Rev. Mat. Iberoam., 1–14

Stable Polynomials over Finite Fields

Domingo Gómez-Pérez, Alejandro P. Nicolás,
Alina Ostafe and Daniel Sadornil

Abstract. We use the theory of resultants to study the stability of an arbitrary polynomial f over a finite field $\mathbb{F}_q$, that is, the property of having all its iterates irreducible. This result partially generalises the quadratic polynomial case described by R. Jones and N. Boston. Moreover, for $p = 3$, we show that certain polynomials of degree three are not stable. We also use the Weil bound for multiplicative character sums to estimate the number of stable arbitrary polynomials over finite fields of odd characteristic.

1. Introduction

For a polynomial f of degree at least 2 and coefficients in a field $\mathbb{K}$, we define the following sequence:

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

A polynomial f is *stable* if $f^{(n)}$ is irreducible over $\mathbb{K}$ for all $n \geq 1$. In this article, $\mathbb{K} = \mathbb{F}_q$ is a finite field with q elements, where $q = p^s$ and p an odd prime.

Studying the stability of a polynomial is an exciting problem which has attracted a lot of attention. However, only few results are known and the problem is far away from being well understood.

The simplest case, when the polynomial is quadratic, has been studied in several works. For example, some results concerning the stability over $\mathbb{F}_q$ and $\mathbb{Q}$ can be found in [3, 4, 8, 12, 13]. In particular, by [13, Proposition 2.3], a quadratic polynomial $f(X) = aX^2 + bX + c \in \mathbb{K}[X]$ over a field $\mathbb{K}$ of odd characteristic and with the unique critical point γ, is stable if the set

$$\{-af(\gamma)\} \cup \{f^{(n)}(\gamma) \mid n \geq 2\}$$

contains no squares. In the case when $\mathbb{K} = \mathbb{F}_q$ is a finite field of odd characteristic, this property is also necessary.

Mathematics Subject Classification (2010): Primary 11L40; Secondary 1T55, 11R09, 37F10.
Keywords: finite fields, irreducible polynomial, iterations of polynomials, discriminant.

In [11] an estimate of the number of stable quadratic polynomials over the finite field $\mathbb{F}_q$ of odd characteristic is given, while in [2] it is proved that almost all monic quadratic polynomials $f \in \mathbb{Z}[X]$ are stable over $\mathbb{Q}$. Furthermore, in [2] it is shown that there are no stable quadratic polynomials over finite fields of characteristic two. One might expect that this is the case over any field of characteristic two, which is not true as it is also shown in [2] where an example of a stable quadratic polynomial over a function field of characteristic two is given.

The goal of this paper is to characterize the set of stable polynomials of arbitrary degree and to devise a test for checking the stability of polynomials.

Our techniques come from theory of resultants and they use the relation between irreducibility of polynomials and the properties of the discriminant of polynomials. Using these techniques, we partially generalize previous results known for quadratic polynomials.

A test for stability of quadratic polynomials was given in [15], where it was shown that checking the stability of such polynomials can be done in time $q^{3/4+o(1)}$. As in [13], for an arbitrary polynomial f over $\mathbb{F}_q$, the set defined by

$$\{f^{(n)}(\gamma_1)\dots f^{(n)}(\gamma_k) \ \mid \ n \geq 1 \ \},$$

where γ_i, $i = 1, \dots, k$, are the roots of the derivative of the polynomial f, plays also an important role in checking the stability of f. In particular, we use techniques based on resultants of polynomials together with the Stickelberger's theorem to prove our results. We introduce analogues of the orbit sets defined in [13] for arbitrary degree $d \geq 2$ polynomials. As in [15], we obtain a nontrivial estimate for the cardinality of these sets for polynomials with irreducible derivative. We also give an estimate for the number of stable arbitrary polynomials which generalises the result obtained in [11] for quadratic stable polynomials.

The outline of the paper is the following: in Section 2 we introduce the preliminaries necessary to understand the paper. These include basic results about resultants and discriminants of polynomials. This section ends with the Stickelberger's result. Next, Section 3 is devoted to proving a necessary condition for the stability of a polynomial. We define a set, which generalizes the orbit set for a quadratic polynomial, and then we give an upper bound on the number of elements of this set. Section 4 gives a new proof of the result that appeared in [2] for cubic polynomials when the characteristic is equal to 3. Finally, in Section 5 we give an estimate of the number of stable polynomials for any degree. For that, we relate the number of stable polynomials with estimates of certain multiplicative character sums.

2. Preliminaries

Before proceeding with the main results, it is necessary to introduce some concepts related to commutative algebra. Let $\mathbb{K}$ be any field and let $f \in \mathbb{K}[X]$ be a polynomial of degree d with leading coefficient a_d. The *discriminant* of f, denoted by

$\mathrm{Disc}(f)$, is defined by

$$\mathrm{Disc}(f) = a_d^{2d-2} \prod_{i<j} (\alpha_i - \alpha_j)^2,$$

where $\alpha_1, \ldots, \alpha_d$ are the roots of f in some extension of $\mathbb{K}$.

It is widely known that for any polynomial $f \in \mathbb{K}[X]$, its discriminant is an element of the field $\mathbb{K}$. Alternatively, it is possible to compute $\mathrm{Disc}(f)$ using resultants. We can define the resultant of two polynomials f and g over $\mathbb{K}$ of degrees d and e, respectively, with leading coefficients a_d and b_e, as

$$\mathrm{Res}\,(f, g) = a_d^e b_e^d \prod (\alpha_i - \beta_j),$$

where α_i, β_j are the roots of f and g, respectively.

Like the discriminant, the resultant belongs to $\mathbb{K}$. In the following lemmas we summarize several known results about resultants without proofs. The interested reader can find them in [7, 14].

Lemma 2.1. *Let $f, g \in \mathbb{K}[X]$ be two polynomials of degrees $d \geq 1$ and $e \geq 1$ with leading coefficients a_d and b_e, respectively. Let $\beta_1, \ldots, \beta_e$ be the roots of g in an extension field of $\mathbb{K}$. Then,*

$$\mathrm{Res}\,(f, g) = (-1)^{de} b_e^d \prod_{i=1}^{e} f(\beta_i).$$

The behaviour of the resultant with respect to the multiplication is given by the next result.

Lemma 2.2. *Let $\mathbb{K}$ be any field. Let $f, g, h \in \mathbb{K}[X]$ be polynomials of degree greater than 1 and $a \in \mathbb{K}$. The following hold:*

$$\mathrm{Res}\,(fg, h) = \mathrm{Res}\,(f, h)\,\mathrm{Res}\,(g, h)\,, \qquad \mathrm{Res}\,(af, g) = a^e \mathrm{Res}\,(f, g)\,,$$

where $\deg g = e$.

The relation between $\mathrm{Disc}(f)$ and $\mathrm{Res}\,(f, f')$ is given by the next statement.

Lemma 2.3. *Let $\mathbb{K}$ be any field and $f \in \mathbb{K}[X]$ be a polynomial of degree $d \geq 2$ with leading coefficient a_d, non constant derivative f' and $\deg f' = k \leq d - 1$. Then, we have the relation*

$$\mathrm{Disc}(f) = C_f \mathrm{Res}\,(f, f')\,,$$

where $C_f = (-1)^{\frac{d(d-1)}{2}} a_d^{d-k-2}$.

One of the main tools used to prove our main result regarding the stability of arbitrary polynomials is the Stickelberger's result, see [18] or [19, Corollary 1], which gives the parity of the number of distinct irreducible factors of a polynomial over a finite field of odd characteristic.

Lemma 2.4. *Suppose $f \in \mathbb{F}_q[X]$, q odd, is a polynomial of degree $d \geq 2$ and is the product of r pairwise distinct irreducible polynomials over $\mathbb{F}_q$. Then $r \equiv d \bmod 2$ if and only if* $\mathrm{Disc}(f)$ *is a square in $\mathbb{F}_q$.*

To count the number of stable polynomials of a given degree we also need the Weil bound for character sums, see [14, Chapter 5].

Lemma 2.5. *Let χ be the multiplicative quadratic character of $\mathbb{F}_q$ and let $f \in \mathbb{F}_q[X]$ be a polynomial of positive degree that is not, up to a multiplicative constant, a square polynomial. Let d be the number of distinct roots of f in its splitting field over $\mathbb{F}_q$. Under these conditions, the following inequality holds*

$$\left| \sum_{x \in \mathbb{F}_q} \chi(f(x)) \right| \leq (d-1)q^{1/2}.$$

3. Stability of arbitrary polynomials

In this section we give a necessary condition for the stability of arbitrary polynomials. For this purpose, we use the following general result known as Capelli's Lemma, see [9].

Lemma 3.1. *Let $\mathbb{K}$ be a field, $f, g \in \mathbb{K}[X]$, and let $\beta \in \overline{\mathbb{K}}$ be any root of g. Then $g(f)$ is irreducible over $\mathbb{K}$ if and only if both g is irreducible over $\mathbb{K}$ and $f - \beta$ is irreducible over $\mathbb{K}(\beta)$.*

We prove now one of the main results about the stability of an arbitrary polynomial. We note that our result partially generalises the quadratic polynomial case presented in [13] which is known to be necessary and sufficient over finite fields.

Theorem 3.2. *Let $q = p^s$, p an odd prime, and $f \in \mathbb{F}_q[X]$ a stable polynomial of degree $d \geq 2$ with leading coefficient a_d, non constant derivative f' and $\deg f' = k \leq d-1$. Then the following hold:*

1. *if d is even, then* $\mathrm{Disc}(f)$ *and $a_d^k \mathrm{Res}\left(f^{(n)}, f'\right)$, $n \geq 2$, are nonsquares in $\mathbb{F}_q$;*
2. *if d is odd, then* $\mathrm{Disc}(f)$ *and $(-1)^{\frac{d-1}{2}} a_d^{(n-1)k+1} \mathrm{Res}\left(f^{(n)}, f'\right)$, $n \geq 2$, are squares in $\mathbb{F}_q$.*

Proof. Let $f \in \mathbb{F}_q[X]$ be a stable polynomial. We assume first that d is even. We have that $f^{(n)}$ is irreducible for any n, and thus, by Capelli's Lemma 3.1, we know that $f - \alpha$ is irreducible over $\mathbb{F}_{q^{d^{n-1}}}$, where α is a root of $f^{(n-1)}$. By Lemma 2.4 this means that $\mathrm{Disc}(f - \alpha)$ is a nonsquare in $\mathbb{F}_{q^{d^{n-1}}}$. Now, taking the norm over

$\mathbb{F}_q$ and using Lemma 2.3, we get

$$\begin{aligned}
&\mathrm{Nm}_{q^{d^{n-1}}|q}\mathrm{Disc}(f-\alpha)\\
&\qquad = \prod_{\substack{\alpha\in\mathbb{F}_{q^{d^{n-1}}}\\ f^{(n-1)}(\alpha)=0}} \mathrm{Disc}(f-\alpha) = \prod_{\substack{\alpha\in\mathbb{F}_{q^{d^{n-1}}}\\ f^{(n-1)}(\alpha)=0}} C_f \mathrm{Res}\,(f-\alpha, f')\\
&\qquad = C_f^{d^{n-1}}\mathrm{Res}\left(\prod_{\substack{\alpha\in\mathbb{F}_{q^{d^{n-1}}}\\ f^{(n-1)}(\alpha)=0}} (f-\alpha), f'\right)\\
&\qquad = C_f^{d^{n-1}}\mathrm{Res}\left(\frac{f^{(n-1)}(f)}{A}, f'\right) = A^{-k}C_f^{d^{n-1}}\mathrm{Res}\left(f^{(n)}, f'\right),
\end{aligned}$$

where C_f is defined by Lemma 2.3, A is the leading coefficient of $f^{(n-1)}$ and $\mathrm{Nm}_{q^{d^{n-1}}|q}$ is the norm map from $\mathbb{F}_{q^{d^{n-1}}}$ to $\mathbb{F}_q$.

Since the norm $\mathrm{Nm}_{q^{d^{n-1}}|q}$ maps nonsquares to nonsquares, we obtain that $A^{-k}C_f^{d^{n-1}}\mathrm{Res}\left(f^{(n)}, f'\right)$ is a nonsquare. Taking into account that $A = a_d^{(d^n-1)/(d-1)}$ and the parity of the exponents involved, the result follows. The case of odd d can be treated in a similar way. □

Theorem 3.2 is interesting because it gives a method for testing the stability of a polynomial. Lemma 2.1 says that the resultant is just the evaluation of $f^{(n)}$ in the roots of f' multiplied by some constants. Taking into account this fact, the quadratic character of a_d and the exponents which are involved in Theorem 3.2, we have the following characterisation.

Corollary 3.3. *Let $q = p^s$, p an odd prime, and $f \in \mathbb{F}_q[X]$ a stable polynomial of degree $d \geq 2$ with leading coefficient a_d, non constant derivative f', $\deg f' = k \leq d-1$ and a_{k+1} the coefficient of X^{k+1} in f. Let γ_i, $i = 1, \ldots, k$, be the roots of the derivative f'. Then the following hold:*

1. *if d is even, then*

$$\mathcal{S}_1 = \left\{ a_d^k \prod_{i=1}^{k} f^{(n)}(\gamma_i) \;\mid\; n > 1 \right\} \bigcup \left\{ (-1)^{\frac{d}{2}} a_d^k \prod_{i=1}^{k} f(\gamma_i) \right\} \tag{3.1}$$

   contains only nonsquares in $\mathbb{F}_q$;

2. *if d is odd, then*

$$\mathcal{S}_2 = \left\{ (-1)^{\frac{(d-1)}{2}+k}(k+1)a_{k+1}a_d^{(n-1)k+1} \prod_{i=1}^{k} f^{(n)}(\gamma_i) \;\mid\; n \geq 1 \right\} \tag{3.2}$$

   contains only squares in $\mathbb{F}_q$.

Proof. The result follows directly from Theorem 3.2 and Lemma 2.1. □

We note that the converse of Corollary 3.3 is not true. Indeed, take any d with $\gcd(d, q-1) = \gcd(d, p) = 1$, $\mathbb{F}_q$ an extension of even degree of $\mathbb{F}_p$ and a_0 a quadratic residue in $\mathbb{F}_q$. Let us consider the polynomial $f(X) = (X - a_0)^d + a_0 \in \mathbb{F}_q[X]$. It is straightforward to see that $f^{(n)}(X) = (X - a_0)^{d^n} + a_0$ and that the set (3.2) is

$$\{(-1)^{\frac{d-1}{2}}\, d\, a_0^{d-1}\}.$$

We note that the polynomial f is reducible. Indeed, let the integer $1 \le e \le q-1$ be such that $ed = 1 \pmod{q-1}$. Then $(a_0^e)^d = a_0$, and thus $-a_0^e + a_0$ is a root of f. On the other hand, since -1 and d are squares in $\mathbb{F}_q$ because both elements belong to $\mathbb{F}_p$ and $\mathbb{F}_q$ is an extension of even degree, the set (3.2) contains only squares.

We finish this section by showing that, when the derivative f' of the stable polynomial f is irreducible, the sets (3.1) and (3.2) are defined by a short sequence of initial elements. The proof follows exactly the same lines as in the proof of [15, Theorem 1]. Indeed, assume $\deg f' = k$ and $\gamma_1, \ldots, \gamma_k \in \mathbb{F}_{q^k}$ are the roots of f'. Using Corollary 3.3 we see that the sets (3.1) and (3.2) contain only non-squares and squares, respectively, and thus, the problem reduces to the cases when $f^{(n)}(\gamma_1) \ldots f^{(n)}(\gamma_k)$ are either all squares or all nonsquares for any $n \ge 1$. It is clear that, when f' is irreducible, taking into account that $\gamma_i = \gamma_1^{q^i}$, $i = 1, \ldots, k-1$, we get for every $1 \le n \le N$,

$$\begin{aligned} f^{(n)}(\gamma_1) \ldots f^{(n)}(\gamma_k) &= f^{(n)}(\gamma_1) \ldots f^{(n)}(\gamma_1^{q^{k-1}}) \\ &= f^{(n)}(\gamma_1) \ldots f^{(n)}(\gamma_1)^{q^{k-1}} \ = \mathrm{Nm}_{q^k|q} f^{(n)}(\gamma_1). \end{aligned}$$

Applying now the same technique with multiplicative character sums as in [15, Theorem 1] (as the argument does not depend on the degree of the polynomial f), we obtain the following estimate:

Theorem 3.4. *For any odd q and any stable polynomial $f \in \mathbb{F}_q[X]$ with irreducible derivative f', $\deg f' = k$, there exists*

$$N = O\left(q^{3k/4}\right)$$

such that for the sets (3.1) *and* (3.2) *we have*

$$\mathcal{S}_1 = \left\{ a_d^k \prod_{i=1}^{k} f^{(n)}(\gamma_i) \ \mid \ 1 < n \le N \right\} \bigcup \left\{ \ (-1)^{\frac{d}{2}} a_d^k \prod_{i=1}^{k} f(\gamma_i) \right\},$$

$$\mathcal{S}_2 = \left\{ \ (-1)^{\frac{(d-1)}{2}+k}(k+1) a_{k+1} a_d^{(n-1)k+1} \prod_{i=1}^{k} f^{(n)}(\gamma_i) \ \mid \ 1 \le n \le N \right\}.$$

4. Non-existence of certain cubic stable polynomials when p=3

The existence of stable polynomials is difficult to prove. For $p = 2$, there are no stable quadratic polynomials as shown in [1], whereas for $p > 2$, there is a big number of them as is shown in [11]. In this section, we show that for certain polynomials of degree 3, $f^{(3)}$ is a reducible polynomial when $p = 3$.

This result also appears in [2], but we think this approach uses new ideas that could be of independent interest. For this approach, we need the following result which can be found in [6, Corollary 4.6].

Lemma 4.1. *Let $q = p^s$ and $f(X) = X^p - a_1X - a_0 \in \mathbb{F}_q[X]$ with $a_1a_0 \neq 0$. Then f is irreducible over $\mathbb{F}_q$ if and only if $a_1 = b^{p-1}$ and $\mathrm{Tr}_{q|p}(a_0/b^p) \neq 0$, where $\mathrm{Tr}_{q|p}$ represents the trace map of $\mathbb{F}_q$ over $\mathbb{F}_p$.*

Based on Lemma 4.1, we can present an irreducibility criterium for polynomials of degree 3 in characteristic 3.

Lemma 4.2. *Let $p = 3$ and $q = 3^s$. Then $f(X) = X^3 - a_2X^2 - a_1X - a_0$ is irreducible over $\mathbb{F}_q$ if and only if*

1. *$a_1 = b^2$ and $\mathrm{Tr}_{q|3}(a_0/b^3) \neq 0$, if $a_2 = 0$ and $a_1 \neq 0$;*
2. *$a_2^4/(a_2^2a_1^2 + a_1^3 - a_0a_2^3) = b^2$ and $\mathrm{Tr}_{q|3}(1/a_2b) \neq 0$, if $a_2 \neq 0$.*

Proof. The case $a_2 = 0$ is a direct application of Lemma 4.1. In the other case, we take the polynomial

$$f(X + a_1/a_2) = (X + a_1/a_2)^3 - a_2(X + a_1/a_2)^2 - a_1(X + a_1/a_2) - a_0 = X^3 - a_2X^2 - a_0 + a_1^2/a_2 + a_1^3/a_2^3 = X^3 - a_2X^2 + (a_1^2a_2^2 + a_1^3 - a_0a_2^3)/a_2^3.$$

Notice that $f(X + a_1/a_2)$ is irreducible if and only if $f(X)$ is irreducible.

We denote $g(X) = f(X + a_1/a_2)$ to ease the notation and g^* *the reciprocal polynomial* of g, i. e.

$$g^*(X) = X^3 g\left(\frac{1}{X}\right).$$

By [14, Theorem 3.13], g^* is irreducible if and only if g is. Applying Lemma 4.1, we get the result. □

For simplicity, we proved an irreducibility criterium for monic polynomials, however the proof holds for non-monic polynomials as well taking into account the principal coefficient.

Using Lemma 4.2 and following the same lines as in [1], we can prove now the following result.

Theorem 4.3. *For any polynomial $f \in \mathbb{F}_3[X]$ of the form $f(X) = a_3X^3 - a_1X - a_0$, at least one of the following polynomials $f, f^{(2)}$ or $f^{(3)}$ is a reducible polynomial.*

Proof. Assume that f, $f^{(2)}$, $f^{(3)}$ are all irreducible polynomials. Using Lemma 3.1, $f^{(3)}$ is irreducible if and only if $f^{(2)}$ is irreducible over $\mathbb{F}_q$ and $f-\gamma$ is irreducible over $\mathbb{F}_{q^9}$, where γ is a root of $f^{(2)}$. Thus, the monic polynomial $h = \frac{f-\gamma}{a_3}$ is irreducible over $\mathbb{F}_{q^9}$ and we can apply now Lemma 4.2 from where we get that $\mathrm{Tr}_{q^9|3}\left(\frac{a_0-\gamma}{a_3b^3}\right) \neq 0$, where $b^2 = a_1$ and $b \in \mathbb{F}_{q^9}$.

Notice that $b \in \mathbb{F}_q$. Indeed, as b is the root of the polynomial $X^2 - a_1$, then either $b \in \mathbb{F}_q$ or $b \in \mathbb{F}_{q^2}$. Since $b \in \mathbb{F}_{q^9}$ we obtain that $b \in \mathbb{F}_q$. Using the properties of the trace map we obtain

$$\mathrm{Tr}_{q^9|3}\left(\frac{a_0-\gamma}{a_3b^3}\right) = \mathrm{Tr}_{q^9|3}\left(\frac{-\gamma}{a_3b^3}\right),$$

and from here we conclude that the right hand side of the last equation is non zero. Using now the transitivity of the trace, see [14, Theorem 2.26], we get

$$\mathrm{Tr}_{q^9|3}\left(\frac{-\gamma}{a_3b^3}\right) = \mathrm{Tr}_{q|3}\left(\mathrm{Tr}_{q^9|q}\left(\frac{-\gamma}{a_3b^3}\right)\right) = \mathrm{Tr}_{q|3}\left(\frac{\mathrm{Tr}_{q^9|q}(-\gamma)}{a_3b^3}\right).$$

Now, $f^{(2)}$ is an irreducible polynomial with roots $\gamma, \gamma^q, \ldots, \gamma^{q^8}$. Thus, $\mathrm{Tr}_{q^9|q}(\gamma)$ is given by the coefficient of the term X^8 in $f^{(2)}$, which is zero. This shows that $\mathrm{Tr}_{q^9|3}(\gamma) = 0$, which is a contradiction with the fact that $f^{(3)}$ is irreducible. □

We note that Theorem 4.3 cannot be extended to infinite fields. As in [2], let $\mathbb{K} = \mathbb{F}_3(T)$ be the rational function field in T over $\mathbb{F}_3$, where T is transcendental over $\mathbb{F}_3$. Take $f(X) = X^3 + T \in \mathbb{K}[X]$. Then it is easy to see that

$$f^{(n)}(X) = X^{3^n} + T^{3^{n-1}} + T^{3^{n-2}} + \cdots + T^3 + T.$$

Now from the Eisenstein criterion for function fields (see [17, Proposition III.1.14], for example), it follows that for every $n \geq 1$, the polynomial $f^{(n)}$ is irreducible over $\mathbb{K}$. Hence, f is stable.

5. On the number of stable polynomials

In this section we obtain an estimate for the number of stable polynomials of a given degree d. We use Corollary 3.3 as our main tool.

For a given d, let $f(X) = a_dX^d + a_{d-1}X^{d-1} + \cdots + a_1X + a_0 \in \mathbb{F}_q[X]$ and we define

$$F_l(a_0, \ldots, a_d) = \prod_{i=1}^{k} f^{(l)}(\gamma_i),$$

which is a polynomial in the variables $a_0, \ldots, a_d$ and with coefficients in $\mathbb{F}_q$.

Following [15], the number of stable polynomials of degree d, which will be denoted by S_d, satisfies the inequality

$$S_d \leq \frac{1}{2^K} \sum_{a_0 \in \mathbb{F}_q} \cdots \sum_{a_d \in \mathbb{F}_q^*} \prod_{l=1}^{K} (1 \pm \chi(F_l(a_0, \ldots, a_d))), \tag{5.1}$$

where χ is the multiplicative quadratic character of $\mathbb{F}_q$ and K is an arbitrary positive integer. The sign of χ depends on d and is chosen in order to count the elements of the orbit of f which satisfy the condition of stability. Since the upper bound of S_d is independent of this choice, let us suppose from now on that χ is taken with $+$. If we expand and rearrange the product, we obtain $2^K - 1$ sums of the shape

$$\sum_{a_0 \in \mathbb{F}_q} \cdots \sum_{a_d \in \mathbb{F}_q^*} \chi\left(\prod_{j=1}^{\mu} F_{l_j}(a_0, \ldots, a_d)\right), \ 1 \leq l_1 < \cdots < l_\mu \leq K,$$

with $\mu \geq 1$ plus one trivial sum correponding to 1 in (5.1).

The upper bound for S_d will be obtained using Lemma 2.5. This result can only be used when $\prod_{j=1}^{\mu} F_{l_j}(a_0, \ldots, a_d)$ is not a square polynomial with respect to some variable. The next lemmas are used to estimate the number of values for $a_0, \ldots, a_{i-1}, a_{i+1}, \ldots, a_d$ such that the resulting polynomial in some variable a_i is a square. The first lemma is a bound on the number of common zeros of two multivariate polynomials. For a proof, we refer the reader to [10].

Lemma 5.1. *Let $F(Y_0, Y_1, \ldots, Y_d), G(Y_0, Y_1, \ldots, Y_d)$ be two polynomials of degree d_1 and d_2, respectively, in $d+1$ variables with*

$$\gcd\left(F(Y_0, Y_1, \ldots, Y_d), G(Y_0, Y_1, \ldots, Y_d)\right) = 1.$$

Then, the number of common roots in $\mathbb{F}_q$ is bounded by $d_1 d_2 q^{d-1}$.

Based on Lemma 5.1, the next result shows that, if the degree of a polynomial $G(Y_0, Y_1, \ldots, Y_d)$ in a variable Y_i is greater than 1, then it is possible to bound the number of "bad" choices for $a_0, \ldots, a_{i-1}, a_{i+1}, \ldots, a_d$, that is, the number of choices for $a_0, \ldots, a_{i-1}, a_{i+1}, \ldots, a_d$ such that $G(a_0, \ldots, a_{i-1}, Y_i, a_{i+1}, \ldots, a_d)$ is a square polynomial in Y_i.

Lemma 5.2. *Let $G \in \mathbb{F}_q[Y_0, \ldots, Y_d]$ be a polynomial of degree D, which is not a square polynomial in the algebraic closure of $\mathbb{F}_q$. Then there exists $i \in \{0, \ldots, d\}$ such that $G(a_0, \ldots, a_{i-1}, Y_i, a_{i+1}, \ldots, a_d)$ is not a square polynomial in Y_i for all but at most $O(D^2 q^{d-1})$ values of $a_0, \ldots, a_{i-1}, a_{i+1}, \ldots, a_d \in \mathbb{F}_q$.*

Proof. Let $G(Y_0, \ldots, Y_d) = G_1(Y_0, \ldots, Y_d)^{d_1} \cdots G_h(Y_0, \ldots, Y_d)^{d_h}$ the decomposition of the polynomial in a product of irreducible polynomials.

Without loss of generality, d_1 is odd because G is not a square of a polynomial up to a multiplicative constant. Moreover, because G_1 is an irreducible factor of G, then $\deg G_1 \leq D$.

We suppose that $G_1(Y_0, \ldots, Y_d)$ depends on some variable Y_i and use it to count the number of choices for $a_0, \ldots, a_{i-1}, a_{i+1}, \ldots, a_d$ such that

- $G(a_0, \ldots, a_{i-1}, Y_i, a_{i+1}, \ldots, a_d)$ is a constant polynomial,
- $G(a_0, \ldots, a_{i-1}, Y_i, a_{i+1}, \ldots, a_d)$ is a nonconstant square polynomial up to a multiplicative constant in the variable Y_i.

There are at most Dq^{d-1} different choices of $a_0, \ldots, a_{i-1}, a_{i+1}, \ldots, a_d$ when the polynomial can be a constant.

Now, we consider in which cases the polynomial is a square of a polynomial when we substitute $a_0, \ldots, a_{i-1}, a_{i+1}, \ldots, a_d$ and how these cases will be counted. We have the following two possible situations:

- $G_1^{d_1}$ is a square, nonconstant polynomial, and because d_1 is not even, then we must have that G_1 has at least one multiple root as a polynomial in Y_i. This is only possible if G_1 and the first derivative with respect to the variable Y_i of G_1 have a common root. Since G_1 is an irreducible polynomial, Lemma 5.1 applies. We remark that the first derivative is a nonzero polynomial. Otherwise G_1 is a reducible polynomial. This can only happen in $(\deg G_1)(\deg G_1 - 1)q^{d-1}$ cases.
- G_1 and G_j have a common root for some $1 \le j \le h$. In this case, using the same argument, there are at most $(\deg G_1)(\deg G_j)q^{d-1}$ possible values for $a_0, \ldots, a_{i-1}, a_{i+1}, \ldots, a_d$ where it happens.

This concludes the proof. □

From Lemmas 2.5 and 5.2, we have the following corollary.

Corollary 5.3. *If $G(Y_0, \ldots, Y_d)$ is a polynomial of degree D, which is not a square polynomial in the algebraic closure of $\mathbb{F}_q$, then*

$$\sum_{a_0,\ldots,a_d \in \mathbb{F}_q} \chi(G(a_0, \ldots, a_d)) = O\left(Dq^{d+1/2}\right)$$

where χ is the quadratic character of $\mathbb{F}_q$.

Proof. The proof follows directly by applying Lemma 2.5 for those polynomials which are nonsquares in some variable a_i. Since these polynomials have degree at most D in the indeterminate a_i (see the proof of Lemma 5.2), we obtain $O(Dq^{d+1/2})$ for this part. For the rest, that is, the square polynomials in the variable a_i, we can apply Lemma 5.2 and use the trivial bound for $O(D^2q^{d-1})$ values of $a_0, \ldots, a_{i-1}, a_{i+1}, \ldots, a_d$. So the total bound becomes $O\left(Dq^{d+1/2} + D^2q^d\right)$. Noticing that for $D > q^{1/2}$ the claimed result is weaker that the trivial bound q^{d+1}, we conclude the proof. □

To use Corollary 5.3 in counting the number of stable polynomials of degree d, we need the following lemma.

Lemma 5.4. *There exists $i = 1, \ldots, m$ such that, for fixed integers $l_1, \ldots, l_\mu$ with $1 \le l_1 < \cdots < l_\mu \le K$, there are at most $O(d^{2K}q^{d-1})$ choices for $a_0, \ldots, a_{i-1}, a_{i+1}, \ldots, a_d$ such that the polynomial*

$$\prod_{j=1}^{\mu} F_{l_j}(a_0, \ldots, a_{i-1}, A_i, a_{i+1}, \ldots, a_d)$$

is a square polynomial in the variable A_i up to a multiplicative constant.

Proof. The proof follows from Lemma 5.2. For this we have to prove that the polynomial

$$\prod_{j=1}^{\mu} F_{l_j}(A_0, \ldots, A_d) \tag{5.2}$$

is not a square polynomial as a multivariate polynomial, up to a multiplicative constant, and, to obtain this, it is enough to prove it for particular choices of the variables.

If the degree d of f is even and coprime to p, we consider the polynomial $f = (X-B)^d+C+B$, where $B,\ C$ are considered as variables. Then $f' = d(X-B)^{d-1}$ (here f' represents the derivative with respect to the variable X) and

$$f^{(n)}(B) = B + H_n(C),$$

where $\deg H_n(C) = d^{n-1}$. Thus, as d is even, we have

$$\prod_{j=1}^{\mu} F_{l_j}(A_0, \ldots, A_d) = \prod_{j=1}^{\mu} (B + H_{l_j}(C))^{d-1},$$

which is not a square polynomial as a multivariate polynomial up to a multiplicative constant.

If d is odd, coprime to p, we consider the following polynomial $f = (X - B)^{d-1}(X-B+1)+C+B$ with the derivative $f' = (X-B)^{d-2}(d(X-B)+d-1)$. Notice that, if the degree of this polynomial is coprime to the characteristic p, then f' has two different roots $B,\ B+(1-d)d^{-1}$. Substituting these in the polynomial f, we get

$$\begin{aligned} f^{(n)}(B) &= B + H_n(C), \\ f^{(n)}(B + (1-d)d^{-1}) &= B + L_n(C), \end{aligned}$$

where $L_n(C) \neq H_n(C)$ and $\deg L_n(C) = \deg H_n(C) = d^{n-1}$. The fact that $L_n(c) \neq H_n(c)$ comes from the following observation:

$$\begin{aligned} H_n(C) &= (H_{n-1}(C))^{d-1}(H_{n-1}(C)+1) + C, \\ L_n(C) &= (L_{n-1}(C))^{d-1}(L_{n-1}(C)+1) + C, \end{aligned} \tag{5.3}$$

where $H_1(C) = C$, and $L_1(C) = C + (1-d)d^{-2}$. It is clear that $H_1(C) \neq L_1(C)$, so now we suppose that $H_n(C) = L_n(C)$ and using the equation (5.3), we get

$$(H_{n-1}(C))^{d-1}(H_{n-1}(C)+1) + C = (L_{n-1}(C))^{d-1}(L_{n-1}(C)+1) + C$$

and thus

$$(C^d + C^{d-1}) \circ H_{n-1}(C) = (C^d + C^{d-1}) \circ L_{n-1}(C).$$

Applying now the Ritt decomposition theorem, see [16], we obtain $H_{n-1}(C) = L_{n-1}(C)$.

In this case, as d is odd, we have

$$\prod_{j=1}^{\mu} F_{l_j}(A_0, \ldots, A_d) = \prod_{j=1}^{\mu} (B + H_{l_j}(C))^{d-2}(B + L_{l_j}(C)),$$

which is not a square polynomial as a multivariate polynomial up to a multiplicative constant.

When the degree of f is not coprime to the characteristic of the field, take $f = (X - B)^d + (X - B)^2 + C + B$ and one can prove following the same path as for the last two cases that the polynomial (5.2) is not a perfect square as a multivariate polynomial up to a multiplicative constant.

The result now follows by applying Lemma 5.2 to the polynomial (5.2). In this case, as in the proof of Lemma 5.2, because G_1 is an irreducible factor of the polynomial (5.2), then there exists $1 \le j \le \mu$ such that G_1 is an irreducible factor of the polynomial $F_{l_j}(A_0, \ldots, A_d)$, which implies that $\deg G_1 \le d^K$. □

Now we are able to find a bound for S_d, the number of stable polynomials of degree d.

Theorem 5.5. *The number of stable polynomials of degree d is $O\left(q^{d+1-1/2\log(2d)}\right)$.*

Proof. The trivial summand of (5.1) can be bounded by $O(q^{d+1}/2^K)$. For the other terms, we apply Corollary 5.3 and Lemma 5.4. Then,

$$S_d = O(q^{d+1}/2^K + d^K q^{d+1/2}).$$

Choosing $K = \lceil \log q / 2\log(2d) \rceil$ the result follows. □

Unfortunately we have not been able to give a lower bound for S_d similar to the quadratic case obtained in [11, Theorem 1]. This is because we do not have a necessary and sufficient condition for the stability of polynomials of degree $d > 2$. We can however show that very frequently we have $S_d \ge \varphi(q-1)$, where $\varphi(k)$ is the Euler function, which comes from the following construction. Assume that a positive integer d and $b \in \mathbb{F}_q$ are such that the binomial $X^d + b$ is irreducible over $\mathbb{F}_q$. By [14, Theorem 3.75], we know that $X^d + b$ is irreducible if and only if each prime factor of d divides the order e of b, but not $(q-1)/e$, and $q \equiv 1 \pmod 4$ if $t \equiv 0 \pmod 4$. If $d \mid (q-1)$ and b is a primitive element of $\mathbb{F}_q$, then $X^d + b$, and thus also $f = (X - b)^d + b \in \mathbb{F}_q[X]$, are irreducible. Furthermore, one can easily prove that $f^{(n)} = (X - b)^{d^n} + b$ is also irreducible for every $n \ge 2$. Since there are $\varphi(q-1)$ primitive elements in $\mathbb{F}_q$ we obtain $S_d \ge \varphi(q-1)$.

Acknowledgement

The authors would like to thank Igor Shparlinski for useful discussions and comments which improved the presentation of the paper and for several corrections in Section 5. We are also grateful to the referee for the useful suggestions.

A. N. was supported by MTM2010-18370-C04-01, A. O. was supported by SNSF Grant 133399 and D. S. was supported by MTM2010-21580-C02-02 and MTM2010-16051.

References

[1] O. Ahmadi. 'A note on stable quadratic polynomials over fields of characteristic two'. *Preprint*, 2010 (available from `http://arxiv.org/abs/0910.4556`).

[2] O. Ahmadi, F. Luca, A. Ostafe, I. Shparlinski. 'On stable quadratic polynomials'. *Glasgow Math. J.*, 54:59-369, 2012.

[3] N. Ali. 'Stalilité des polynômes'. *Acta Arithmetica*, 119:53–63, 2005.

[4] M. Ayad D. L. McQuillan. 'Irreducibility of the iterates of a quadratic polynomial over a field'. *Acta Arithmetica*, 93(1):87–97, 2000.

[5] E. R. Berlekamp. *'Algebraic coding theory'*. McGraw-Hill Book Co., New York, 1968.

[6] I. Blake, X. Gao, A. Menezes R. Mullin. *'Application of finite fields'*. Kluwer, 1993.

[7] D. Cox, J. Little, D. O'Shea. *'Ideals, varieties, and algorithms. An introduction to computational algebraic geometry and commutative algebra.'*. Undergraduate Texts in Mathematics. Springer, New York. 2007.

[8] L. Danielson B. Fein. 'On the irreducibility of the iterates of $x^n - b$.' *Proc. Am. Math. Soc.*, 130(6):1589–1596, 2002.

[9] B. Fein M. Schacher. 'Properties of iterates and composites of polynomials'. *J. London Math. Soc.*, 54(3):489–497, 1996.

[10] J. von zur Gathen J. Gerhard. *'Modern computer algebra'*. Cambridge University Press, 1999.

[11] D. Gómez A. P. Nicolás. 'An estimate on the number of stable quadratic polynomials'. *Finite Field and their Applications*, 16(6):401–405, 2010.

[12] R. Jones. 'The density of prime divisors in the arithmetic dynamics of quadratic polynomials'. *J. Lond. Math. Soc.*, 78:523–544, 2008.

[13] R. Jones N. Boston. 'Settled polynomials over finite fields'. *Proc. Amer. Math. Soc.*, 140:1849–11863, 2012.

[14] R. Lidl H. Niederreiter. *'Finite fields'*, volume 20 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, 1997.

[15] A. Ostafe I. Shparlinski. 'On the length of critical orbits of stable quadratic polynomials'. *Proc. Amer. Math. Soc.*, 138(8):2653–2656, 2010.

[16] J. Ritt. 'Prime and composite polynomials'. *Trans. Amer. Math. Soc.*, 23:51–66, 1922.

[17] H. Stichtenoth. *'Algebraic function fields and codes'*. Springer-Verlag, Berlin, 1993.

[18] L. Stickelberger. 'Uber eine neue eigenschaft der diskriminanter algebraischer zahlkorper. *Verh. 1 Internat. Math. Kongresses*, 1897.

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

Received ??

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

Alejandro P. Nicolás: Departamento de Matemática Aplicada, Universidad de Valladolid, Spain
E-mail: anicolas@maf.uva.es

Alina Ostafe: Department of Computing, Macquarie University, Sydney, NSW 2109, Australia
E-mail: alina.ostafe@mq.edu.au

Daniel Sadornil: Department of Mathematics, University of Cantabria, Santander 39005, Spain
E-mail: dsadornild@unican.es