EXPANSIONS OF QUADRATIC MAPS IN PRIME FIELDS

MEI-CHU CHANG

(Communicated by Bryna Kra)

Abstract. Let $f(x) = ax^2 + bx + c \in \mathbb{Z}[x]$ be a quadratic polynomial with $a \not\equiv 0 \pmod p$. Take $z \in \mathbb{F}_p$ and let $O_z = \{f_i(z)\}_{i \in \mathbb{Z}^+}$ be the orbit of $z$ under $f$, where $f_i(z) = f(f_{i-1}(z))$ and $f_0(z) = z$. For $M < |O_z|$, we study the diameter of the partial orbit $O_M = \{z, f(z), f_2(z), \ldots, f_{M-1}(z)\}$ and prove that there exists $c_1 > 0$ such that

$$\text{diam } O_M \gtrsim \min \left\{Mp^{c_1}, \frac{1}{\log p} M^{\frac{4}{5}p^{\frac{1}{5}}, \frac{1}{\text{log log } M}} \right\}.$$

For a complete orbit $C$, we prove that

$$\text{diam } C \gtrsim \min \{p^{5c_1}, e^{T/4} \},$$

where $T$ is the period of the orbit.

Introduction

This paper belongs to the general theme of dynamical systems over finite fields. Let $p$ be a prime and $\mathbb{F}_p$ the finite field of $p$ elements, represented by the set $\{0, 1, \ldots, p-1\}$. Let $f \in \mathbb{F}_p[x]$ be a polynomial, which we view as a transformation of $\mathbb{F}_p$. Thus if $z \in \mathbb{F}_p$ is some element, we consider its orbit

$$(0.1)\quad z_0 = z, \quad z_{n+1} = f(z_n), \quad n = 0, 1, \ldots,$$

which eventually becomes periodic. The period $T_z = T$ is the smallest integer satisfying

$$(0.2)\quad \{z_n : n = 0, 1, \ldots, T-1\} = \{z_n : n \in \mathbb{N}\}.$$

We are interested in the metrical properties of orbits and partial orbits. More precisely, for $M < T_z$, we define

$$(0.3)\quad \text{diam } O_M = \max_{0 \leq n < M} |z_n - z|.$$

Following the papers [GS] and [CGOS], we study the expansion properties of $f$, in the sense of establishing lower bounds on $\text{diam } O_M$. Obviously, if $M \leq T$, then $\text{diam } O_M \geq M$. 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 $M \leq p^{1/2}$, Weil’s theorem becomes inapplicable and
lower bounds on \( \text{diam } \mathcal{O}_M \) based on Vinogradov’s theorem were established in [CGOS]. Our paper is a contribution of this line of research. We restrict ourselves to quadratic polynomials, though certainly the methods can be generalized. (See [CCGHSZ] for a generalization of Proposition 2 and Theorem 2 to higher degree polynomials and rational maps.)

Our first result is the following.

**Theorem 1.** There is a constant \( c_1 > 0 \) such that if \( f(x) = ax^2 + bx + c \in \mathbb{Z}[x] \) with \( (a, p) = 1 \), then with the above notation, for any \( z \in \mathbb{F}_p \) and \( M \leq T_z \),

\[
\text{diam } \mathcal{O}_M \gtrsim \frac{1}{\log p} \min \left\{ M^{p^{c_1}}, M^{\frac{4}{5}}, M^{\frac{1}{11} \log \log M} \right\}.
\]

In view of Theorem 2, one could at least expect that \( \text{diam } \mathcal{O}_M \gtrsim \min(p^c, e^{cM}) \) as is the case when \( M = T_z \).

In the proof, we distinguish the cases \( \text{diam } \mathcal{O}_M > p^{c_0} \) and \( \text{diam } \mathcal{O}_M \leq p^{c_0} \), where \( c_0 > 0 \) is a suitable constant. First, we again exploit exponential sum techniques (though, from the analytical side, our approach differs from [CGOS] and exploits a specific multilinear setup of the problem). More precisely, Proposition 2 in §1 states that (for \( M \leq T \) large enough)

\[
\text{diam } \mathcal{O}_M \gtrsim \frac{1}{\log p} \min \left( M^{\frac{4}{5}}, M^{\frac{1}{11} \log M} \right).
\]

(Note that (0.3) is a clear improvement over Theorem 8 from [CGOS] for the case \( d = 2 \).)

When \( \text{diam } \mathcal{O}_M \leq p^{c_0} \), a different approach becomes available as explained in Proposition 2. In this situation, we are able to replace the \((\mod p)\) iteration by a similar problem in the field \( \mathbb{C} \) of complex numbers, for an appropriate quadratic polynomial \( F(z) \in \mathbb{Q}[z] \). Elementary arithmetic permits us to then prove that \( \log \text{diam } \mathcal{O}_M \) is at least as large as \( \frac{1}{10} \log M \log \log M \).

Interestingly, assuming \( C \) is a complete periodic cycle and \( \text{diam } C < p^{c_0} \), the transfer argument from Proposition 2 enables us to invoke bounds on the number of rational preperiodic points of a quadratic map, for instance the results from R. Benedetto [B]. The conclusion is the following.

**Theorem 2.** There is a constant \( c_0 > 0 \) such that if \( f(x) = ax^2 + bx + c \in \mathbb{Z}[x] \) with \( (a, p) = 1 \) and \( C \subset \mathbb{F}_p \) is a periodic cycle for \( f \) of length \( T \), then

\[
\text{diam } C \gtrsim \min\{p^{c_0}, e^{T/4}\}.
\]

1. **Diameter of Partial Orbits**

Let \( f(x) = ax^2 + bx + c \in \mathbb{Z}[x] \), where \( a \neq 0 \pmod{p} \). Fix \( x_0 \in \mathbb{F}_p \) and denote the orbit of \( x_0 \) by

\[
\mathcal{O}_{x_0} = \{f_j(x_0)\}_{j \in \mathbb{Z}^+},
\]

where \( f_j(x_0) = f(f_{j-1}(x_0)) \) and \( f_0(x_0) = x_0 \). The period of the orbit of \( x_0 \) under \( f \) is denoted \( T = T_{x_0} = |\mathcal{O}_{x_0}| \). For \( A \subset \mathbb{F}_p \), we denote the diameter of \( A \) by

\[
\text{diam } A = \max_{x,y \in A} \frac{1}{p} \|x - y\|,
\]

\( h \leq g \) if there exist constants \( C, M \) such that \( |h(x)| \leq Cg(x) \) for all \( x > M \).
where $\|a\|$ is the distance from $a$ to the nearest integer. We are interested in the expansion of part of an orbit.

**Proposition 1.** For $1 \ll M < T$, consider a partial orbit

$$O_M = \{x_0, f(x_0), f_2(x_0), \ldots, f_{M-1}(x_0)\}.$$  

Then

$$\text{(1.1) }\text{diam }O_M \gtrsim \frac{1}{\sqrt{\log p}} \min(M^{5/4}, M^{4/5}p^{1/5}).$$

**Proof.** Let $M_1 = \text{diam }O_M$. Take $I \subset \mathbb{F}_p$ with $|I| = M_1$ and $O_M \subset I$; then

$$\text{(1.2) }|f(I) \cap I| \geq M - 1.$$  

We will express (1.2) using exponential sums.

Let $0 \leq \varphi \leq 1$ be a smooth function on $\mathbb{F}_p$ such that $\varphi = 1$ on $I$ and $\text{supp }\varphi \subset \tilde{I}$, where $\tilde{I}$ is an interval with the same center and double the length of $I$. Equation (1.2) implies that

$$\sum_{x \in I} \varphi(f(x)) \geq M$$

and expanding $\varphi$ in Fourier gives

$$\varphi(x) = \sum_{\xi \in \mathbb{F}_p} \hat{\varphi}(\xi)e_p(x\xi), \text{ with } \hat{\varphi}(\xi) = \frac{1}{p} \sum_{x \in \mathbb{F}_p} \varphi(x)e_p(-x\xi).$$

Combining these gives

$$\text{(1.3) }\sum_{\xi \in \mathbb{F}_p} |\hat{\varphi}(\xi)| \sum_{x \in I} e_p(\xi f(x)) \gtrsim M.$$  

We will estimate $\sum_{x \in I} e_p(\xi f(x))$ using van der Corput-Weyl.

Take $M_0 = O(M)$, e.g. $M_0 = \frac{1}{100}M$. Then

$$\text{(1.4) }\left| \sum_{x \in I} e_p(\xi f(x)) \right| \leq \frac{1}{M_0} \sum_{0 \leq y < M_0} \left| \sum_{x \in I} e_p(\xi(2x^2 + 2axy + bx)) \right| + O(M_0)$$

$$\leq \frac{1}{\sqrt{M_0}} \left[ \sum_{0 \leq y < M_0} \left| \sum_{x \in I} e_p(\xi(x^2 + 2axy + bx)) \right|^2 \right]^{1/2} + O(M_0)$$

$$= \frac{1}{\sqrt{M_0}} \left[ \sum_{0 \leq y < M_0} \sum_{x_1, x_2 \in I} e_p(\xi(x_1 - x_2)(a(x_1 + x_2) + 2ay + b)) \right]^{1/2} + O(M_0).$$

(The second inequality is by Cauchy-Schwarz.)

Take $\varphi$ sufficiently smooth so as to ensure that

$$\text{(1.5) }\sum_{\xi \in \mathbb{F}_p} |\hat{\varphi}(\xi)| = O(1).$$

Equations (1.3) and (1.4) imply

$$\sum_{\xi \in \mathbb{F}_p} |\hat{\varphi}(\xi)| \sum_{0 \leq y < M_0} \sum_{x_1, x_2 \in I} e_p(\xi(x_1 - x_2)(a(x_1 + x_2) + 2ay + b)) \gtrsim M^{3/2}.$$
Hence by Cauchy-Schwarz and (1.5),

\[
\sum_{\xi \in \mathbb{F}_p} |\hat{\varphi}(\xi)| \left| \sum_{0 \leq y < M_0 \atop x_1, x_2 \in I} e_p (\xi(x_1 - x_2)(a(x_1 + x_2) + 2ay + b)) \right| \gtrsim M^3.
\]

Fix \(x_1 + x_2 = s \leq 2M_1\); then

\[
\sum_{\xi \in \mathbb{F}_p} |\hat{\varphi}(\xi)| \left| \sum_{0 \leq y < M_0 \atop x \in I} e_p (\xi(2x - s)(as + 2ay + b)) \right| \gtrsim \frac{M^3}{2M_1}.
\]

Next, for \(z \in \mathbb{F}_p\), denote \(\eta(z) = |\{(x,y) \in I \times [1,M_0] : (2x-s)(2ay+b+as) \equiv z \pmod{p}\}|\),

and write the left hand side of (1.7) as

\[
\sum_{\xi \in \mathbb{F}_p} |\hat{\varphi}(\xi)| \left| \sum_{z \in \mathbb{F}_p} \eta(z) e_p(\xi z) \right| \\
\leq \left( \sum_{\xi \in \mathbb{F}_p} |\hat{\varphi}(\xi)|^2 \right)^{1/2} \left( \sum_{\xi \in \mathbb{F}_p} \left| \sum_{z \in \mathbb{F}_p} \eta(z) e_p(\xi z) \right|^2 \right)^{1/2} \\
= \left( \frac{1}{p} \sum_{x \in \mathbb{F}_p} |\varphi(x)|^2 \right)^{1/2} \sqrt{p} \left( \sum_{z \in \mathbb{F}_p} \eta(z)^2 \right)^{1/2} \\
< 2M_1^{1/2} \left( \sum_{z \in \mathbb{F}_p} \eta(z)^2 \right)^{1/2},
\]

by Cauchy-Schwarz and Parseval.

Recall that \((a,p) = 1\). Let \(I' = I - \frac{s}{2}\), \(I'' = [1,M_0] + \frac{b+as}{2a} \subset \mathbb{F}_p\) so that

\[
\sum_{z \in \mathbb{F}_p} \eta(z)^2 = E(I',I''),
\]

the multiplicative energy of \(I'\) and \(I''\).

It is well-known that

\[
E(I',I'') \leq \log p \max \left\{ |I'||I''|, \frac{|I'|^2|I''|^2}{p} \right\} \\
\leq \log p \max \left\{ M_1 M, \frac{M_1^2 M^2}{p} \right\}.
\]

Thus, by (1.7), (1.9) and (1.10),

\[
\frac{M_1^3}{M_1} \lesssim M_1^{1/2} (\log p)^{1/2} \max \left\{ M_1^{1/2} M^{1/2}, \frac{M_1 M}{p^{1/2}} \right\}.
\]

Distinguish the cases \(M_1 M \leq p\) and \(M_1 M > p\), and then (1.11) implies

\[
M_1 \gtrsim \min \left\{ (\log p)^{-1/4} M^{5/4}, (\log p)^{-1/5} M^{4/5} p^{1/5} \right\}.
\]
2. Partial orbits of small diameters

For $M < p^{c_0}$, one obtains the following stronger result. (Notation is as in Proposition 1)

**Proposition 2.** There exists $c_0 > 0$ such that

$$\text{(2.1)} \quad \text{diam } \mathcal{O}_M > \min \left( p^{c_0}, M \frac{1}{\log \log M} \right).$$

Consequently,

$$\text{(2.2)} \quad \text{diam } \mathcal{O}_M \gtrsim \min \left\{ Mp^{c_0}, \frac{1}{\log p} M^\frac{\epsilon}{p}, M \frac{1}{\log \log M} \right\}.$$

**Proof.** Let $\mathcal{O}_M = \{x_0, x_1, \ldots, x_{M-1}\}$ with $x_j = f(x_{j-1})$ as before, and let diam $\mathcal{O}_M = M_1$. Since $|x_j - x_0| \leq M_1$, we can write $x_j = x_0 + z_j$ with $z_j \in [-M_1, M_1]$. Thus, $a, b, c, x_0$ satisfy the $M - 1$ equations

$$a(x_0 + z_j)^2 + b(x_0 + z_j) + c \equiv x_0 + z_{j+1} \pmod{p}, \quad j = 0, \ldots, M - 2,$$

and the $\mathbb{F}_p$-variety

$$\mathcal{V}_p = \bigcap_{j=0}^{M-2} \{(r + z_j)^2 + v(r + z_j) + w = u(r + z_{j+1}) \pmod{p}\}$$

in the variables $(u, v, w, r) \in \mathbb{F}_p^4$ is therefore nonempty. Note that the coefficients of the $M - 1$ defining polynomials in $\mathbb{Z}[u, v, w, r]$ are $O(M_1^2)$.

Assume

$$\text{(2.3)} \quad M_1 < p^{c_0}$$

with $c_0 > 0$ small enough. Elimination theory\(^2\) implies that $\mathcal{V}_p \neq \emptyset$ is a $\mathbb{C}$-variety. Hence there are $U, V, W, R \in \mathbb{C}$ such that for all $j$,

$$(R + z_j)^2 + V(R + z_j) + W = U(R + z_{j+1}), \quad j = 0, \ldots, M - 2.$$  

Obviously, $U \neq 0$, since $z_1, \ldots, z_{M-2}$ are distinct. We therefore have a quadratic polynomial

$$\text{(2.4)} \quad F(z) := \frac{1}{U} (R + z)^2 + \frac{V}{U} (R + z) + \frac{W}{U} - R = A z^2 + B z + C,$$

satisfying

$$\text{(2.5)} \quad F(z_j) = z_{j+1} \quad \text{in } \mathbb{C}, \quad \text{for } j = 0, \ldots, M - 2.$$  

Since $z_0 = 0$, (2.4) and (2.5) imply $C = z_1 \in \mathbb{Z} \cap [-M_1, M_1]$, and the equations

$$z_1^2 A + z_1 B = z_2 - z_1,$$

$$z_2^2 A + z_2 B = z_3 - z_1$$

imply $A, B \in \mathbb{Q}$ with $A = \frac{a}{d}, B = \frac{b}{d}$, and $a, b, d \in \mathbb{Z}$ being $O(M_1^3)$. Equation (2.5) becomes

$$\text{(2.6)} \quad z_{j+1} = \frac{a}{d} z_j^2 + \frac{b}{d} z_j + C.$$  

\(^2\)See [C], where a similar elimination procedure was used in a combinatorial problem. In particular, see [C], Lemma 2.14 and its proof.
Hence
\[ \frac{a}{d}z_{j+1} + \frac{b}{2d} = \left( \frac{a}{d}z_j + \frac{b}{2d} \right)^2 + C\frac{a}{d} - \frac{b^2}{4d^2} + \frac{b}{2d}. \]

Putting
\[ y_j = \frac{a}{d}z_j + \frac{b}{2d} \in \frac{1}{2d}\mathbb{Z}, \quad j = 0, \ldots, M - 1, \]
and
\[ \frac{r}{s} = C\frac{a}{d} - \frac{b^2}{4d^2} + \frac{b}{2d} \quad \text{with } s > 0, (r, s) = 1, |r|, s = O(M_1^t), \]
gives
\[ (2.7) \quad y_{j+1} = y_j^2 + \frac{r}{s}, \quad j = 0, \ldots, M - 2. \]
Next, write \( y_j = \alpha_j/\beta_j \), where \( \beta_j \mid 2d \) and \((\alpha_j, \beta_j) = 1\); thus (2.7) gives
\[ (2.8) \quad \frac{\alpha_{j+1}}{\beta_{j+1}} = \frac{\alpha_j^2}{\beta_j^2} + \frac{r}{s}, \quad j = 0, \ldots, M - 2. \]

Note also that
\[ (2.9) \quad |\alpha_j| = O(M_1^4). \]

Write the prime factorizations
\[ s = \prod_p p^{v(p)} \quad \text{and} \quad \beta_j = \prod_p p^{v_j(p)}, \quad j = 0, \ldots, M - 1. \]

Claim. \( 2v_j(p) \leq v(p), \) for \( j < M - O(\log \log M_1). \)

Proof. We may assume \( v_j(p) > 0. \)

Case 1. \( 2v_j(p) > v_{j+1}(p). \)

Fact (2.1) (which will be stated at the end of this section) and (2.8) imply that \( v(p) = 2v_j(p). \)

Case 2. \( 2v_j(p) \leq v_{j+1}(p). \)

Again, we separate two cases.

Case 2.1. \( 2v_{j+1}(p) > v_{j+2}(p). \) Reasoning as in Case 1, we have
\[ v(p) = 2v_{j+1}(p) \geq 2^2v_j(p) > 2v_j(p). \]

Case 2.2. \( 2v_{j+1}(p) \leq v_{j+2}(p). \) Therefore, \( v_{j+2}(p) \geq 2^2v_j(p). \) We repeat the argument for Case 2 with \( j = j + 1. \) Continuing this process, after \( \tau \) steps, we obtain either \( v(p) \geq 2v_j(p) \) or
\[ (2.10) \quad v_{j+\tau}(p) \geq 2^\tau v_j(p), \]
when necessarily \( \tau \leq \log v_{j+\tau}(p) \leq \log \log \beta_{j+\tau} \leq \log \log d \leq \log \log M_1. \) Since \( j + \tau \leq M, \) the claim is proved. \( \square \)

It follows from the claim that \( \beta_j^2 \mid s \) for \( j < M - O(\log \log M_1). \) Back to (2.8), if \( v(p) > 2v_j(p) \) for some \( j < M - O(\log \log M_1), \) then \( v_{j+1}(p) = v(p). \) This contradicts the fact that \( \beta_{j+1}^2 \mid s. \) So we conclude that
\[ (2.11) \quad \beta_j^2 = s = s_1^2 \quad \text{for } j < M - O(\log \log M_1). \]
Hence
\[(2.12)\]
\[\alpha_{j+1} = \frac{\alpha_j^2}{s_j} + \frac{r}{s_j},\]
which implies
\[(2.13)\]
\[\alpha_j^2 + r \equiv 0 \pmod{s_j}.\]
Let \(s_j = \prod p_i^{v_i}\). Then \(\alpha_j\) satisfies \((2.13)\) if and only if \(\alpha_j\) satisfies \(\alpha_j^2 + r \equiv 0 \pmod{p_i^{v_i}}\) for all \(i\). Since \(-r\) is a quadratic residue modulo \(p_i^{v_i}\) if and only if it is a quadratic residue modulo \(p\) for odd prime \(p\), we have
\[(2.14)\]
\[
\left|\pi_{s_j}(\alpha_j)\right| \leq 2 \cdot 2^{\omega(s_j)} < e^{\frac{\log s_j}{\log \log s_j}} < e^{\frac{4 \log M_1}{\log \log M_1}}.
\]
Here \(\pi_{s_j}(\alpha_j)\) is the projection of \(\alpha_j\) in \(\mathbb{Z}_{s_j}\).

To show \(M_1 > M^{\frac{1}{4} \log \log M}\), we assume
\[(2.15)\]
\[\log M_1 < \frac{1}{13} \log M \log \log M.\]
Then \((2.14)\) implies there exists \(\xi \in \mathbb{Z}_{s_j}\) such that
\[(2.16)\]
\[
|J| = \left|\left\{0 \leq j \leq \frac{M}{2} : \pi_{s_j}(\alpha_j) = \xi\right\}\right| > M^{1/2}.
\]
Thus
\[\alpha_{j_1} - \alpha_{j_2} \in s_j \mathbb{Z}, \text{ for } j_1, j_2 \in J,\]
and
\[|\alpha_{j_1} - \alpha_{j_2}| \geq s_1, \text{ for } j_1 \neq j_2 \in J.\]
In particular, there exists \(j \in J\) such that
\[(2.17)\]
\[
|\alpha_j| \geq \frac{M^{1/2}}{8} s_j \text{ and } |\alpha_j| - |r|^{1/2} > \frac{M^{1/2}}{8} s_j.
\]
Claim. Either \(|\alpha_j| > 10|r|^{1/2}\) or \(|\alpha_{j+1}| > 10|r|^{1/2}\).

Proof. Assume
\[(2.18)\]
\[
|\alpha_j|, |\alpha_{j+1}| < 10|r|^{1/2}.
\]
Hence, \(|r|^{1/2} \gtrsim M^{1/2} s_j\) by \((2.17)\). From \((2.12), (2.17)\) and \((2.18)\),
\[
10|r|^{1/2} s_j > |\alpha_{j+1}| s_j = |\alpha_j^2 + r| \\
\geq (|\alpha_j| + |r|^{1/2})(|\alpha_j| - |r|^{1/2}) \\
\geq |r|^{1/2} \cdot \frac{M^{1/2}}{8} s_j,
\]
a contradiction, proving the claim.

Thus, there exists \(j < M/2\) such that either
\[(2.19)\]
\[|\alpha_j| > 10s_1 \text{ and } |\alpha_j| > 10|r|^{1/2}\]
or
\[(2.20)\]
\[|\alpha_j| > 10s_1 \text{ and } |\alpha_{j+1}| > 10|r|^2.\]
Clearly, \((2.19)\) implies \((2.20)\). Indeed, by \((2.12)\),
\[
|\alpha_{j+1}| \geq \frac{1}{s_j} |\alpha_j^2 - |r| | \geq \frac{99}{100s_j} \alpha_j^2 > 2|\alpha_j|.
\]
Iteration shows that
\[ |\alpha_j + \frac{M}{3}| > 2^k |\alpha_j| > 2^{k+1}, \]
contradicting (2.9). This proves (2.1).

Combining Proposition 1 and (2.1), we have (2.2). \qed

**Fact 2.1.** Let \( \frac{a_1}{d_1}, \frac{a_2}{d_2}, \frac{a_3}{d_3} \in \mathbb{Q} \) be rational numbers in lowest terms, and \( p^{v_p(d_i)} || d_i \).
If \( \frac{a_1}{d_1} + \frac{a_2}{d_2} + \frac{a_3}{d_3} = 0 \) and \( v_p(d_1) \geq v_p(d_2) \geq v_p(d_3) \), then \( v_p(d_1) = v_p(d_2) \).

3. Full cycles

In this section, we will prove Theorem 2.

Assume \( M_1 = \text{diam} \ C < p^{c_0} \) with \( c_0 \) as in Proposition 2. The proof of Proposition 2 gives a quadratic polynomial (cf. (2.7))
\[ F(z) = z^2 + \frac{r}{s} \]
with \( r, s \in \mathbb{Z}, |s| = O(M_1^6) \)
and a rational \( F \)-cycle \( \{y_j\}_{0 \leq j < T} \), i.e.
\[ y_{j+1} = F(y_j) \quad \text{for} \quad 0 \leq j \leq T - 2 \]
and \( F(y_{T-1}) = y_0 \).

We now invoke a result of R. Benedetto [B], which gives quantitative bounds on the number of preperiodic points of a polynomial \( f \) in a number field (\( z \) is preperiodic if the set \( \{z, f(z), f(f(z)), \ldots\} \) is finite). According to Theorem 7.1 in [B], the number of preperiodic points of \( F \) in \( \mathbb{Q} \) is bounded by
\[ (2\sigma + 1) [\log_2(2\sigma + 1) + \log_2(\log_2(2\sigma + 1) - 1) + 2] \]
with \( \sigma \) the number of primes where \( F \) has bad reduction. Hence \( \sigma \leq \omega(s) \leq \frac{\log M_1}{\log \log M_1} \) and (3.2) implies
\[ T < 4 \log M_1 = 4 \log \text{diam} \ C. \]

**Acknowledgements**

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

**References**


Department of Mathematics, University of California, Riverside, California 92521

E-mail address: mcc@math.ucr.edu