ON POSTCRITICALLY FINITE UNICRITICAL POLYNOMIALS

XAVIER BUFF

Abstract. We study the number of conjugacy classes of postcritically finite unicritical polynomials with a given period and preperiod.

Introduction

In this note, we study polynomials $f : \mathbb{C} \to \mathbb{C}$ of degree $D \geq 2$ from a dynamical point of view, i.e., we consider sequences defined by iteration:

$$z_0 \in \mathbb{C} \quad \text{and} \quad z_n := f(z_{n-1}) = f^{\circ n}(z_0).$$

The point z_0 is *periodic* if there is an integer $n \geq 1$ such that $f^{\circ n}(z_0) = z_0$. If p is the smallest integer with this property, we call it the *period* of z_0. The point z_0 is *(pre)periodic* if there exists a (smallest) integer $k \geq 0$ such that $f^{\circ k}(z_0)$ is periodic of period p. We say that k is the preperiod and that p is the *period*.

We shall study polynomials of the form

$$f_c(z) = z^D + c, \quad c \in \mathbb{C}.$$

Those polynomials have a unique critical point at $z = 0$. We are interested in the parameters $c \in \mathbb{C}$ for which 0 is either periodic or preperiodic. In that case, the critical orbits are finite and the polynomial is *postcritically finite*. More precisely, for $k \geq 0$ and $p \geq 1$, set

$$\mathcal{C}_{k,p} := \big\{ c \in \mathbb{C} \ ; \ 0 \text{ is (pre)periodic with preperiod } k \text{ and period } p \text{ for } f_c \big\}.$$

Proposition 1. *Assume $k \geq 0$ and $p \geq 1$. If $c \in \mathcal{C}_{k,p}$, then c is an algebraic integer. If $p \geq 2$, then c is an algebraic unit.*

One objective is to determine the cardinal of the set $\mathcal{C}_{k,p}$. Following Milnor [M], for $p \geq 1$, we shall define positive integers $\nu_D(p)$ by the formula:

$$D^p = \sum_{q|p} \nu_D(p) \quad \Longleftrightarrow \quad \nu_D(p) = \sum_{q|p} \mu\left(\frac{p}{q}\right) D^q$$

to be summed over all divisors $1 \leq q \leq p$, where μ is the Möbius function defined by $\mu(n) = (-1)^m$ if n is the product of m distinct primes with $m \geq 0$ and $\mu(n) = 0$ otherwise.

This integer $\nu_D(p)$ is the number of periodic points of period p of the polynomial $f_0 : \mathbb{C} \to \mathbb{C}$. The first values of $\nu_D(p)$ are given in Table 1.

Set

$$N(k,p) := \operatorname{card}(\mathcal{C}_{k,p}) \quad \text{and} \quad N(p) := N(0,p).$$

The following count is well known. We shall recall the proof in §1.

This research was supported in part by the ANR grant Lambda ANR-13-BS01-0002.

p	1	2	3	4	5	6
$\nu_D(p)$	D	D^2-D	D^3-D	D^4-D^2	D^5-D^2	$D^6-D^3-D^2+D$

TABLE 1. The first values of $\nu_D(p)$.

Proposition 2. *For all $p \geq 1$, we have*

$$N(p) = \frac{\nu_D(p)}{D}.$$

Corollary 3. *We have the following equivalent:*

$$N(p) \sim D^{p-1} \quad as \quad p \to \infty.$$

It is not difficult to see that $N(1,p) = 0$ for all $p \geq 1$. Indeed, if $f_c(0) = c$ is periodic of period p, then $c = f_c^{\circ p}(c) = \big(f_c^{\circ p}(0)\big)^D + c$, so that $f_c^{\circ p}(0) = 0$ and 0 is periodic. Thus, $\mathcal{C}_{1,p} = \emptyset$. Our contribution is the following count.

Proposition 4. *For $k \geq 2$ and and $p \geq 1$, we have*

$$N(k,p) = (D-1)\big(D^{k-1} - \varepsilon(k,p)\big)N(p)$$

where $\varepsilon(k,p) = 1$ if p divides $k-1$ and 0 otherwise.

Corollary 5. *We have the following equivalent*

$$N(k,p) \sim D^{k-1}(D-1)N(p) \quad as \quad k+p \to \infty \quad with \quad k \geq 2.$$

Corollary 6. *For each $D \geq 2$, there exists a constant $\kappa > 0$ such that for all $k \geq 2$ and all $p \geq 1$,*

$$N(p) \geq \kappa D^p \quad and \quad N(k,p) \geq \kappa D^{k+p}.$$

ACKNOWLEDGMENTS

We thank Thomas Gauthier for raising the questions studied in this note. The results presented here were inspired by fruitful discussions with Adam Epstein and Sarah Koch.

1. THE PERIODIC CASE

Let $F_p \in \mathbb{Z}[c]$ be the polynomial defined by

$$F_p(c) := f_c^{\circ p}(0).$$

Note that $F_0 = 0$ and $F_p = F_{p-1}^D + c$.

Example. We have that

$$F_0 = 0, \quad F_1 = c, \quad F_2 = c^D + c.$$

Proposition 7 (Gleason)**.** *For $p \geq 1$, the polynomials F_p have simple roots.*

Proof. For $p \geq 1$, we have $F_p = F_{p-1}^D + c$, so that

$$F_p' = DF_{p-1}^{D-1}F_{p-1}' + 1 \equiv 1 \mod D.$$

Since F_p is monic, the resultant of F_p and F_p' is equal to $1 \mod D$, in particular it does not vanish. □

Corollary 8. *For $p \geq 1$, there exists a (unique) monic polynomial $R_p \in \mathbb{Z}[c]$, such that the following holds. For $p \geq 1$*

$$F_p = \prod_{q|p} R_q.$$

For $p = 1$, $R_1 = c$ and for $p \geq 2$, the constant coefficient of R_p is 1.

Proof. The roots of F_p are exactly the parameters $c \in \mathcal{C}_q$ with q dividing p. So, if q divides p and c is a root of F_q, then c is a root of F_p. Since the roots of F_q are simple, it follows from Proposition 7 that F_q divides F_p. Thus, we have the required factorization.

The polynomials F_p are monic. In addition $R_1 = F_1 = c$ divides F_p and the constant coefficient of F_P/R_1 is 1. It follows by induction on $p \geq 2$ that the polynomial R_p is monic with constant coefficient 1. □

The roots of R_p are exactly the parameters $c \in \mathcal{C}_{0,p}$.

Example. For $D = 2$, we have $F_4 = R_1 R_2 R_4$ with

$$R_1 = c, \quad R_2 = c + 1 \quad \text{and} \quad R_4 = c^6 + 3c^5 + 3c^4 + 3c^3 + 2c^2 + 1.$$

The following conjecture is part of the folklore.

Conjecture 1. *For $D = 2$ and $p \geq 1$, the polynomial R_p is irreducible over $\mathbb{Z}$.*

We will now discus a generalization of this conjecture for $D \geq 3$. Let us first observe that for each $p \geq 1$, we have $F_p(c) = cG_p(c^{D-1})$ for some monic polynomial $G_p \in \mathbb{Z}[b]$ with constant coefficient equal to 1. Indeed, this property holds for $p = 1$ with $G_p = 1$. And if it holds for some $p \geq 1$, then

$$F_{p+1}(c) = c^D G_p^D(c^{D-1}) + c = cG_{p+1}(c^{D-1}) \quad \text{with} \quad G_{p+1}(b) = bG_p^D(b) + 1.$$

Since $F_p(c) = cG_p(c^{D-1})$, we see that for $p \geq 2$, $R_p(c) = S_p(c^{D-1})$ for some monic polynomial $S_p \in \mathbb{Z}[b]$.

Example. We have

$$S_1 = 1, \quad S_2 = b + 1 \quad \text{and} \quad S_3 = b(b+1)^D + 1.$$

It may be tempting to conjecture that for all $D \geq 2$ and all $p \geq 1$, the polynomial S_p is irreducible over $\mathbb{Z}$. However, the following observation shows that this is not true (compare with [S]).

Proposition 9. *The polynomial S_3 is irreducible over $\mathbb{Z}$ if and only if D is not congruent to 1 modulo 6.*

Proof. On the one hand, if $D \equiv 1 \mod 6$, then $b^2 + b + 1$ divides S_3. Indeed, let $\omega \neq 1$ be a cube-root of unity. Then $\omega + 1$ is a 6-th root of unity and

$$S_3(\omega) = \omega(\omega + 1)^D + 1 = \omega(\omega + 1) + 1 = \omega^2 + \omega + 1 = 0.$$

On the other hand, observe that

$$S_3(b) = P(b + 1) \quad \text{with} \quad P(x) := x^D(x - 1) + 1 = x^{D+1} - x^D + 1.$$

If S_3 is reducible, then P is reducible and we may write $P = P_1 P_2$ with $P_1 \in \mathbb{Z}[x]$ and $P_2 \in \mathbb{Z}[x]$ monic polynomials of respective degree $D_1 \geq 1$ and $D_2 \geq 1$. The

product of the constant coefficients of P_1 and P_2 is equal to 1, so that both are equal to $\varepsilon \in \{-1, +1\}$. Set

$$R(x) := \varepsilon x^{D_2} P_1(x) P_2(1/x) \quad \text{and} \quad S(x) := \varepsilon x^{D_1} P_1(1/x) P_2(x).$$

Note that $R \in \mathbb{Z}[x]$ and $S \in \mathbb{Z}[x]$ are monic polynomials with constant coefficient equal to 1. In addition, $R(x) = x^{D+1} S(1/x)$, so that if $R(x) = \sum_{j=0}^{D+1} a_j x^j$, then $S(x) = \sum_{j=0}^{D+1} a_j x^{D+1-j}$. Moreover,

$$RS = PQ \quad \text{with} \quad Q(x) = x^{D+1} P(1/x) = x^{D+1} - x + 1.$$

Identifying the coefficients of x^{D+1} on both sides yields $\sum_{j=0}^{D+1} a_j^2 = 3$. Thus, there are exactly three coefficients a_j which are non zero, and they are equal to ± 1. We already know that $a_{D+1} = a_0 = 1$. So, there exist $j \in [\![2, D]\!]$ and $a_j \in \{-1, +1\}$ such that

$$R(x) = x^{D+1} + a_j x^j + 1 \quad \text{and} \quad S(x) = 1 + a_j x^{D+1-j} + x^{D+1}.$$

Comparing RS to PQ again, we see that we necessarily have $j = 1$ or $j = D$ and $a_j = -1$. In other words, either $R = P$ and $P_2(x) = \varepsilon x^{D_2} P_2(1/x)$, or $S = P$ and $P_1(x) = \varepsilon x^{D_1} P_1(1/x)$. In the first case, the roots of P_2 are common roots of P and Q. In the second case, the roots of P_1 are common roots of P and Q.

To complete the proof, observe that if $x^{D+1} - x^D + 1 = x^{D+1} - x + 1 = 0$, then $x^D - x = 0$ and $x \neq 0$, so that $x^{D-1} = 1$. Thus, $x^2 - x + 1 = x^{D+1} - x + 1 = 0$, x is a 6-th root of unity and $D = 1 \mod 6$. □

It might be interesting to study whether there are other values of D and p for which the polynomial S_p is not irreducible over $\mathbb{Z}$. Adam Epstein would probably call those *algebraic conspiracies*.

We shall conclude §1 with the proofs of Proposition 2 and Corollary 3.

Proof of Proposition 2. An elementary induction shows that the degree of F_p is D^{p-1}. In addition, $c \in \mathcal{C}_p$ if and only if $R_p(c) = 0$ and moreover, R_p has simple roots. Thus, the degree of R_p is $N(p)$. As a consequence,

$$D^{p-1} = \deg(F_p) = \sum_{q|p} \deg(R_q) = \sum_{q|p} N(q).$$

The Möbius Inversion Formula immediately yields

$$N(p) = \sum_{q|p} \mu\left(\frac{p}{q}\right) D^{q-1} = \frac{\nu_D(p)}{D}. \qquad \square$$

Proof of Corollary 3. As $p \to \infty$, we have

$$\left|N(p) - D^{p-1}\right| \leq \sum_{q=1}^{\lfloor p/2 \rfloor} D^{q-1} = \frac{D^{\lfloor p/2 \rfloor} - 1}{D - 1} = o(D^{p-1}). \qquad \square$$

2. The preperiodic case

We shall now study the case where the preperiod k is at least 2. Note that if $c \in \mathcal{C}_{k,p}$, then c is a root of $F_{k+p} - F_p$. However, if $\ell \leq k$ and if q divides p, then any point $c \in \mathcal{C}_{\ell,q}$ is also a root of $F_{k+p} - F_p$. It follows that $F_{k+p} - F_p$ is not irreducible over $\mathbb{Z}$. We shall first study a corresponding factorization. Our result relies on the following Lemma (compare to the appendix in [E]).

Lemma 1. *Assume $K > k \geq 1$ and $\omega^D = 1$ with $\omega \neq 1$. Then, $F_K - \omega F_k$ has simple roots.*

Proof. We first do a preliminary comment. Let P_α be the minimal polynomial of $\alpha := 1 - \omega$. Since α is an algebraic integer, $P_\alpha \in \mathbb{Z}[x]$. Observe that

$$x^D - 1 = (x-1)(1 + x + \cdots + x^{D-1}) = (x-1) \cdot \prod_\zeta (x - \zeta),$$

where ζ ranges in the set of D-roots of unity different from 1. The constant coefficient $a_\alpha \in \mathbb{Z}$ of P_α is the product of the Galois conjugates of $\alpha = 1 - \omega$. It divides $\prod_\zeta (1 - \zeta) = 1 + 1^1 + \cdots + 1^{D-1} = D$.

Now, assume c_0 is a root of $F_K - \omega F_k$. Observe that the monic polynomial $F_K^D - F_k^D \in \mathbb{Z}[c]$ vanishes at c_0, so that, c_0 is an algebraic integer. Note that

$$F'_K - \omega F'_k = \alpha + D \cdot \big(F_{K-1}^{D-1} F'_{K-1} - \omega F_{k-1}^{D-1} F'_{k-1}\big).$$

So, if c_0 were a root of $F'_K - \omega F'_k$, then we would have $\alpha = D\beta$, for some algebraic integer β. Let $P_\beta \in \mathbb{Z}[y]$ be the minimal polynomial of β and let $a_\beta \in \mathbb{Z}$ be its constant coefficient. Then,

$$P_\alpha(x) = D^m P_\beta(x/D) \quad \text{with} \quad m := \deg(P_\alpha).$$

As a consequence, $D^m a_\beta = a_\alpha$ divides D, so that $m = 1$. This can occur only if $\alpha \in \mathbb{Q}$, i.e., only if $\omega = -1$. In that case, we have $2 = D\beta$ and so, $D = 2$ and $\beta = 1$. This proves that when $D \neq 2$ and $\omega \neq -1$, the roots of $F_K - \omega F_k$ are simple.

It remains to prove that when $D = 2$, the roots of $F_K + F_k$ are simple. Note that $F_K + F_k = F_{K-1}^2 + F_{k-1}^2 + 2c$. So, the derivative is

$$F'_K + F'_k = 2\big(1 + F_{K-1} F'_{K-1} + F_{k-1} F'_{k-1}\big),$$

so that $(F'_K + F'_k)/2 \in \mathbb{Z}[c]$. We shall prove that

$$\rho := \text{resultant}\left(F_K + F_k, \frac{F'_K + F'_k}{2}\right) \equiv 1 \mod 2.$$

It follows that the resultant does not vanish and $F_K + F_k$ has simple roots.

We have that

$$F'_{K-1} \equiv 1 \mod 2 \quad \text{and} \quad F'_{k-1} \equiv 1 \mod 2,$$

so that

$$1 + F_{K-1} F'_{K-1} + F_{k-1} F'_{k-1} \equiv 1 + F_{K-1} + F_{k-1} \mod 2.$$

We also have

$$F_K + F_k \equiv F_{K-1}^2 + F_{k-1}^2 \mod 2 \equiv (F_{K-1} + F_{k-1})^2 \mod 2.$$

Since $(F_{K-1} + F_{k-1})^2$ is monic and since $1 + F_{K-1} + F_{k-1}$ takes the value 1 at the roots of $(F_{K-1} + F_{k-1})^2$, we have that

$$\rho \equiv \text{resultant}\big((F_{K-1} + F_{k-1})^2, 1 + F_{K-1} + F_{k-1}\big) \mod 2 \equiv 1 \mod 2. \qquad \square$$

We deduce the following result.

Corollary 10. *For each $k \geq 1$ and each $p \geq 1$, there exists a (unique) monic polynomial $R_{k,p} \in \mathbb{Z}[c]$, such that the following holds. For $k \geq 1$ and $p \geq 1$,*

$$F_{k+p} - F_k = \prod_{\substack{1 \leq \ell \leq k \\ q|p}} R_{\ell,q} \cdot \prod_{q|p} R_q^{\delta_k(q)} \quad \text{with} \quad \delta_k(q) := D + (D-1) \left\lfloor \frac{k-1}{q} \right\rfloor.$$

If $k = 1$, then $R_{1,p} = 1$. If $k \geq 2$ the constant coefficient of $R_{k,p}$ is equal to D if $p = 1$ and is equal to 1 otherwise.

Proof. We shall prove the result by induction on $k \geq 1$. If $k = 1$, then

$$F_{1+p} - F_1 = F_p^D = \prod_{q|p} R_q^D.$$

So, the result holds with $R_{1,p} = 1$.

Assume $k \geq 2$ and suppose the property holds for $k-1$. Set $K := k + p$ and observe that c is a root of $F_K - F_k$ if and only if $c \in \mathcal{C}_{\ell,q}$ for somme $\ell \in [\![0, k]\!]$ and some q dividing p. In addition,

$$F_K - F_k = F_{K-1}^D - F_{k-1}^D = \prod_{\omega^D=1} (F_{K-1} - \omega F_{k-1}).$$

According to Lemma 1, if $\omega \neq 1$, the polynomial $F_{K-1} - \omega F_{k-1}$ has simple roots. In addition, c is a common root of $F_{K-1} - \omega_1 F_{k-1}$ and $F_{K-1} - \omega_2 F_{k-1}$ with $\omega_1 \neq \omega_2$ if and only if $F_{K-1}(c) = F_{k-1}(c) = 0$. In that case, $c \in \mathcal{C}_q$ with q dividing both $k-1$ and $p = (K-1) - (k-1)$. As a consequence, c is a root of $F_K - F_k$ if and only if either

- $c \in \mathcal{C}_{k,q}$ with q dividing p, or
- c is a root of $F_{K-1} - F_{k-1}$ and

$$\operatorname{ord}_c(F_K - F_k) = \operatorname{ord}_c(F_{K-1} - F_{k-1}) + \begin{cases} D-1 & \text{if } c \in \mathcal{C}_q \text{ with } q | \gcd(k-1, p), \text{ or} \\ 0 & \text{otherwise.} \end{cases}$$

It follows that

$$\frac{F_K - F_k}{F_{K-1} - F_{k-1}} = \prod_{\substack{\omega^D=1 \\ \omega \neq 1}} (F_{K-1} - \omega F_{k-1}) = \prod_{q|p} R_{k,q} \cdot \prod_{\substack{q|p \\ q|k-1}} R_q^{D-1}, \tag{1}$$

for some monic polynomials $R_{k,q} \in \mathbb{Z}[c]$. Thus,

$$F_K - F_k = \prod_{\substack{1 \leq \ell \leq k \\ q|p}} R_{\ell,q} \cdot \prod_{q|p} R_q^{\delta_k(q)}$$

with

$$\delta_k(q) := \begin{cases} \delta_{k-1}(q) & \text{if } q \text{ does not divide } k-1 \\ \delta_{k-1}(q) + D - 1 & \text{if } q \text{ divides } k-1. \end{cases}$$

Finally, assume $k \geq 2$. Since the polynomials R_q have constant coefficient 1 except $R_1 = c$, Equation (1) implies that the product of the constant coefficients of the polynomials $R_{k,q}$ for q dividing p is

$$\prod_{\substack{\omega^D=1 \\ \omega \neq 1}} (1 - \omega) = D.$$

For $p = 1$, this shows that the constant coefficient of $R_{k,1}$ is D. By induction on $p \geq 1$, we get that for $p \geq 2$, the constant coefficient of $R_{k,p}$ is 1. □

We may now the proofs of the results announced in the introduction.

Proof of Proposition 1. If $c \in \mathcal{C}_{k,p}$, then c is a root of $F_{k+p} - F_k \in \mathbb{Z}[c]$. This polynomial is monic, so that c is an algebraic integer. If $p \geq 2$, then c is a root of $R_{k,p}$ which, according to Corollaries 8 and 10, is monic with constant coefficient equal to 1. In that case, c is an algebraic unit. □

Proof of Proposition 4. On the one hand, it follows from Equation (1) that for all $k \geq 2$ and all $p \geq 1$,

$$\deg(F_K - F_k) - \deg(F_{K-1} - F_{k-1}) = \sum_{q|p} \big(N(k,q) + (D-1)\varepsilon(k,q)N(q)\big).$$

On the other hand

$$\begin{aligned}\deg(F_K - F_k) - \deg(F_{K-1} - F_{k-1}) &= D^{K-1} - D^{K-2} \\ &= (D-1)D^{k+p-2} = \sum_{q|p} (D-1)D^{k-1}N(q).\end{aligned}$$

As a consequence, for all $k \geq 2$ and all $p \geq 1$,

$$N(k,p) + (D-1)\varepsilon(k,p)N(p) = (D-1)D^{k-1}N(p). \qquad \square$$

Proof of Corollary 5. Assume $k + p \to \infty$. Either $k \to \infty$, in which case $\varepsilon(k,p) = \mathrm{o}(D^{k-1})$ and $D^{k-1} - \varepsilon(k,p) \sim D^{k-1}$. Or k is bounded and $p \to \infty$. In that case $\varepsilon(k,p) = 0$ and $D^{k-1} - \varepsilon(k,p) = D^{k-1}$ for p large enough. □

Proof of Corollary 6. As $p \to \infty$, $N(p) \sim D^{p-1}$ and for all $p \geq 1$, $N(p) > 0$. So, there is a constant $\kappa_0 > 0$ such that $N(p) \geq \kappa_0 D^p$. As $k + p \to \infty$,

$$N(k,p) \sim D^{k-1}(D-1)N(p) \geq \kappa_0(1 - 1/D)D^{k+p}$$

and for all $k \geq 2$ and all $p \geq 1$, $N(k,p) > 0$. So, there is a constant κ_1 such that $N(k,p) \geq \kappa_1 D^{k+p}$. □

References

[E] A. L. Epstein *Integrality and rigidity for postcritically finite polynomials*, Bull. London Math. Soc. 44 (2012), 39–46.

[M] J. Milnor *On Rational Maps with Two Critical Points*, Experiment. Math. **9**, Issue 4 (2000), 481–522.

[S] E. Selmer *On the Irreducibility of Certain Trinomials*, Math. Scand., **4** n° 2 (1957), 287–302.

E-mail address: xavier.buff@math.univ-toulouse.fr

Institut de Mathématiques de Toulouse, Université Paul Sabatier, 118, route de Narbonne, 31062 Toulouse Cedex, France