Polynomial iteration in characteristic p [*][†]

Mei-Chu Chang[‡]
Department of Mathematics
University of California, Riverside
mcc@math.ucr.edu

Abstract

Let $f(x) = \sum_{s=0}^d a_s x^s \in \mathbb{Z}[x]$ be a polynomial with $a_d \not\equiv 0 \bmod p$. Take $z \in \mathbb{F}_p$ and let $\mathcal{O}_z = \{f_i(z)\}_{i \in \mathbb{Z}^+} \subset \mathbb{F}_p$ be the orbit of z under f, where $f_i(z) = f(f_{i-1}(z))$ and $f_0(z) = z$. For $M < |\mathcal{O}_z|$, we study the diameter of the partial orbit $\mathcal{O}_{z,M} = \{z, f(z), f_2(z), \dots, f_{M-1}(z)\}$ and prove that

$$\text{diam } \mathcal{O}_{z,M} \gtrsim \min \left\{ M^{\,c \log\log M},\ Mp^{\,c},\ M^{\frac{1}{2}} p^{\frac{1}{2}} \right\},$$

where 'diameter' is naturally defined in $\mathbb{F}_p$ and c depends only on d.

For a complete orbit $\mathcal{C}$, we prove that

$$\text{diam } \mathcal{C} \gtrsim \min\{p^{\,c}, e^{\,T/4}\},$$

where T is the period of the orbit.

[*]2000 *Mathematics Subject Classification.*Primary 11B50, 37A45, 11B75; Secondary 11T23, 37F10 11G99.

[†]*Key words.* dynamical system, orbits, additive combinatorics, exponential sums.

[‡]Research partially financed by the National Science Foundation.

1 Introduction.

The main theme of this note is to understand better the expansion properties of polynomial maps $f(x) = \sum_{s=0}^{d} a_s x^s \in \mathbb{F}_p[x]$ acting on $\mathbb{F}_p$. This line of investigation was initiated in [GS], and in [C1] estimates were obtained for quadratic polynomials. Thus our purpose here is to extend the results from [C1] to the general case, which seems to involve some significant algebra issues.

While polynomial iteration and orbits over the complex numbers are well-studied, not much have been done for finite characteristic. Take $z \in \mathbb{F}_p$ and let $\mathcal{O}_z = \{f_i(z)\}_{i\in\mathbb{Z}^+} \subset \mathbb{F}_p$ be the orbit of z under f, where $f_i(z) = f(f_{i-1}(z))$ and $f_0(z) = z$. For $M < |\mathcal{O}_z|$, we study the diameter of the partial orbit $\mathcal{O}_{z,M} = \{z, f(z), f_2(z), \dots, f_{M-1}(z)\}$ and prove that

$$\operatorname{diam} \mathcal{O}_{z,M} \gtrsim \min\left\{M^{\,c\log\log M},\ Mp^{\,c},\ M^{\frac{1}{2}}p^{\frac{1}{2}}\right\}, \tag{1.1}$$

where 'diameter' is naturally defined in $\mathbb{F}_p$ and c depends only on d.

For a complete orbit $\mathcal{C}$, we prove that

$$\operatorname{diam} \mathcal{C} \gtrsim \min\{p^{\,c}, e^{\,T/4}\}, \tag{1.2}$$

where T is the period of the orbit.

Eventually, part of the strategy in proving (1.1) and (1.2) is to "lift" the problem from $\mathbb{F}_p$ to $\mathbb{C}$, which constitutes the main difficulty in our analysis. Once the issue is reduced to complex orbits of polynomials, estimate (1.2) is derived from the work of R. Benedetto [B] on preperiodic points over global fields. Some conjectures made in [B], if correct, would even give stronger results.

It is certainly a challenging question to improve the lower bound (1.1), which is likely not the final truth on this question. The merit of (1.1) as stated is that for small M one obtains an estimate superpolynomial in M. Also, this problem fits obviously in a broader context of expansion and iteration of rational maps over finite fields. The exploration of this area is in an early stage and should be interesting from both algebraic and analytic perspectives.

Let p be a prime and $\mathbb{F}_p$ the finite field of p elements, represented by the set $\{0, 1, \dots, p-1\}$. Let $f \in \mathbb{F}_p[x]$ be a polynomial and $z \in \mathbb{F}_p$ be some element, we consider its orbit

$$z_0 = z,\ z_{n+1} = f(z_n), \quad n = 0, 1, \dots. \tag{1.3}$$

The *period* $T_z = T$ is the smallest integer satisfying

$$\{z_n : n = 0, 1, \dots, T-1\} = \{z_n : n \in \mathbb{N}\}. \tag{1.4}$$

Define

$$\text{diam } \mathcal{O}_{z,M} = \max_{0 \le n < M} p \left\| \frac{z_n - z}{p} \right\|. \tag{1.5}$$

Following the papers [GS] and [CGOS], we establish lower bounds on diam $\mathcal{O}_{z,M}$. Obviously, if $M \le T$, then diam $\mathcal{O}_{z,M} \ge M$. But, assuming that f is nonlinear and $M = o(p)$, one reasonably expects that the diameter of the partial orbit is much larger. Results along these lines were obtained in [GS] under the additional assumption that $M > p^{\frac{1}{2}+\epsilon}$. In this situation, Weil's theorem on exponential sums permits proving equidistribution of the partial orbit. For $M \le p^{1/2}$, Weil's theorem becomes inapplicable and lower bounds on diam $\mathcal{O}_{z,M}$ based on Vinogradov's theorem were established in [CGOS].

The idea of the proof follows that of quadratic polynomial in [C1]. The work is Theorem 1 in §2.

2 Our results.

Most of our effort is to prove the following.

Theorem 1. *Let* $f(x) = \sum_{s=0}^{d} a_s x^s \in \mathbb{F}_p[x]$ *with* $(a_d, p) = 1$. *For* $z \in \mathbb{F}_p$ *and* $M \le T_z$, *assume*

$$\text{diam}\mathcal{O}_{z,M} < p^c.$$

Then

$$\text{diam}\mathcal{O}_{z,M} \gg M^{\, c \log \log M}, \tag{2.1}$$

where c *depends only on* d.

We will use the following lower bound on the diameters. (See Corollary 9 [CCGHSZ].)

Theorem CCGHSZ. *For any polynomial* $f \in \mathbb{F}_p[x]$ *of degree* $d \ge 2$, $z \in \mathbb{F}_p$ *and* $M \le T_z$, *we have*

$$\text{diam}\mathcal{O}_{z,M} \gg \min\{M^{1/2}p^{1/2},\ M^{1+1/(2^{d-1}-1)} \log p^{-\epsilon}\},$$

as $p \to \infty$.

Combining Theorem 1 and Theorem CCGHSZ, we obtain

Theorem 2. *Let* $f(x) = \sum_{s=0}^{d} a_s x^s \in \mathbb{F}_p[x]$ *with* $(a_d, p) = 1$*, then for any* $z \in \mathbb{F}_p$ *and* $M \leq T_z$*,*

$$\text{diam } \mathcal{O}_{z,M} \gtrsim \min \left\{ M^{\, c \log \log M},\ M p^{\, c},\ M^{\frac{1}{2}} p^{\frac{1}{2}} \right\}, \tag{2.2}$$

where c *depends only on* d*.*

For $\mathcal{C}$ a complete periodic cycle and diam $\mathcal{C} < p^{\, c_0}$, the transfer argument from Theorem 1 enables us to invoke bounds on the number of rational pre-periodic points of a polynomial map, for instance the results from R. Benedetto [B]. The conclusion is the following.

Theorem 3. *Let* $f(x) = \sum_{s=0}^{d} a_s x^s \in \mathbb{F}_p[x]$ *with* $(a_d, p) = 1$*, and let* $\mathcal{C} \subset \mathbb{F}_p$ *be a periodic cycle for* f *of length* T_z*, then*

$$\text{diam } \mathcal{C} \gtrsim \min\{p^{\, c}, e^{\, T/4}\ \}, \tag{2.3}$$

where c *depends only on* d*.*

3 Proof of Theorem 1.

The set up.

Lemma 1. *Let* $D =$ diam $\mathcal{O}_{z,M}$ *and let*

$$f(x) = \sum_{s=0}^{d} a_s x^s \in \mathbb{F}_p[x],\ a_d \not\equiv 0 \pmod p,$$

$$f(x_j) \equiv x_{j+1}, \pmod p \quad \text{for } 0 \leq j < M.$$

Assume
(i). All x_j, $0 \leq j < M$ *are distinct.*
(ii). $|x_j - x_0| \leq D < p^{c(d)}$ *for all* $j < M$*.*

Then there exist a polynomial $F(x) = b_d x^d + b_{d-2}x^{d-2} + \cdots + b_0 \in \mathbb{Z}[x], b_d \neq 0$, *and* $q \in \mathbb{Z}_+$, *such that*

(a). $x_{j+1} - x_0 = \frac{1}{q}F(x_j - x_0)$ *for all* $j < M$.

(b). $|b_s|$, $q < D^C$.

(c). $(q, b_{d-2}, \cdots, b_0) = 1$.

Proof.

For $0 \leq j < M$, consider the polynomials

$$\Phi_j(\xi, \alpha_0, \cdots, \alpha_d) = \sum_{s=0}^{d} \alpha_s (x_j - x_0 + \xi)^s - (x_{j+1} - x_0 + \xi) \in \mathbb{Z}[\xi, \alpha_0, \cdots, \alpha_d],$$

whose coefficients are bounded by CD^d, by (ii).

Claim. $\bigcap_{j=0}^{M-1}[\Phi_j = 0] \not\subset [\alpha_d = 0]$.

We will use the following Quantitative Nullstellensatz theorem. (Also see [C2] where a similar elimination procedure was used in a combinatorial problem. In particular, see Lemma 2.14 in [C2] and its proof.)

Theorem (Quantitative Nullstellensatz)

Let $f_1, \cdots, f_r \in \mathbb{Z}[x_1, \cdots, x_m]$ *with* $\deg f_s \leq d$, *and let* $V = \bigcap[f_s = 0]$ *be the variety defined by* $\{f_s\}_s$. *Assume* $f \in \mathbb{Z}[x_1, \cdots, x_m]$ *vanishing on* V.

Then there exist $A \in \mathbb{Z} \setminus \{0\}$, *and* $g_1, \cdots, g_r \in \mathbb{Z}[x_1, \cdots, x_m]$ *such that*

$$Af^k = \sum g_i f_i \quad \textit{and}$$

$$\log A < C(m, d)H,$$

where $H = \max(H(f_i), H(f))$ *and the height of a polynomial* g *is the maximum of logrithms of the coefficients of* g.

Proof of Claim.

Otherwise, Quantitative Nullstellensatz implies there are $\Psi_j \in \mathbb{Z}[\xi, \alpha_0, \cdots, \alpha_d]$ and $A \in \mathbb{Z} \setminus \{0\}$ such that, in particular,

$$A\alpha_d^k = \sum \Phi_j \Psi_j \text{ for some } k \in \mathbb{Z}_+ \tag{3.1}$$

and

$$|A| < D^C. \tag{3.2}$$

Taking $\xi_0 = x_0, \alpha_0 = a_0, \cdots, \alpha_d = a_d$, we have $\Phi_j(x_0, a_0, \cdots, a_d) = f(x_j) - x_{j+1} \equiv 0 \pmod{p}$, so that $Aa_d^k \equiv 0 \pmod{p}$, i.e. $A \equiv 0 \pmod{p}$. Hence $|A| \geq p$, contradicting (3.2). □

The claim implies that there is a polynomial $G(x) = \sum_{s=0}^{d} \beta_s x^s \in \mathbb{C}[x]$, $\beta_d \neq 0$ such that $G(x_j - x_0) = x_{j+1} - x_0$ for $j < M$.

Considering the system of linear equations $G(x_j - x_0) = x_{j+1} - x_0$ for $0 \leq j < M$ (with β_s as variables), where $x_0, \cdots, x_{M-1}$ are distinct by assumption (i). It follows that $\beta_s \in \mathbb{Q}$. i.e. $\beta_s = \frac{b'_s}{q_1}$ with $|b'_s|$, $q_1 < D^C$.

Let $F_1(x) = \sum_{s=0}^{d} b'_s x^s$. We will eliminate the x^{d-1}-term by translation. Take

$$y = x + \frac{b'_{d-1}}{d}.$$

Therefore, $y_j = \frac{z_j}{d}$ with $z_j = (x_j - x_0)d + b'_{d-1}$, satisfies the equation

$$y_{j+1} = \frac{1}{q_2} F_2(y_j), \tag{3.3}$$

where $F_2(x) \in \mathbb{Z}[x]$ is of degree d, with coefficients bounded by D^C and has no x^{d-1}-term, and $q_2 \in \mathbb{Z}_+$, $q_2 < D^C$.

Rewrite (3.3) as

$$z_{j+1} = \frac{1}{q} F(z_j), \tag{3.4}$$

(In particular,

$$F(z_j) \equiv 0 \pmod{q}.) \tag{3.5}$$

where $F(x) = b_d x^d + b_{d-2} x^{d-2} + \cdots + b_0 \in \mathbb{Z}[x]$,

$$(q, b_d, b_{d-2}, \cdots, b_0) = 1, \tag{3.6}$$

and $|b_d|, |b_{d-2}|, \cdots, |b_0|, q < D^C$.

To see that we may assume (c), we take $p | (q, b_{d-2}, \cdots, b_0)$. Then (3.6) implies $(b_d, p) = 1$ and (3.5) implies that $b_d z_j^d \equiv 0 \pmod{p}$, and hence $z_j \equiv 0 \pmod{p}$ for all j. Replacing z_j by $\tilde{z}_j = \frac{z_j}{p}$, we have

$$\tilde{z}_{j+1} = \frac{1}{q}(b_d p^{\,d-1}\, \tilde{z}_j^{\,d} + b_{d-2} p^{\,d-3}\, \tilde{z}_j^{\,d-2} + \cdots + b_1 \tilde{z}_j + b'_0), \;\; b'_0 = \frac{b_0}{p}.$$

This proves Lemma 1.

To prove Theorem 1, we factor $F(x)$ over an extension K of $\mathbb{Q}$

$$F(x) = b_d \prod_{s=1}^{d} \left(x - \frac{\xi_s}{b_d} \right), \quad \xi_s \in \mathcal{O}_K, \tag{3.7}$$

where $\mathcal{O}_K$ is the ring of integers of K.

Hence,

$$\sum_s \xi_s \ . \tag{3.8}$$

Let $q = \prod p^{v_p}$ with $v_p \geq 1$.

First, we handle the large prime factors p of q.

Case 1. $p > d$.

Lemma 2. *Assume $p|q$, $p > d$ and Property (c) in Lemma 1. Then $F^{(t)}(z_j) \not\equiv 0 \pmod p$ for some $t \leq d-1$.*

Proof. Assume the contrary. Then

$$F^{(d-1)}(z_j) = d! b_d z_j \equiv 0 \pmod p \tag{3.9}$$

implies

$$b_d z_j \equiv 0 \pmod p.$$

Iterating, for $0 \leq s \leq d-2$, gives

$$F^{(s)}(z_j) = s! b_s \equiv 0 \pmod p, \tag{3.10}$$

which implies

$$b_s \equiv 0 \pmod p,$$

contradicting Property (c). □

Write $b_d = p^{v'_p}\ b'_d$ with $v'_p \geq 0$ and $(b'_d, p) = 1$. Assume

$$v_p > v'_p \ . \tag{3.11}$$

Let $\mathcal{P}$ be a prime ideal of $\mathcal{O}_K$ over p and $\alpha \geq 1$ its exponent, i.e. $p = \mathcal{P}^\alpha \mathcal{P}_1 \cdots$. By (3.5),

$$F(z_j) \equiv 0 \pmod{p^{v_p}}, \tag{3.12}$$

which, together with (3.7), imply

$$b_d^{d-1}F(z_j) = \prod_{s=1}^{d}(b_d z_j - \xi_s) \qquad (\bmod\ \mathcal{P}^{(v_p'(d-1)+v_p)\alpha}). \tag{3.13}$$

Claim. There exist $s \leq d$ and $u = u(s) > \alpha v_p'$ such that

$$b_d z_j - \xi_s \equiv 0 \pmod{\mathcal{P}^u}. \tag{3.14}$$

Proof of Claim. Assume $u \leq \alpha v_p'$ such that for all $s \leq d$, (3.14) holds.

We want to show

$$u \leq \left[\frac{d-1}{d}\,\alpha\ v_p'\right]. \tag{3.15}$$

Clearly, from (3.14), for $t \leq d-1$, taking derivative t times of the product in (3.13) gives

$$b_d^{d-1}F^{(t)}(z_j) \equiv 0 \qquad (\bmod\ \mathcal{P}^{t\alpha v_p'+(d-t)u}). \tag{3.16}$$

Lemma 2 implies

$$\alpha v_p'(d-1) \geq t\alpha v_p' + (d-t)u \geq du, \tag{3.17}$$

which is (3.15).

Assume the claim fails. i.e. assume for all s, if (3.14) holds, then $u_s \leq \alpha v_p'$. From (3.13) and (3.15), taking average of the exponent of $\mathcal{P}$, there is some $s \leq d$ and $\sigma_p := u_s$ such that

$$b_d z_j - \xi_s \equiv 0 \qquad (\bmod\ \mathcal{P}^{\sigma_p}), \tag{3.18}$$

where σ_p satisfies

$$(d-1)\sigma_p \geq \alpha(v_p'(d-1)+v_p) - \left[\frac{d-1}{d}\,\alpha\ v_p'\right]. \tag{3.19}$$

In particular, by (3.11)

$$\sigma_p > \alpha v_p'\ .$$

This is a contradiction. Hence the claim is proved. □

Note that by (3.14), z_j is determined by $\xi_s \pmod{\mathcal{P}^{\sigma_p - \alpha v'_p}}$ with $s = s(p)$, and hence it is determined by $\xi_s \pmod{p^{\sigma'_p}}$ with σ'_p the smallest integer satisfying

$$\alpha\sigma'_p \geq \sigma_p - \alpha v'_p \, . \tag{3.20}$$

The case of small prime factors p of q requires some easy modification.

Case 2. $p \leq q$.

Lemma 2'. *Assume $p|q$, $p \leq d$ and Property (c) in Lemma 1. Then $F^{(t)}(z_j) \not\equiv 0 \pmod{p^C}$ for some constant $C = C(d)$.*

Inequalities (3.17) and (3.15) have to be replaced by

$$\alpha v'_p(d-1) + C \geq du \tag{3.21}$$

and

$$u \leq \frac{d-1}{d}\,\alpha\; v'_p + C. \tag{3.22}$$

Also, instead of (3.19), we use

$$(d-1)\sigma_p \geq \alpha(v'_p(d-1) + v_p) - \frac{d-1}{d}\,\alpha\; v'_p - C. \tag{3.23}$$

Define

$$Q' = \prod_{v_p > v'_p} p^{\sigma'_p} \tag{3.24}$$

with σ'_p defined by (3.20).

What we proved is that

$$\big|\{\pi_{Q'}(z_j) : j < M\}\big| \leq d^{\,\omega(Q')} \leq d^{\,\omega(q)} < c^{\,\frac{\log D}{\log\log D}}. \tag{3.25}$$

Our goal is to prove that

$$D > M^{c \log\log M}. \tag{3.26}$$

Assume (3.26) fails. Then (3.25) implies $|\{\pi_{Q'}(z_j) : j < M\}| < M^{o(1)}$, and there is a large subset $\mathcal{J} \subset \{1, 2, \cdots, [\frac{M}{2}]\}$, $|\mathcal{J}| > \sqrt{M}$ such that $z_i \equiv z_j \pmod{Q'}$ for any $i, j \in \mathcal{J}$. In particular, there is some $j \in \mathcal{J}$ such that

$$|z_j| > C_1 Q', \quad \text{and} \quad \left|z_j - \frac{\xi_s}{b_d}\right| > C_1 Q' \ \text{ for } \ s = 1, \cdots, d \tag{3.27}$$

with C_1 an arbitrary constant at most $\left[\frac{\sqrt{M}}{2(d+1)}\right]$.

Returning to (3.4) and (3.7), we have

$$q\ |z_{j+1}| = |b_d| \prod_{s=1}^{d} \left| z_j - \frac{\xi_s}{b_d} \right| . \tag{3.28}$$

Let

$$Q = \prod_{v_p > v_p'} p^{v_p - v_p'} . \tag{3.29}$$

Identity (3.28) clearly implies

$$Q\ |z_{j+1}| \geq \prod_{s=1}^{d} \left| z_j - \frac{\xi_s}{b_d} \right| . \tag{3.30}$$

It follows from (3.8) that

$$d\ \max_s \left| z_j - \frac{\xi_s}{b_d} \right| \geq \sum_{s=1}^{d} \left| z_j - \frac{\xi_s}{b_d} \right| \geq d\ |z_j|.$$

Hence,

$$\max_s \left| z_j - \frac{\xi_s}{b_d} \right| \geq \frac{1}{3}\Big(|z_j| + \max_s \frac{|\xi_s|}{b_d} \Big). \tag{3.31}$$

From (3.27), (3.31), and (3.30), we have

$$Q\ |z_{j+1}| \geq \frac{1}{3}(C_1 Q')^{d-1}\Big(|z_j| + \max_s \frac{|\xi_s|}{b_d} \Big). \tag{3.32}$$

Claim. $Q \leq (Q')^{d-1}\ C$.
Proof of Claim.

We want to show that

$$v_p - v_p' \leq \sigma_p'(d-1) \ \text{ for } p > d \ \text{ and } \ v_p > v_p' . \tag{3.33}$$

By (3.20) and (3.19), this amounts to

$$\alpha v_p - \alpha v_p' \leq \sigma_p(d-1) - \alpha v_p'(d-1),$$

which follows from

$$\alpha v_p - \alpha v'_p \leq v_p\alpha + (d-1)v'_p\alpha - \left[\frac{d-1}{d}\,\alpha\, v'_p\right] - \alpha v'_p(d-1),$$

and hence (3.33).

For $p \leq d$, instead of (3.33), we derive from (3.23) that

$$v_p - v'_p < \sigma'_p(d-1) + C. \tag{3.34}$$

Together with (3.24) and (3.29). the claim follows from (3.33) and (3.34).□

Therefore, choose C_1 appropriately, (3.32) implies that

$$|z_{j+1}| > 10\left(|z_j| + \max_s \frac{|\xi_s|}{b_d}\right). \tag{3.35}$$

It follows that

$$\left|z_{j+1} - \frac{\xi_s}{b_d}\right| > \frac{9}{10}|z_{j+1}| > 9|z_j| > 9C_1Q',$$

so that z_{j+1} still satisfies condition (3.27). In particular, $|z_{j+1}| > 10|z_j|$, $|z_{j+2}| > 10|z_{j+1}|, \cdots, |z_{j+[\frac{M}{2}]}| > 10^{\frac{M}{2}}$. Hence $10^{\frac{M}{2}} < D^C$, which is a contradiction and proves (3.26).

Acknowledgement. The author would like to thank the referee for many helpful comments and the mathematics department of University of California at Berkeley for hospitality.

References

[B] R. Benedetto, *Preperiodic points of polynomials over global fields* , J. Reine Angew. Math. 608 (2007), 123153.

[BY] C. A. Berenstein, A. YGER, *Effective Bezout identities in Q[Z1, . . . , Zn]*, Acta Math., 166 (1991), 69-120.

[CCGHSZ] M.-C. Chang, J. Cilleruelo, M. Garaev, J. Hernandez, I. Shparlinski, A. Zumalacarregui *Points on curves in small boxes and applications* (preprint).

[C1] M.-C. Chang, *Expansions of quadratic maps in prime fields* , Proc. Amer. Math. Soc. (to appear).

[C2] M.-C. Chang, *Factorization in Generalized Arithmetic Progressions and Application to the Erdos-Szemeredi Sum-Product Problems*, Geom. Funct. Anal. Vol. 13, (2003), 720-736.

[CGOS] J. Cilleruelo, M. Garaev, A. Ostafe, I. Shparlinski, *On the concentration of points of polynomial maps and applications*, Math. Zeit., (to appear).

[GS] J. Gutierrez, I. Shparlinski, *Expansion of orbits of some dynamical systems over finite fields* Bull. Aust. Math. Soc. 82 (2010), 232-239.