TWO QUESTIONS OF HUGUIN ON THE MULTIPLIER POLYNOMIALS OF $z^d + c$, ANSWERED AT TWENTY-FIVE PAIRS (d, n)

KOREA SUPERINTELLIGENCE LABS

Abstract. For $d \geq 2$ let $f_c(z) = z^d + c$, let $M_n \in \mathbb{Z}[c, \lambda]$ be the n-th multiplier polynomial of this family and let $\Delta_n = \operatorname{disc}_\lambda M_n \in \mathbb{Z}[c]$. Huguin factors $\Delta_n = a_n Q_n R_n^2$ with a_n a squarefree integer, the roots of Q_n being the parameters at which f_c has a cycle of period n and multiplier 1, and the roots of R_n the parameters at which f_c has two distinct cycles of period n with the same multiplier; he asks whether Q_n and R_n ever share a root, and whether $a_n = \pm 1$ for all n. Both questions survive only in the e-print of *Unicritical polynomial maps with rational multipliers* and in his thesis: the subsection carrying them was removed from the published version.

We answer both questions at twenty-five pairs (d, n) with $2 \leq d \leq 10$, namely all $n \leq 6$ for $d = 2$, all $n \leq 4$ for $d = 3$, all $n \leq 3$ for $d = 4$ and $n \leq 2$ for $5 \leq d \leq 10$. In every one of them Q_n and R_n have no common root in $\mathbb{C}$, and $a_n = \pm 1$; twelve of these pairs lie beyond the range in which the first question was previously settled or the data displayed, and ten beyond the range in which the second one was. The answers are certified by exact Bézout identities $uQ_n + vR_n = m$ over $\mathbb{Z}[c]$ with m a nonzero integer of up to 9465 decimal digits, together with explicit identities $\Delta_n = a_n Q_n R_n^2$; we record the polynomials R_n, which do not seem to have appeared in print for any $n \geq 2$, and the resulting sign data, in which $a_2 = +1$ occurs exactly at $d = 4$ and $d = 8$ in the computed range. All identities are checked by the Lean 4 kernel.

1. Introduction

1.1. **The polynomials.** Fix an integer $d \geq 2$ and consider the unicritical family

$$f_c(z) = z^d + c, \qquad c \in \mathbb{C},$$

whose members represent, up to affine conjugacy, all polynomial maps of degree d with a single critical point. Write $\boldsymbol{f}(z) = z^d + c \in \mathbb{Z}[c][z]$ for the generic member. For $n \geq 1$ let $\Phi_n \in \mathbb{Z}[c, z]$ be the n-th dynatomic polynomial, characterised by $\boldsymbol{f}^{\circ n}(z) - z = \prod_{k \mid n} \Phi_k(z)$ and of z-degree $\nu(n) = \sum_{k \mid n} \mu(n/k) d^k$, and let $M_n \in \mathbb{Z}[c, \lambda]$ be the n-th *multiplier polynomial*, the unique polynomial monic in λ with

$$M_n(c, \lambda)^n = \operatorname{res}_z\big(\Phi_n(z),\, \lambda - (\boldsymbol{f}^{\circ n})'(z)\big).$$

Its $\nu(n)/n$ roots are the multipliers of the period-n cycles of f_c, one root per cycle. Set

$$\Delta_n(c) = \operatorname{disc}_\lambda M_n(c, \lambda) \in \mathbb{Z}[c].$$

The parameters where Δ_n vanishes are exactly those where two period-n multipliers collide, which happens either because two distinct period-n cycles acquire the same multiplier or because a single cycle has multiplier 1 and is then a double root of M_n; the roots of Δ_n of odd multiplicity are precisely the parameters of the second kind ([2], which refers for this to [7, Proposition 9]; compare [8]). Huguin separates

the two phenomena. With $P_{k,l}(c) = \operatorname{res}_\lambda\big(C_l(\lambda), M_k(c,\lambda)\big)$, where C_l is the l-th cyclotomic polynomial, he defines $Q_n \in \mathbb{Z}[c]$ by

$$M_n(c,1) \;=\; Q_n(c) \prod_{k\mid n,\ k\neq n} P_{k,\,n/k}(c),$$

so that the roots of Q_n are precisely the parameters c_0 for which f_{c_0} has a cycle of period n and multiplier 1 — the cusps of the primitive period-n hyperbolic components of the multibrot set — and then proves that there are a unique squarefree integer a_n and a unique $R_n \in \mathbb{Z}[c]$ with positive leading coefficient such that

$$\Delta_n \;=\; a_n\, Q_n\, R_n^2, \tag{1}$$

the roots of R_n being precisely the parameters c_0 for which f_{c_0} has two distinct cycles of period n with the same multiplier.

1.2. **The questions.** The factorisation (1) is a tool in [2], not its subject: the main theorem there is that a unicritical polynomial map all of whose multipliers are rational is a power map or a Chebyshev map, which is evidence for Milnor's conjecture [5] that power maps, Chebyshev maps and flexible Lattès maps are the only rational maps whose multipliers are all integers. The questions below are a by-product of that proof, and they concern the factors Q_n and R_n themselves. We quote them verbatim.

Question 1 ([2], Question 54; in French, [4], Question 1.68)**.** Does there exist an integer $n \geq 1$ such that the polynomials Q_n and R_n have a common root? Equivalently, does there exist an integer $n \geq 1$ and a unicritical polynomial map $f\colon \mathbb{C} \to \mathbb{C}$ of degree d that has both a cycle with period n and multiplier 1 and two distinct cycles with period n and the same multiplier?

Question 2 ([2], Question 55; in French, [4], Question 1.69)**.** Do we have $a_n = \pm 1$ for all $n \geq 1$?

Question 1 is expected to have a negative answer and Question 2 a positive one; the evidence offered for each is one sentence, saying that a computation in SageMath confirms it "for small values of d and n", with no pair (d,n) named and no polynomial R_n displayed. What is proved in [2] is the case $n = 1$ of both questions, in closed form and for every d:

$$Q_1(c) = (-1)^d\big(d^d c^{d-1} - (d-1)^{d-1}\big), \qquad R_1(c) = d^{\frac{d(d-1)}{2}}\, c^{\frac{(d-1)(d-2)}{2}}, \qquad a_1 = (-1)^{\frac{d(d+1)}{2}}, \tag{2}$$

from which Q_1 and R_1 visibly have no common root and $a_1 = \pm 1$. For $d = 2$, Question 2 is settled for every n in Huguin's thesis ([4], Remarque 1.78). The input, stated already in [2], is that the periodic points of $f_{-t^d}\colon z \mapsto z^d - t^d$ have Laurent expansions in $t^{-(d-1)}$ with coefficients in $\mathbb{Q}(\omega)$, ω a primitive d-th root of unity, and hence so do their multipliers. The thesis makes this an indexing of the period-n points of f_{-t^d} by the period-n points of the one-sided shift on the d-th roots of unity, and its Proposition 1.77 then writes $\Delta_n(-t^d)$ as the product of the squares $(\lambda_j - \lambda_k)^2$ over the unordered pairs of distinct period-n multipliers, so that the leading coefficient of $\Delta_n(-t^d)$ is a square in $\mathbb{Q}(\omega)$. Remarque 1.78 combines this, at $d = 2$, with the fact that the leading coefficient of $Q_n(-t^2)$ is $\pm 2^{m_n}$ with $m_n = \nu(n) - \sum_{k\mid n,\ k\neq n} \varphi(n/k)\,\nu(k)/k$ even, and reads $a_n = \pm 1$ off (1), a_n being

squarefree. It is the first half that is special: it delivers a square in $\mathbb{Q}(\omega)$, and $\mathbb{Q}(\omega) = \mathbb{Q}$ only when $d = 2$. So Question 1 is, as far as we know, open for every d, and Question 2 is settled for all n when $d = 2$ and, again as far as we know, open for every $d \geq 3$.

A bibliographic point shapes what is and is not known here, and is easy to get wrong. The subsection containing the definitions of $P_{k,l}$, Q_n, a_n, R_n, the factorisation (1) and both questions is present in the e-print [2] and, in French, in the thesis [4]; it was removed in editing from the published version [3], and a good deal went with it: that paper has two numbered sections and no appendix against the e-print's three and one, it mentions neither Q_n nor R_n nor $P_{k,l}$ anywhere, its own two numbered questions are about other things entirely, and its bibliography — twelve items against the e-print's sixteen — no longer contains [8], which is what [2] cites for the roots of Q_n. Consequently the questions are absent from the citation graph of the published paper, and we have found no later work that addresses them: of the three papers citing [3] that we could locate, each cites it only for its main theorem, and a search of a large full-text mirror of the arXiv turned up no occurrence of the polynomials R_n or of the integers a_n in this sense outside [2] and [4]. We have found no printed value of R_n for any $n \geq 2$. This is a negative search result and should be read as "not found", not as "does not exist"; in particular the unpublished SageMath check reported in [2] may well cover some of the smaller pairs (d, n) treated below.

1.3. **Results.** We settle both questions at the twenty-five pairs (d, n) of Table 1.

Theorem 3. *Let (d, n) be one of the twenty-five pairs of Table 1, that is, $2 \leq d \leq 10$ with*

$$n \leq 6 \ (d = 2), \qquad n \leq 4 \ (d = 3), \qquad n \leq 3 \ (d = 4), \qquad n \leq 2 \ (5 \leq d \leq 10).$$

Then Q_n and R_n have no common root in $\mathbb{C}$: there is no $c_0 \in \mathbb{C}$ for which $f_{c_0}(z) = z^d + c_0$ has both a cycle of period n and multiplier 1 and two distinct cycles of period n with the same multiplier. Moreover $\Delta_n = a_n Q_n R_n^2$ with $a_n = \pm 1$, the sign being the one listed in Table 1.

Theorem 3 is the union of the statements proved cell by cell in Sections 4 and 5, where they are separated according to what was already known: the pairs with $n = 1$, the pairs $(2, n)$ with $n \leq 4$ and the pair $(3, 2)$ are re-derivations of what [2] proves or displays, and the whole $d = 2$ column of the second question is covered by [4], Remarque 1.78. The remaining twelve pairs for Question 1 and ten pairs for Question 2 are, as far as we could determine, new. The data behind them — in particular the polynomials R_n, of degree up to 1674 — is recorded in Section 6, and its two-sided character is recorded in Section 7: the statement is one about characteristic zero and about these n only, and we exhibit primes at which the same Q_n and R_n do acquire a common root.

1.4. **Method.** A common root of Q_n and R_n in $\mathbb{C}$ is destroyed by a single exact identity

$$u(c)\, Q_n(c) + v(c)\, R_n(c) = m, \qquad u, v \in \mathbb{Z}[c], \quad m \in \mathbb{Z} \setminus \{0\}, \tag{3}$$

because $m \neq 0$ in $\mathbb{C}$. This is a polynomial identity over $\mathbb{Z}$; no resultant theory and no dynamics enter its verification, which is a finite comparison of integer coefficients. The same data yields (1) as a second such identity. Two structural facts keep the

certificates small: Q_n and Δ_n lie in $\mathbb{Z}[d^d c^{d-1}]$, and R_n is c^{ε} times an element of that subring, so a pair (d, n) can be stored in the single variable $w = d^d c^{d-1}$, dividing every degree by $d-1$ and clearing the powers of d^d out of the coefficients: at $(d, n) = (10, 2)$ this turns degree 1674 into degree 186.

The identities (3) and (1) are what a machine checks here; the step that identifies the tabulated coefficient lists with Huguin's Q_n, R_n, Δ_n is an exact computation carried out beforehand and is not part of the formal verification. Section 6 says precisely what that computation was and against which published values it was gated.

2. Preliminaries

We use [2] for all facts in this section; they are stated there for the family $f_c(z) = z^d + c$ with c an indeterminate over $\mathbb{Z}$, and go back, for the parts concerning the discriminant, to [7] and [8]; for dynatomic polynomials in general see [10]. For the integrality statement that puts M_n into $\mathbb{Z}[d^d c^{d-1}, \lambda]$, [2] refers the reader to [6, Theorem 1.1].

Proposition 4 ([2])**.** *Let $d \geq 2$ and $n \geq 1$.*

1. *M_n lies in $\mathbb{Z}[d^d c^{d-1}, \lambda]$, is monic in λ of degree $\nu(n)/n$, and has degree $(d-1)\nu(n)/d$ in c.*
2. *$M_n(c, 1)$ and each $P_{k,l}$ lie in $\mathbb{Z}[d^d c^{d-1}]$ and have leading coefficient ± 1 there; $M_n(c, 1)$ is separable, so Q_n is well defined by the displayed factorisation, lies in $\mathbb{Z}[d^d c^{d-1}]$, has leading coefficient ± 1 there, and its roots are simple and are exactly the parameters c_0 at which f_{c_0} has a cycle of period n and multiplier 1.*
3. *There are a unique squarefree integer a_n and a unique $R_n \in \mathbb{Z}[c]$ with positive leading coefficient satisfying $\Delta_n = a_n Q_n R_n^2$, and the roots of R_n are exactly the parameters c_0 at which f_{c_0} has two distinct cycles of period n with the same multiplier.*

Part (3) is the reason a single factorisation determines a_n: exhibiting *any* identity $\Delta_n = a Q_n S^2$ with a squarefree and S of positive leading coefficient forces $a = a_n$ and $S = R_n$. In particular, exhibiting one with $a = \pm 1$ answers Question 2 for that pair (d, n), and this is how every statement about a_n below is proved.

Remark 5. Proposition 4(3) is Proposition 52 of [2], which states it with the additional clause that R_n lies in $\mathbb{Z}[d^d c^{d-1}]$. As literally written that clause is not correct, and the closed forms (2) of the source itself — its Example 53 — are a counterexample: at $d = 3$, $n = 1$ they give $R_1(c) = 27c$, while $\mathbb{Z}[d^d c^{d-1}] = \mathbb{Z}[27c^2]$ contains no polynomial of odd degree; likewise $R_1(c) = 5^{10} c^6 \notin \mathbb{Z}[5^5 c^4]$ at $d = 5$, the exponents available in $\mathbb{Z}[5^5 c^4]$ being the multiples of 4. What holds, and what is used below, is the weaker

$$R_n(c) = c^{\varepsilon_n} \rho_n\big(d^d c^{d-1}\big) \qquad \text{for some } \rho_n \in \mathbb{Z}[w] \text{ and } \varepsilon_n \geq 0 \text{ with } (d-1) \mid 2\varepsilon_n.$$

For the pairs treated here this shape is exhibited explicitly and is part of what is verified below; in general the exponent pattern follows from $\Delta_n, Q_n \in \mathbb{Z}[d^d c^{d-1}]$, which forces every exponent occurring in R_n^2 to be a multiple of $d-1$ and hence $R_n(\omega c) = \pm R_n(c)$ for each $(d-1)$-st root of unity ω. Nothing else in [2] rests on the clause: outside Proposition 52 the symbol R_n occurs there only in Example 53, in the sentence recording that Q_1 and R_1 have no common root, in Question 54

and in the paragraph leading to Question 55, and none of those appeals to the membership; nor does the proof of Proposition 52 itself, which establishes only the order formula $\operatorname{ord}_{c_0} \Delta_n = \varepsilon_n(c_0) + 2\kappa_n(c_0)$. Since the subsection was removed from [3], no erratum exists. (This reading was checked against the text of the single arXiv version, v1 of 4 September 2020, on 30 August 2026, and the numbering above is that version's.) The values of ε_n we compute are listed in Table 1: they vanish at every even d in our range, and at odd d they are multiples of $(d-1)/2$, as the congruence $(d-1) \mid 2\varepsilon_n$ allows.

Throughout, w denotes the variable $d^d c^{d-1}$, we write $D = d^d$ and $e = d - 1$, so that $w = Dc^e$, and for a pair (d, n) we write

$$Q_n(c) = q(Dc^e), \qquad R_n(c) = c^{\varepsilon}\rho(Dc^e), \qquad \Delta_n(c) = \delta(Dc^e)$$

with $q, \rho, \delta \in \mathbb{Z}[w]$ and $\varepsilon \geq 0$.

3. Certificates

The two lemmas of this section are the entire deductive content of the paper; everything else is the finite verification of their hypotheses at twenty-five pairs (d, n).

Lemma 6 (Bézout certificate)**.** *Let R be a commutative ring, let $P, S \in \mathbb{Z}[X]$, and suppose there are $u, v \in \mathbb{Z}[X]$ and $m \in \mathbb{Z}$ with $uP + vS = m$ in $\mathbb{Z}[X]$. If the image of m in R is nonzero, then P and S have no common root in R.*

Proof. Evaluating the identity at a common root x_0 gives $m = 0$ in R. □

Taking $R = \mathbb{C}$ gives the characteristic-zero statement; taking $R = \overline{\mathbb{F}_p}$ gives the same conclusion over a field of characteristic p *provided* $p \nmid m$. This proviso is exactly the boundary of what a certificate proves, and Section 7 shows that the boundary is real.

The reduction to the variable w costs one extra hypothesis, because R_n may vanish at $c = 0$ while the Bézout identity in w is blind there: $w = 0$ when $c = 0$.

Lemma 7 (cell lemma)**.** *Let K be a field, let $D \in \mathbb{Z}$, let $e \geq 1$ and $\varepsilon \geq 0$ be integers, and let $q, \rho, u, v \in \mathbb{Z}[w]$ and $m \in \mathbb{Z}$ satisfy $uq + v\rho = m$ in $\mathbb{Z}[w]$. Put*

$$Q(c) = q(Dc^e), \qquad R(c) = c^{\varepsilon}\rho(Dc^e) \qquad \in \mathbb{Z}[c].$$

If $m \neq 0$ and $q(0) \neq 0$ in K, then Q and R have no common root in K.

Proof. Let $c_0 \in K$ satisfy $Q(c_0) = R(c_0) = 0$ and put $w_0 = Dc_0^e$. From $R(c_0) = 0$ either $c_0 = 0$ or $\rho(w_0) = 0$. In the first case $w_0 = 0$ and $0 = Q(c_0) = q(0) \neq 0$, a contradiction. In the second, evaluating $uq + v\rho = m$ at w_0 gives $m = u(w_0)q(w_0) + v(w_0)\rho(w_0) = u(w_0)Q(c_0) = 0$, again a contradiction. □

The hypothesis $q(0) \neq 0$ says that $Q_n(0) \neq 0$, that is, that the power map $z \mapsto z^d$ has no cycle of period n and multiplier 1; its multipliers are all equal to d^n. It is not removable (Proposition 25).

Lemma 8 (factorisation certificate)**.** *In the situation of Lemma 7, let $\delta \in \mathbb{Z}[w]$, let $a \in \mathbb{Z}$ and let $s \geq 0$ satisfy $2\varepsilon = es$. If*

$$D^s\,\delta \;=\; a\,q\,\rho \cdot \left(w^s \rho\right) \qquad \text{in } \mathbb{Z}[w]$$

and $D \neq 0$ in K, then $\Delta(c) = a\,Q(c)\,R(c)^2$ for every $c \in K$, where $\Delta(c) = \delta(Dc^e)$.

Proof. Evaluate at $w_0 = Dc^e$ and use $w_0^s = D^s c^{es} = D^s c^{2\varepsilon}$:

$$D^s \delta(w_0) = a\, q(w_0)\, \rho(w_0)^2\, D^s c^{2\varepsilon} = D^s\, a\, Q(c)\, R(c)^2.$$

Cancel $D^s \neq 0$. □

By Proposition 4(3), an identity as in Lemma 8 with $a \in \{+1, -1\}$ and ρ of positive leading coefficient identifies a with a_n and $c^\varepsilon \rho(w)$ with R_n, and so answers Question 2 at that pair.

4. Question 1 at twenty-five pairs

In each of the following statements, Q_n and R_n are Huguin's polynomials for the stated degree d, of the degrees listed in Table 1, and the dynamical reformulation is the equivalence recorded in Proposition 4.

Theorem 9. *Let $d = 2$ and $n \in \{5, 6\}$. Then Q_n and R_n have no common root in $\mathbb{C}$: no $c_0 \in \mathbb{C}$ is such that $z^2 + c_0$ has both a cycle of period n with multiplier 1 and two distinct cycles of period n with the same multiplier. Here $\deg Q_5 = 11$, $\deg R_5 = 28$, $\deg Q_6 = 20$ and $\deg R_6 = 85$.*

Theorem 10. *Let $d = 3$ and $n \in \{3, 4\}$. Then Q_n and R_n have no common root in $\mathbb{C}$. Here $\deg Q_3 = 12$, $\deg R_3 = 44$, $\deg Q_4 = 40$ and $\deg R_4 = 350$.*

Theorem 11. *Let $d = 4$ and $n \in \{2, 3\}$. Then Q_n and R_n have no common root in $\mathbb{C}$. Here $\deg Q_2 = 6$, $\deg R_2 = 18$, $\deg Q_3 = 39$ and $\deg R_3 = 372$.*

Theorem 12. *Let $n = 2$ and $5 \leq d \leq 10$. Then Q_2 and R_2 have no common root in $\mathbb{C}$. Here $\deg R_2 = 62, 155, 327, 609, 1044, 1674$ for $d = 5, 6, 7, 8, 9, 10$ respectively, and the Bézout constants of the certificates have from 120 to 9465 decimal digits.*

The remaining pairs of Table 1 are those that [2] settles or from whose displayed data the answer can be read off; we record them because the same apparatus proves them, not as new results.

Proposition 13. *Q_n and R_n have no common root in $\mathbb{C}$ for $n = 1$ and every $2 \leq d \leq 10$, for $d = 2$ and $n \leq 4$, and for $d = 3$ and $n = 2$.*

Proof of Theorems 9–12 and Proposition 13. Let (d, n) be one of the twenty-five pairs of Table 1. We exhibit four integer polynomials q, ρ, u, v in the variable $w = d^d c^{d-1}$, together with an integer $\varepsilon \geq 0$ and a nonzero integer m, such that

$$Q_n(c) = q\big(d^d c^{d-1}\big), \quad R_n(c) = c^\varepsilon \rho\big(d^d c^{d-1}\big), \quad uq + v\rho = m,$$

the last identity holding in $\mathbb{Z}[w]$, and such that $q(0) \neq 0$; Lemma 7 with $K = \mathbb{C}$ then gives the conclusion. Two things are finite computations, and are the only computations involved. First, the verification of $uq + v\rho = m$: the two products are expanded and compared coefficient by coefficient, over $\mathbb{Z}$ and in full, with no floating point, no modular reconstruction and no randomisation. For $(d, n) = (2, 5)$, for instance, $\deg u = 27$ and $\deg v = 10$ in w against $\deg q = 11$ and $\deg \rho = 28$, so the comparison is of 39 integer coefficients, the largest of the inputs having 85 decimal digits; at $(10, 2)$ the same comparison involves coefficients of several thousand digits. Second, the evaluation $q(0) \neq 0$, which is the reading of a single integer. Both were carried out by the Lean 4 kernel (Section 9); no search over an unbounded set occurs anywhere, and no pair (d, n) outside Table 1 is asserted.

The construction of the certificates, as opposed to their verification, was done by the extended Euclidean algorithm in $\mathbb{Q}[w]$ followed by clearing of denominators; how the polynomials q, ρ, δ themselves were obtained, and against what they were checked, is described in Section 6. □

Remark 14. The certificates are not merely nonconstructive existence statements: they exhibit m. At $(d, n) = (2, 5)$,

$$m = 2^{21} \cdot 3^9 \cdot 11^6 \cdot 29 \cdot 31^{19} \cdot 4217^3 \cdot 86131^2 \cdot M,$$

a number of 93 decimal digits whose cofactor M is an 82-bit integer that we did not factor and that has no prime divisor below 10^5. By Lemma 6, every prime at which the reductions of Q_5 and R_5 acquire a common factor divides m. The largest constant in the table, at $(10, 2)$, has 9465 decimal digits.

5. Question 2 at twenty-five pairs

Theorem 15. *Let $d = 3$. Then $\Delta_3 = Q_3 R_3^2$ and $\Delta_4 = -Q_4 R_4^2$; that is, $a_3 = +1$ and $a_4 = -1$. So Question 2 has a positive answer at $(d, n) = (3, 3)$ and $(3, 4)$; these are the first pairs beyond the data displayed in* [2]*, whose $d = 3$ examples stop at $n = 2$, and the question remains open in general for every $d \geq 3$.*

Theorem 16. *Let $d = 4$. Then $a_2 = a_3 = +1$, that is, $\Delta_n = Q_n R_n^2$ for $n \in \{2, 3\}$.*

Theorem 17. *Let $n = 2$. Then $a_2 = -1, -1, -1, +1, -1, -1$ for $d = 5, 6, 7, 8, 9, 10$ respectively. Together with $a_2 = -1$ at $d = 2, 3$ and $a_2 = +1$ at $d = 4$, this makes $a_2 = +1$ occur exactly at $d = 4$ and $d = 8$ in the range $2 \leq d \leq 10$.*

Proposition 18. *$\Delta_n = a_n Q_n R_n^2$ with $a_n = \pm 1$ holds, with the signs of Table 1, for $n = 1$ and every $2 \leq d \leq 10$, for $d = 2$ and every $n \leq 6$, and for $d = 3$, $n = 2$. These pairs are covered by results of* [2] *and* [4]*: the closed form* (2) *gives $a_1 = (-1)^{d(d+1)/2}$ for every d, matching the computed value at each $d \leq 10$; Remarque 1.78 of* [4] *gives $a_n = \pm 1$ for all n when $d = 2$; and the pair* $(3, 2)$ *is read off the value of Δ_2 displayed in* [2]*. The individual signs, e.g. $a_n = -1$ for all $n \leq 6$ at $d = 2$, follow from those results together with a comparison of leading coefficients and are not claimed as new.*

Proof of Theorems 15–17 and Proposition 18. For each pair (d, n) we exhibit, in addition to q and ρ as above, a polynomial $\delta \in \mathbb{Z}[w]$ with $\Delta_n(c) = \delta(d^d c^{d-1})$, a sign $a \in \{+1, -1\}$ and an integer $s \geq 0$ with $2\varepsilon = (d-1)s$, satisfying

$$\left(d^d\right)^s \delta = a\, q\, \rho \cdot \left(w^s \rho\right) \qquad \text{in } \mathbb{Z}[w].$$

This is again a comparison of finitely many integer coefficients — at $(3, 4)$, for example, of the $\deg \delta + 1 = 371$ coefficients in w of two products — and again it was carried out in full by the Lean 4 kernel. Lemma 8 converts it into $\Delta_n(c) = a\, Q_n(c) R_n(c)^2$ for all $c \in \mathbb{C}$, and since ρ has positive leading coefficient and a is squarefree, the uniqueness in Proposition 4(3) identifies a with a_n. The statement that the sign is what the table says is therefore not an approximation: it is the value of the invariant a_n. □

Remark 19. The sign a_2 is $+1$ exactly at $d = 4$ and $d = 8$ in the computed range, that is, exactly when $4 \mid d$. This is an observation from nine values of d and we do not claim it as a pattern; the natural next test is $d = 11, 12, 16$, and the cost of $d = 12$ is a few minutes of computation. The sign is at any rate not constant in

d	n	$\nu(n)$	$\deg Q_n$	$\deg R_n$	$\deg \Delta_n$	ε_n	a_n	digits of m
2	1	2	1	0	1	0	-1	1
2	2	2	0	0	0	0	-1	1
2	3	6	1	1	3	0	-1	2
2	4	12	3	4	11	0	-1	7
2	5	30	11	28	67	0	-1	93
2	6	54	20	85	190	0	-1	530
3	1	3	2	1	4	1	$+1$	2
3	2	6	2	3	8	1	-1	3
3	3	24	12	44	100	0	$+1$	130
3	4	72	40	350	740	0	-1	3518
4	1	4	3	3	9	0	$+1$	3
4	2	12	6	18	42	0	$+1$	29
4	3	60	39	372	783	0	$+1$	2617
5	1	5	4	6	16	2	-1	6
5	2	20	12	62	136	2	-1	120
6	1	6	5	10	25	0	-1	10
6	2	30	20	155	330	0	-1	411
7	1	7	6	15	36	3	$+1$	16
7	2	42	30	327	684	3	-1	1046
8	1	8	7	21	49	0	$+1$	22
8	2	56	42	609	1260	0	$+1$	2486
9	1	9	8	28	64	4	-1	31
9	2	72	56	1044	2144	4	-1	4983
10	1	10	9	36	81	0	-1	40
10	2	90	72	1674	3420	0	-1	9465

TABLE 1. The twenty-five pairs (d, n). Degrees are in c; ε_n is the power of c that must be removed from R_n before the rest is a polynomial in $w = d^d c^{d-1}$, which is in general smaller than the order of vanishing of R_n at $c = 0$; m is the Bézout constant of the certificate for that pair. Note the consistency check $\deg Q_n + 2\deg R_n = \deg \Delta_n$, which holds in every row.

d — it is $+1$ at $(4, 1)$ and -1 at $(2, 1)$, see Proposition 21 — nor constant in n at fixed d: at $d = 3$ it alternates $+, -, +, -$ over $n \le 4$.

6. The data and how it was obtained

The polynomials were computed in PARI/GP with exact arithmetic over $\mathbb{Z}[c]$, following the definitions of Section 2 literally: Φ_n by exact division in $\mathbb{Z}[c][z]$; M_n as the λ-monic n-th root of $\mathrm{res}_z(\Phi_n, \lambda - (\boldsymbol{f}^{\circ n})')$; $\Delta_n = \mathrm{disc}_\lambda M_n$; $P_{k,l} = \mathrm{res}_\lambda(C_l, M_k)$ and $Q_n = M_n(c, 1)/\prod_{k|n,\, k\neq n} P_{k,n/k}$; and finally the splitting of Δ_n/Q_n as $a_n R_n^2$. The pipeline reproduces exactly every polynomial displayed in [2]: the multiplier polynomials $M_1, \dots, M_4$ and discriminants $\Delta_1, \dots, \Delta_4$ for $d = 2$, and $M_1, M_2, \Delta_1, \Delta_2$ for $d = 3$, together with the closed forms (2) for general d, whose sign $(-1)^{d(d+1)/2}$ agrees with the computed a_1 at every $d \le 10$. Every emitted coefficient list was then re-derived by an independent implementation, and the Bézout and factorisation identities were asserted there before any of them was verified formally.

A second gate, independent of [2], is available at $d = 2$ for the two largest n we reach. Following [7], [1] factors the multiplier polynomial at $\lambda = 1$ as $\delta_n(1, c) = \prod_{k|n} \Delta_{n,k}$, in which the roots of $\Delta_{n,n}$ are the parameters at which two orbits of period n collide; so $\Delta_{n,n}$ and Q_n agree up to sign, as do the remaining factors and the $P_{k,n/k}$. The e-print of [1] prints $\Delta_{n,n}$ for $z^2 + c$ and $n = 5, 6, 7, 8$ in an ancillary file, and our Q_5 is that file's $\Delta_{5,5}$ coefficient for coefficient, our Q_6 its $-\Delta_{6,6}$. Independently of the file, our $P_{1,5} = w^4 + w^3 + w^2 - 9w + 31$ and our Q_5 reproduce all three entries of that paper's factorisation table at $n = 5$; those are displayed in Section 8.

As a further check of the identification of Q_n with the cusp polynomial, the degree sequence $1, 0, 1, 3, 11, 20$ of Q_n for $d = 2$, $n \le 6$ agrees with the first six terms of [9], "Mu-molecules in Mandelbrot set whose seeds have period n", whose offset is $n = 1$; and the degrees $11, 20, 57, 108$ of the four polynomials in the ancillary file just cited are its terms $n = 5, \dots, 8$. That sequence counts the primitive period-n hyperbolic components of the Mandelbrot set, and the formula recorded with it, $a(n) = 2l(n) - \sum_{k|n} \varphi(n/k)\, l(k)$ with $l(n) = \nu(n)/2$, is literally $\deg_c M_n(c, 1) - \sum_{k|n,\, k\neq n} \deg_c P_{k,n/k}$, since $\deg_c M_n = \nu(n)/2$ and $\deg_c P_{k,l} = \varphi(l)\,\nu(k)/2$ when $d = 2$.

As an example of the data, at $(d, n) = (2, 5)$, in the variable $w = 4c$,

$$\begin{aligned} Q_5(c) &= w^{11} + 31w^{10} + 416w^9 + 3404w^8 + 20548w^7 + 98258w^6 + 370146w^5 \\ &\quad + 1171676w^4 + 3301996w^3 + 7507332w^2 + 15699857w + 28629151, \\ R_5(c) &= 2^{21} w^{15} \big(w^{13} + 56w^{12} + 1372w^{11} + 19312w^{10} + 171712w^9 + 975104w^8 \\ &\quad + 2947072w^7 - 4571136w^6 - 115474432w^5 - 764411904w^4 \\ &\quad - 3179282432w^3 - 9193914368w^2 - 17716740096w - 17179869184 \big). \end{aligned}$$

Here Q_5 is monic in w, as Proposition 4(2) requires, and R_5 has positive leading coefficient, as its normalisation requires. The factor w^{15} reflects the six period-5 cycles of the power map $z \mapsto z^2$, all of multiplier 2^5: each of the $\binom{6}{2} = 15$ coinciding pairs contributes to the order of vanishing of R_5 at $c = 0$, which here is exactly 15.

7. What the certificates do not prove

A coprimality statement is easy to make vacuously or to over-read. The following propositions delimit it from both sides; all are verified in the same way as the theorems above.

Proposition 20. *The conclusion of Theorem 3 is a statement about characteristic zero, and fails in positive characteristic. Explicitly, the reductions of Q_n and R_n have a common root: for $d = 2$, $n = 5$, at $c = 1$ in $\mathbb{F}_3$ and at $c = 9$ in $\mathbb{F}_{11}$; for $d = 2$, $n = 6$, at $c = 3$ in $\mathbb{F}_5$; for $d = 3$, $n = 4$, at $c = 9$ in $\mathbb{F}_{31}$; for $d = 4$, $n = 3$, at $c = 5$ in $\mathbb{F}_{11}$; and for $d = 8$, $n = 2$, at $c = 5$ in $\mathbb{F}_7$.*

Each of these primes divides the corresponding Bézout constant m, as Lemma 6 demands; the certificate is silent exactly there.

Proposition 21. *The sign a_n is not constant. At $(d, n) = (4, 1)$ one has $a_1 = +1$, and the identity $\Delta_1 = -Q_1 R_1^2$ fails already at the integer point $c = 1$.*

Proposition 22. *The certificates cannot be strengthened to $m = \pm 1$: for $d = 2$ and $n \in \{4, 5\}$ there are no $u, v \in \mathbb{Z}[c]$ with $uQ_n + vR_n = 1$. Indeed $R_n(0) = 0$*

while $Q_4(0) = 135$ and $Q_5(0) = 28629151$, so evaluation at $c = 0$ would force $Q_n(0)$ to be a unit of $\mathbb{Z}$. Thus Q_n and R_n generate a proper ideal of $\mathbb{Z}[c]$, and $m \neq 0$, rather than m invertible, is the right hypothesis in Lemma 6.

Proposition 23. *The statement is not vacuous through R_n having no roots. For $d = 2$ and $n \in \{4, 5, 6\}$ the power-map parameter $c = 0$ and the Chebyshev parameter $c = -2$ are both roots of R_n, while*

$$Q_n(0) = 135,\ 28629151,\ -3063651608241,$$

$$Q_n(-2) = -17,\ -285417,\ -245246990625$$

for $n = 4, 5, 6$ respectively.

The two parameters have one-line dynamical explanations — all period-n cycles of $z \mapsto z^2$ share the multiplier 2^n, and $z \mapsto z^2 - 2$ is a Chebyshev map, whose period-n multipliers are $\pm 2^n$ — and neither map has a period-n cycle of multiplier 1. So R_n genuinely has roots that Q_n misses, and Theorem 3 says that they never meet.

Proposition 24. *Coprimality is not automatic in this circle of polynomials: for $d = 2$, $n = 5$, every root of Q_5 is a root of Δ_5, since $Q_n \mid \Delta_n$ by (1).*

Proposition 25. *The hypothesis $q(0) \neq 0$ of Lemma 7 cannot be dropped. Take $D = 4$, $e = 1$, $\varepsilon = 1$, $q = w$, $\rho = 1$, $u = 0$, $v = 1$, so that $uq + v\rho = 1 \neq 0$ and every other hypothesis holds; then $Q(c) = 4c$ and $R(c) = c$ share the root $c = 0$.*

8. Two remarks outside the formal development

The following two observations are computations we ran alongside the certificates. Unlike the numbered statements above they are not part of the verified development, and we record them as measurements rather than as claims.

Remark 26 (bad primes). For each pair (d, n) the primes at which the reductions of Q_n and R_n acquire a common factor all divide the Bézout constant m, so the factorisation of m bounds the set of bad primes. Below 10^5 these primes are, for instance,

$$\{2, 3, 11, 29, 31, 4217, 86131\} \quad \text{at } (2, 5),$$

$$\{2, 3, 5, 7, 13, 29, 61, 79, 211, 239, 409, 2693, 3331\} \quad \text{at } (2, 6).$$

The lists are one-sided: the unfactored cofactors of m range from 67 to 24160 bits, so we can assert that these primes are bad but not that no others are. The nearest published data of this shape is the table of prime factorisations of $\operatorname{disc}(\Delta_{n,d})$ and $\operatorname{res}(\Delta_{n,d}, \Delta_{n,e})$ for $z^2 + c$, $n \leq 8$, in [1]. Those are invariants of Q_n and the $P_{k,l}$ alone — R_n never enters — and so are different numbers from ours. At $n = 5$ the three entries are, in our notation and as we recompute them,

$$\operatorname{disc} P_{1,5} = 2^{24} \cdot 5^7 \cdot 11^2, \qquad \operatorname{res}(P_{1,5}, Q_5)^2 = 2^{232} \cdot 11^6 \cdot 31^{18} \cdot 86131^2,$$

$$\operatorname{disc} Q_5 = 2^{274} \cdot 3^{12} \cdot 31^{27} \cdot 3701 \cdot 4217^3.$$

The third of these shares the primes $2, 3, 31, 4217$ with our $(2, 5)$ list, and differs from it at 29 and at 3701; the two remaining primes of our list, 11 and 86131, occur in the second.

Remark 27 (the frontier). The cost of a pair is dominated by the computation of M_n. At $d = 2$ the measured times were 1.0 s at $n = 5$ and 54 s at $n = 6$, a factor of roughly 55 per step in n; at $n = 7$, where $\nu(7) = 126$, the computation was stopped, unfinished, after 25 CPU-minutes. Extrapolating, $(2, 7)$ would need a few CPU-hours and produce a certificate of order 10 MB, with $\deg \Delta_7 \approx 1071$ and $\deg R_7 \approx 507$; it is the first pair we did not reach. The whole of Table 1 cost about six CPU-minutes to produce.

9. Verification

Every lemma, theorem and proposition of Sections 3, 4, 5 and 7 is formalised and machine-checked in Lean 4 against Mathlib — their mathematical content, that is; the attributions and the statements of openness carried alongside some of them are bibliographic, and are sourced in the introduction. The source is available with this paper (repository reference to be added at submission). The polynomials are carried as integer coefficient lists with an evaluation map into an arbitrary commutative ring; Lemmas 6, 7 and 8 are proved once in that generality, and each pair (d, n) of Table 1 supplies its own $q, \rho, \delta, u, v, m, a$ and discharges the arithmetic hypotheses. Every certificate identity is closed by the kernel's own reduction (`decide`), not by compiled evaluation (`native_decide`), so the Lean compiler's code generator is not part of the trusted base for any statement here; the axiom set of each theorem is a subset of {`propext`, `Classical.choice`, `Quot.sound`} and contains no `sorryAx`. What the formal development does *not* contain is the identification of the tabulated coefficient lists with Huguin's Q_n, R_n and Δ_n; that rests on the exact computation described in Section 6 and gated against the published values there. Certifying it as well would require formalising, upward from the data, the identities $\prod_{k|n} \Phi_k = \boldsymbol{f}^{\circ n}(z) - z$ and $M_n(c, 1) = Q_n \prod_{k|n, k\neq n} P_{k,n/k}$ — both cheap — and $M_n(\lambda)^n = \operatorname{res}_z(\Phi_n, \lambda - (\boldsymbol{f}^{\circ n})')$, which is a $\nu(n) \times \nu(n)$ characteristic polynomial over $\mathbb{Z}[c]$ and is out of reach at $\nu(n) = 54$. The total size of the certificates is about 4.2 MB.

10. Questions

(1) So far as we could determine, Question 1 remains open for every d, and Question 2 for every $d \geq 3$. Nothing in the method here bears on either in general: a Bézout certificate settles one pair (d, n) and says nothing about the next.
(2) For Question 2 at $d \geq 3$, the argument of [4], Remarque 1.78 stops because $\mathbb{Q}(\omega) \neq \mathbb{Q}$ for $d \geq 3$; a norm or Galois argument over $\mathbb{Q}(\omega)$ is the obvious route, and we know of no attempt at one.
(3) Is $a_2 = +1$ if and only if $4 \mid d$? True for $2 \leq d \leq 10$; $d = 11, 12, 16$ would be cheap to test.
(4) The first pair we could not reach is $(d, n) = (2, 7)$. A method for M_n that beats the observed factor of 55 per step in n — bivariate interpolation of res_z at integer points is the natural candidate — would move the frontier for all of $d = 2$.

References

[1] John R. Doyle, Holly Krieger, Andrew Obus, Rachel Pries, Simon Rubinstein-Salzedo and Lloyd West, *Reduction of dynatomic curves*, Ergodic Theory Dynam. Systems **39** (2019), no. 10, 2717–2768, DOI 10.1017/etds.2017.140; arXiv:1703.04172. The polynomials $\Delta_{n,n}$ for

$z^2 + c$ and $n = 5, 6, 7, 8$ are in the ancillary file `delta_nn.txt` of the e-print, and the tables of factorisations are in its subsection "Tables".

[2] Valentin Huguin, *Unicritical polynomial maps with rational multipliers*, arXiv:2009.02422v1 (4 September 2020); this is the only version. The definitions of $P_{k,l}$, Q_n, a_n and R_n, the factorisation (1) and both questions are in Section 3.3, "Discriminants of the multiplier polynomials", the last subsection before Appendix A. In that version's numbering, (1) and the uniqueness of (a_n, R_n) are Proposition 52, the closed forms (2) are Example 53, and the two questions are Question 54 and Question 55, the last two numbered environments of the body.

[3] Valentin Huguin, *Unicritical polynomial maps with rational multipliers*, Conform. Geom. Dyn. **25** (2021), 79–87, DOI 10.1090/ecgd/359. This is the published version of [2]; it does not contain the material on Q_n and R_n, nor either question.

[4] Valentin Huguin, *Étude algébrique des points périodiques et des multiplicateurs d'une fraction rationnelle*, Ph.D. thesis, Université Toulouse III Paul Sabatier, defended 22 October 2021, NNT 2021TOU30170; HAL tel-03466529. In French. Questions 1.68 and 1.69, in Section 1.3, are the counterparts of Questions 54 and 55 of [2]; Proposition 1.77 and Remarque 1.78 are in Section 1.4. The two deposited versions, v1 and v2, differ only in their cover pages, and the numbering is the same in both.

[5] John Milnor, *On Lattès maps*, in: Dynamics on the Riemann sphere, Eur. Math. Soc., Zürich, 2006, pp. 9–43.

[6] John Milnor, *Arithmetic of unicritical polynomial maps*, in: Frontiers in complex dynamics, Princeton Math. Ser., vol. 51, Princeton Univ. Press, Princeton, NJ, 2014, pp. 15–24.

[7] Patrick Morton, *On certain algebraic curves related to polynomial maps*, Compositio Math. **103** (1996), no. 3, 319–350.

[8] Patrick Morton and Franco Vivaldi, *Bifurcations and discriminants for polynomial maps*, Nonlinearity **8** (1995), no. 4, 571–584.

[9] The On-Line Encyclopedia of Integer Sequences, sequence A006876.

[10] Joseph H. Silverman, *The arithmetic of dynamical systems*, Graduate Texts in Mathematics, vol. 241, Springer, New York, 2007.