deg h_{n-\mu} + (\deg g\mu)d^{n-\mu} = \delta(d^{n-\mu} - \delta^iT^i) + (d^\mu - \delta)d^{n-\mu} = d^n - \delta^{i+1}T^i = \deg g_n.$$

Otherwise, again by Lemma 2.2 (iv), \( \deg g_n = d^n \), and so

\[
\delta \deg h_{n-\mu} + (\deg g_\mu) d^{n-\mu} \leq \delta d^{n-\mu} + (d^\mu - \delta)d^{n-\mu} = d^n = \deg g_n.
\]

Hence \( \deg q \geq (\deg g_\mu) d^{n-\mu} \geq d^{n-\mu} \). Moreover, we have \( \gcd(h_\mu, q) = \gcd(g_\mu, q) = 1 \) for all \( 1 \leq k < n \) by Lemma 2.3 (ii), and therefore \( \psi(n) \geq \deg q \geq d^{n-\mu} \). This covers the case \( 1 \leq \deg g < \deg h \), as there \( \mu = 1 \).

On the other hand, where \( \deg g_\mu = 0 \), we set \( u = f^{(e)} \), and \( F = f^{(n-e)} \). If \( \epsilon \leq \mu \), then by definition \( \deg g_\epsilon \leq \deg h_\epsilon \). Otherwise, \( \epsilon = \mu + k \), with \( k \neq i \epsilon \), \( i \epsilon + \epsilon \), and so by Lemma 2.2 (iv), we have \( \deg g_\epsilon \leq \deg h_\epsilon \). Hence, by (2), \( f^{(n)} = h^{m-1}_\epsilon g_{n-\epsilon} q/r \), where \( m \geq l \). We thus obtain \( \deg r = \deg h_n - \deg g_{n-\epsilon} \). Note that \( T < d^n \), as if this were not the case, by Lemma 2.2 (iv) we would have

\[
\deg h_{n+\epsilon} = d^{n+\epsilon} - \delta T = d^{n+\epsilon} - d^\mu d^\epsilon = 0,
\]

giving \( f^{(n+\epsilon)} \in F[X] \), a contradiction by Lemma 2.3. In particular, this means that \( d^n - Td^{n-\epsilon} \geq d^{n-\epsilon} \). Hence, if \( n = \mu + \epsilon \), then \( n - \epsilon = \mu + \epsilon \), so by Lemma 2.2 (iv), we have

\[
\deg r = d^n - \delta T = d^n - Td^{n-\epsilon} \geq d^{n-\epsilon}.
\]

Otherwise, once again using Lemma 2.2 (iv), \( \deg h_n = d^n \), and so

\[
\deg r = d^n - \deg g_{n-\epsilon} \geq d^n - Td^{n-\epsilon} \geq d^{n-\epsilon}.
\]

To conclude, by Lemma 2.3 (iii), we have that \( \gcd(h_\mu, r) = \gcd(g_\mu, r) = 1 \) for all \( 1 \leq k < n \), and thus \( \psi(n) \geq \deg r \geq d^{n-\epsilon} \). This completes the proof.

3. Proof of Theorem 1.3

First recall a lower bound from Lambe [10], on the number of solutions to a linear Diophantine inequality:

**Lemma 3.1.** Suppose that \( m \) and \( x_0, \ldots, x_{r-1} \) are positive integers such that \( \gcd(x_0, \ldots, x_{r-1}) = 1 \). Then the number of non-negative integer solutions \( a_0, \ldots, a_{r-1} \) to the inequality

\[
\sum_{i=0}^{r-1} a_i x_i \leq m,
\]

is at least

\[
\left(\frac{m+r}{r}\right)^{r-1} \prod_{i=0}^{r-1} \frac{1}{x_i},
\]

with equality when \( x_0 = \ldots = x_{r-1} = 1 \).

Now, set \( m = \bar{n} \). Since \( \alpha \) is a root of \( X^m h(X) - g(X) \), we have \( \alpha^m = f(\alpha) \). As \( m \) is a power of \( q \), applying the Frobenius automorphism iteratively gives

\[
\alpha^{m^i} = f^{(i)}(\alpha), \quad i \geq 0.
\]

Consider the set

\[
S = \left\{ \sum_{i=0}^{t-1} a_i m^i : \sum_{i=0}^{t-1} a_i d^i \leq n - 1 \right\}.
\]

We will show that the powers \( \alpha^a \), with \( a \in S \), are distinct in \( \mathbb{F}_{q^n} \), so from Lemma 3.1 \( \alpha \) has order at least

\[
\#S \geq \binom{n+t-1}{t} \prod_{i=0}^{t-1} \frac{1}{d^i}.
\]
Suppose that there exist integers \( a \neq b \) in \( S \) such that \( \alpha^a = \alpha^b \). Writing \( a = \sum_{i=0}^{t-1} a_i m^i \) and \( b = \sum_{i=0}^{t-1} b_i m^i \), we have

\[
\prod_{i=0}^{t-1} (\alpha^i)^{a_i} = \prod_{i=0}^{t-1} (\alpha^i)^{b_i}.
\]

The equation (9) then gives

\[
\prod_{i=0}^{t-1} (f^{(i)}(\alpha))^{a_i} = \prod_{i=0}^{t-1} (f^{(i)}(\alpha))^{b_i}.
\]

Let

\[
k_1(X) = \prod_{a_i > b_i} g_i(X)^{a_i - b_i} \prod_{a_i < b_i} h_i(X)^{b_i - a_i},
\]

and

\[
k_2(X) = \prod_{a_i < b_i} g_i(X)^{b_i - a_i} \prod_{a_i > b_i} h_i(X)^{a_i - b_i}.
\]

Then \( k_1(\alpha) = k_2(\alpha) \). Since \( \alpha \) has degree \( n \) and \( k_1 \) and \( k_2 \) have degree at most

\[
\sum_{i=0}^{t-1} \max \{a_i, b_i\} d^i \leq n - 1,
\]

we have \( k_1(X) = k_2(X) \). Thus \( \prod_{i=0}^{t-1} (f^{(i)}(X))^{a_i - b_i} = 1 \). Then \( a_i - b_i = 0 \) for each \( i \) by Corollary 1.2, and hence \( a = b \), a contradiction.

In light of Theorem 1.3, we wish to determine whether such a pair \((g, h)\) of suitable polynomials always exists for all \( n \). If this is so, we can construct a reliable algorithm for finding elements of high order in \( \mathbb{F}_q^n \). Namely, checking \( X^n h(X) - g(X) \) for irreducible factors of degree \( n \), for each appropriate pair \( (g, h) \in \mathbb{F}_q[X]^2 \).

The case where \( h(X) = 1 \) is considered in [8], where it is reasonably conjectured, but not proved, that for every \( n \), there exists \( g \in \mathbb{F}_q[X] \) with \( \deg g \leq 2 \log_q n \), such that \( X^n - g(X) \) has an irreducible factor of degree \( n \).

For our more general situation, we make the following weaker conjecture,

**Conjecture 3.2.** Suppose \( n \geq 1 \), and let \( T \) be the set of pairs \((g, h) \in \mathbb{F}_q[X]^2\) of degree not exceeding \( d := \lfloor 2 \log_q n \rfloor \) such that \( f = g/h \) satisfies the conditions from Corollary 1.2. Then there exists \((g, h) \in T\) such that \( X^n h(X) - g(X) \) has an irreducible factor of degree \( n \).

To give some evidence for this conjecture, we first obtain a rough lower bound for the order of \( T \). See [2] for the next lemma, regarding the probability that two polynomials in \( \mathbb{F}_q[X] \) are relatively prime.

**Lemma 3.3.** Let \( g \) and \( h \) be randomly chosen from the set of polynomials in \( \mathbb{F}_q[X] \) of degree \( a \) and \( b \) respectively, where \( a \) and \( b \) are not both zero. Then the probability that \( g \) and \( h \) are relatively prime is \( 1 - 1/q \).

Clearly, every pair \((g, h) \in \mathbb{F}_q[X]^2\) with \( \deg g = d \), \( \deg h = d - 1 \) and \( \gcd(g, h) = 1 \) is an element of \( T \). Thus, Lemma 3.3 gives

\[
\#T \geq \left( 1 - \frac{1}{q} \right) \cdot (q - 1)q^d \cdot (q - 1)q^{d-1} \geq \frac{(q - 1)^3}{q^2} q^{4 \log_q n} = \frac{(q - 1)^3}{q^2} n^4.
\]

(10)
Now, consider the following result from [8]:

**Lemma 3.4.** Let $P_q(m,n)$ be the probability of a random polynomial in $\mathbb{F}_q[X]$ of degree $m \geq n$ having at least one irreducible factor of degree $n$. Then

$$P_q(m,n) \sim \frac{1}{n}, \text{ as } n \to \infty,$$

uniformly for $q$ and $m \geq n$.

If we model $X^n h(X) - g(X)$ as a random polynomial in $\mathbb{F}_q[X]$ for each $(g,h) \in T$, Lemma 3.4, in conjunction with (10), suggests that for large $n$, we expect on the order of $n^3$ pairs $(g,h) \in T$ such that $X^n h(X) - g(X)$ has an irreducible factor of degree $n$. Thus it is plausible that at least one such pair exists.

4. **Proof of Theorem 1.4**

For the following we use the polynomial $ABC$-theorem (proved first by Stothers [20], then independently by Mason [12] and Silverman [19]).

**Lemma 4.1.** Let $\mathbb{F}$ be a field and let $A,B,C \in \mathbb{F}[X]$ be relatively prime polynomials such that $A + B + C = 0$ and not all of $A,B$ and $C$ have vanishing derivative. Then

$$\max \{\deg A, \deg B, \deg C\} \leq \deg \text{rad}(ABC) - 1,$$

where, for $f \in \mathbb{F}[X]$, rad($f$) is the product of the distinct monic irreducible factors of $f$.

For the convenience of having rational function’s derivative non-vanishing being equivalent to it being non-constant, we now restrict the field $\mathbb{F}$ to having characteristic 0. The results of this section could be extended to characteristic $p$, given stronger conditions to ensure that our choice of $A$, $B$ or $C$ has non-vanishing derivative.

We now prove Theorem 1.4. Suppose $F_1(X,u(X)), \ldots, F_n(X,u(X))$ are multiplicatively independent, and and assume that no proper subset of these is also multiplicatively dependent, as we can remove functions until this is the case. Then every zero and pole of $F_i$ for $1 \leq i \leq n$ must be a zero or pole of $F_j$ for some $j \neq i$. This is because otherwise we would require $k_i = 0$ in the equation

$$\prod_{\ell=1}^n F_\ell(X,u(X))^{k_\ell} = 1,$$

and hence the proper subset $\{F_\ell(X,u(X)) : 1 \leq \ell \leq n, \ell \neq i\}$ would be multiplicatively dependent. Hence, if $\alpha$ is a zero or pole of $F_i(X,u(X))$, there exists $j \neq i$ such that $F_i(\alpha,Y)$ and $F_j(\alpha,Y)$ have the common zero or pole $u(\alpha)$, giving $R_{ij}(\alpha) = 0$. Thus, any zero or pole of $F_i(X,u(X))$ for $1 \leq i \leq n$ is a zero of $\prod_{1 \leq \ell \leq n} \prod_{i < j \leq n} R_{ij}$. In particular, since for all $i \neq j$, $R_{ij}$ is not identically zero, we have

$$\deg \text{rad} \prod_{i=1}^n G_i(X,u(X)) H_i(X,u(X)) \leq \sum_{1 \leq i < j \leq n} \sum_{1 \leq \ell \leq n} \deg R_{ij} = E.$$

Now, for $1 \leq i \leq n$, write

$$F_i(X,Y) = \frac{G_i(X,Y)}{H_i(X,Y)} = \frac{\sum_{\nu=0}^{\epsilon_i} g_{i,\nu}(X) Y^\nu}{\sum_{\nu=0}^{\epsilon_i} h_{i,\nu}(X) Y^\nu},$$

respectively.
and assume, without loss of generality, that $g_{i,e_i}$ is not identically zero (if it is, we can replace $G_i$ with $H_i$, and $g_{i,e_i}$ with $h_{i,e_i}$ in the following definitions). For $1 \leq i < j \leq n$, define

$$D_{ij}(X) = \gcd(g_{i,e_i}(X)G_j(X, u(X)), g_{j,e_j}(X)u(X)^{e_j-e_i}G_i(X, u(X))),$$

and set

$$A(X) = \frac{g_{i,e_i}(X)G_j(X, u(X))}{D_{ij}(X)}, \quad B(X) = -\frac{g_{j,e_j}(X)u(X)^{e_j-e_i}G_i(X, u(X))}{D_{ij}(X)},$$

and $C = -(A + B)$. Then $A, B$, and $C$ are relatively prime polynomials with $A + B + C = 0$. We have that

$$(13) \quad \deg A = \deg g_{i,e_i} + \deg g_{j,e_j} + e_j \deg u - \deg D_{ij},$$

which is positive if $\deg u \geq d_n$, as $e_j \geq 1$, and $R_{ij} \neq 0$ ensures that $A \nmid B$. Thus $A$ has non-vanishing derivative. Moreover, in $C$, the term in $u(X)^{e_j}$ cancels out, giving

$$(14) \quad \deg C \leq (e_j - 1) \deg u + \max\{\deg g_{i,e_i} + \deg g_{j,e_j-1} - \deg g_{j,e_j}, \deg g_{i,e_i-1}\} - \deg D_{ij}.$$

Therefore, we have by Lemma 4.1 and (13),

$$\deg A = \deg g_{i,e_i} + \deg g_{j,e_j} + e_j \deg u - \deg D_{ij} \leq \max\{\deg A, \deg B, \deg C\} \leq \deg \text{rad} ABC - 1 \leq \deg \text{rad} G_iG_j + \deg g_{i,e_i} + \deg g_{j,e_j} + \deg C - 1.$$ 

Then, (12) and (14) give

$$e_j \deg u - \deg D_{ij} \leq E + (e_j - 1) \deg u + \max\{\deg g_{i,e_i} + \deg g_{j,e_j-1} - \deg g_{j,e_j}, \deg g_{i,e_i-1}\} - \deg D_{ij}$$

and hence,

$$\deg u \leq E + \max\{\deg g_{i,e_i} + \deg g_{j,e_j-1} - \deg g_{j,e_j}, \deg g_{i,e_i-1}\} - 1 \leq E + 2d_n - 1.$$ 

Therefore, for $1 \leq i \leq n$, $G_i(X, u(X))$ is a product of at most $E$ distinct irreducible factors, with degree not exceeding $e_n(E + 2d_n - 1) + d_n$. If $w_0, \ldots, w_{E-1}$ are the respective multiplicities of said factors, then the number of possibilities for $G_i(X, u(X))$ is at most the number of non-negative integer solutions to the inequality

$$\sum_{j=0}^{E-1} w_j \leq e_n(E + 2d_n - 1) + d_n,$$

which is at most $(e_n(E + 2d_n - 1) + E + d_n)^{E}$ from Lemma 3.1. This also gives the number of possibilities for (monic) $u$ if there exists $1 \leq i \leq n$ such that $F_i \in \mathbb{F}[X,Y]$. Otherwise, we obtain the same bound for possible $H_i(X, u(X))$, and hence the number of possibilities for $F_i(X, u(X))$, and hence $u$, does not exceed $(e_n(E + 2d_n - 1) + E + d_n)^{E}$. This completes the proof. \qed
5. Comments

Considering Theorem 1.1 (i), it is of interest to obtain upper bounds for the value $e$ when it is finite. That is, bounds for the period of 0 under iteration of a polynomial $f$. When $K/F_q$ is a field extension of degree $n$, Halter-Koch and Konečná [9] determine the set of all possible cycle lengths in $K$ of polynomials over $F_q$. That is,

$$\text{Cycl}(K/F_q) = \{ dm : 1 \leq d \leq N, 1 \leq m \mid n \},$$

where $N$ is the number of irreducible monic polynomials of degree $n$ over $F_q$. This bounds finite $e$ above by $nN$, which equals $q$ (an obvious bound) when $K = F_q$.

In [17], we have the following results by Pezda for a discrete valuation domain of zero characteristic $R$, with finite residue field of cardinality $N(P)$, and the special cases of $\mathbb{Z}_p$ ($p$-adic integers) and rings of integers in algebraic number fields over the rationals. When $e$ is finite:

- If $f \in R[X]$, $e$ does not exceed $N(P)(N(P) - 1)p^{C(p)}$, where $C(p) = 1 + \frac{\log(\text{ord}_p)}{\log 2}$.
- If $f \in \mathbb{Z}_p[X]$, $e$ does not exceed $p^2$.
- If $R$ is the ring of all integers in an algebraic number field of degree $n$ over the rationals and $f \in R[X]$, $e$ does not exceed $(2^n - 1)2^{n+1}$.

Narkiewicz [13, 14, 15] also characterised cycle lengths of polynomials in certain rings. Again for $f \in R[X]$ with finite $e$ we have

- If $R$ is the ring of integers in a cubic field of negative discriminant, then $e \leq 6$.
- If $R$ is the ring of integers in a quadratic number field, then $e \leq 7$.
- If $R = \mathbb{Z}_{\sqrt{n}}$ for a positive, square-free integer $n$, then $e \leq 6$.

In [4], Canci gives an upper bound on the length of finite orbits of rational functions over number fields. Namely, if $K$ is a number field, and $S$ is a finite set of cardinality $s$ of places of $K$, containing all the archimedean ones, then for rational maps with good reduction outside $S$, finite $e$ is bounded above by

$$[\exp(10^{12})(s+1)^8(\log(5(s+1)))^8]^s.$$  

Bounds on the values of the values of $\epsilon$, $\mu$ and $\nu$ in the rational function case are similarly of interest.

Also, note that in the case $F = \mathbb{C}$, Theorem 1.4 could be generalised to several variables, where $F_i \in \mathbb{C}(X_1, \ldots, X_m, Y)$ and $u \in \mathbb{C}[X_1, \ldots, X_m]$, using an appropriate analogue of Mason’s theorem (for example [1, Theorem 2]).

Acknowledgement

The author would like to thank Alina Ostafe and Igor Shparlinski for their useful ideas, comments and encouragement.

References

[1] M. Bayat and H. Teimoori, A new bound for an extension of Mason’s theorem for functions of several variables, Archiv der Mathematik, Vol. 82 (2004), pp. 230-239.
[2] A. Benjamin and C. Bennett, The probability of relatively prime polynomials, Mathematics Magazine, Vol. 80 (2007), pp. 196-202.
[3] E. Bombieri, D. Masser and U. Zannier, *Intersecting a curve with algebraic subgroups of multiplicative groups*, Int. Math. Res. Not., Vol. 20 (1999), pp. 1119-1140.

[4] J.K. Canci, *Finite orbits for rational functions*, Indag. Mathem., Vol. 18 (2007), No. 2, pp. 203-214.

[5] S. Carter, *Rational function decomposition of polynomials*, RHUMJ, Vol. 13 (2012), No. 2, pp. 54-62.

[6] A. Dubickas and M. Sha, *Multiplicative dependence of the translations of algebraic numbers* (Preprint), 2016, available at [https://arxiv.org/abs/1608.05458](https://arxiv.org/abs/1608.05458).

[7] C. Fuchs and U. Zannier, *Composite rational functions expressible with few terms*, J. Eur. Math. Soc., Vol. 14 (2010), pp. 175-208.

[8] S. Gao, *Elements of provable high order in finite fields*, Proc. Amer. Math. Soc., Vol. 127 (1999), No. 6, pp. 1615-1623.

[9] F. Halter-Koch and P. Konečná, *Polynomial cycles in finite extension fields*, Mathematica Slovaca, Vol. 52 (2002), No. 5, pp. 531-535.

[10] T.A. Lambe, *Bounds on the number of feasible solutions to a knapsack problem*, SIAM J. Applied Math., Vol. 26 (1974), No. 2, pp. 302-305.

[11] R. Lidl and H. Niederreiter, *Finite Fields*, Addison-Wesley, Reading, MA, 1983. (Now distributed by Cambridge University Press.)

[12] R.C. Mason, *Diophantine equations over function fields*, London Mathematical Society Lecture Note Series, Vol. 96 (1984), Cambridge University Press, Cambridge.

[13] W. Narkiewicz, *Polynomial cycles in cubic fields of negative discriminant*, Funct. Approx. Comment. Math., Vol. 35 (2006), pp. 261-269.

[14] W. Narkiewicz and R. Marszalek, *Finite polynomial orbits in quadratic rings*, Ramanujan J., Vol 12 (2006), No. 1, pp. 91-130.

[15] W. Narkiewicz, *Polynomial cycles in certain rings of rationals*, J. Theor. Nombres Bordeaux, Vol. 14 (2002), No. 2, pp. 529-552.

[16] R. Popovych, *On elements of high order in general finite fields*, Algebra Discrete Math., Vol. 18 (2014), No. 18, pp. 295-300.

[17] T. Pezda, *Polynomial cycles in certain local domains*, Acta Arithmetica, Vol. 66 (1994), No. 1, pp. 11-22.

[18] J.H. Silverman, *Rational Functions with a Polynomial Iterate*, Journal of Algebra, Vol. 180 (1996), No. 54, pp. 102-110.

[19] J.H. Silverman, *The S-unit equation over function fields*, Proc. Camb. Philos. Soc., Vol. 95 (1984), pp. 3-4.

[20] W.W. Stothers, *Polynomial identities and Hauptmoduln*, Q. J. Math. Oxf., Vol. 32 (1981), No. 3, pp. 349-370.

[21] U. Zannier, *On the number of terms of a composite polynomial*, Acta Arithmetica, Vol. 127 (2007), No. 2, pp. 157-167.