On the length of critical orbits of stable quadratic polynomials

Ostafe, Alina ; Shparlinski, Igor E

DOI: https://doi.org/10.1090/S0002-9939-10-10404-3

PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 138, Number 8, August 2010, Pages 2653–2656
S 0002-9939(10)10404-3
Article electronically published on March 30, 2010

ON THE LENGTH OF CRITICAL ORBITS OF STABLE QUADRATIC POLYNOMIALS

ALINA OSTAFE AND IGOR E. SHPARLINSKI

(Communicated by Ken Ono)

Abstract. We use the Weil bound of multiplicative character sums, together with some recent results of N. Boston and R. Jones, to show that the *critical orbit* of quadratic polynomials over a finite field of q elements is of length $O(q^{3/4})$, improving upon the trivial bound q.

1. Introduction

Let $\mathbb{F}_q$ be a finite field of q elements. For a polynomial $f \in \mathbb{F}_q[X]$ we define the sequence of iterations:

$$f^{(0)}(X) = X, \qquad f^{(n)}(X) = f\left(f^{(n-1)}(X)\right), \quad n = 1, 2, \ldots .$$

Following [1, 2, 8, 9], we say that f is *stable* if all polynomials $f^{(n)}$ are irreducible over $\mathbb{F}_q$.

We now assume that q is odd.

As in [9], for a quadratic polynomial $f(X) = aX^2 + bX + c \in \mathbb{F}_q[X]$, $a \neq 0$, we define $\gamma = -b/(2a)$ as the unique critical point of f (that is, the zero of the derivative f') and consider the set

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

which is called the *critical orbit* of f. 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 $n \geq 0$. Accordingly, for the smallest value of t_f with the above condition, 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 on whether $s = 1$ or $s \geq 2$ in the above). It is shown in [7, 8, 9] that critical orbits play a very important role in the dynamics of polynomial iterations.

Trivially we have $t_f \leq q + 1$. In fact, by the *Birthday Paradox* one expects that t_f is of order $q^{1/2}$ (for a sufficiently large q). Indeed, it is natural to expect that the map $x \mapsto f(x)$ behaves like a random map on $\mathbb{F}_q$, for which the trajectory length is of this order; see [4] for a detailed treatment of cycle structure of random maps on finite sets. For example, the Pollard integer factorisation algorithm (where a quadratic

Received by the editors September 22, 2009.
2010 *Mathematics Subject Classification.* Primary 11L40, 11T06, 37P25.

polynomial $f(X) = X^2 + c$ is iterated in a residue ring; see [3, Section 5.2.1]) is based on this assumption.

Here we obtain a nontrivial upper bound on the orbit length of stable quadratic polynomials:

Theorem 1. *For any odd q and any stable quadratic polynomial $f \in \mathbb{F}_q[X]$ we have*

$$t_f = O\left(q^{3/4}\right).$$

By [9, Proposition 3], a quadratic polynomial $f \in \mathbb{F}_q[X]$ is stable if the *adjusted orbit*

$$\overline{\mathrm{Orb}}(f) = \{-f(\gamma)\} \cup \mathrm{Orb}(f)$$

contains no squares. We also recall that $\alpha \in \mathbb{F}_q$ is a square if either $\alpha = 0$ or $\alpha^{(q-1)/2} = 1$, which can be tested (via repeated squaring) in $O(\log q)$ field operations. Combining these with the bound of Theorem 1, we immediately obtain:

Corollary 2. *For any odd q, a quadratic polynomial $f \in \mathbb{F}_q[X]$ can be tested for stability in time $q^{3/4+o(1)}$.*

Our proof is based on the Weil bound for multiplicative character sums with polynomials; see [6, Theorem 11.23].

Finally, we remark that estimating the size of the set of stable quadratic polynomials $aX^2 + bX + c \in \mathbb{F}_q[X]$ is a very interesting question to which we hope our technique can apply as well.

2. Proof of Theorem 1

Let χ be the quadratic character of $\mathbb{F}_q$.

By [9, Proposition 3], if a quadratic polynomial $f \in \mathbb{F}_q[X]$ is stable, then $\mathrm{Orb}(f)$ contains no squares, that is, $\chi\left(f^{(n)}(\gamma)\right) = -1$, $n = 2, 3, \ldots$.

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

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

which we rewrite as

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

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 (1) that

$$t_f - 1 \le \#\mathcal{T}_q(K), \tag{2}$$

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

$$\#\mathcal{T}_q(K) = \frac{1}{2^K} \sum_{x \in \mathbb{F}_q} \prod_{k=1}^{K} \left(1 - \chi\left(f^{(k)}(x)\right)\right) \tag{3}$$

since for every $x \in \mathcal{T}_q(K)$ the product on the right hand side of (3) is 2^K; otherwise it 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 $f^{(k)}(x) \ne 0$ for $x \in \mathbb{F}_q$).

Just expanding the product in (3), we obtain $2^k - 1$ character sums of the shape

$$(-1)^\nu \sum_{x \in \mathbb{F}_q} \chi\left(\prod_{j=1}^{\nu} f^{(k_j)}(x)\right), \qquad 1 \le k_1 < \ldots < k_\nu \le K, \tag{4}$$

with $\nu \ge 1$ and one trivial sum that equals q (corresponding to the terms 1 in the product in (3)).

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

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

are a perfect square in the algebraic closure of $\mathbb{F}_q$. Therefore the Weil bound (see [6, Theorem 11.23]) applies to every sum (4) and implies that each of them is $O(2^K q^{1/2})$. Therefore

$$\#\mathcal{T}_q(K) = \frac{1}{2^K} q + O(2^K q^{1/2}). \tag{5}$$

Choosing K to satisfy

$$2^K \le q^{1/4} < 2^{K+1}$$

and combining (2) and (5), we conclude the proof.

3. Comments

It is certainly interesting to obtain nontrivial estimates on the size S_q of the set of triples $(a, b, c) \in \mathbb{F}_q^* \times \mathbb{F}_q \times \mathbb{F}_q$ which correspond to stable quadratic polynomials $f(X) = aX^2 + bX + c$. Denoting by $F_k(a, b, c)$ the kth element of the critical orbit of f, we see that for any integer parameter K we have

$$S_q \le \#\mathcal{W}_q(K), \tag{6}$$

where

$$\mathcal{W}_q(K) = \left\{(a, b, c) \in \mathbb{F}_q^* \times \mathbb{F}_q \times \mathbb{F}_q \ : \ \chi\left(F_k(a, b, c)\right) = -1, \ k = 1, \ldots, K\right\},$$

and as before χ denotes the quadratic character of $\mathbb{F}_q$. As in the proof of Theorem 1, we have

$$\#\mathcal{W}_q(K) \le \frac{1}{2^K} \sum_{(a,b,c) \in \mathbb{F}_q^* \times \mathbb{F}_q \times \mathbb{F}_q} \prod_{k=1}^{K} \left(1 - \chi\left(F_k(a, b, c)\right)\right) \tag{7}$$

since for every triple $(a, b, c) \in \mathcal{W}_q(K)$ the product on the right hand side of (7) is 2^K; otherwise it is either 0 (when $\chi(F_k(a, b, c)) = 1$ for at least one $k = 1, \ldots, K$) or 1 (when $F_1(a, b, c) = \ldots = F_K(a, b, c) = 0$).

Clearly $F_k(a, b, c)$ is a rational function in a, b, c of degree at most $O(2^k)$. Thus expanding the product in (7), we obtain $2^K - 1$ character sums of the shape

$$(-1)^\nu \sum_{(a,b,c) \in \mathbb{F}_q^* \times \mathbb{F}_q \times \mathbb{F}_q} \chi\left(\prod_{j=1}^{\nu} F_{k_j}(a, b, c)\right), \quad 1 \le k_1 < \ldots < k_\nu \le K, \tag{8}$$

with $\nu \ge 1$ and one trivial sum corresponding to 1 in (7). Assuming that one can prove that the Weil-type bound $O(2^K q^{5/2})$ applies to all of them, we obtain from (6) that $S_q = O(q^3/2^K + 2^K q^{5/2})$ and optimising the choice of K we derive

$S_q = O(q^{11/4})$. In fact, for a nontrivial estimate of S_q it is enough to show that almost all sums (8) admit a nontrivial estimate, which has actually been recently done in [5], where the bound $S_q = O(q^{14/5})$ is obtained.

Acknowledgements

The authors are grateful to Rafe Jones and Arne Winterhof for a careful reading of the preliminary version of the manuscript and for many useful comments.

During the preparation of this paper, the first author was supported in part by the Swiss National Science Foundation Grant No. 121874 and the second author by the Australian Research Council Grant No. DP0556431.

References

[1] N. Ali, 'Stabilité des polynômes', *Acta Arith.*, **119** (2005), 53–63. MR2163517 (2006h:11125)
[2] M. Ayad and D. L. McQuillan, 'Irreducibility of the iterates of a quadratic polynomial over a field', *Acta Arith.*, **93** (2000), 87–97. MR1760091 (2001c:11031)
[3] R. Crandall and C. Pomerance, *Prime numbers: A computational perspective*, 2nd ed., Springer-Verlag, New York, 2005. MR2156291 (2006a:11005)
[4] P. Flajolet and A.M. Odlyzko, 'Random mapping statistics', *Lecture Notes in Comput. Sci.*, **434** (1990), 329–354. MR1083961
[5] D. Gomez and A. P. Nicolás, 'An estimate on the number of stable quadratic polynomials', preprint, 2010.
[6] H. Iwaniec and E. Kowalski, *Analytic number theory*, Amer. Math. Soc., Providence, RI, 2004. MR2061214 (2005h:11005)
[7] R. Jones, 'Iterated Galois towers, associated martingales, and the p-adic Mandelbrot set', *Compositio Math.*, **43** (2007), 1108–1126. MR2360312 (2008i:11131)
[8] R. Jones, 'The density of prime divisors in the arithmetic dynamics of quadratic polynomials', *J. Lond. Math. Soc.*, **78** (2008), 523–544. MR2439638 (2010b:37239)
[9] R. Jones and N. Boston, 'Settled polynomials over finite fields,' preprint, 2009.

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

Department of Computing, Macquarie University, Sydney, NSW 2109, Australia
E-mail address: igor@ics.mq.edu.au