Rev. Mat. Iberoam. **30** (2014), no. 4, 1123–1134
DOI 10.4171/RMI/809

On irreducible divisors of iterated polynomials

Domingo Gómez-Pérez, Alina Ostafe and Igor E. Shparlinski

Abstract. D. Gómez-Pérez, A. Ostafe, A. P. Nicolás and D. Sadornil have recently shown that for almost all polynomials $f \in \mathbb{F}_q[X]$ over the finite field of q elements, where q is an odd prime power, their iterates eventually become reducible polynomials over $\mathbb{F}_q$. Here we combine their method with some new ideas to derive finer results about the arithmetic structure of iterates of f. In particular, we prove that the nth iterate of f has a square-free divisor of degree of order at least $n^{1+o(1)}$ as $n \to \infty$ (uniformly in q).

1. Introduction

For a field $\mathbb{K}$ and a polynomial $f \in \mathbb{K}[X]$ we define the sequence:

$$f^{(0)}(X) = X, \quad f^{(n)}(X) = f\big(f^{(n-1)}(X)\big), \quad n = 1, 2, \dots .$$

The polynomial $f^{(n)}$ is called the nth iterate of the polynomial f.

Following [1], [2], [10], [11], and [15], we say that a polynomial $f \in \mathbb{K}[X]$ is *stable* if all of its iterates are irreducible over $\mathbb{K}$.

Gómez-Pérez and Nicolás [7], developing some ideas from [16], prove that there are $O(q^{5/2}(\log q)^{1/2})$ stable quadratic polynomials over a finite field $\mathbb{F}_q$ of q elements for an odd prime power q, where the implied constant is absolute. We also note that in [8] an upper bound is given on the number of stable polynomials of degree $d \geqslant 2$ over $\mathbb{F}_q$.

Here, we continue to study the arithmetic properties of iterated polynomials and obtain several new results about their multiplicative structure.

First, we combine the method of Gómez-Pérez and Nicolás [7] with some new ideas to show that, if q is odd, then for almost all quadratic polynomials $f \in \mathbb{F}_q[X]$ the number $r_n(f)$ of irreducible divisors of the nth iterate $f^{(n)}$ grows at least linearly with n if n is of order at most $\log q$. Our tools to prove this are resultants of iterated polynomials, the Stickelberger's theorem [19] and estimates of certain character sums.

Mathematics Subject Classification (2010): Primary 11T06; Secondary 11L40.
Keywords: iterations of polynomials, irreducible divisors.

For the values of n beyond this threshold, we use a different technique, related to Mason's proof of the ABC-conjecture in its polynomial version, see [13], [18], to give a lower bound on the largest degree $D_n(f)$ of the irreducible divisors of $f^{(n)}$. It is interesting to recall that Faber and Granville [4] have used (in a different way) the classical version of the ABC-conjecture for the integers to study the arithmetic of elements in the orbits of polynomial dynamical systems over $\mathbb{Z}$.

Note that our lower bound on $D_n(f)$ is reminiscent of lower bounds on the largest prime divisor of nonlinear recursive sequences over the integers, see [4], [10], and [17].

Our approach and some results used to derive lower bounds on $r_n(f)$ and $D_n(f)$ are readily combined to obtain the lower bound $n^{1+o(1)}$ as $n \to \infty$ (uniformly in q) on the largest degree of square-free divisors of $f^{(n)}$.

The outline of the paper is the following. In Section 2 we give the notation used throughout the paper as well as collect some basic properties needed in the proofs of the main results. In Section 3, we collect all results about discriminants and then, in Section 4, we provide bounds on character sums related with discriminants of iterated polynomials. In Section 5 we recall the result of Mason [13]. These preliminary results are used in the following sections. More precisely, Section 6 contains an estimate of the number of distinct irreducible factors of a polynomial iterate. In Section 7 we show that, if $f \neq f_d X^d$, then there is always an irreducible factor of large degree for high order iterates of the polynomial f. Finally, in Section 8 we combine both approaches and also use some of the previous results to derive some nontrivial information about the arithmetic structure of $f^{(n)}$ that applies to any n.

2. Notation

Let p be an odd prime number and let $q = p^s$ for some positive integer s. We denote by $\mathbb{F}_q$ the finite field of q elements and by χ the quadratic character of $\mathbb{F}_q$.

We use $\mathbb{F}_q[X]$ to denote the ring of polynomials with coefficients in $\mathbb{F}_q$. Polynomials in this ring are denoted by the letters f, g and h. We usually use $f_0, \ldots, f_d$ to represent the coefficients of a polynomial $f \in \mathbb{F}_q[X]$, that is,

$$f = f_d X^d + \cdots + f_1 X + f_0,$$

where $f_d \neq 0$ is the *leading coefficient* of f. As usual, f' denotes the formal derivative of $f \in \mathbb{F}_q[X]$.

Throughout the paper the implied constants in symbols 'O' and '$\gg$' may occasionally, where obvious, depend on a small positive parameter ε but are absolute otherwise (we recall that $A = O(B)$ and $B \gg A$ is equivalent to $|A| \leqslant cB$ for some positive constant c). Also, we write $F(n) = o(G(n))$ as $n \to \infty$, which means that

$$\lim_{n\to\infty} \frac{F(n)}{G(n)} \to 0.$$

3. Discriminants and iterates of polynomials

We use the following well-known properties of the discriminant $\mathrm{Disc}\,(f)$ and the resultant $\mathrm{Res}\,(f,g)$ of polynomials $f,g \in \mathbb{K}[X]$, see [6], [20], that hold over any field $\mathbb{K}$.

Lemma 1. *Let $f,g \in \mathbb{K}[X]$ be polynomials of degrees $d \geqslant 1$ and $e \geqslant 1$, respectively, with leading coefficients f_d and g_e, and let $h \in \mathbb{K}[X]$. Suppose that the derivative f' is a polynomial of degree $k \leqslant d-1$ and denote by $\beta_1,\ldots,\beta_e$ the roots of g in an extension field. Then we have:*

i) $\mathrm{Disc}\big(f\big) = (-1)^{d(d-1)/2}\, f_d^{d-k-2}\,\mathrm{Res}(f,f')$;

ii) $\mathrm{Res}\big(f,g\big) = (-1)^{de}\, g_e^d \prod_{i=1}^{e} f(\beta_i)$;

iii) $\mathrm{Res}\big(fg,h\big) = \mathrm{Res}\big(f,h\big)\,\mathrm{Res}\big(g,h\big)$.

From the definition of the resultant, it is clear that two polynomials f and g are coprime if and only if $\mathrm{Res}\big(f,g\big) \neq 0$.

To study the discriminants of iterates of polynomials, it is necessary to have a close-form formula for the resultant of polynomials under compositions. In [14], the following chain rule for resultants is proved.

Lemma 2. *Let f and g be as in Lemma 1 and let $h \in \mathbb{K}[X]$ with $\deg h = \ell$ and leading coefficient h_ℓ. Then*

$$\mathrm{Res}\big(f(h),g(h)\big) = \big(h_\ell^{de}\,\mathrm{Res}\big(f,g\big)\big)^{\ell}.$$

It is clear from Lemma 2 that f and g are coprime if and only if for any nonconstant polynomial h we have $\mathrm{Res}\big(f(h),g(h)\big) \neq 0$ (note that this is also a consequence of the Euclidean algorithm).

Also, Lemma 2 implies the following formula for the discriminant of polynomial iterates.

Lemma 3. *Let $f \in \mathbb{F}_q[X]$ be a polynomial of degree $d \geqslant 2$ with leading coefficient f_d and nonconstant derivative f' of degree $k \leqslant d-1$. Suppose that γ_i, $i=1,\ldots,k$, are the roots of the derivative f'. Then, for $n \geqslant 1$, we have*

$$\mathrm{Disc}\big(f^{(n)}\big) = (-1)^{d(d(d-1)/2+k)}\, f_d^{\frac{d^n-1}{d-1}\left((k-1)d^n + k\frac{d^n-d}{d-1}+2d\right)} \big((k+1)\,f_{k+1}\big)^{d^n} \cdot \mathrm{Disc}\big(f^{(n-1)}\big)^d \prod_{i=1}^{k} f^{(n)}(\gamma_i).$$

Proof. Simple calculations show that the leading coefficient of $f^{(n)}$ is

$$f_d^{(d^n-1)/(d-1)} \tag{3.1}$$

and we also have

$$\deg\big(f^{(n)}\big)' = k\,\frac{d^n-1}{d-1} \qquad \text{for } n \geqslant 2. \tag{3.2}$$

Indeed, one can prove this by induction over n and we show it only for $\deg(f^{(n)})'$ as the formula (3.1) for the leading coefficient of $f^{(n)}$ can be obtained using the same idea. As $\deg f' = k$, for $n = 1$ the formula (3.2) is true. We assume that (3.2) is true also for the first $n-1$ iterates. We have

$$\deg\left(f^{(n)}\right)' = \deg\left(f' \cdot (f^{(n-1)})'(f)\right) = k + k\,d\,\frac{d^{n-1}-1}{d-1} = k\,\frac{d^n-1}{d-1}.$$

Thus, applying Lemma 1 (i) we derive

$$\begin{aligned}\operatorname{Disc}\left(f^{(n)}\right) &= (-1)^{d^n(d^n-1)/2}\, f_d^{\frac{d^n-1}{d-1}\left(d^n - k\frac{d^n-1}{d-1}-2\right)} \operatorname{Res}\left(f^{(n)}, (f^{(n)})'\right)\\ &= (-1)^{d^2(d-1)/2}\, f_d^{\frac{d^n-1}{d-1}\left(d^n - k\frac{d^n-1}{d-1}-2\right)} \operatorname{Res}\left(f^{(n)}, (f^{(n)})'\right).\end{aligned} \tag{3.3}$$

Taking into account that $\left(f^{(n)}\right)' = f' \cdot \left(f^{(n-1)}\right)'(f)$ and applying Lemma 1 (iii) and Lemma 2, we derive

$$\begin{aligned}\operatorname{Res}\left(f^{(n)}, f^{(n)\prime}\right) &= \operatorname{Res}\left(f^{(n)}, f' \cdot (f^{(n-1)})'(f)\right)\\ &= \operatorname{Res}\left(f^{(n)}, (f^{(n-1)})'(f)\right) \operatorname{Res}\left(f^{(n)}, f'\right)\\ &= \left(f_d^{kd^{n-1}\frac{d^{n-1}-1}{d-1}} \operatorname{Res}\left(f^{(n-1)}, \left(f^{(n-1)}\right)'\right)\right)^d \operatorname{Res}\left(f^{(n)}, f'\right).\end{aligned} \tag{3.4}$$

Using Lemma 1 (i), we derive

$$\begin{aligned}&\operatorname{Res}\left(f^{(n-1)}, (f^{(n-1)})'\right)\\ &\quad = (-1)^{d^2(d-1)/2}\, f_d^{\frac{d^{n-1}-1}{d-1}\left(-d^{n-1}+k\frac{d^{n-1}-1}{d-1}+2\right)} \operatorname{Disc}\left(f^{(n-1)}\right),\end{aligned} \tag{3.5}$$

while by Lemma 1 (ii) we obtain

$$\operatorname{Res}\left(f^{(n)}, f'\right) = (-1)^{kd}\left((k+1)f_{k+1}\right)^{d^n} \prod_{i=1}^{k} f^{(n)}(\gamma_i). \tag{3.6}$$

Substituting (3.5) and (3.6) in (3.4) and using (3.3), we finish the proof. □

We also note that a similar computation has been given by Jones and Manes (see [12], Lemma 3.1 and Theorem 3.2) for iterated rational functions.

For a polynomial $f = f_d X^d + \cdots + f_1 X + f_0 \in \mathbb{F}_q[X]$ defined as in Lemma 3, it is convenient to introduce the following notation

$$G_n(f_d, \ldots, f_0) = \prod_{i=1}^{k} f^{(n)}(\gamma_i), \quad n \geqslant 1,$$

where γ_i, $i = 1, \ldots, k$, are the roots of f', which is clearly a polynomial in $f_d, \ldots, f_0$ and having the degree $O(d^n)$ in the variable f_0. We need the following result, which has been proved in [8], Lemma 5.2:

Lemma 4. *For fixed integers $K \geqslant 1$ and $k_1, \ldots, k_\mu$ such that $1 \leqslant k_1 < \cdots < k_\mu \leqslant K$, the polynomial*

$$\prod_{j=1}^{\mu} G_{k_j}(f_d, \ldots, f_0)$$

is a square polynomial in the variable f_0 up to a multiplicative constant only for $O(d^{2K} q^{d-1})$ choices of $f_1, \ldots, f_d$.

4. Bounds of some character sums

For an integer n we consider the sums

$$T_1(n) = \sum_{f_0 \in \mathbb{F}_q} \cdots \sum_{f_d \in \mathbb{F}_q} \left| \sum_{\ell=1}^{n} \chi\big(G_\ell(f_d, \ldots, f_0)\, G_{\ell+1}(f_d, \ldots, f_0)\big) \right|^2,$$

$$T_2(n) = \sum_{f_0 \in \mathbb{F}_q} \cdots \sum_{f_d \in \mathbb{F}_q} \left| \sum_{\ell=1}^{n} \chi\left(f_d^{k\ell} G_\ell(f_d, \ldots, f_0)\right) \right|^2,$$

with the quadratic character χ of $\mathbb{F}_q$, where k is as in Lemma 3.

Lemma 5. *Let $f = f_d X^d + \cdots + f_1 X + f_0 \in \mathbb{F}_q[X]$ be defined as in Lemma 3. For any integer $n \geqslant 1$, we have*

$$T_i(n) = O\big(n^2 d^n q^{d+1/2} + n^2 d^{2n} q^d + n q^{d+1}\big), \qquad i = 1, 2.$$

Proof. Squaring and changing the order of summation, we obtain

$$T_1(n) = \sum_{\ell,m=1}^{n} \sum_{f_d \in \mathbb{F}_q} \cdots \sum_{f_0 \in \mathbb{F}_q} \chi\left(G_\ell(f_d, \ldots, f_0)\, G_{\ell+1}(f_d, \ldots, f_0)\right.$$
$$\left. \cdot\, G_m(f_d, \ldots, f_0)\, G_{m+1}(f_d, \ldots, f_0)\right).$$

Fix $\ell, m, f_1, \ldots, f_d$ and define the following polynomial in f_0,

$$G_{\ell,m} = G_\ell(f_d, \ldots, f_0)\, G_{\ell+1}(f_d, \ldots, f_0)\, G_m(f_d, \ldots, f_0)\, G_{m+1}(f_d, \ldots, f_0).$$

We consider the following three cases:

- If $G_{\ell,m}$ is not a square polynomial in f_0, we use the Weil bound (see, for example, Theorem 11.23 in [9]) and estimate the sum over f_0 as $O(d^n q^{1/2})$. In this case, for the $n(n-1)$ values of $\ell \neq m$ and the $O(q^d)$ choices of $f_1, \ldots, f_d$, the total contribution from all such terms is $O\left(n^2 d^n q^{d+1/2}\right)$.
- If $\ell \neq m$ and $G_{\ell,m}$ is a square polynomial, we use the trivial estimate q for the sum over f_0. By Lemma 4, $G_{\ell,m}$ is a square polynomial for $O(d^{2n} q^{d-1})$ values of the fixed parameters $f_1, \ldots, f_d$ for each of the $n(n-1)$ pairs (ℓ, m) with $\ell \neq m$. So, the total contribution from all such terms is $O\left(n^2 d^{2n} q^d\right)$.
- Finally, for each of the n pairs (ℓ, m) with $\ell = m$, there are q^d possible choices for $f_1, \ldots, f_d$. So, the total contribution from all such terms is $O\left(n q^{d+1}\right)$.

Combining the preceding observations, we obtain

$$T_1(n) = O\big(n^2\, d^n\, q^{d+1/2} + n^2\, d^{2n}\, q^d + n\, q^{d+1}\big),$$

and the first part of the result follows.

By the same argument (with some natural simplifications due to a simpler shape of the sum $T_2(n)$), we obtain the same estimate for $T_2(n)$. □

5. Polynomial *ABC* theorem and divisors of iterated polynomials

Some of our results are also based on the Mason theorem [13] that gives a polynomial version of the ABC conjecture, see also [18].

For a polynomial $f \in \mathbb{F}_q[X]$, we denote the product of all monic irreducible divisors of f by $\mathrm{rad}(f)$.

Lemma 6. *Let A, B and C be nonzero polynomials over $\mathbb{F}_q$ with $A + B + C = 0$ and $\gcd(A, B, C) = 1$. If $\deg A \geqslant \deg \mathrm{rad}(ABC)$, then $A' = 0$.*

Recall that we denote the largest degree of irreducible factors of $f^{(n)}$ by $D_n(f)$. In order to apply Lemma 6 we need the following simple statement.

Lemma 7. *For a nonconstant polynomial $f \in \mathbb{F}_q[X]$,*

$$D_n(f) \geqslant D_{n-1}(f) \quad \text{for } n \geqslant 2.$$

Proof. Now assume that $D_{n-1}(f) = D$ for some positive integer D. Let $g \in \mathbb{F}_q[X]$ be an irreducible divisor of $f^{(n-1)}$ with $\deg g = D$. Then we obviously have $g(f) \mid f^{(n)}$. Now, if $g(f)$ has a root $\alpha \in \mathbb{F}_{q^m}$ then g has a root $f(\alpha)$ in $\mathbb{F}_{q^m}$ too. Because g is irreducible, we have $m \geqslant \deg g$. Thus $g(f)$ has an irreducible factor of degree at least D. □

We denote by $\Delta_n(f)$ the largest degree of a square-free divisor of $f^{(n)}$. That is, $\Delta_n(f) = \deg \mathrm{rad}(f^{(n)})$.

Lemma 8. *For a nonconstant polynomial $f \in \mathbb{F}_q[X]$,*

$$\Delta_n(f) \geqslant \Delta_{n-1}(f) \quad \text{for } n \geqslant 2.$$

Proof. Assume that

$$f^{(n-1)} = A \prod_{i=1}^{s} g_i^{\alpha_i},$$

where A is the leading coefficient of $f^{(n-1)}$ (see (3.1) for an explicit formula) and $g_1, \ldots, g_s$ are the distinct monic irreducible divisors of $f^{(n-1)}$ of multiplicities $\alpha_1, \ldots, \alpha_s$, respectively, with

$$\Delta_{n-1}(f) = \sum_{i=1}^{s} \deg g_i.$$

Then

$$f^{(n)} = A \prod_{i=1}^{s} g_i(f)^{\alpha_i}.$$

As $g_1, \dots, g_s$ are relatively prime, we see from Lemma 2 that the polynomials $g_1(f), \dots, g_s(f)$ are also relatively prime. Thus

$$\Delta_n(f) = \sum_{i=1}^{s} \deg \mathrm{rad}(g_i(f)).$$

As in the proof of Lemma 7 we see that $\deg \mathrm{rad}(g_i(f)) \geqslant \deg g_i$, $i = 1, \dots, s$, which concludes the proof. □

6. Growth of the number of irreducible factors under iteration for small n

Let $f \in \mathbb{F}_q[X]$. We recall that $r_n(f)$ denotes the number of monic irreducible divisors of $f^{(n)}$. Using the remark after Lemma 2, we have that if g_1 and g_2 are two different irreducible prime factors of $f^{(n)}$, then $g_1(f)$ and $g_2(f)$ are coprime.

Clearly, this means that $r_n(f)$ is a nondecreasing function. Now, we show that $r_n(f)$ grows at least linearly for n of order at most $\log q$.

Theorem 9. *For any fixed $\varepsilon > 0$, for all but $o(q^{d+1})$ degree d polynomials $f \in \mathbb{F}_q[X]$, we have*

$$r_n(f) \geqslant (0.5 + o(1))\, n,$$

when $n \to \infty$ and $L \geqslant n$, where

$$L = \left\lceil \left(\frac{1}{2 \log d} - \varepsilon \right) \log q \right\rceil.$$

Proof. Clearly we can discard q^d polynomials f with $f(0) = 0$.

We consider first the case when d is even. In this case,

$$\chi\left(G_\ell(f_d, \dots, f_0)\right) = \chi(\mathrm{Disc}\big(f^{(\ell)}\big)).$$

We apply Lemma 5 with $n \leqslant L$. Note that $d^{2n} = O(q^{1-2\varepsilon \log d})$ and thus $T_1(n) = O\left(nq^{d+1}\right)$. Therefore, the number of tuples $(f_d, \dots, f_0) \in \mathbb{F}_q^{d+1}$ with

$$\left| \sum_{\ell=1}^{n} \chi\left(G_\ell(f_d, \dots, f_0)\, G_{\ell+1}(f_d, \dots, f_0)\right) \right| \geqslant n^{2/3}$$

does not exceed $T_1(n) n^{-4/3} = O(q^{d+1} n^{-1/3}) = o(q^{d+1})$ when $n \to \infty$.

Hence, we discard the $o(q^{d+1})$ polynomials $f = f_d X^d + \dots + f_1 X + f_0 \in \mathbb{F}_q[X]$, which correspond to such tuples $(f_d, \dots, f_0)$.

We also discard the polynomials $f = f_d X^d + \dots + f_1 X + f_0 \in \mathbb{F}_q[X]$ corresponding to tuples $(f_d, \dots, f_0)$ for which

$$G_\ell(f_d, \dots, f_0) \cdot G_{\ell+1}(f_d, \dots, f_0) = 0 \tag{6.1}$$

for some $\ell = 1, \ldots, n$. Since each of the polynomials G_ℓ and $G_{\ell+1}$ is a nonzero polynomial of degree $O(d^\ell) = O(d^n)$, for each ℓ there are at most $O(d^n q^d)$ possibilities for $(f_d, \ldots, f_0) \in \mathbb{F}_q^{d+1}$ satisfying (6.1). Thus, we see that there are $O(n\, d^n q^d) = o(q^{d+1})$ such polynomials (note that since a zero polynomial is a square polynomial this also follows from Lemma 4).

For the remaining polynomials, we have

$$\chi\left(G_\ell(f_d, \ldots, f_0)\, G_{\ell+1}(f_d, \ldots, f_0)\right) \neq 0,$$

and also

$$\left|\sum_{\ell=1}^{n} \chi\left(G_\ell(f_d, \ldots, f_0)\, G_{\ell+1}(f_d, \ldots, f_0)\right)\right| < n^{2/3}.$$

Thus, for these polynomials we have

$$\chi\left(G_\ell(f_d, \ldots, f_0)\, G_{\ell+1}(f_d, \ldots, f_0)\right) = -1$$

for $n/2 + O(n^{2/3})$ values of $\ell = 1, \ldots, n$. We now see from Lemma 3 that

$$\chi\big(\mathrm{Disc}\big(f^{(\ell)}\big)\big) \neq \chi\big(\mathrm{Disc}\big(f^{(\ell+1)}\big)\big) \qquad (6.2)$$

for $n/2 + O(n^{2/3})$ values of $\ell = 1, \ldots, n$.

Now we use the Stickelberger theorem (see [19] or the recent reference [3]) which says that the number r_ℓ of distinct irreducible factors of $f^{(\ell)}$ satisfies $r_\ell(f) \equiv d^\ell \pmod 2$ if and only if $\mathrm{Disc}\big(f^{(\ell)}\big)$ is a square in $\mathbb{F}_q$.

By (6.2), the fact that the degree is even, and using the Stickelberger theorem [19], $r_\ell(f)$ and $r_{\ell+1}(f)$ have different parities for $n/2 + O(n^{2/3})$ values of $\ell = 1, \ldots, n$. Since clearly $r_\ell(f)$ is nondecreasing, we have $r_{\ell+1}(f) > r_\ell(f)$ for such values of ℓ. Thus,

$$r_n(f) \geqslant n/2 + O(n^{2/3}).$$

For odd d we note that $r_\ell(f)$ and $r_{\ell+1}(f)$ are of different parity when

$$\chi\left(f_d^{k\ell} G_\ell(f_d, \ldots, f_0)\right) = -1$$

and proceed in exactly the same way using Lemma 5 for the sum T_2. □

7. Lower bound on the degrees of irreducible factors of iterates for large n

Recall that for a polynomial $f \in \mathbb{F}_q[X]$ we denote by $D_n(f)$ the largest degree of irreducible factors of $f^{(n)}$. We are now ready to prove the main result of this section.

Theorem 10. *Let $f \in \mathbb{F}_q[X]$ be of degree d with $\gcd(d, q) = 1$. Assume that $f \neq f_d X^d$. Then*

$$D_n(f) > \frac{\log(d^{n-1}/2)}{\log q}.$$

Proof. We fix an integer n and define D as the largest integer satisfying

$$2q^D \leqslant d^{n-1}. \tag{7.1}$$

Note that, if $d^{n-1} < 2q$, then $\log(d^{n-1}/2) < \log q$ and the bound is trivial. On the other hand, if $d^{n-1} > 2q$ then $D \geqslant 1$. We can also assume that $n \geqslant 2$ as otherwise the bound is also trivial.

Now, from the definition of D we conclude that

$$D + 1 > \frac{\log(d^{n-1}/2)}{\log q}.$$

We prove the statement by contradiction, so we suppose that

$$D_n(f) \leqslant D.$$

By Lemma 7 we have

$$D_{n-1}(f) \leqslant D_n(f).$$

This means that the polynomial $f^{(n)}f^{(n-1)}$ factors as a product of irreducible polynomials of degree at most D.

Any root of $f^{(n)}$ or $f^{(n-1)}$ belongs to $\mathbb{F}_{q^j}$ with $j \leqslant D$. Then, the product $f^{(n)}f^{(n-1)}$ has at most

$$\sum_{j=1}^{D} q^j \leqslant 2q^D$$

distinct roots.

Clearly, f has a root $\alpha \neq 0$ in some extension field of $\mathbb{F}_q$, so $G|f$, where $G = X - \alpha$.

Furthermore, we can write

$$f^{(n-1)} - G(f^{(n-1)}) - \alpha = 0$$

and apply Lemma 6 with $A = f^{(n-1)}$, $B = -G(f^{(n-1)})$ and $C = -\alpha$. Using that $G(f^{(n-1)}) \mid f(f^{(n-1)}) = f^{(n)}$ we derive

$$d^{n-1} < \deg \operatorname{rad}(G(f^{(n-1)})f^{(n-1)}) \leqslant \deg \operatorname{rad}(f^{(n)}f^{(n-1)}) \leqslant 2q^D.$$

Hence we obtain $d^{n-1} < 2q^D$, which contradicts the choice of D. □

8. Uniform bound

Note that Theorem 10 becomes nontrivial for n having about the same size as those n for which Theorem 9 stops working. Hence, they can be combined in the following result that provides some nontrivial information about the arithmetic structure of iterates that applies to all n and q. Let, as before, $\Delta_n(f)$ denote the largest degree of a square-free divisor of $f^{(n)}$.

Theorem 11. *If* $\gcd(d,q) = 1$*, then, for any fixed* $\varepsilon > 0$*, for all but* $o(q^{d+1})$ *polynomials* $f \in \mathbb{F}_q[X]$ *of degree* d*, for* $n \geqslant 1$*, we have*

$$\Delta_n(f) \gg n^{1-\varepsilon}.$$

Proof. First, we note that by Lemma 3, $\mathrm{Disc}\big(f^{(n)}\big) = 0$ is possible only if

$$\mathrm{Disc}\big(f^{(n-1)}\big) = 0 \quad \text{or} \quad G_n(f_d, \ldots, f_0) = \prod_{i=1}^{k} f^{(n)}(\gamma_i) = 0.$$

Thus, as in the proof of Theorem 9 (where we count the number of solutions to (6.1)), we see that for any fixed $\varepsilon > 0$, for all but $o(q^{d+1})$ polynomials $f \in \mathbb{F}_q[X]$ of degree d, for every $n \leqslant L$ with

$$L = \left\lceil \left(\frac{1}{2\log d} - \varepsilon\right) \log q \right\rceil,$$

we have $\mathrm{Disc}\big(f^{(n)}\big) \neq 0$ and thus $\Delta_n(f) = d^n$.

Therefore, for every $n \leqslant q^{1/2}$, since by Lemma 8 we know that $\Delta_n(f)$ is monotonic, for all but $o(q^{d+1})$ polynomials $f \in \mathbb{F}_q[X]$ of degree d we have

$$\Delta_n(f) \geqslant \min\{d^n, d^L\} \gg n^{1-\varepsilon}. \tag{8.1}$$

For $n > q^{1/2}$, by Theorem 10, for all but $O(q) = o(q^{d+1})$ polynomials $f \in \mathbb{F}_q[X]$ of degree d we have

$$\Delta_n(f) \geqslant D_n(f) \gg \frac{1}{\log q} n \gg \frac{n}{\log n} \gg n^{1-\varepsilon}. \tag{8.2}$$

Combining (8.1) and (8.2), we conclude the proof. □

9. Comments and open questions

We note that an analogue of Theorems 9 and 11 can also be obtained for almost all monic polynomials. Probably the most interesting question is to extend the bound of Theorem 9 to any n (beyond the current threshold $n = O(\log q)$).

Although we do not know how to obtain such a result, we can construct some examples of polynomials for which r_n grows linearly (which, as we have mentioned, appears to the expected rate of growth). Indeed, take any quadratic polynomial $f(X) = X^2 + 2aX + a^2 - a \in \mathbb{F}_q[X]$ with $a \in \mathbb{F}_q$ and set $\gamma = -a$. Clearly $f(\gamma) = \gamma$.

Thus, $f^{(n)}(\gamma) = \gamma$ for any $n = 1, 2, \ldots$. We now get from Lemma 3 that

$$\mathrm{Disc}\big(f^{(n)}\big) = (-1)^{n-1}\gamma.$$

So, if -1 is a nonsquare in $\mathbb{F}_q$ (for example, for a prime $q = p \equiv 3 \pmod 4$), then $\mathrm{Disc}\big(f^{(n)}\big)$ is a square or a nonsquare depending only on the parity of n. Therefore, for this polynomial we have $r_n(f) \geqslant n$ for any $n \geqslant 1$. A concrete example is given by $f(X) = X^2 + X + 2 \in \mathbb{F}_3[X]$ (we take $a = 2$ in the above construction).

In [11] the *critical orbit* of a quadratic polynomial f is defined as the set $\{f^{(n)}(\gamma) \mid n \geqslant 2\} \cup \{-f(\gamma)\}$, where γ is the root of the derivative. This coincides with the set

$$\{G_n(f_0, f_1, f_2) \mid n \geqslant 2\} \cup \left\{\frac{f_1^2}{2f_0} - f_2\right\}.$$

It is certainly interesting to investigate various properties of the sequence $u_n = G_n(f_0, \dots, f_d)$ for fixed $f_0, \dots, f_d \in \mathbb{F}_q$.

Currently, most of the known results concern only quadratic polynomials. For example, the sequence u_n becomes eventually periodic when $d = 2$. If f' is an irreducible polynomial of degree k, then $G_n(f_0, \dots, f_d) = \mathrm{Norm}_{\mathbb{F}_{q^k}/\mathbb{F}_q}(f^{(n)}(\gamma))$ is the norm of $f^{(n)}(\gamma)$ in $\mathbb{F}_q$. Apart from these two cases, very little is known about the sequence u_n for general polynomials f.

The sparsity, or number of monomials, is another important characteristic of polynomials and it is certainly interesting to obtain lower bounds on the number of monomials of the iterates $f^{(n)}$. For iterates of polynomials and even rational functions over a field of characteristic zero such bounds can be derived from the results of [5].

Finally, we note that similar questions can also be asked for iterates of rational functions, which is yet another challenging direction of research.

Acknowledgement. The authors would like to thank the referee for his very careful reading and many suggestions which have improve the quality of the exposition.

References

[1] Ali, N.: Stabilité des polynômes. *Acta Arith.* **119** (2005), no. 1, 53–63.

[2] Ayad, M. and McQuillan, D. L.: Irreducibility of the iterates of a quadratic polynomial over a field. *Acta Arith.* **93** (2000), no. 1, 87–97. Corrigendum: *Acta Arith.* **99** (2001), no. 1, 97.

[3] Dalen, K.: On a theorem of Stickelberger. *Math. Scand.* **3** (1955), 124–126.

[4] Faber, X. and Granville, A.: Prime factors of dynamical sequences. *J. Reine Angew. Math.* **661** (2011), 189–214.

[5] Fuchs, C. and Zannier, U.: Composite rational functions expressible with few terms. *J. Eur. Math. Soc.* **14** (2012), no. 1, 175–208.

[6] von zur Gathen, J. and Gerhard, J.: *Modern computer algebra.* Cambridge University Press, New York, 1999.

[7] Gómez-Pérez, D. and Nicolás, A. P.: An estimate on the number of stable quadratic polynomials. *Finite Fields Appl.* **16** (2010), no. 6, 401–405.

[8] Gómez-Pérez, D., Nicolás, A. P., Ostafe, A. and Sadornil, D.: Stable polynomials over finite fields. *Rev. Mat. Iberoam.* **30** (2014), no. 2, 523–535.

[9] Iwaniec, H. and Kowalski, E.: *Analytic number theory.* American Mathematical Society Colloquium Publications 53, Amer. Math. Soc., Providence, RI, 2004.

[10] Jones, R.: The density of prime divisors in the arithmetic dynamics of quadratic polynomials. *J. Lond. Math. Soc. (2)* **78** (2008), no. 2, 523–544.

[11] Jones, R. and Boston, N.: Settled polynomials over finite fields. *Proc. Amer. Math. Soc.* **140** (2012), no. 6, 1849–1863.

[12] Jones, R. and Manes, M.: Galois theory of quadratic rational functions. *Comment. Math. Helv.* **89** (2014), no. 1, 173–213.

[13] Mason, R. C.: *Diophantine equations over functions fields*. London Mathematical Society Lecture Note Series 96, Cambridge University Press, Cambridge, 1984.

[14] McKay, J. H. and Wang, S. S. S.: A chain rule for the resultant of two polynomials. *Arch. Math. (Basel)* **53** (1989), no. 4, 347–351.

[15] Odoni, R. W. K.: The Galois theory of iterates and composites of polynomials. *Proc. London Math. Soc. (3)* **51** (1985), no. 3, 385–414.

[16] Ostafe, A. and Shparlinski, I. E.: On the length of critical orbits of stable quadratic polynomials. *Proc. Amer. Math. Soc.* **138** (2010), no. 8, 2653–2656.

[17] Shparlinski, I. E.: The number of different prime divisors of recurrent sequences. *Mat. Zametki* **42** (1987), no. 4, 494–507

[18] Snyder, N.: An alternate proof of Mason's theorem. *Elem. Math.* **55** (2000), no. 3, 93–94.

[19] Stickelberger, L.: Über eine neue Eigenschaft der Diskriminanten algebraischer Zahlkörper. In *Verh. 1 Internat. Math. Kongresses, 1897*, 182–193. Leipzig, 1898.

[20] Swan, R. G.: Factorization of polynomials over finite fields. *Pacific J. Math.* **12** (1962), 1099–1106.

Received June 22, 2012; revised October 10, 2012.

Domingo Gómez-Pérez: Department of Mathematics, University of Cantabria, Santander 39005, Spain.
E-mail: domingo.gomez@unican.es

Alina Ostafe: School of Mathematics and Statistics, The University of New South Wales, Sydney NSW 2052, Australia.
E-mail: alina.ostafe@unsw.edu.au

Igor E. Shparlinski: Department of Computing, Macquarie University, Sydney, NSW 2109, Australia.
E-mail: igor.shparlinski@unsw.edu.au

D. G.-P. would like to thank Macquarie University for its hospitality and support during his visit in 2012, when this work was initiated. During the preparation of this paper, D. G.-P. was partially supported by the Spanish Government Projects MTM2011-24678 and TIN2011-27479-C04-04, A. O. was partially supported by the Swiss National Science Foundation Grant PA00P2–139679, and I. S. was partially supported by the Australian Research Grant DP130100237.