Glasgow Math. J. **54** (2012) 359–369. © Glasgow Mathematical Journal Trust 2012.
doi:10.1017/S001708951200002X.

ON STABLE QUADRATIC POLYNOMIALS

OMRAN AHMADI
Claude Shannon Institute, University College Dublin, Dublin 4, Ireland
e-mail:omran.ahmadi@ucd.ie

FLORIAN LUCA
Instituto de Matemáticas, Universidad Nacional Autonoma de México,
C.P. 58089, Morelia, Michoacán, Mexico
e-mail: fluca@matmor.unam.mx

ALINA OSTAFE
Institut für Mathematik, Universität Zürich, Winterthurerstrasse 190 CH-8057, Zürich, Switzerland
e-mail: alina.ostafe@math.uzh.ch

and IGOR E. SHPARLINSKI
Department of Computing, Macquarie University, Sydney, NSW 2109, Australia
e-mail: igor.shparlinski@mq.edu.au

(Received 27 June 2010; revised 15 April 2011; accepted 10 October 2011)

Abstract. We recall that a polynomial $f(X) \in K[X]$ over a field K is called stable if all its iterates are irreducible over K. We show that almost all monic quadratic polynomials $f(X) \in \mathbb{Z}[X]$ are stable over $\mathbb{Q}$. We also show that the presence of squares in so-called critical orbits of a quadratic polynomial $f(X) \in \mathbb{Z}[X]$ can be detected by a finite algorithm; this property is closely related to the stability of $f(X)$. We also prove there are no stable quadratic polynomials over finite fields of characteristic 2 but they exist over some infinite fields of characteristic 2.

2010 *Mathematics Subject Classification.* 11C08, 11T06, 37P05

1. Introduction. For a field K and a polynomial $f(X) \in K[X]$ we define the sequence of iterations:

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

Following [**1**, **2**, **12**, **13**, **14**], we say that $f(X)$ is *stable* if all polynomials $f^{(n)}(X)$ are irreducible over K.

As in [**13**], for a quadratic polynomial $f(X) = aX^2 + bX + c \in K[X]$, where the characteristic of K is not 2, we define $\gamma = -b/2a$ as the unique critical point of f (that is, zero of the derivative f') and consider the set

$$\mathrm{Orb}(f) = \big\{f^{(n)}(\gamma) \ : \ n = 2, 3, \dots\big\},$$

which is called the *critical orbit* of f (we note that this definition is more convenient for our purpose but slightly deviates from the one more common in literature which also includes $f^{(1)}(\gamma) = f(\gamma)$ in $\mathrm{Orb}(f)$).

If $K = \mathbb{F}_q$, q odd, clearly there is some t such that $f^{(t)}(\gamma) = f^{(s)}(\gamma)$ for some positive integer $s < t$. Then $f^{(n+t)}(\gamma) = f^{(n+s)}(\gamma)$ for any $n \geqslant 0$. Accordingly, for the smallest value of t with the above property denoted by t_f, we have

$$\mathrm{Orb}(f) = \{f^{(n)}(\gamma) \ : \ n = 2, \ldots, t_f\}$$

and $\#\mathrm{Orb}(f) = t_f - 1$ or $\#\mathrm{Orb}(f) = t_f - 2$ (depending whether $s = 1$ or $s \geqslant 2$).

It is shown in [**11**, **12**, **13**] that critical orbits play a very important role in the dynamics of polynomial iterations. In particular, by [**13**, Proposition 2.3], a quadratic polynomial $f(X) \in K[X]$ is stable if the set $\{-f(\gamma)\} \cup \mathrm{Orb}(f)$ contains no squares. In the case when $K = \mathbb{F}_q$ is a finite field of odd characteristic, this property is also necessary.

Here, we obtain several more results about stable polynomials. First of all we show that non-stable quadratic polynomials over $\mathbb{Z}$ form a very sparse set. This is certainly expected since most polynomials over $\mathbb{Z}$ are irreducible. Thus treating $f^{(n)}$ as "random" polynomials of degree 2^n, we arrive to the above heuristic expectation. We also show that the existence of squares in critical orbits of quadratic polynomials over $\mathbb{Z}$ can be effectively tested.

We note that for finite fields the situation is quite different. For example, Gomez and Nicolás [**7**], developing some ideas from [**15**], have proved that there are $O(q^{5/2}(\log q)^{1/2})$ stable quadratic polynomials over $\mathbb{F}_q$ for an odd prime power q. Note that in [**7**] a weaker bound $O(q^{5/2} \log q)$ is asserted but optimising the choice of the parameter K to satisfy $2^K \leqslant q^{1/2}(\log q)^{-1/2} \leqslant 2^{K+1}$ in the proof of [**7**, Theorem 1], one easily obtains the claimed improvement, see also [**8**] for an upper bound on the number of stable polynomials of a given degree d over $\mathbb{F}_q$. Here, we extend the result of [**15**] on the length of critical orbits of stable quadratic polynomials over a finite field of odd characteristic to stable compositions of quadratic polynomials with an arbitrary polynomial.

We also show that over finite fields of characteristic 2 stable quadratic polynomials do not exist. In fact, we derive it as a corollary of a more general result about stability of shifted *linearised polynomials*.

2. Stable polynomials over $\mathbb{Q}$.

Using [**12**, Theorem 4.4], we first show that almost all monic quadratic polynomials $f(X) \in \mathbb{Z}[X]$ are stable over $\mathbb{Q}$.

THEOREM 1. *Let $E(A, B)$ be the number of pairs $(a, b) \in \mathbb{Z}^2$ with $|a| \leqslant A$ and $|b| \leqslant B$ for which $f(X) = X^2 + aX + b$ is irreducible but not stable over $\mathbb{Q}$. Then we have*

$$E(A, B) = O\left(\min\{A^{3/2}, B^{3/4}\}\right).$$

Proof. Given an irreducible polynomial $f(X) = X^2 + aX + b \in \mathbb{Z}[X]$, we denote by $\gamma = -a/2$ its critical point and write it as

$$f(X) = (X - \gamma)^2 + \delta,$$

where

$$\delta = b - a^2/4.$$

https://doi.org/10.1017/S001708951200002X Published online by Cambridge University Press

By [**12**, Theorem 4.4], we see that if $f(X)$ is not stable over $\mathbb{Q}$, then either

$$|\delta - \gamma| \leqslant 6 + 3\sqrt{|\gamma| + 1}, \tag{1}$$

or

$$\sqrt{f^{(2)}(\gamma)} \in \mathbb{Q}. \tag{2}$$

Clearly, condition (1) implies that $b = a^2/4 + O(|a|^{1/2})$. Thus, if $|b| \leqslant B$ then the above condition can be satisfied only if $|a| \leqslant C_1 B^{1/2}$ where $C_1 > 0$ is some absolute constant. Furthermore, for every fixed a, there are at most $O(|a|^{1/2})$ possible values of b. Thus, (1) holds for at most

$$O\left(\sum_{|a| \leqslant \min\{A, C_1 B^{1/2}\}} |a|^{1/2}\right) = O\left(\min\{A^{3/2}, B^{3/4}\}\right)$$

pairs $(a, b) \in \mathbb{Z}^2$ with $|a| \leqslant A$ and $|b| \leqslant B$.

For condition (2), we note that

$$\begin{aligned} f^{(2)}(\gamma) &= \frac{a^4 - 4a^3 - 8a^2 b + 16ab + 16b^2 + 16b}{16} \\ &= \frac{(2b + a^2 - 2a - 2)^2 - (8a + 4)}{16}. \end{aligned}$$

Hence, if (2) is satisfied, then

$$(2b + a^2 - 2a - 2)^2 - (8a + 4) = r^2$$

for some integer r, which implies that

$$(s - r)(s + r) = 8a + 4, \tag{3}$$

where $s = 2b + a^2 - 2a - 2$.

We now see that for a fixed value for a, the number of solutions $(r, s) \in \mathbb{Z}^2$ to equation (3) is at most $2\tau(|8a + 4|)$, where $\tau(k)$ is the number of positive integer divisors of an integer $k \geqslant 1$. We also notice that when a and s are fixed, the number b is uniquely defined.

Furthermore, since $r - s$ and $r + s$ are divisors of $8a + 4$, we have $s = O(|a|) = O(A)$. Thus, $b = a^2 + O(A)$. This implies that (2) is possible only for $|a| \leqslant C_2 B^{1/2}$, where $C_2 > 0$ is some absolute constant.

Thus, using the well-known bound on the mean value of the divisor function (see [**9**, Theorem 320]), we conclude that (2) holds for at most

$$\begin{aligned} 2 \sum_{|a| \leqslant \min\{A, C_2 B^{1/2}\}} \tau(|8a + 4|) &\leqslant 2 \sum_{k \leqslant 8\min\{A, C_2 B^{1/2}\} + 4} \tau(k) \\ &= O\left(\min\{A \log A, B^{1/2} \log B\}\right) \end{aligned}$$

pairs $(a, b) \in \mathbb{Z}^2$ with $|a| \leqslant A$ and $|b| \leqslant B$, and this last expression is dominated by the number of such pairs for which (1) holds. $\square$

Taking $A = B = H$ we obtain:

Corollary 2. *Let $E(H)$ be the number of pairs $(a, b) \in \mathbb{Z}^2$ with*

$$\max\{|a|, |b|\} \leqslant H$$

for which $f(X) = X^2 + aX + b$ is irreducible but not stable over $\mathbb{Q}$. We then have

$$E(H) = O(H^{3/4}).$$

We also derive from Theorem 1 and [**7**, Lemma 2] that almost all quadratic polynomials $f(X) \in \mathbb{Z}[X]$ are stable over $\mathbb{Q}$. To prove this, we need the following result which is given in [**7**, Lemma 2] for the case of finite fields. However, its proof applies to any field.

Lemma 3. *Let $\mathbb{F}$ be a field. Let $f(X) \in \mathbb{F}[X]$ and $\alpha \in \mathbb{F}^*$. Then $f(X)$ is stable if and only if $g(X) = \alpha^{-1}f(\alpha X)$ is stable.*

Theorem 4. *Let $F(H)$ be the number of triples $(a, b, c) \in \mathbb{Z}^3$ with*

$$\max\{|a|, |b|, |c|\} \leqslant H$$

for which $f(X) = aX^2 + bX + c$ is irreducible but not stable over $\mathbb{Q}$. We then have

$$F(H) \leqslant H^{3/2+o(1)} \quad \text{as} \quad H \to \infty.$$

Proof. Discarding the $O(H^2)$ triples (a, b, c) with $a = 0$ and $\max\{|b|, |c|\} \leqslant H$, we note that Lemma 3 taken with $\alpha = a^{-1}$, implies that $f(X) = aX^2 + bX + c \in \mathbb{Z}[X]$ is stable if and only if $g(X) = X^2 + bX + ac$ is stable. We also see that each such polynomial $g(X)$ corresponds to at most $\tau(|g(0)|)$ values of a and c, and thus to at most $\tau(|g(0)|)$ polynomials $f(X)$. Recalling the estimate $\tau(k) = k^{o(1)}$ as $k \to \infty$ on the divisor function (see [**9**, Theorem 317]), we derive that

$$F(H) \leqslant E(H, H^2)H^{o(1)} \qquad \text{as} \quad H \to \infty.$$

Applying Theorem 1, we conclude the proof. □

Although over $K = \mathbb{Q}$ the property that the set $\{-f(\gamma)\} \cup \mathrm{Orb}(f)$ contains no squares is known not to be necessary, it is still interesting to understand whether it can be efficiently tested.

Theorem 5. *For an irreducible polynomial $f(X) = aX^2 + bX + c \in \mathbb{Z}[X]$, if $f^{(n)}(\gamma)$ is a square, then*

$$n < \exp\left(2^{1377}H^{80}\right),$$

where $H = \max\{|a|, |b|, |c|, 3\}$.

Proof. Put $g(X) = X^2 + 2bX + 4ac$. By applying repeatedly the relation $4af(x) = g(2ax)$, we have for all $n \geqslant 2$,

$$a2^{n+1}f^{(n)}(x) = g\big(a2^n f^{(n-1)}(x)\big) = g^{(2)}\big(a2^{n-1}f^{(n-2)}x\big) = \cdots = g^{(n)}(2ax).$$

https://doi.org/10.1017/S001708951200002X Published online by Cambridge University Press

Thus, $2^{n+1}af^{(n)}(\gamma) = g^{(n)}(-b) \in \mathbb{Z}$. If $\delta \in \{0, 1\}$ is such that $n + 1 \equiv \delta \pmod 2$, then we write $2^{\delta}a = a_0a_1^2$, where a_0 and a_1 are integers with a_0 squarefree. We now see that if $f^{(n)}(\gamma) = \eta^2$ for some rational number η, then

$$g^{(n)}(-b) = 2^{n+1}a\eta^2 = a_0(2^{(n+1-\delta)/2}a_1\eta)^2 \in \mathbb{Z},$$

which implies that $y = 2^{(n+1-\delta)/2}a_1\eta \in \mathbb{Z}$. Thus, putting $x = g^{(n-2)}(-b)$, we get that (x, y) is an integer solution to

$$g^{(2)}(x) = a_0y^2. \tag{4}$$

Put

$$G(X) = a_0g^{(2)}(X) = c_0X^4 + c_1X^3 + c_2X^2 + c_3X + c_4, \tag{5}$$

where

$$\begin{aligned} &c_0 = a_0, \quad c_1 = a_0b, \quad c_2 = a_0(4b^2 + 8ac + 2b),\\ &c_3 = a_0(16abc + 4b^2), \quad c_4 = a_0(16a^2c^2 + 8abc + 4ac). \end{aligned} \tag{6}$$

Putting $z = a_0y$, we see that equation (4) leads to an integer solution (x, z) to the equation

$$G(x) = z^2. \tag{7}$$

We now observe that $G(X)$ has only simple roots. For if not, there exists a common root ζ of $G(\zeta) = a_0g(g(\zeta))$ and $G'(\zeta) = a_0g'(g(\zeta))g'(\zeta)$. If $g'(\zeta) = 0$, then $\zeta = -b \in \mathbb{Z}$, so $g(\zeta)$ is an integer root of $g(X)$, which is false because $g(X)$ is irreducible since it is obtained from $f(X)$ by an affine transformation. Similarly, if $g'(g(\zeta)) = 0$, we get that $g(\zeta) = -b$ is an integer root of both $g'(X)$ and $g(X)$, which again contradicts the irreducibility of $g(X)$. By the celebrated result of Baker [**3**], if

$$F(X) = c_0X^d + c_1X^{d-1} + \cdots + c_d \in \mathbb{Z}[X]$$

is a polynomial of degree d with at least three simple roots, then all integer solutions (u, v) of the diophantine equation $F(u) = v^2$ satisfy

$$\max\{|u|, |v|\} \leqslant \exp(\exp(\exp((d^{10d}K)^{d^2}))),$$

where $K = \max\{|c_0|, \ldots, |c_m|\}$. We apply this with $F(X) = G(X)$, which has $d = 4$ simple roots. From list (6), and the fact that $|a_0| \leqslant 2|a|$, one checks easily that $K \leqslant 56H^5$. Thus,

$$(d^{10d}K)^{d^2} \leqslant (4^{40} \times 56 \times H^5)^{16} < (4^{43} \times H^5)^{16} = 2^{1376}H^{80}.$$

Thus, we get that

$$|g^{(n-2)}(-b)| \leqslant \exp\left(\exp\left(\exp\left(2^{1376}H^{80}\right)\right)\right). \tag{8}$$

We next show that if $u \in \mathbb{Z}$ is such that $|u| > H^8$, then $|g(u)| > |u|^{e^{1/e}}$. Indeed, observe that for such u we have

$$|g(u)| \geqslant |u|^2 - (4H^2+2)|u| \geqslant u^2 - (H^4-1)|u|^{e^{1/e}} > |u|^{e^{1/e}}. \tag{9}$$

The first inequality above is obvious, the second follows from the fact that $H^4 - 1 > 2H^2 + 2$, which is true for all $H \geqslant 3$, whereas the third follows because it is equivalent to

$$|u| > H^{4/(2-e^{1/e})},$$

which holds for us because $|u| > H^8$ and $8 > 4/(2-e^{1/e})$.

We now compute $g^{(m)}(-b)$ for all $m = 1, 2, \ldots, 2H^8+2$. Assume first that $|g^{(m)}(-b)| \leqslant H^8$ for all such m. Since there are $2H^8+2$ such m and only $2H^8+1$ integers v such that $|v| \leqslant H^8$, it follows that there exists $m_1 < m_2$ such that $g^{(m_1)}(-b) = g^{(m_2)}(-b)$. Thus, in this case $\mathcal{H} = \mathrm{Orb}(g)$ is finite and since $2^{n+1}af^{(n)}(\gamma) \in \mathcal{H}$ for all positive integers n, we get that

$$\lim_{n\to\infty} f^{(n)}(\gamma) = 0,$$

which contradicts the recurrence

$$f^{(n+1)}(\gamma) = f(f^{(n)}(\gamma)) = a(f^{(n)}(\gamma))^2 + bf^{(n)}(\gamma) + c$$

as $c \neq 0$. This implies that there exists m_0 in $\{1, 2, \ldots, 2H^8+2\}$ with $|g^{(m_0)}(-b)| > H^8$. Then, by (9), putting $B = g^{(m_0)}(-b)$, we have

$$|g^{(m_0+1)}(-b)| = |g(B)| > |B|^{e^{1/e}}$$

and then by a simple inductive argument we derive

$$|g^{(n-2)}(-b)| = |g^{(m_0+(n-m_0-2))}(B)| > |B|^{e^{(n-m_0-2)/e}}.$$

Comparing the last inequality above with (8), and using that $B \geqslant H^8 > e$, we get

$$\exp(n-m_0-2)/e) < \exp\left(\exp\left(2^{1376}H^{80}\right)\right),$$

so

$$\begin{aligned} n &< \exp\left(2^{1376}H^{80}+1\right) + m_0 + 2 \leqslant \exp\left(2^{1376}H^{80}+1\right) + 2H^8 + 3 \\ &< \exp\left(2^{1377}H^{80}\right), \end{aligned}$$

which concludes the argument. □

In particular we see from Theorem 5 that the presence of squares in $\mathrm{Orb}(f)$ can be detected in a finitely many steps.

3. Stable polynomials over finite fields. As in [**15**], we estimate the length of the critical orbit, and therefore the complexity of testing even degree polynomials $f(X)$ in $\mathbb{F}_q[X]$, with q odd, for stability.

We need first the following result (see [**13**, Lemma 2.5]), which characterises completely the stability of quadratic polynomials over finite fields:

Lemma 6. *Let K be a field of odd characteristic, $f(X) = aX^2 + bX + c \in K[X]$, and $\gamma = -b/2a$ be the critical point of f. Suppose that $h \in K[X]$ is such that $h(f^{(n-1)})$ has degree d and is irreducible over K for some $n \geqslant 1$. Then $h(f^{(n)})$ is irreducible over K if $(-a)^d h(f^{(n)}(\gamma))$ is not a square in K. If K is finite then we may replace the "if" statement with an "if and only if" statement.*

Given two polynomials f and $g \in \mathbb{F}_q[X]$, we write $g \circ f$ for the composition $F(X) = g(f(X))$.

Let now f be an irreducible quadratic polynomial and $g \in \mathbb{F}_q[X]$ be an irreducible polynomial of degree d. Define $F = g \circ f \in \mathbb{F}_q[X]$ which is a polynomial of degree $2d$.

By Lemma 6, taken with $n = 1$ and $h = F^{(n-1)} \circ g$ we have the following easy result:

Lemma 7. *Let $F = g \circ f \in \mathbb{F}_q[X]$, where $f, g \in \mathbb{F}_q[X]$ and $\deg f = 2$. Assume that $F^{(n-1)} \circ g$ is irreducible over $\mathbb{F}_q$ for some $n \geqslant 1$. Then $F^{(n)}$ is irreducible over $\mathbb{F}_q$ if and only if $F^{(n)}(\gamma)$ is not a square in $\mathbb{F}_q$, where $\gamma = -b/2a$ is the critical point of f.*

We consider the set

$$\mathrm{Orb}_\gamma(F) = \left\{F^{(n)}(\gamma) \ : \ n = 2, 3, \ldots\right\},$$

which for $g(X) = X$ coincides with $\mathrm{Orb}(f)$. We call it the γ-*critical orbit* of F. As before, we notice that there is some t such that $F^{(t)}(\gamma) = F^{(s)}(\gamma)$ for some positive integer $s < t$. Then $F^{(n+t)}(\gamma) = F^{(n+s)}(\gamma)$ for any $n \geqslant 0$. Accordingly, we denote by t_F the smallest value of t with the above condition. We then have

$$\mathrm{Orb}_\gamma(F) = \left\{F^{(n)}(\gamma) \ : \ n = 2, \ldots, t_F\right\}$$

and $\#\mathrm{Orb}_\gamma(F) = t_F - 1$, or $\#\mathrm{Orb}_\gamma(F) = t_F - 2$ (depending whether $s = 1$ or $s \geqslant 2$ in the above).

Trivially, we have $t_F \leqslant q + 1$. Here, we obtain a nontrivial upper bound on the orbit length t_F of stable compositions $F = g \circ f$ where $f, g \in \mathbb{F}_q[X]$, $\deg f = 2$, $\deg g = d$ which for $d = 1$ coincides with [**15**, Theorem 1].

Theorem 8. *For any odd q and any stable polynomial $F = g \circ f \in \mathbb{F}_q[X]$, where $f = aX^2 + bX + c \in \mathbb{F}_q[X]$ and $g \in \mathbb{F}_q[X]$ of degree d, we have*

$$t_F = O\left(q^{1-\alpha_d}\right),$$

where

$$\alpha_d = \frac{\log 2}{2\log(4d)}.$$

Proof. The proof follows using exactly the same technique as the proof of [**15**, Theorem 1]. Let χ be the quadratic character of $\mathbb{F}_q$.

We know that $F^{(n)}$ is an irreducible polynomial for any $n \geqslant 1$. This implies that $G_{n-1} = F^{(n-1)} \circ g$ is an irreducible polynomial. Indeed, if G_{n-1} is not irreducible, then we can write it as $G_{n-1} = G_1G_2$, where $G_1, G_2 \in \mathbb{F}_q[X]$ are nonconstant polynomials. Then $F^{(n)} = G_{n-1}(f) = G_1(f)G_2(f)$, which is in contradiction with the irreducibility of $F^{(n)}$. We now apply Lemma 7, and conclude that if $F \in \mathbb{F}_q[X]$ is stable then the set $\mathrm{Orb}_\gamma(F)$ contains no squares. That is, $\chi\left(F^{(n)}(\gamma)\right) = -1, n = 2, 3, \ldots$.

https://doi.org/10.1017/S001708951200002X Published online by Cambridge University Press

We fix an integer parameter K and note that for any $n \geqslant 1$, we have simultaneously

$$\chi\left(F^{(k+n)}(\gamma)\right) = -1, \qquad k = 1, \ldots, K,$$

which we rewrite as

$$\chi\left(F^{(k)}\left(F^{(n)}(\gamma)\right)\right) = -1, \qquad k = 1, \ldots, K. \tag{10}$$

Since by the definition of t_F, the values $F^{(n)}(\gamma)$, $n = 1, \ldots, t_F - 1$, are pairwise distinct elements of $\mathbb{F}_q$, we derive from (10) that

$$t_F - 1 \leqslant \#\mathcal{T}_q(K), \tag{11}$$

where

$$\mathcal{T}_q(K) = \left\{x \in \mathbb{F}_q \ : \ \chi\left(F^{(k)}(x)\right) = -1, \ k = 1, \ldots, K\right\}.$$

We have

$$\#\mathcal{T}_q(K) = \frac{1}{2^K} \sum_{x \in \mathbb{F}_q} \prod_{k=1}^{K} \left(1 - \chi\left(F^{(k)}(x)\right)\right), \tag{12}$$

since for every $x \in \mathcal{T}_q(K)$ the product on the right-hand side of (12) is 2^K and is 0 when $\chi(F^{(k)}(x)) = 1$ for at least one $k = 1, \ldots, K$ (note that since by our assumption $F^{(k)}(X)$ is irreducible over $\mathbb{F}_q$, we have that $F^{(k)}(x) \neq 0$ for all $x \in \mathbb{F}_q$).

Expanding the product in (12), we obtain $2^K - 1$ character sums of the shape

$$(-1)^{\nu} \sum_{x \in \mathbb{F}_q} \chi\left(\prod_{j=1}^{\nu} F^{(k_j)}(x)\right), \qquad 1 \leqslant k_1 < \cdots < k_{\nu} \leqslant K, \tag{13}$$

with $\nu \geqslant 1$ and one trivial sum that equals q (corresponding to the terms equal to 1 in the product in (12)).

Clearly, $F^{(k)}(X)$ is a polynomial of degree $2^k d^k$. Furthermore, by our assumption, each one of the polynomials $F^{(k)}(X)$ is irreducible, therefore none of the polynomials

$$\prod_{j=1}^{\nu} F^{(k_j)}(X) \in \mathbb{F}_q[X], \qquad 1 \leqslant k_1 < \cdots < k_{\nu} \leqslant K,$$

is a perfect square in the algebraic closure of $\mathbb{F}_q$. Thus, the Weil bound (see [**10**, Theorem 11.23]), applies to every sum (13) and implies that each one of them is $O(2^K d^K q^{1/2})$. Hence,

$$\#\mathcal{T}_q(K) = \frac{1}{2^K} q + O\left(2^K d^K q^{1/2}\right). \tag{14}$$

Choosing K to satisfy

$$(4d)^K \leqslant q^{1/2} < (4d)^{K+1}$$

and combining (11) and (14), we get the desired result. $\square$

We recall that a polynomial $\ell(X) \in \mathbb{F}_q[X]$ is called *linearised* if it is of the form

$$\ell(X) = \sum_{j=0}^{\nu} a_j X^{p^j},$$

where p is the characteristic of $\mathbb{F}_q$.

We now show that there are no stable shifted linearised polynomials. In particular, there are no stable quadratic polynomials over finite fields of characteristic 2. Our proof is based on one well-known statement which describes the irreducibility of polynomials of the form $\ell(X) - b \in \mathbb{F}_q[X]$, where $\ell(X)$ is a linearised polynomial over $\mathbb{F}_q$ (see [**4**, Lemma 3.17]).

LEMMA 9. *Let $q = p^m$, where p is a prime and $m \geqslant 1$ is an integer. Suppose that $\ell(X)$ is a linearised polynomial over $\mathbb{F}_q$ of degree p^ν with $\nu \geqslant 2$. Then for any $b \in \mathbb{F}_q$, the polynomial $\ell(X) - b$ is irreducible if and only if*

$$p = \nu = 2,$$

and $\ell(X)$ has the form

$$\ell(X) = X(X + A)(X^2 + AX + B),$$

with $A, B \in \mathbb{F}_q$ such that $X^2 + AX + B$ and $X^2 + BX + b$ are both irreducible.

We now show that there are no stable shifted linearised polynomials over a finite field, which is a generalisation of [**14**, Corollary 1.6].

THEOREM 10. *Let $q = p^m$, where p is a prime as $m \geqslant 1$ is an integer, and let $f(X) = \ell(X) + \alpha \in \mathbb{F}_q[X]$, where $\ell(X)$ is a linearised polynomial over $\mathbb{F}_q$ of degree p^ν with $\nu \geqslant 1$. Then $f^{(n)}(X)$ is reducible over $\mathbb{F}_q$ for $n \geqslant 3$.*

Proof. We note that for any $k \geqslant 1$,

$$f^{(k)}(X) = \widetilde{\ell}(X) + \widetilde{\alpha},$$

where $\widetilde{\ell}(X) \in \mathbb{F}_q[X]$ is a linearised polynomial of degree $p^{\nu k}$ and $\widetilde{\alpha} \in \mathbb{F}_q$. When $p \neq 2$, then, by Lemma 9, we get that the polynomial $f(X)$ is not irreducible, and thus not stable. Thus, we assume that $p = 2$. In this case, applying again Lemma 9 we obtain that for $k \geqslant 3$, $f^{(k)}(X)$ is a reducible polynomial over $\mathbb{F}_q$, which concludes the proof. $\square$

As a simple consequence, we obtain that there are no stable quadratic polynomials over finite fields of characteristic 2.

COROLLARY 11. *Let q be even, and let $f(X) = aX^2 + bX + c \in \mathbb{F}_q[x]$. Then one of $f(X)$, $f^{(2)}(X)$ or $f^{(3)}(X)$ is reducible over $\mathbb{F}_q$.*

The following example shows that Corollary 11 cannot be extended to infinite fields. Let $K = \mathbb{F}_2(T)$ be the rational function field in T over $\mathbb{F}_2$, where T is transcendental over $\mathbb{F}_2$. Take $f(X) = X^2 + T \in K[X]$. Then it is easy to see that

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

https://doi.org/10.1017/S001708951200002X Published online by Cambridge University Press

Now, from the Eisenstein criterion for function fields (see, for example, [**16**, Proposition III.1.14]), it follows that for every $n \geqslant 1$, the polynomial $f^{(n)}(X)$ is irreducible over K. Hence, $f(X)$ is stable.

In fact, it is easy to show that a composition $f \circ g$ of two nonlinear Eisenstein polynomials is an Eisenstein polynomial again, see [**14**, Lemma 2.2]. This simple observation allows one to construct explicit examples of stable polynomials over many fields such as $\mathbb{Q}$ or p-adic and function fields.

4. Comments. We note that in condition (2) we have not used the full strength of [**12**, Theorem 4.4]. However, surprisingly enough, the bound of Theorem 1 is dominated by the polynomials for which (1) is satisfied. Maybe a more careful examination of this case may help to improve Theorem 1.

Certainly, the bound of Theorem 5 can easily be improved by tightening up our argument and also via using more modern estimates on size of solutions of Diophantine equations (see, for example, [**5**, **6**] and the references therein, for such better explicit estimates).

It is also interesting to investigate whether the stability of a quadratic polynomial $f(X) \in \mathbb{Z}[X]$ can be tested in finitely many steps. We note that Theorem 5 does not imply such a test.

Acknowledgements. The authors are grateful to Rafe Jones for discussions and to Domingo Gomez for the idea of the proof of Theorem 4. During the preparation of this paper, O. A. was supported in part by the Claude Shannon Institute, Science Foundation Ireland Grant 06/MI/006, F. L. by Grant SEP-CONACyT 79685 and PAPIIT 100508, A. O. by SNSF Grant 121874, and I. S. by the ARC Grant DP1092835.

REFERENCES

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

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

3. A. Baker, Bounds for the solutions of the hyperelliptic equation, *Proc. Cambridge Philos. Soc.* **65** (1969), 439–444.

4. I. F. Blake, X. H. Gao, A. J. Menezes, R. C. Mullin, S. A. Vanstone and T. Yaghoobian, *Application of finite fields* (Kluwer, 1993).

5. B. Brindza, On S-integral solutions of the equation $y^m = f(x)$, *Acta Math. Hungar.* **44** (1984), 133–139.

6. Y. Bugeaud, Bounds for the solutions of superelliptic equations, *Compositio Math.* **107** (1997), 187–219.

7. D. Gomez and A. P. Nicolás, An estimate on the number of stable quadratic polynomials, *Finite Fields Appl.* **16** (2010), 329–333.

8. D. Gomez-Perez, A. P. Nicolás, A. Ostafe and D. Sadornil, Stable polynomials over finite fields, *Preprint* (2011).

9. G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers* (Oxford University Press, Oxford, 1979).

10. H. Iwaniec and E. Kowalski, *Analytic number theory* (Amer. Math. Soc. Providence, RI, 2004).

11. R. Jones, Iterated Galois towers, associated martingales, and the p-adic Mandelbrot set, *Compositio Math.* **43** (2007), 1108–1126.

12. R. Jones, The density of prime divisors in the arithmetic dynamics of quadratic polynomials, *J. London Math. Soc.* **78** (2008), 523–544.

13. R. Jones and N. Boston, Settled polynomials over finite fields, *Proc. Amer. Math. Soc.* (to appear).

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

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

16. H. Stichtenoth, *Algebraic function fields and codes* (Springer-Verlag, Berlin, 1993).