IRREDUCIBILITY OF POLYNOMIALS WITH A LARGE GAP

WILLIAM SAWIN, MARK SHUSTERMAN, AND MICHAEL STOLL

ABSTRACT. We generalize an approach from a 1960 paper by Ljunggren, leading to a practical algorithm that determines the set of $N > \deg c + \deg d$ such that the polynomial

$$f_N(x) = x^N c(x^{-1}) + d(x)$$

is irreducible over $\mathbb{Q}$, where $c, d \in \mathbb{Z}[x]$ are polynomials with nonzero constant terms and satisfying suitable conditions. As an application, we show that $x^N - kx^2 + 1$ is irreducible for all $N \geq 5$ and $k \in \{3, 4, \ldots, 24\} \setminus \{9, 16\}$. We also give a complete description of the factorization of polynomials of the form $x^N + kx^{N-1} \pm (lx + 1)$ with $k, l \in \mathbb{Z}$, $k \neq l$.

1 Introduction

Providing irreducibility criteria for integral polynomials is by now a classical topic, as can be seen for instance from the books [Pra04] by Prasolov or [Sch00] by Schinzel. Yet, the irreducibility of most polynomials cannot be established using the classical techniques, and many problems remain open. One example is the irreducibility of random polynomials, as studied for instance in [BSK16]. Another challenge, motivated by the calculation of Galois groups, lies in finding irreducibility criteria for trinomials. Indeed, in various works such as [CMS97, CMS99, MS96, Osa87], Galois groups are calculated under an irreducibility assumption. The purpose of this work is to obtain such irreducibility criteria. More generally, we consider polynomials "with a large gap", by which we mean polynomials of the form

$$f_N(x) = x^N c(x^{-1}) + d(x)\,,$$

where c and d are fixed polynomials in $\mathbb{Z}[x]$ with $c(0), d(0) \neq 0$ and we are interested in the irreducibility of f_N for large N. Polynomials of this type and their factorization into irreducibles have been considered in various contexts; see for example [Sch67, FFK00, FM04, DFV13, HVW13]. The main contributions of this paper are to give an improved bound for N such that the factorization of f_N can be controlled and to present an algorithm that can in many cases determine the factorizations of all f_N. This requires c and d to satisfy some additional conditions.

For a polynomial f, we set $\tilde{f}(x) = x^{\deg f} f(x^{-1})$ and we say that f is *reciprocal* if $\tilde{f} = \pm f$. If $f \neq 0$, we define the *non-reciprocal part* of $f \in \mathbb{Z}[x]$ to be f divided by all reciprocal and non-constant irreducible factors in its prime factorization over $\mathbb{Z}[x]$. Similarly, we define the *non-cyclotomic part* of f to be f divided by all irreducible factors that are cyclotomic polynomials. (Both of these are only defined up to a sign, but the sign is irrelevant for our purposes.) Since we are interested in the irreducibility of f_N above, we can always assume

Date: March 28, 2018.
2010 *Mathematics Subject Classification.* 11R09, 12E05, 11C08, 13P05.

that $\gcd_{\mathbb{Z}[x]}(\tilde{c}, d) = 1$, since otherwise this gcd will give a trivial divisor of f_N for all N. We will in addition assume that f_N is not reciprocal, which is equivalent to $c \neq \pm d$.

Note that "irreducible" in this paper always means "irreducible over $\mathbb{Q}$".

There are systematically occurring nontrivial factorizations of f_N.

Definition 1.1. A pair (c, d) of polynomials $c, d \in \mathbb{Z}[x]$ with $c(0), d(0) \neq 0$ is *Capellian* when $-d(x)/c(x^{-1})$ is a pth power in $\mathbb{Q}(x)$ for some prime p or $d(x)/c(x^{-1})$ is 4 times a fourth power in $\mathbb{Q}(x)$.

The name honors Alfredo Capelli, who showed that for a in a field K, the polynomials $x^N - a$ are irreducible in $K[x]$ for all N if and only if a is not a pth power for some prime p or -4 times a fourth power in K; see [Cap01]. So when (c, d) is Capellian (and only then), we get factorizations of f_N coming from factorizations of $y^n + d(x)/c(x^{-1})$. We will restrict to non-Capellian pairs (c, d) in the following, but we note that the results below continue to hold when (c, d) is Capellian and N is not a multiple of p (when $-d(x)/c(x^{-1})$ is a pth power) or 4 (when $d(x)/c(x^{-1})$ is 4 times a fourth power).

The main general result is a consequence of work by Schinzel.

Theorem 1.2 (Schinzel)**.** *Let* $c, d \in \mathbb{Z}[x]$ *with* $c(0), d(0) \neq 0$*. Assume that* $\gcd_{\mathbb{Z}[x]}(\tilde{c}, d) = 1$*, that* $c \neq \pm d$ *and that* (c, d) *is not Capellian. Then there is a bound* N_0 *depending only on* c *and* d *such that for* $N > N_0$*, the non-reciprocal part of* f_N *is irreducible.*

Proof. This can be deduced from Theorem 74 in [Sch00]; see also [Sch69, Theorem 2], where the result is stated over $\mathbb{Q}$ and explicit bounds are given. Let

$$F(x_1, x_2) = x_2\tilde{c}(x_1) + d(x_1); \quad \text{then} \quad F(x, x^{N-\deg c}) = f_N(x).$$

Since (c, d) is non-Capellian, we deduce that $F(y_1^{m_{11}}y_2^{m_{21}}, y_1^{m_{12}}y_2^{m_{22}})$ is irreducible for any matrix $M = (m_{ij}) \in \mathbb{Z}^{2\times 2}$ of rank 2 and such that $(1, n)$ is an integral linear combination of the rows of M, for some n. This is a fairly easy consequence of Capelli's Theorem [Cap01].

Schinzel's theorem tells us that for some $1 \leq r \leq 2$, there is a matrix $M = (m_{ij}) \in \mathbb{Z}^{r\times 2}$ of rank r such that $(1, N - \deg c)$ is an integral linear combination of the rows of M and such that the entries of M are bounded by a constant C only depending on F. When $r = 1$, then up to a sign, $M = (1\ N - \deg c)$, so $N \leq \deg c + C$. When $r = 2$, then

$$\tilde{F}(y_1, y_2) = F(y_1^{m_{11}}y_2^{m_{21}}, y_1^{m_{12}}y_2^{m_{22}})$$

is irreducible by the above. Our assumptions on c and d imply that f_N is not reciprocal, which implies that $L\tilde{F} = \tilde{F}$ in the notation of [Sch69]. Then Schinzel's theorem says that the factorization of the non-reciprocal part Lf_N of f_N corresponds to the factorization of $L\tilde{F} = \tilde{F}$. But the latter is irreducible, hence the non-reciprocal part of f_N is irreducible as well. So the claim holds with $N_0 = \deg c + C$, and C depends only on F, which in turn depends only on c and d. □

For a polynomial $f \in \mathbb{Z}[x]$, we define its *weight* $\|f\|$ to be the squared Euclidean length of its coefficient vector (i.e., the sum of the squares of the coefficients). The explicit bounds given in [Sch69] then amount to

$$N_0 \leq \deg c + \exp\left(\tfrac{5}{16} \cdot 2^{(\|c\|+\|d\|)^2}\right)(2 + \max\{2, (\deg c)^2, (\deg d)^2\})^{\|c\|+\|d\|}.$$

Now consider a reciprocal irreducible factor h of f_N. Then $h = \pm\tilde{h}$ also divides $\tilde{f}_N$, so h divides $\gcd(f_N, \tilde{f}_N)$, which in turn divides

$$x^{\deg c}\tilde{d}(x)f_N(x) - x^{\deg d}\tilde{c}(x)\tilde{f}_N(x) = x^{\deg c}d(x)\tilde{d}(x) - x^{\deg d}c(x)\tilde{c}(x) = x^n r(x)\,,$$

where $n \in \mathbb{Z}_{\geq 0}$ and $r \in \mathbb{Z}[x]$ are such that $r(0) \neq 0$. Since $f_N(0) \neq 0$, it follows that h divides r, and the assumptions $\gcd_{\mathbb{Z}[x]}(\tilde{c}, d) = 1$ and $c \neq \pm d$ guarantee that $r \neq 0$. So any reciprocal irreducible factor h of f_N divides the fixed polynomial r of degree at most $2m$, where $m = \max\{\deg c, \deg d\}$. By Lemma 2.1 below, it follows that h must be a cyclotomic polynomial when

$$N > N_1 = \deg c + \deg d + \begin{cases} \dfrac{2m}{\log\theta}\log(\|c\| + \|d\|) & \text{if } m \leq 27, \\ m(\log 6m)^3 \log(\|c\| + \|d\|) & \text{otherwise,} \end{cases}$$

where Lehmer's constant $\theta \approx 1.17628$ is defined in Section 2. This leads to the following.

Corollary 1.3. *Under the assumptions of Theorem 1.2, if* $N > \max\{N_0, N_1\}$*, then the non-cyclotomic part of* f_N *is irreducible.*

By the above, every cyclotomic divisor of f_N must divide r, which leads to a finite set of possible cyclotomic divisors. If a cyclotomic polynomial Φ_n divides f_N for some N, then it clearly divides $f_{N'}$ if and only if $N' \equiv N \bmod n$. So each cyclotomic polynomial that occurs as a factor of some f_N does so exactly for N in some arithmetic progression. Whence:

Corollary 1.4. *Under the assumptions of Theorem 1.2, the set of* $N > \deg c + \deg d$ *such the polynomial* f_N *is irreducible is the complement of the union of a finite set with a finite union of arithmetic progressions. Both the finite set and the finite union of arithmetic progressions can be determined effectively.*

Proof. The first statement is clear from the discussion above. It remains to prove effectivity. Given c and d, we compute r and find all cyclotomic polynomials Φ_n dividing r. For each such Φ_n, we check if Φ_n divides f_N for a complete set of representatives $N > \deg c + \deg d$ of the residue classes mod n. If it does, then it does so for precisely one representative, which gives rise to one of the arithmetic progressions. Otherwise there is no arithmetic progression coming from Φ_n. We obtain the finite set by checking the irreducibility of f_N for all $\deg c + \deg d < N \leq \max\{N_0, N_1\}$ by standard algorithms. Note that there is an explicit and hence effective bound on $\max\{N_0, N_1\}$. □

There are examples where the finite union of residue classes is all of $\mathbb{Z}_{>\deg c+\deg d}$, but without a single cyclotomic polynomial dividing all f_N (as is the case for $x^N - 2x + 1$). The following example is due to Schinzel [Sch00, Remark 3 in Section 6.4]. Take

$$c = 12\,, \qquad d = 3x^9 + 8x^8 + 6x^7 + 9x^6 + 8x^4 + 3x^3 + 6x + 5\,.$$

We have the cyclotomic factors

$$\begin{aligned} 1+x & \quad \text{if } N \equiv 1 \bmod 2, \\ 1+x+x^2 & \quad \text{if } N \equiv 2 \bmod 3, \\ 1+x^2 & \quad \text{if } N \equiv 2 \bmod 4, \\ 1-x+x^2 & \quad \text{if } N \equiv 4 \bmod 6 \quad \text{and} \\ 1-x^2+x^4 & \quad \text{if } N \equiv 0 \bmod 12; \end{aligned}$$

the remaining part of f_N is irreducible for all $N > 9$ as can be shown by our algorithm.

Of course, the explicit bound given by Schinzel is much too large to make this procedure practical even for c and d of very small degree and weight. There are results that improve on this bound, the best of which seems to be the following; see [FFK00].

Theorem 1.5 (Filaseta, Ford, Konyagin)**.** *In Theorem 1.2, we can take*

$$N_0 \le N_{FFK} = \deg c + 2\max\{5^{4w-15}, \max\{\deg c, \deg d\}(5^{2w-8}+\tfrac{1}{4})\},$$

where $w = \|c\| + \|d\| + t$ *and* t *is the number of terms in* c *and* d*.*

In [DFV13] a similar result is shown for the non-cyclotomic part of f_N, but their bound B_2 is much larger than our N_1.

Our main contribution is the following.

Theorem 1.6. *Let* $c, d \in \mathbb{Z}[x]$ *with* $c(0), d(0) \neq 0$*. We assume that* $\gcd_{\mathbb{Z}[x]}(\tilde{c}, d) = 1$*, that* $c \neq \pm d$ *and that* (c, d) *is robust in the sense of Definition 4.2. Then we can take*

$$N_0 \le (1 + \deg c + \deg d)2^{\|c\|+\|d\|}$$

in Theorem 1.2 and in Corollary 1.3.

The main disadvantage of our result compared to Theorem 1.5 is the additional condition that (c, d) is robust. It is satisfied in many cases of interest (for example, when $c = 1$ and d is irreducible and primitive in the sense that the gcd of its coefficients is 1), but not always. There are some advantages that make up for this, though:

1. Our bound for N_0 is considerably smaller than N_{FFK}.
2. We describe an algorithm that computes a suitable N_0 for any given robust pair (c, d); this bound is usually much smaller than $(1 + \deg c + \deg d)2^{\|c\|+\|d\|}$. In Section 5, we present some evidence indicating that the worst-case growth of the bound obtained by our algorithm should be quadratic instead of exponential in $\|c\| + \|d\|$.
3. When the degrees and weights of c and d are reasonably small, our algorithm is entirely practical and can be used to produce the complete list of irreducible factors of f_N of degree $\le N/2$ (the degree will in fact be uniformly bounded) for all $N > \deg c + \deg d$. See Section 7 for examples.

We remark that for polynomials c, d with coefficients in $\{0, 1\}$, even stronger results can be shown; see [FM04], where a result similar to Theorem 1.2 is obtained with a bound that is linear in $\max\{\deg c, \deg d\}$. Even assuming that (c, d) is robust (which is not always

the case), examples show that we cannot hope for better than quadratic bounds with our method.

Considering the various upper bounds on N_0, we may wonder what the optimal bound might be. Let us define $N_{\mathrm{opt}}(\delta, w)$ to be the smallest value of N_0 such that the statement of Theorem 1.2 holds for all c, d with $\deg c + \deg d = \delta$ and $\|c\| + \|d\| \le w$. Note that $N_{\mathrm{opt}}(\delta, w)$ is well-defined, since there are only finitely many such pairs (c, d). Since a factorization of f_N leads to an analogous factorization of $f_N(x^k)$ for any $k \ge 1$, we see that $N_{\mathrm{opt}}(k\delta, w) \ge kN_{\mathrm{opt}}(\delta, w)$. To get a lower bound on $N_{\mathrm{opt}}(\delta, w)$, we can fix an irreducible polynomial p and try to find c, d such that p divides f_N for large N. For example, defining the Fibonacci numbers as usual by $F_0 = 0$, $F_1 = 1$, $F_{n+1} = F_n + F_{n-1}$, we see easily that

$$x^2 - x - 1 \quad \text{divides} \quad x^N - F_N x - F_{N-1}\,,$$

which implies that

$$N_{\mathrm{opt}}(\delta, w) \ge \frac{\delta \log w}{2 \log \phi}\,,$$

where $\phi = (1 + \sqrt{5})/2$ is the golden ratio. As long as $\deg p \le \delta + 1$, we can always write α^N as $-d(\alpha)$ with $\deg d \le \delta$, where α is a root of p, which gives that p divides $x^N + d(x)$. By Lemma 2.1, this will give a lower bound on $N_{\mathrm{opt}}(\delta, w)$ that cannot be larger than

$$\delta + \frac{\delta + 1}{\log \theta} \log w\,,$$

assuming that Lehmer's constant is the optimal lower bound for $M(p)$. (Asymptotically, we can replace $\log w$ by $\frac{1}{2} \log w$; this comes from using the better estimate

$$\max\{s(c), s(d)\} \le \sqrt{\max\{\deg c, \deg d\}}\sqrt{\|c\| + \|d\|}$$

in the proof of Lemma 2.1.)

So if we want to show that $N_{\mathrm{opt}}(\delta, w)$ grows faster than $\delta \log w$, then we have to work with polynomials p such that $(\deg p)/(\log M(p))$ grows faster than δ. But as soon as the difference between $\deg p$ and δ is large, the coefficients of p must satisfy many algebraic equations of a degree that grows linearly with N in order to have a pair (c, d) such that p divides f_N. This appears difficult to accomplish in a systematic way. So we would like to propose the following questions as a motivation for further study.

Question 1.7. Fix $\delta > 1$. Is $\dfrac{N_{\mathrm{opt}}(\delta, w)}{\log w}$ bounded?

Question 1.8. Is perhaps even $\dfrac{N_{\mathrm{opt}}(\delta, w)}{\delta \log w}$ bounded?

One possibly interesting data point is $N_{\mathrm{opt}}(1, 26) \ge 14$, coming from

$$x^{14} + 4x + 3 = (x + 1)(x^3 - x^2 + 1)(x^{10} + x^8 - x^7 - 2x^5 - x^3 + 2x^2 + x + 3)\,.$$

The key idea of our approach for proving Theorem 1.6 is based on a neat trick due to Ljunggren [Lju60] (see also [Pra04, Section 2.3]), which can be used to show (for example) that $x^n - x - 1$ is irreducible for all n. After proving the lemma that provides the bound N_1 for Corollary 1.3 in Section 2, we recall Ljunggren's approach in Section 3 and then develop

our generalization in Section 4. In Section 5, we discuss the growth of a quantity m_0 that depends on c and d; this quantity enters into the bound N_0 in Theorem 1.6. In Section 6, we describe an improvement of the algorithm used in determining m_0. We end with a collection of sample applications in Section 7. For example, we answer the following question that was asked on *MathOverflow* [MO] and was a motivation for this work:

$$\textit{Are the polynomials } x^{2k+1} - 7x^2 + 1 \textit{ irreducible over } \mathbb{Q}?$$

For some families of pairs (c, d), we can use our algorithm to produce a uniformly small bound N_0. This leads to a complete analysis of the factorization patterns of polynomials of the form $x^N + kx^{N-1} \pm (lx + 1)$, where k and l are distinct integers.

We would like to thank Michael Filaseta for some useful comments on an earlier version of this paper and Umberto Zannier for a very helpful discussion of Schinzel's contributions and relations with unlikely intersections.

2 An application of heights

In this section, we provide the result necessary to obtain the bound N_1 in Corollary 1.3. This is also relevant for the discussion of lower bounds on N_0.

For a polynomial

$$f(x) = c \prod_{j=1}^{n} (x - \alpha_j) \in \mathbb{C}[x]\,,$$

its *Mahler measure* is defined to be

$$M(f) = |c| \prod_{j=1}^{n} \max\{1, |\alpha_j|\};$$

see for example [Sch00, Section 3.4]. If $f \in \mathbb{Z}[x]$, then $M(f) \geq 1$, and it is a known fact that $M(f) = 1$ if and only if f is (up to a sign) a product of a power of x and cyclotomic polynomials. It is an open question ("Lehmer's problem") whether there is a lower bound > 1 for $M(f)$ when f is not of this form. The record polynomial in this respect was already found by Lehmer; it is

$$x^{10} + x^9 - x^7 - x^6 - x^5 - x^4 - x^3 + x + 1\,,$$

and its Mahler measure is *Lehmer's constant* $\theta \approx 1.17628$ (which is its unique real root > 1). By [MRW08], the smallest Mahler measure of a non-cyclotomic polynomial of degree up to 54 is indeed θ. In general, the best currently known explicit bound seems to be due to Voutier [Vou96]; a slightly less good, but simpler variant is the estimate (Corollary 2 in [Vou96])

$$\log M(p) > \frac{2}{(\log(3 \deg p))^3}$$

for $p \in \mathbb{Z}[x]$ irreducible with $M(p) > 1$. If p is non-reciprocal, then we have the stronger (and optimal) bound

$$M(p) \geq \theta_0\,,$$

where $\theta_0 \approx 1.3247$ is the unique real root and also the Mahler measure of $x^3 - x - 1$; this result is due to Smyth [Smy71] (see also [Sch00, Corollary 5 in Section 6.1]).

The *absolute logarithmic Weil height* of an algebraic number α can be defined as

$$h(\alpha) = \frac{\log M(p_\alpha)}{\deg p_\alpha},$$

where $p_\alpha \in \mathbb{Z}[x]$ is the minimal polynomial of α over $\mathbb{Q}$ scaled so that its coefficients are coprime integers. We will simply call $h(\alpha)$ the *height* of α. There is an alternative definition of $h(\alpha)$ in terms of a complete system of absolute values on any finite extension of $\mathbb{Q}$ containing α, from which one can easily deduce the following properties.

(1) For $N \in \mathbb{Z}$ and $\alpha \in \bar{\mathbb{Q}}$, we have that $h(\alpha^N) = |N|\, h(\alpha)$.
(2) For $p, q \in \mathbb{Z}[x]$ and $\alpha \in \bar{\mathbb{Q}}$, we have that

$$h\Big(\frac{p(\alpha)}{q(\alpha)}\Big) \le \log \max\{s(p), s(q)\} + \max\{\deg p, \deg q\}\, h(\alpha).$$

Here $s(f)$ is the sum of the absolute values of the coefficients of f.

See for example [HS00, Part B].

Lemma 2.1. *Let $p \in \mathbb{Z}[x]$ be irreducible, non-constant and non-cyclotomic. If $\gcd(\tilde{c}, d) = 1$ and p divides f_N, then*

$$N \le \deg c + \deg d + \frac{\deg p}{\log M(p)} \log(\|c\| + \|d\|).$$

This implies that

$$N \le \deg c + \deg d + \begin{cases} \dfrac{\deg p}{\log \theta_0} \log(\|c\| + \|d\|) & \text{if } p \text{ is non-reciprocal,} \\ \dfrac{\deg p}{\log \theta} \log(\|c\| + \|d\|) & \text{if } \deg p \le 54, \\ \frac{1}{2}(\deg p)(\log(3 \deg p))^3 \log(\|c\| + \|d\|) & \text{otherwise.} \end{cases}$$

Proof. We can assume that p is primitive (i.e., the gcd of its coefficients is 1). Let $\alpha \in \bar{\mathbb{Q}}$ be a root of p. The condition $\gcd(\tilde{c}, d) = 1$ implies that when p divides f_N, then p does not divide $\tilde{c}$. So if p divides f_N, then $f_N(\alpha) = 0$ and $\alpha \ne 0$, $c(\alpha^{-1}) \ne 0$, which implies that $\alpha^N = -d(\alpha)/c(\alpha^{-1})$. Since p is not cyclotomic and $\alpha \ne 0$, we have that $h(\alpha) > 0$. From the two properties of the height stated above, we deduce that

$$\begin{aligned} N h(\alpha) = h(\alpha^N) &= h\Big(\frac{-d(\alpha)}{c(\alpha^{-1})}\Big) = h\Big(\frac{-\alpha^{\deg c} d(\alpha)}{\tilde{c}(\alpha)}\Big) \\ &\le (\deg c + \deg d) h(\alpha) + \log \max\{s(c), s(d)\} \\ &\le (\deg c + \deg d) h(\alpha) + \log(\|c\| + \|d\|). \end{aligned}$$

Using that $h(\alpha) = (\log M(p))/(\deg p)$, this gives the first result. The remaining estimates follow from this and the lower bounds on $M(p)$ mentioned above. □

Assume that $N > N_1$. Then by Corollary 1.3, a non-cyclotomic irreducible factor $p \in \mathbb{Z}[x]$ of f_N must also be non-reciprocal. By [Smy71], we have $M(p) \geq \theta_0$. The multiplicativity of the Mahler measure and Landau's inequality $M(f) \leq \sqrt{\|f\|}$ (see [HS00, Lemma B.7.3.1 (iii)]) then give that

$$\theta_0^n \leq M(f_N) \leq \sqrt{\|c\| + \|d\|}\,,$$

where n is the number of non-cyclotomic irreducible factors of f_N. This shows that

$$n \leq \frac{\log(\|c\| + \|d\|)}{2\log\theta_0}\,.$$

3 Ljunggren's trick

As a motivation for our approach, we recall how Ljunggren deals with the polynomials $x^n + \varepsilon x + \varepsilon'$ with $\varepsilon, \varepsilon' \in \{\pm 1\}$. (Actually, he considers general trinomials $x^n \pm x^m \pm 1$ and also quadrinomials, but for our expository purposes, the special case is sufficient. The result for $m = 1$ was obtained earlier by Selmer [Sel56], but with a different method.)

Let $R = \mathbb{Z}[x, x^{-1}]$ be the ring of Laurent polynomials with integral coefficients. We note that its unit group is $R^\times = \{\pm x^n : n \in \mathbb{Z}\}$, and we write $f \sim g$ when $f, g \in R$ are equal up to multiplication by a unit. Note that $f \sim g$ implies that $f(x)f(x^{-1}) = g(x)g(x^{-1})$. We will also make use of the fact that $\|f\|$ is the coefficient of x^0 in $f(x)f(x^{-1})$.

Let now $f_N(x) = x^N + \varepsilon x + \varepsilon'$ for some $N \geq 2$; then $\|f_N\| = 3$. Assume that f_N factors as $f_N(x) = g(x)h(x)$ with $g, h \in \mathbb{Z}[x]$ non-constant. Set $G(x) := g(x)h(x^{-1}) \in R$. We obviously have that

$$f_N(x)f_N(x^{-1}) = G(x)G(x^{-1})\,; \tag{3.1}$$

in particular, $\|G\| = \|f_N\| = 3$. So we can write $G(x) \sim x^m + \eta x^k + \eta'$ with $\eta, \eta' \in \{\pm 1\}$. Comparing coefficients in (3.1) then shows that $G(x) \sim f_N(x)$ or $G(x) \sim f_N(x^{-1})$. Swapping g and h if necessary, we can assume that $G(x) \sim f_N(x)$; then $h(x) \mid_R G(x^{-1}) \sim f_N(x^{-1})$, which implies that h divides the reversed polynomial $\tilde{f}_N(x) = x^N f_N(x^{-1}) = \varepsilon' x^N + \varepsilon x^{N-1} + 1$ in $\mathbb{Z}[x]$. We obtain that

$$h(x) \mid \varepsilon \tilde{f}_N(x) - \varepsilon\varepsilon' f_N(x) = x(x^{N-2} - \varepsilon')\,.$$

So h divides $\varepsilon' f_N - \varepsilon' x^2(x^{N-2} - \varepsilon') = x^2 + \varepsilon\varepsilon' x + 1$.

There are now two cases:

1. $\varepsilon' = \varepsilon$. Then $h(x) = x^2 + x + 1$. Let ω be a primitive cube root of unity. Then $h \mid f_N$ if and only if $f_N(\omega) = 0$. We have that $f_N(\omega) = \omega^{N \bmod 3} - \varepsilon\omega^2$, which vanishes if and only if $\varepsilon = 1$ and $n \equiv 2 \bmod 3$. We conclude that $x^N - x - 1$ is irreducible for all $N \geq 2$ and that $x^N + x + 1$ is irreducible when $N \not\equiv 2 \bmod 3$, whereas $x^N + x + 1$ splits as $x^2 + x + 1$ times another irreducible factor when $N \equiv 2 \bmod 3$.
2. $\varepsilon' = -\varepsilon$. Then $h(x) = x^2 - x + 1$ has roots $-\omega$, $-\omega^2$, so h divides f_N if and only if $f_N(-\omega) = 0$. In this case, $f_N(-\omega) = (-1)^N\omega^{N \bmod 3} + \varepsilon\omega^2$. So we conclude that $x^N + x - 1$ is irreducible for $N \not\equiv 5 \bmod 6$, whereas $x^N - x + 1$ is irreducible for $N \not\equiv 2 \bmod 6$. When N is in the excluded residue class mod 6, then the polynomial splits as $x^2 - x + 1$ times another irreducible factor.

4 The main result

We will now generalize this approach to families of polynomials "with a large gap": as in Section 1, we fix $c, d \in \mathbb{Z}[x]$ with $c(0), d(0) \neq 0$ and consider the polynomials

$$f_N(x) = x^N c(x^{-1}) + d(x)$$

for $N > \deg c + \deg d$. In the special case considered in Section 3, we had $c = 1$ and $d = \pm x \pm 1$.

The key part of Ljunggren's trick was the implication

$$f_N(x) f_N(x^{-1}) = G(x) G(x^{-1}) \quad \Longrightarrow \quad G(x) \sim f_N(x) \quad \text{or} \quad G(x) \sim f_N(x^{-1}).$$

We now show that for any fixed N, this implication is in fact equivalent to the statement of Theorem 1.2, under suitable assumptions on c and d.

Proposition 4.1. *Let $c, d \in \mathbb{Z}[x]$ with $c(0), d(0) \neq 0$ be such that $c \neq \pm d$. Then for each $N > \deg c + \deg d$, the following two statements are equivalent.*

(1) *If $G \in R$ satisfies $G(x)G(x^{-1}) = f_N(x)f_N(x^{-1})$, then $G(x) \sim f_N(x)$ or $G(x) \sim f_N(x^{-1})$.*
(2) *The non-reciprocal part of f_N is irreducible.*

Proof. We note that the assumptions on c and d imply that f_N is not reciprocal.

We first show that (1) implies (2). Consider a factorization $f_N(x) = g(x)h(x)$. We set $G(x) = g(x)h(x^{-1})$ as in Ljunggren's trick. Then $G(x)G(x^{-1}) = f_N(x)f_N(x^{-1})$, so by (1), we have that $G(x) \sim f_N(x)$ or $G(x) \sim f_N(x^{-1})$. By swapping the roles of g and h if necessary, we can assume that we are in the first case. This implies that $g\tilde{h} = \pm f_N = \pm gh$, so that $\tilde{h} = \pm h$, and h is reciprocal. We have therefore shown that in any factorization of f_N, one factor is reciprocal. Now write $f_N = g_1 \cdots g_m h$, where $g_1, \ldots, g_m$ are the non-reciprocal irreducible factors and h is the product of the reciprocal irreducible factors. Then $m \geq 1$, since f_N is non-reciprocal. If $m = 1$, then g_1 is the non-reciprocal part of f_N and irreducible, so we are done. So assume now that $m \geq 2$. We show that $g_i g_j$ must be reciprocal for all $1 \leq i < j \leq m$. It suffices to do this for $(i, j) = (1, 2)$. Since g_1 is non-reciprocal, in the factorization $f_N = g_1 \cdot (g_2 \cdots g_m h)$, the second factor must be reciprocal. Since g_2 is non-reciprocal, $g_3 \cdots g_m h$ is then also non-reciprocal. So in the factorization $f_N = (g_1 g_2) \cdot (g_3 \cdots g_m h)$, now the first factor must be reciprocal, proving the claim made above. If $m = 2$, this implies that f_N is reciprocal, a contradiction. If $m \geq 3$, then the fact that $g_1 g_2$, $g_2 g_3$ and $g_1 g_3$ are all reciprocal implies that $g_1 = \pm \tilde{g}_2 = \pm g_3 = \pm \tilde{g}_1$ (if h_1, h_2 are irreducible in $\mathbb{Z}[x]$ and non-reciprocal and $h_1 h_2$ is reciprocal, then $h_1 = \pm \tilde{h}_2$), contradicting that g_1 is non-reciprocal. So $m = 1$ is the only possibility.

Now we show the converse. Assume that $G \in R$ satisfies $G(x)G(x^{-1}) = f_N(x)f_N(x^{-1})$. Replacing G by $x^n G(x)$ for a suitable $n \in \mathbb{Z}$, we can assume without loss of generality that $G \in \mathbb{Z}[x]$ and $G(0) \neq 0$. Then $\deg G = N$, and we have that $G(x)\tilde{G}(x) = f_N(x)\tilde{f}_N(x)$. Comparing the factorizations of both sides into irreducibles, we see that there is a factorization $f_N = gh$ such that $G = \pm g\tilde{h}$. Since f_N is not reciprocal, at least one of g and h must be non-reciprocal as well; we can assume that this is g (otherwise we replace G by $\tilde{G}$). Since by (2), the non-reciprocal part of f_N is irreducible, g must contain the unique

non-reciprocal irreducible factor of f_N, hence h is reciprocal. But then $\tilde{h} = \pm h$, and so $G = \pm f_N$. □

The idea is now to obtain a better lower bound for N such that statement (1) above holds, which will then lead to the same better bound in Theorem 1.2. We need a condition on c and d for this to work.

Definition 4.2. A pair (c, d), where $c, d \in \mathbb{Z}[x]$ with $c(0), d(0) \neq 0$, is *weakly robust*, if for each further pair of polynomials $a, b \in \mathbb{Z}[x]$ such that $ab = cd$, it follows that $\|a\| + \|b\| \geq \|c\| + \|d\| - 1$. The pair (c, d) is *robust* if for all (a, b) as above, the additional relation $a(x)a(x^{-1}) + b(x)b(x^{-1}) = c(x)c(x^{-1}) + d(x)d(x^{-1})$ implies that $(a, b) = \pm(c, d)$ or $\pm(d, c)$, and whenever $\|a\|+\|b\| = \|c\|+\|d\|-1$, we have $a+b \neq 0$. (This last condition can be relaxed; compare the proof of Lemma 4.5.)

We note that the relation $a(x)a(x^{-1}) + b(x)b(x^{-1}) = c(x)c(x^{-1}) + d(x)d(x^{-1})$ implies that $\|a\| + \|b\| = \|c\| + \|d\|$; this is simply the equality of the coefficients of x^0 on both sides.

For example, the pair (c, d) is robust when $c = 1$ and d is primitive and irreducible or when c and d are both primitive and irreducible and $\|cd\| \geq \|c\| + \|d\| - 2$.

If $f \in \mathbb{Z}[x]$ and $m \in \mathbb{Z}_{\geq 0}$, we write $f|_m$ for f truncated to degree $< m$ (i.e., $f|_m$ is the remainder when dividing f by x^m).

Lemma 4.3. *Let* $a, b, f \in \mathbb{Z}[x]$ *with* $\deg a, \deg b < 2m$, $\deg f < m$, $f(0) \neq 0$ *and* $(ab)|_{2m} = f$. *Then one of the following is true.*

(1) $ab = f$;
(2) $ab \neq f$, $a|_m \cdot b|_m \neq f$ *and* $\|a|_m\| + \|b|_m\| \leq \|a\| + \|b\| - 1$;
(3) $ab \neq f$, $a|_m \cdot b|_m = f$ *and* $\|a|_m\| + \|b|_m\| \leq \|a\| + \|b\| - 2$.

Proof. We can assume that $ab \neq f$. We write $a = \underline{a} + \overline{a}x^m$, $b = \underline{b} + \overline{b}x^m$, where $\underline{a} = a|_m$ and $\underline{b} = b|_m$. Then

$$ab = \underline{a}\,\underline{b} + (\underline{a}\,\overline{b} + \overline{a}\,\underline{b})x^m + \overline{a}\,\overline{b}x^{2m} \equiv f \bmod x^{2m}\,.$$

If $\underline{a}\,\underline{b} \neq f$, then $\underline{a}\,\overline{b} + \overline{a}\,\underline{b} \neq 0$, so $\overline{a} \neq 0$ or $\overline{b} \neq 0$, which implies that $\|\overline{a}\| + \|\overline{b}\| \geq 1$ and so gives (2). If $\underline{a}\,\underline{b} = f$, then $\underline{a}\,\overline{b} + \overline{a}\,\underline{b} \equiv 0 \bmod x^m$. In this case, $\overline{a} = \overline{b} = 0$ is not possible, since $ab \neq f$. Since $\underline{a}(0), \underline{b}(0) \neq 0$, it then follows that $\overline{a} \neq 0$ and $\overline{b} \neq 0$, which implies that $\|\overline{a}\| + \|\overline{b}\| \geq 2$ and so gives (3). □

Corollary 4.4. *Assume that* (c, d) *is weakly robust. Then there is*

$$m_0 \leq (1 + \deg c + \deg d)2^{\|c\|+\|d\|-1}$$

such that for all $m > m_0$, *if* $a, b \in \mathbb{Z}[x]$ *with* $\deg a, \deg b < m$ *satisfy* $(ab)|_m = cd$, *then*

$$ab = cd \qquad \text{or} \qquad \|a\| + \|b\| > \|c\| + \|d\|\,.$$

Proof. Consider $m > (1 + \deg c + \deg d)2^{\|c\|+\|d\|-1}$. Assume there are $a, b \in \mathbb{Z}[x]$ of degree less than m with $(ab)|_m = cd$, but $ab \neq cd$ and $\|a\| + \|b\| \leq \|c\| + \|d\|$. By iteratively applying Lemma 4.3, we either find that $\|a|_{1+\deg c+\deg d}\| + \|b|_{1+\deg c+\deg d}\| \leq 1$, which is absurd, as $a(0), b(0) \neq 0$, or else that there is some $m' < m$ such that $a|_{m'} \cdot b|_{m'} = f$ and $\|a|_{m'}\| + \|b|_{m'}\| \leq \|c\| + \|d\| - 2$, which contradicts the weak robustness of (c, d). □

We note that for any given pair (c, d), we can effectively determine the optimal bound m_0 by successively computing the sets

(4.1)
$$T_m = \{(a, b) \mid a, b \in \mathbb{Z}[x],\ \deg a, \deg b < m,\ ab \equiv cd \bmod x^m,\ \|a\| + \|b\| \leq \|c\| + \|d\|\}$$

for $m = 1, 2, \ldots$, until $ab = cd$ for all $(a, b) \in T_m$. Since forgetting the x^m term gives a natural map $T_{m+1} \to T_m$, it is easy to construct T_{m+1} from T_m. In Section 6, we explain how this approach can be improved to give a more efficient procedure. In Section 5, we discuss the dependence of m_0 on c and d in more detail.

We can now get our better bound for robust pairs.

Lemma 4.5. *Assume that (c, d) is a robust pair. Then statement (1) in Proposition 4.1 holds for all $N > N_0$, where*

$$N_0 \leq (1 + \deg c + \deg d)2^{\|c\|+\|d\|}\,.$$

Proof. As in the proof of Proposition 4.1, we can assume that $G \in \mathbb{Z}[x]$ with $G(0) \neq 0$. Then we can write $G(x) = x^N a(x^{-1}) + b(x)$ with $a, b \in \mathbb{Z}[x]$, $\deg a < \lceil (N+1)/2 \rceil$, $\deg b < \lceil N/2 \rceil$, and we have that

$$\begin{aligned} &c(x)d(x) + x^N\big(c(x)c(x^{-1}) + d(x)d(x^{-1})\big) + x^{2N}c(x^{-1})d(x^{-1}) \\ &\qquad = x^N f_N(x)f_N(x^{-1}) = x^N G(x)G(x^{-1}) \\ &\qquad = a(x)b(x) + x^N\big(a(x)a(x^{-1}) + b(x)b(x^{-1})\big) + x^{2N}a(x^{-1})b(x^{-1})\,. \end{aligned} \tag{4.2}$$

We assume that $\lceil N/2 \rceil > \max\{\deg c, \deg d\}$; this implies that

$$a(x)b(x) \equiv c(x)d(x) \bmod x^{\lceil N/2 \rceil}\,.$$

Now we assume in addition that $\lceil N/2 \rceil > m_0$, where m_0 is as in Corollary 4.4. Note that

$$\|c\| + \|d\| = \|f_N\| = \|G\| = \|a\| + \|b\| \geq \|a|_{\lceil N/2 \rceil}\| + \|b\|\,.$$

By Corollary 4.4, it follows that $a|_{\lceil N/2 \rceil}b = cd$. When N is odd, then $a|_{\lceil N/2 \rceil} = a$, so $ab = cd$. Comparing the expressions in (4.2), we see that we also must have that

$$a(x)a(x^{-1}) + b(x)b(x^{-1}) = c(x)c(x^{-1}) + d(x)d(x^{-1})\,,$$

and so by robustness of (c, d), it follows that $(a, b) = \pm(c, d)$ or $\pm(d, c)$, which is equivalent to $G = \pm f_N$ or $G = \pm\tilde{f}_N$, proving the claim. When N is even, then either $\deg a < N/2$ and we can conclude as for N odd. Or else (again by robustness) $\|a|_{N/2}\| + \|b\| = \|c\| + \|d\| - 1$ and so $a = a|_{N/2} \pm x^{N/2}$. We change notation and write a for what was $a|_{N/2}$, so that now

$$G(x) = x^N a(x^{-1}) \pm x^{N/2} + b(x) \qquad \text{and} \qquad ab = cd\,.$$

In this case, we need to assume that $N/4 > \deg c + \deg d$ (note that this case is only possible when there is a factorization $cd = ab$ with $\|a\| + \|b\| = \|c\| + \|d\| - 1$, which we can check beforehand). Then, comparing the expressions again, we see that $a + b = 0$ (this uses that $\deg a, \deg b \leq \deg a + \deg b = \deg c + \deg d < N/4$), which contradicts robustness. So this case cannot occur. (Comparing the "middle part" of the two polynomials gives the additional relation $2a(x)a(x^{-1}) + 1 = c(x)c(x^{-1}) + d(x)d(x^{-1})$, so it would be sufficient to require that this cannot hold when $cd = -a^2$.)

This shows the claim with

$$N_0 = 2\max\{\deg c, \deg d, m_0\}$$

when there is no pair (a, b) with $ab = cd$ and $\|a\| + \|b\| < \|c\| + \|d\|$, whereas in the other case, we can take

$$N_0 = \max\{4\deg(cd), 2m_0\}.$$

Since $m_0 \leq (1 + \deg c + \deg d)2^{\|c\|+\|d\|-1}$ by Corollary 4.4 and $\|c\| + \|d\| \geq 2$, we can take $N_0 = (1 + \deg c + \deg d)2^{\|c\|+\|d\|}$ in all cases. □

Combining Lemma 4.5 with Proposition 4.1 now immediately gives Theorem 1.6.

We note that we do not use the assumption that (c, d) is non-Capellian in our proof. Since the result excludes the existence of "Capellian" factorizations, this implies that a robust pair (c, d) is necessarily non-Capellian.

Remark 4.6. An alternative proof of Theorem 1.2 via Proposition 4.1 can be obtained from work of Bombieri and Zannier on unlikely intersections. The relevant result can be found in [BMZ07, Theorem 1.6] (or [Sch00, Appendix by Zannier]). Iterating their result (with

$$P(x_1, x_2, x_3, \ldots, x_n) = x_2 c(x_1^{-1}) + d(x_1) \quad \text{and} \quad Q(x_1, x_2, x_3, \ldots, x_n) = a_3x_3 + \ldots + a_nx_n\,,$$

where $(a_3, \ldots, a_n)$ runs through all vectors of nonzero integers of weight at most w; in our case $\zeta_j = 1$ for all j) leads to the following statement.

Let $c, d \in \mathbb{Z}[x]$ with $c(0), d(0) \neq 0$, $\gcd_{\mathbb{Z}[x]}(\tilde{c}, d) = 1$ and (c, d) not Capellian. For any $w > 0$ there is $N_{BZ}(c, d, w)$ with the following property. If $N > N_{BZ}(c, d, w)$ and $g \in R$ has weight $\|g\| \leq w$, then either f_N divides g in R, or else the gcd of f_N and g is a product of cyclotomic polynomials.

From this, it is easy to conclude that statement (1) in Proposition 4.1 holds as soon as $N > N_{BZ}(c, d, \|c\| + \|d\|)$ when c and d satisfy the assumptions in Theorem 1.2. This proves Theorem 1.2 with $N_0 = N_{BZ}(c, d, \|c\| + \|d\|)$. The bound is effective, but is not made explicit in [BMZ07].

5 Growth of m_0

We write $m_0(c, d)$ for the optimal value of m_0 in Corollary 4.4. The bound

$$m_0(c, d) \leq (1 + \deg c + \deg d)2^{\|c\|+\|d\|-1}$$

obtained in Corollary 4.4 is exponential in the weight of c and d. At least in some cases, we can do better.

Lemma 5.1. *Let $k, l \in \mathbb{Z}$ and set $c = 1 + kx$, $d = 1 + lx$. Note that (c, d) is robust.*

(1) *If $|k - l| \geq 6$, then $m_0(1 + kx, 1 + lx) = 2$.*
(2) *If $2 \leq |k - l| \leq 5$ and $\max\{|k|, |l|\} \geq 3$, then $m_0(1 + kx, 1 + lx) = 3$.*
(3) *If $|k - l| \leq 1$, then $m_0(1 + kx, 1 + lx) = 1$.*

The exceptional cases are given by

$$m_0(1, 1 + 2x) = 4\,,\ m_0(1 + x, 1 - x) = 2\,,\ m_0(1 + 2x, 1 - x) = 5\,,\ m_0(1 + 2x, 1 - 2x) = 4\,,$$

together with $m_0(1 + lx, 1 + kx) = m_0(1 + kx, 1 + lx) = m_0(1 - kx, 1 - lx)$.

Proof. We can assume that $k \le l$. We write (without loss of generality)

$$a = 1 + a_1x + a_2x^2 + a_3x^3 + \dots \qquad \text{and} \qquad b = 1 + b_1x + b_2x^2 + b_3x^3 + \dots$$

with $a_1 \le b_1$. The condition $ab \equiv cd \bmod x^m$ is then

$$a_1 + b_1 = k + l\,, \quad a_2 + a_1b_1 + b_2 = kl\,, \quad a_3 + a_2b_1 + a_1b_2 + b_3 = 0\,, \quad \dots\,;$$

we look at the first $m-1$ equations. The condition $\|a\| + \|b\| \le \|c\| + \|d\|$ is

$$a_1^2 + b_1^2 + a_2^2 + b_2^2 + a_3^2 + b_3^2 + \dots \le k^2 + l^2\,.$$

Write $a_1 = k + \alpha$; then $b_1 = l - \alpha$, $\alpha \le (l-k)/2$, and

$$k^2 + l^2 \ge a_1^2 + b_1^2 = k^2 + l^2 - 2\alpha(l - k - \alpha)\,,$$

which implies that $\alpha \ge 0$. If $\alpha = 0$, then $(a, b) = (c, d)$, and we are done. So we now assume that $\alpha \ge 1$. Since $\alpha \le (l-k)/2$, this is not possible when $l - k \le 1$, which proves case (3).

When $m \ge 3$, then the coefficient of x^2 gives us that

$$a_2 + b_2 = kl - a_1b_1 = -\alpha(l - k - \alpha)\,,$$

which implies that

$$k^2 + l^2 - (a_1^2 + b_1^2) = 2\alpha(l - k - \alpha) \ge a_2^2 + b_2^2 \ge \frac{\alpha^2(l - k - \alpha)^2}{2}$$

and therefore that

$$\alpha(l - k - \alpha) \le 4\,.$$

This is impossible when $l - k \ge 6$, which proves case (1).

The remaining cases are

$$(\alpha, l - k) = (1,2)\,,\ (1,3)\,,\ (1,4)\,,\ (1,5)\,,\ (2,4)\,.$$

Then $a_2 + b_2 = -1, -2, -3, -4, -4$, and $\|a_2\| + \|b_2\| \le 2, 4, 6, 8, 8$, respectively. In the cases $(1,5)$ and $(2,4)$, we must have that $a_2 = b_2 = -2$, which implies that $a_3 = b_3 = 0$; this leads to a contradiction for $m \ge 4$ unless $(k, l) = (-2, 2)$. In the case $(1,3)$ with $\{a_2, b_2\} = \{0, -2\}$, we obtain a similar contradiction unless $k \in \{-2, -1\}$. We consider the remaining cases in turn.

- $l = k + 2$, $a_1 = k + 1 = b_1$, $a_2 = -1$, $b_2 = 0$.
  This gives that $\|a_3\| + \|b_3\| \le 1$ and $a_3 + b_3 = k + 1$, which is impossible unless $k \in \{-2, -1, 0\}$.
- $l = k + 3$, $a_1 = k + 1$, $b_1 = k + 2$, $a_2 = b_2 = -1$.
  This gives that $\|a_3\| + \|b_3\| \le 2$ and $a_3 + b_3 = 2k + 3$, which is impossible unless $k \in \{-2, -1\}$.
- $l = k + 4$, $a_1 = k + 1$, $b_1 = k + 3$, $\{a_2, b_2\} = \{-1, -2\}$.
  This gives that $\|a_3\| + \|b_3\| \le 1$ and $a_3 + b_3 = 3k + 5$ or $3k + 7$, which is impossible unless $k = -2$.

This proves case (2). The exceptional values can be determined by the algorithm sketched after the proof of Corollary 4.4. □

We can also deal with $(c,d) = (1+kx, l)$. Such a pair (with $|l| > 1$ and $k \neq 0$; note that $|l| = 1$ is covered by Lemma 5.1) is robust if and only if $|k| \geq |l|/p$, where p is the smallest prime divisor of l. We give a result for slightly larger $|k|$. Note that by changing the sign of x or of $d = l$, we can assume without loss of generality that $k, l > 0$.

Lemma 5.2. *Let $l \geq 5$; let $k \geq 1$ if l is prime and $k > \sqrt{p^2 + l^2/p^2}$ otherwise, where p is the smallest prime divisor of l. If $k \leq l^2/2$, then $m_0(1+kx, l) = 1$.*

Proof. We have to show that the only pair of polynomials $a = a_0 + a_1 x$, $b = b_0 + b_1 x$ such that $1 \leq a_0 \leq b_0$, $\|a\| + \|b\| \leq 1 + k^2 + l^2$ and $ab \equiv l + klx \bmod x^2$ is $(a,b) = (1+kx, l)$. The last condition is equivalent to the pair of equations

$$a_0 b_0 = l \qquad \text{and} \qquad a_0 b_1 + a_1 b_0 = kl\,.$$

If $a_0 = 1$ and therefore $b_0 = l$, then we have to solve $b_1 + la_1 = kl$ under the condition that $a_1^2 + b_1^2 \leq k^2$. The equation implies that l divides b_1. Writing $b_1 = l\beta$, we have that $a_1 = k - \beta$ and $(k-\beta)^2 + l^2\beta^2 \leq k^2 \leq (l+1)^2$. Since $l \geq 5$, $4l^2 > (l+1)^2$, which implies that $\beta \in \{-1, 0, 1\}$. If $\beta = 0$, then $(a,b) = (1+kx, l)$ as desired. In the other cases, we obtain that $l^2 \leq 2k - 1 \leq l^2 - 1$, a contradiction. If l is prime, then $(1, l)$ is the only possibility for (a_0, b_0), so in this case, we are done.

Now assume that $1 < a_0 \leq b_0$; then $a_0 \geq p$. It is easy to see (using the Cauchy-Schwarz inequality, for example) that $a_0 b_1 + a_1 b_0 = kl$ implies that

$$a_1^2 + b_1^2 \geq \frac{k^2 l^2}{a_0^2 + b_0^2}\,.$$

From

$$\frac{k^2 l^2}{a_0^2 + b_0^2} \leq a_1^2 + b_1^2 \leq 1 + k^2 + l^2 - (a_0^2 + b_0^2)$$

we conclude that

$$k^2 \leq (a_0^2 + b_0^2)\frac{1 + l^2 - (a_0^2 + b_0^2)}{l^2 - (a_0^2 - b_0^2)} = a_0^2 + b_0^2 + \frac{a_0^2 + b_0^2}{l^2 - (a_0^2 + b_0^2)}\,.$$

Since $p \geq 2$, we have that $a_0^2 + b_0^2 \leq 4 + l^2/4$, which together with $l \geq 5$ implies that the last fraction is strictly less than 1. Since k^2 and $a_0^2 + b_0^2$ are both integers, we must have that $k^2 \leq a_0^2 + b_0^2 \leq p^2 + l^2/p^2$, contradicting our assumption on k. So the case under consideration is impossible; this finishes the proof. □

Remark 5.3. For the robust pairs $(1+kx, l)$ with $l > 1$ that are not covered by Lemma 5.2, it appears that $m_0(1+kx, l) \leq 2$, except for $m_0(1+2x, 4) = 4$ and $m_0(1+3x, 9) = 3$. It should be possible to prove this, but the arguments seem to get rather technical.

Remark 5.4. Experiments suggest that better bounds are likely to be true in other cases as well.

(1) For $c = 1$, $d = 1 - kx^2$ with $k \geq 2$ not a square, $m_0(c,d)$ seems to grow at most linearly with k:

k	2	3	5	6	7	8	10	11	12	13	14	15	17	18	19	20	21	22	23	24
m_0	8	11	23	23	20	29	34	37	39	44	46	48	54	69	71	66	66	58	59	76

(2) It looks like $m_0(1, 1+kx^2) = 4$ when $k \geq 6$.

(3) It appears that $m_0(1, 1+kx-kx^2) = k^2 - 2k$ when $k \geq 3$ or $k \leq -5$.

(4) For $c = 1$, $d = 1 + kx^3$, k not a cube, $m_0(c, d)$ appears to grow linearly with k again:

k	1	2	3	4	5	6	7	9	10	11
m_0	3	12	13	14	16	24	26	26	31	35

(5) We have that $m_0(1, 1+2x^k) = 4k$ for all $k \geq 1$. (For comparison, the bound from the proof above is $32(k+1)$.)

(6) It looks like $m_0(1, 1+3x^k) = 3k$ when $3 \nmid k$ (with exceptions for $k = 4$ and $k = 8$) and $m_0(1, 1+3x^k) = 13l$ when $k = 3l$.

(7) It appears that the growth of $m_0(1, 1+kx^k)$ is quadratic in k:

k	1	2	3	4	5	6	7	8
m_0	1	8	13	16	26	48	37	66

Heuristically, we expect that the weight of any pair has to grow after increasing m by a bounded amount, which would translate into a bound that is linear in $\|c\| + \|d\|$. However, it turns out that this is wrong. We define, for $\delta \in \mathbb{Z}_{\geq 1}$ and $\alpha > 0$,

$$\mu_\alpha(\delta) = \limsup_{\|c\|+\|d\| \to \infty} \frac{m_0(c, d)}{\delta(\|c\| + \|d\|)^\alpha},$$

where (c, d) runs over all robust pairs with $\deg(cd) = \delta$. We write $T_m(c, d)$ for the set T_m defined in (4.1) for the pair (c, d).

We note that it is easy to see that $m_0(c(x^n), d(x^n)) \geq n m_0(c, d)$ (if $(a, b) \in T_m(c, d)$, then $(a(x^n), b(x^n)) \in T_{nm}(c(x^n), d(x^n))$), which implies that $\mu_\alpha(n\delta) \geq \mu_\alpha(\delta)$.

Proposition 5.5.

$$\mu_1(1) \geq \frac{1}{2}, \qquad \mu_2(2) \geq \frac{1}{144}, \qquad \mu_2(3) \geq \frac{3}{200}, \qquad \mu_2(4) \geq \frac{25}{1568},$$

and

$$\liminf_{k \to \infty} \mu_2(k) \geq \frac{25}{1568}.$$

Proof. For $\delta = 1$, consider $c = 1$ and $d = (k+1) - kx$ for $k \in \mathbb{Z} \setminus \{-1, 0\}$. Since d is primitive, (c, d) is clearly robust. We have that

$$(a, b) := \left(1 - x, \frac{1 - x^{k^2}}{1 - x} + k\right) \in T_{k^2}\big(1, (k+1) - kx\big)$$

(note that $\|a\| + \|b\| = 2 + (k+1)^2 + k^2 - 1 = 2k^2 + 2k + 2 = \|c\| + \|d\|$), which shows that $m_0(1, d) \geq k^2$. This implies that

$$\mu_1(1) \geq \lim_{|k| \to \infty} \frac{k^2}{1 \cdot (2k^2 + 2k + 2)} = \frac{1}{2}.$$

For $\delta \geq 2$, we consider the following general construction. Take positive integers L, M and N and fix a factorization $1 - x^L = \Phi\Psi$ with $\Phi(0) = \Psi(0) = 1$. We set

$$t = \Phi \frac{1 - x^{LMN}}{1 - x^{LM}} \qquad \text{and} \qquad u = \Psi \frac{1 - x^{LM}}{1 - x^L};$$

then $tu = 1 - x^{LMN} \equiv 1 \bmod x^{LMN}$. We further fix a primitive polynomial $p \in \mathbb{Z}[x]$ such that $\deg(\Phi p) = \delta$. Then for $k \in \mathbb{Z} \setminus \{0\}$,

$$t\big(u + kp(1 - x^{LM})\big) \equiv 1 + kp\Phi \bmod x^{LMN}$$

and

$$\begin{aligned} \|t\| + \|u + kp(1 - x^{LM})\| &= N\|\Phi\| + \|u + kp\| + k^2\|p\| \\ &= N\|\Phi\| + M\|\Psi\| + 2k^2\|p\| + O(k)\,. \end{aligned}$$

Consider $c = 1$ and $d = 1 + kp\Phi$. We note that d is primitive when $k \in g\mathbb{Z}$, where g is the content of $p - p(0)$. We can then choose $k = \ell g$, where ℓ is a prime not dividing the leading coefficient of p; then d is irreducible by the Eisenstein criterion applied to $\tilde{d}$. Also, $\|c\| + \|d\| = \|1\| + \|1 + kp\Phi\| = k^2\|p\Phi\| + O(k)$. So we can choose M and N satisfying

$$N\|\Phi\| + M\|\Psi\| \leq k^2\big(\|p\Phi\| - 2\|p\|\big) - O(k)\,;$$

then $(t, u + kp(1 - x^{LM})) \in T_{LMN}(c, d)$ and $m_0(c, d) \geq LMN$. The maximal value of LMN is obtained when

$$N\|\Phi\| \approx M\|\Psi\| \approx \frac{\|p\Phi\| - 2\|p\|}{2} k^2\,,$$

which gives

$$m_0(c, d) \geq LMN \approx \frac{L\big(\|p\Phi\| - 2\|p\|\big)^2}{4\|\Phi\|\|\Psi\|} k^4$$

and so, letting $|k| \to \infty$ (through values such that d is primitive and irreducible),

$$\mu_2(\delta) \geq \frac{L}{4\delta\|\Phi\|\|\Psi\|}\Big(1 - 2\frac{\|p\|}{\|p\Phi\|}\Big)^2.$$

For $\delta = 2$, we take $\Phi = 1 - x$, $L = 1$, $p = 1 - x$ (or $\Phi = 1 + x + x^2$, $L = 3$, $p = 1$), which gives the bound $1/144$. For $\delta = 3$, we take $\Phi = 1 + x + x^2$, $L = 3$, $p = 1 + x$, which gives the bound $3/200$. For $\delta = 4$, we take $\Phi = 1 + x + x^2 + x^3$, $L = 4$, $p = 1 + x$, which gives the bound $25/1568$.

For $\delta = 4\nu$, we have $\mu_2(\delta) \geq \mu_2(4)$ by the discussion above. For $\delta = 4\nu + j$ with $\nu \geq 1$ and $j \in \{1, 2, 3\}$, we use $\Phi = 1 + x^\nu + x^{2\nu} + x^{3\nu}$, $L = 4\nu$, $p = x^j(1 + x^\nu)$, which gives that $\mu_2(\delta) \geq \frac{4\nu}{4\nu+j}\frac{25}{1568}$; this implies the last claim. □

Remark 5.6. Computations indicate that the pairs (Φ, p) we have chosen in the proof give the optimal limit value for degrees up to 4. Furthermore, it appears that $(1+x+x^2+x^3, 1+x)$ leads to the overall maximal limit value. We have not attempted to prove this, though.

Experimental evidence suggests that in the degree 1 case, the pairs achieving a new maximal m_0 (for all pairs of no larger weight) are indeed of the form given in the proof (starting from weight 86), and the pair (a, b) giving the maximum is also as given in the proof. For degrees 2, 3 and 4, from some point on, the pairs giving large values of m_0 are also of

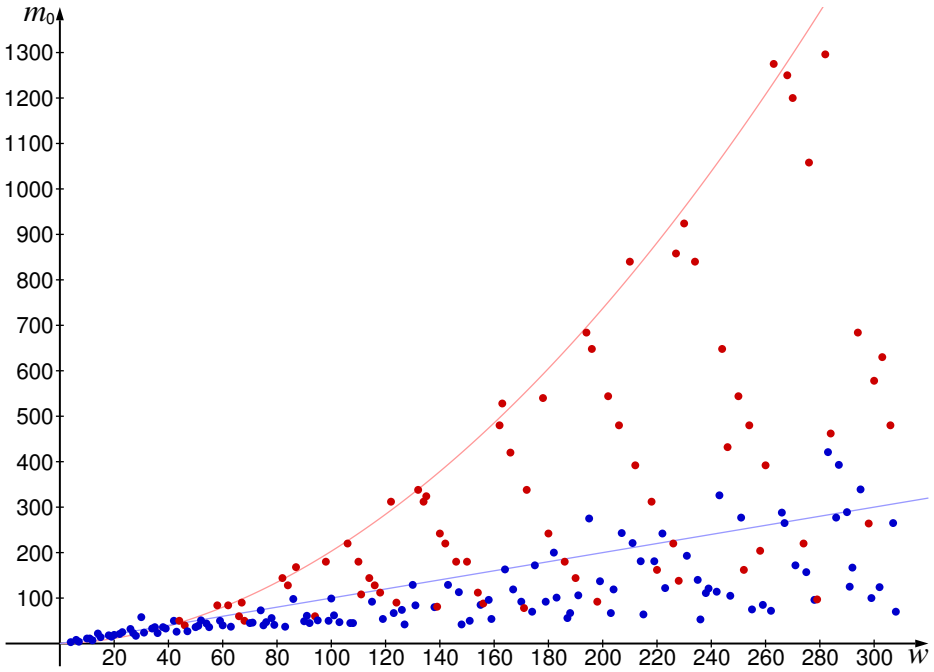

FIGURE 1. Maximal values of $m_0(1,d)$ for robust pairs $(1,d)$ of given weight $\|1\| + \|d\| = w$ and with $\deg d = 2$. Red dots indicate values obtained by pairs covered by the construction in the proof of Proposition 5.5. The red curve is $m_0 = \frac{1}{72}w^2 + \frac{\sqrt{3}}{27}w^{3/2}$, the blue curve is $m_0 = w$.

the same general form as those in the proof above (or slight variations thereof, where u is multiplied by some small degree polynomial q). This is illustrated for degree 2 in Figure 1.

This is a strong indication that the construction in the proof is essentially optimal, which, in conjunction with Remark 5.6, leads us to propose the following conjecture.

Conjecture 5.7.

$$\mu_1(1) = \frac{1}{2}, \qquad \mu_2(2) = \frac{1}{144}, \qquad \mu_2(3) = \frac{3}{200}, \qquad \mu_2(4) = \frac{25}{1568},$$

and

$$\lim_{k\to\infty} \mu_2(k) = \frac{25}{1568}.$$

This would imply that for any fixed degree δ, there is a constant C_δ such that for all robust pairs (c,d) with $\deg(cd) = \delta$, we have the following upper bound:

$$m_0(c,d) \le C_\delta(\|c\| + \|d\|)^2.$$

It appears likely that this can be strengthened to

$$m_0(c,d) \le C(\deg c + \deg d)(\|c\| + \|d\|)^2$$

with a constant C. Feeding this into the proof of Theorem 1.6, this would imply that we can improve the bound for N_0 to

$$N_0 \le (\deg c + \deg d)\max\{4, 2C(\|c\| + \|d\|)^2\}.$$

6 An improvement of the algorithm determining m_0

When $\|c\| + \|d\|$ is not very small, the sets T_m defined in (4.1) can get rather large, which makes the algorithm sketched after the proof of Corollary 4.4 rather slow. Here we describe how we can reduce the size of the sets we have to consider, which gives a more efficient algorithm.

In a first step, we determine a lower bound μ on m_0 by reducing the sets T_m to the (say) 1000 pairs (a, b) with smallest weight $\|a\| + \|b\|$ (if $\#T_m > 1000$) before computing T_{m+1} from T_m. The heuristic here is that the pairs of smallest weight have the best chance of producing a pair for large m.

The second step is then to construct the sets T_m successively as in the original algorithm, but to prune them of as many pairs as possible without changing the final result, with the goal to keep the sets small. We can remove a pair (a, b) from T_m when $m > \deg(cd)$ and we can show that any extension $(a + a_1x^m, b + b_1x^m)$ with

$$\deg a_1, \deg b_1 < m_1 = \min\{m, \mu - m\} \quad \text{and} \quad (a + a_1x^m)(b + b_1x^m) \equiv cd \bmod x^{m+m_1}$$

would have $\|a\| + \|a_1\| + \|b\| + \|b_1\| > \|c\| + \|d\|$. We can get a lower bound for $\|a_1\| + \|b_1\|$ if we allow real instead of integral coefficients. Writing $ab = cd + hx^m$, we have to solve the following linear system in the coefficients of a_1 and b_1:

$$ba_1 + ab_1 \equiv -h \bmod x^{m_1}.$$

If M is the matrix such that this system is $(a_1, b_1)M = -h$ (where we identify a_1, b_1 and h with their coefficient vectors), then the minimum is given by the squared Euclidean length η of hM^+, where $M^+ = (M^\top M)^{-1}M^\top$ is the pseudoinverse of M. So we compute η, and if $\eta > \|c\| + \|d\| - (\|a\| + \|b\|)$, then we know that (a, b) does not have any descendents in T_{m+m_1} and so will not lead to a better lower bound on m_0 than μ. We can therefore discard (a, b) in this case. This leads to considerably smaller sets T_m than before.

An alternative approach (that has the advantage of requiring only a modest amount of memory) is to use a best-first search that at each level always expands the pair (a, b) of smallest weight that has not yet been considered. As soon as we find a terminal node, i.e., a pair (a, b) with $ab \neq cd$ that cannot be extended further, we have a lower bound for m_0, which we can use to prune the search tree as described above. When we find another terminal node at a higher level m, then we update the lower bound.

7 Some examples

We present some applications of our algorithm. We begin with a generalization of the family that figured in the MO question mentioned in the introduction. In the following, $r \in \mathbb{Z}[x]$ is the polynomial defined in Section 1; recall that it has the property that any reciprocal factor of f_N divides r.

Example 7.1. Let k be an integer with $|k| \geq 3$. Then there is an integer $N_k \geq 2$ such that for all $N > N_k$, the polynomial $x^N - kx^2 + 1$ is irreducible over $\mathbb{Q}$.

This follows by taking $c(x) = 1$ and $d(x) = 1 - kx^2$ in Corollary 1.3. Note that here $r = k(x^4 - kx^2 + 1)$, so (since $|k| > 2$) r has no cyclotomic factors, implying that the non-cyclotomic part of f_N is f_N itself.

If in addition, k is not a square, then d is irreducible, so (c, d) is robust, and our Theorem 1.6 applies. For the original question with $k = 7$, we find that $m_0(1, 1 - 7x^2) = 20$ (see Remark 5.4), so we can take $N_7 = 40$. Checking smaller N separately, we find that $x^N - 7x^2 + 1$ is irreducible for all $N \geq 5$ and for $N = 3$, whereas

$$x^4 - 7x^2 + 1 = (x^2 - 3x + 1)(x^2 + 3x + 1)\,.$$

We similarly find that $x^N - kx^2 + 1$ is irreducible for $N \geq 5$ when $3 \leq k \leq 24$ (and k is not a square). Our implementation of the procedure that determines m_0 gets quite slow beyond that point, but it is certainly tempting to conjecture that the statement remains true for larger k.

We remark that for $k \leq -3$, we can easily show that the polynomial is irreducible for all $N \geq 3$: Comparing the polynomial with its dominant term and using Rouché's theorem, we see that it has exactly two roots of absolute value < 1 (and none of absolute value 1), which are complex conjugate, so would have to be roots of the same irreducible factor. But then any other factor would have all its roots of absolute value strictly larger than 1, which is impossible. (This is a variant of Perron's criterion; see Example 7.3 below.)

Note that for $0 < |k| \leq 2$, we do indeed get arithmetic progressions of N such that $x^N - kx^2 + 1$ is reducible: $N \equiv 4 \bmod 12$ for $k = 1$, $N \equiv 1 \bmod 3$ for $k = -1$, everything for $k = 2$, and $N \equiv 0 \bmod 4$ for $k = -2$.

Example 7.2. We can also deal with $x^N - 4x^2 + 1$, even though the pair $(1, 1 - 4x^2)$ is *not* robust. In this case, it is not hard to show that (up to a common sign change and order) for $m > 12$, the set T_m defined after the proof of Corollary 4.4 consists of the pairs

$$(1, 1 - 4x^2)\,, \qquad (1 + 2x, 1 - 2x)\,,$$
$$(1 + 2x + x^{m-1}, 1 - 2x - x^{m-1})\,, \qquad (1 + 2x - x^{m-1}, 1 - 2x + x^{m-1})\,,$$
$$(1 + 2x + 2x^{m-1}, 1 - 2x - 2x^{m-1}) \quad \text{and} \quad (1 + 2x - 2x^{m-1}, 1 - 2x + 2x^{m-1})\,.$$

Assume we are given G with $G(x)G(x^{-1}) \sim f_N(x)f_N(x^{-1})$; write $G \sim x^N a(x^{-1}) + b(x)$ as before. If N is odd (and large), then $(a, b) \in T_{(N+1)/2}$ and $\|a\| + \|b\| = \|f_N\| = 18$. This forces (up to sign and order)

$$(a, b) = (1, 1 - 4x^2) \qquad \text{or} \qquad (a, b) = (1 + 2x \pm 2x^{(N-1)/2}, 1 - 2x \mp 2x^{(N-1)/2})\,.$$

In the first case, $G \sim f_N$. In the second case, we easily see that $G(x)G(x^{-1}) \not\sim f_N(x)f_N(x^{-1})$, for example by comparing coefficients of $x^{(N-1)/2}$. If N is even, then (up to sign and replacing by the reversed polynomial) $G(x) = x^N a(x^{-1}) + \gamma x^{N/2} + b(x)$ with $(a, b) \in T_{N/2}$ satisfying $\|a\| + \|b\| + \gamma^2 = 18$. This rules out

$$(a, b) = (1 + 2x, 1 - 2x) \qquad \text{and} \qquad (a, b) = (1 + 2x \pm x^{N/2-1}, 1 - 2x \mp x^{N/2-1})\,,$$

since γ^2 would have to be 8 or 6. Then $\gamma = 0$, and we have essentially the same two cases as for odd N, with the slight difference that $G(x) = x^N + 2x^{N-1} \pm 2x^{N/2+1} \mp 2x^{N/2-1} - 2x + 1$ has a small gap between the middle two terms in the "bad" case; we still obtain a contradiction, though.

For families of the form $x^N - k^2x + 1$ with $k \geq 3$, the size of the sets T_m does not stabilize as for $k = 2$, but grows fairly quickly, so a simple analysis like the one above is no longer possible. It may still be true, however, that for large enough m, these sets can be described using finitely many "patterns", which might make the situation amenable to a similar analysis.

Example 7.3. We fix $k, l \in \mathbb{Z}$ with $k \neq l$ and consider the polynomial

$$f_N = x^N + kx^{N-1} + lx + 1 \qquad \text{for} \quad N \geq 3\,.$$

(When $k = l$, then f_N is reciprocal, so that Theorem 1.2 does not apply.) We recall *Perron's irreducibility criterion* [Per07, Theorem I] (or [Pra04, Theorem 2.2.5]), which says that a polynomial

$$f = x^N + a_{N-1}x^{N-1} + \ldots + a_0 \in \mathbb{Z}[x] \qquad \text{with} \quad a_0 \neq 0$$

is irreducible when $|a_{N-1}| > 1 + |a_0| + \ldots + |a_{N-2}|$. This shows that f_N is irreducible for all $N \geq 3$ whenever $\big||k| - |l|\big| \geq 3$. (When $|l|$ is the larger absolute value, then we apply the criterion to $\tilde{f}_N$.)

This leaves (up to symmetry) the cases $l = k + 1$, $l = k + 2$ and $-2 \leq k + l \leq 2$. We note that

$$r(x) = (k - l)\big(x^2 + (k + l)x + 1\big) = (k - l)f_2(x)\,,$$

so that possible reciprocal irreducible factors for $N > N_0$ must be cyclotomic (since they divide f_N for two different N) and are as follows.

$$\begin{aligned}
k + l = -2\colon &\qquad x - 1 \mid f_N \quad \text{for all } N\\
k + l = \ \ 2\colon &\qquad x + 1 \mid f_N \quad \text{for } N \equiv 0 \bmod 2\\
k + l = \ \ 1\colon &\qquad x^2 + x + 1 \mid f_N \quad \text{for } N \equiv 2 \bmod 3\\
k + l = \ \ 0\colon &\qquad x^2 + 1 \mid f_N \quad \text{for } N \equiv 2 \bmod 4\\
k + l = -1\colon &\qquad x^2 - x + 1 \mid f_N \quad \text{for } N \equiv 2 \bmod 6
\end{aligned}$$

We also note that except when $k + l = -2$, we have that f_3 has no rational root and is therefore irreducible. Also, f_4 has no rational root unless $k + l = \pm 2$. It is easy to see that the only factorization of f_4 as a product of two quadratics is (up to exchanging k and l)

$$x^4 - 3x^3 + 3x + 1 = (x^2 - x - 1)(x^2 - 2x - 1)\,.$$

Similarly, we find that the only factorization of f_5 as a product of a quadratic and a cubic, apart from the systematically occurring factor $x^2 + x + 1$ when $k + l = 1$, is

$$x^5 - 2x^4 + x + 1 = (x^2 - x - 1)(x^3 - x^2 - 1)\,.$$

Except for the systematically occurring factor $x^2 + 1$ when $k + l = 0$, there is only the following factorization of f_6 into a quadratic and a quartic.

$$x^6 - 2x^5 + 2x + 1 = (x^2 - x - 1)(x^4 - x^3 - x - 1)\,.$$

There are no factorizations into two cubics. (Writing

$$x^6 + kx^5 + lx + 1 = (x^3 + sx^2 + tx \pm 1)(x^3 + ux^2 + vx \pm 1)$$

and comparing coefficients gives three equations to be solved for $s, t, u, v \in \mathbb{Z}$. In both cases, the equations define an affine curve of genus 1. Its projective closure is in both

cases isomorphic to the elliptic curve with label 20a4 in the Cremona database, which has exactly two rational points, both of which are at infinity for our affine models).

If we exclude for now the cases with $\max\{|k|,|l|\} \le 2$, then Lemma 5.1 tells us that $m_0 \le 3$ in all cases of interest. So we can take $N_0 = 6$ in Theorem 1.6. Since we have discussed the cases $3 \le N \le 6$ above, we see that in the cases $l = k+1$ and $l = k+2$, f_N is always irreducible, and in the cases $-2 \le k+l \le 2$, f_N factors as the cyclotomic factor given above times an irreducible polynomial, with the only exception of f_4 when $(k,l) = \pm(-3,3)$.

The remaining cases (with $-2 \le k < l \le 2$) can be dealt with using the algorithm implied by the proof of Theorem 1.6. This finally gives the following complete list of exceptional factorizations (for $k < l$).

$$\begin{aligned} x^4 - 3x^3 + 3x + 1 &= (x^2 - x - 1)(x^2 - 2x - 1) \\ x^5 - 2x^4 + x + 1 &= (x^2 - x - 1)(x^3 - x^2 - 1) \\ x^6 - 2x^5 + 2x + 1 &= (x^2 + 1)(x^2 - x - 1)^2 \\ x^7 - 2x^6 + 2x + 1 &= (x^3 - x - 1)(x^4 - 2x^3 + x^2 - x - 1) \end{aligned}$$

A similar analysis for

$$f_N = x^N + kx^{N-1} - (lx + 1)$$

(still with $k \ne l$) gives the following cyclotomic factors.

$$\begin{aligned} k + l = \ \ 2: &\qquad x + 1 \mid f_N \quad \text{for } N \equiv 1 \bmod 2 \\ k + l = \ \ 0: &\qquad x^2 + 1 \mid f_N \quad \text{for } N \equiv 0 \bmod 4 \\ k + l = -1: &\qquad x^2 - x + 1 \mid f_N \quad \text{for } N \equiv 5 \bmod 6 \end{aligned}$$

The exceptional factorizations (for $k < l$) are:

$$\begin{aligned} x^5 - x^4 - 2x - 1 &= (x^2 - x - 1)(x^3 + x + 1) \\ x^7 - 2x^6 - 2x - 1 &= (x^3 - x^2 + 1)(x^4 - x^3 - x^2 - 2x - 1) \\ x^8 - x^7 - x - 1 &= (x^2 + 1)(x^3 - x^2 + 1)(x^3 - x - 1) \end{aligned}$$

Example 7.4. Let $k, l \in \mathbb{Z}$ be nonzero and coprime. Then $x^N + kx + l$ is irreducible for all but finitely many N if and only if $k + l \ne -1$, $|k - l| \ne 1$ and $(k,l) \ne (1,1), (-1,1), (1,-1)$. We have seen in Section 3 that the polynomial is reducible for N in certain residue classes if $(k,l) = (1,1)$, $(-1,1)$ or $(1,-1)$. If $k + l = -1$, then $f_N(1) = 0$ for all N. If $k - l = \pm 1$, then $f_N(-1) = 0$ for all even or all odd N.

So it remains to show that f_N is irreducible for all large N when (k,l) is not one of the exceptional pairs. We have seen this for $(k,l) = (-1,-1)$ in Section 3. In general,

$$r(x) = klx^2 + (k^2 + l^2 - 1)x + kl\,,$$

so the only possible cyclotomic divisors are Φ_1, Φ_2, Φ_3, Φ_4 and Φ_6. In the first case, $f_N(1) = 0$ for infinitely many N, which is equivalent to $k + l = -1$. In the second case, $f_N(-1) = 0$ for infinitely many N, which is equivalent to $k - l = \pm 1$. In the last three cases, r must be proportional to $x^2 + x + 1$, $x^2 + 1$ or $x^2 - x + 1$, respectively. This forces $(k,l) = (\pm 1, \pm 1)$, which are the cases dealt with in Section 3. In all other cases, f_N must be irreducible for N large.

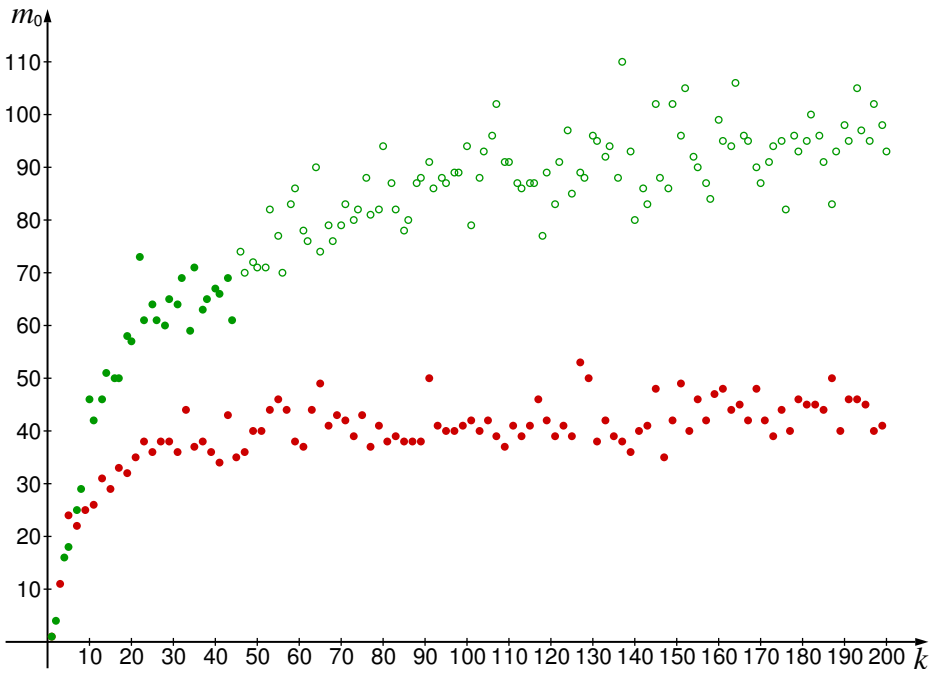

FIGURE 2. Values of m_0 for $c = 1$, $d = 2 + kx$ with k odd (red) and for $c = 1$, $d = 3 + kx$ with $3 \nmid k$ (green), $1 \le k \le 200$. The values indicated by the hollow dots are likely, but not proven to be true (the sets T_m were cut to the 10 000 pairs of smallest weight).

We note that by Perron's criterion (see Example 7.3), the polynomials $x^N \pm (kx + 1)$ are irreducible for all $N \ge 2$ when $|k| \ge 3$. (The criterion is not applicable when $|l| \ge 2$, since the reversed polynomial is not monic.) This was part of the discussion in Example 7.3 (corresponding to $(k, l) = (0, k)$ in the notation used there). What makes this case particularly amenable to our method is the uniform (and small) bound on m_0. We remark that for $|l| \ge 2$, the behavior of m_0 does not appear to follow a clear pattern. For example, when $l = 2$ or 3, m_0 first grows, but then seems to flatten out; compare Figure 2. However, this is misleading. Note that when $|l| \ge 2$, we have that $f_N(l) = 0$ for $k = -l^{N-1} - 1$, which provides a factor $(x - l)$ of f_N not dividing r, implying that $N \le 2m_0$. This shows that

$$\limsup_{|k|\to\infty} \frac{m_0(1, l + kx)}{\log |k|} > 0$$

and in particular that

$$\limsup_{|k|\to\infty} m_0(1, l + kx) = \infty .$$

Example 7.5. We consider trinomials $f_N = x^N + kx^{N-1} + l$ with $k, l \in \mathbb{Z}$, $|l| \ge 2$ (the case $|l| = 1$ is covered by Example 7.3), where $N \ge 3$. By Perron's criterion, f_N is irreducible whenever $|k| > |l| + 1$, so we can restrict to $|k| \le |l| + 1$. By Lemma 5.2, when $l \ge 5$, we have that $m_0(1 + kx, l) = 1$ if either l is prime and $k \ne 0$ or $|k| > \sqrt{p^2 + l^2/p^2}$, where p is the smallest prime divisor of l. This also holds for $2 \le |l| \le 4$ with the exceptions $m_0(1 \pm 3x, \pm 2) = 2$ and $m_0(1 \pm 3x, \pm 4) = 2$. Except in these two cases, we can therefore

take $N_0 = 2$ in Theorem 1.6. This is still true for $(k,l) = (\pm 3, \pm 2)$. In the other exceptional case, we have the factorizations

$$x^3 \pm (3x^2 - 4) = (x \pm 2)^2 (x \mp 1)\,. \tag{7.1}$$

So for $N \geq 3$ and $(k,l) \neq \pm(3,-4)$, the only possible low degree factors of f_N must divide $r = kx^2 + (k^2 + 1 - l^2)x + k$. We can have a factor $x \pm 1$ when $k = -l - 1$ (then $x - 1$ divides f_N for all N) or $k = \pm l + 1$ (then $x + 1$ divides f_N for all even N or all odd N). The only other cyclotomic factors possible are $x^2 + 1$, $x^2 + x + 1$ and $x^2 - x + 1$; their occurrence would imply that $l^2 = k^2 + 1$ or $l^2 = k^2 \mp k + 1$, which is impossible for $l \neq \pm 1$.

Any root of f_N other than ± 1 must be a divisor d of l with $|d| \geq 2$; d must also be a root of r. The latter implies that d divides k, so we can write $k = \kappa d$ with $\kappa \in \mathbb{Z}$. Then $r(d) = 0$ implies that $l^2 = (\kappa+1)(\kappa d^2+1)$, whereas $f_N(d) = 0$ implies that $-l = d^N(\kappa+1)$. Combining these relations, we get that $d^N l + \kappa d^2 + 1 = 0$, implying that $d^2 \mid 1$, a contradiction.

Combining this reasoning with Perron's criterion (for $|k| > |l|+1$), we obtain the following.

Proposition 7.6. *Let $k, l \in \mathbb{Z}$ with $k \neq 0$, $|l| \geq 2$ and either $|l|$ prime or $|k| > \sqrt{p^2 + l^2/p^2}$, where p is the smallest prime divisor of l. Then for $N \geq 3$, the polynomial*

$$f_N = x^N + kx^{N-1} + l$$

is either irreducible or factors as $x \pm 1$ times an irreducible polynomial, except for the factorizations given in (7.1).

This improves on Theorem 1 in [Har12], where the assumption $2|k| \geq |l| + 2$ is made, which is stronger than our assumption when l is odd.

Example 7.7. Define a sequence of polynomials with coefficients in $\{0,1\}$ by $h_0 = 1$ and $h_{n+1} = h_n + x^k$, where $k > \deg h_n$ is minimal with the property that $h_n + x^k$ is reducible. Then

$$h_7 = x^{35} + x^{34} + x^{33} + x^{32} + x^{16} + x^{15} + x^3 + 1\,.$$

In [FFN06] it is shown that h_8 does not exist. This can also be deduced from our main result, as follows. We consider

$$f_N = x^N + h_7 = x^N + x^{35} + x^{34} + x^{33} + x^{32} + x^{16} + x^{15} + x^3 + 1 \qquad \text{for } N \geq 36,$$

so $c = 1$ and

$$d = h_7 = (x+1)(x^{34} + x^{32} + x^{15} + x^2 - x + 1) =: ab\,,$$

where both factors are irreducible. We have that $\|c\| + \|d\| = 9$ and $\|a\| + \|b\| = 8$; since $b \neq -a$, our pair (c,d) is robust. Also,

$$r = d\tilde{d} - x^{35} = \Phi_7 h$$

with a non-cyclotomic factor h of degree 64. Using that $d \equiv 1 \bmod \Phi_7$, it is easy to see that Φ_7 never divides f_N. It is also not hard to verify that h never divides f_N: we note that h has a complex root α of absolute value ≈ 1.125. Comparing the logarithms of $|d(\alpha)|$ and $|\alpha|$ shows that $\alpha^N + d(\alpha) = 0$ has no solution $N \in \mathbb{Z}_{\geq 36}$. So Theorem 1.6 tells us that f_N is irreducible for all $N > N_0$, and we can determine a suitable N_0, as follows. We compute $m_0 = 48$ with the method sketched after Corollary 4.4. The proof of Lemma 4.5 shows that $N_0 = \max\{4\deg(d), 2m_0\} = 140$ is sufficient. We then check that f_N is also irreducible for $N \leq N_0$. (We note that the proof in [FFN06] relies on similar ideas; see [Fil99].)

References

[BSK16] Lior Bary-Soroker and Gady Kozma, *Irreducible polynomials of bounded height*, October 14, 2016. Preprint, arXiv:1710.05165. ↑1

[BMZ07] E. Bombieri, D. Masser, and U. Zannier, *Anomalous subvarieties—structure theorems and applications*, Int. Math. Res. Not. IMRN **19** (2007), Art. ID rnm057, 33, DOI 10.1093/imrn/rnm057. MR2359537 ↑4.6

[Cap01] A. Capelli, *Sulla riduttiblitá della funzione* $x^n - A$ *in un campo qualunque di razionalitá*, Math. Ann. **54** (1901), 602–603 (Italian).JFM 32.0112.03 ↑1, 1

[CMS97] S. D. Cohen, A. Movahhedi, and A. Salinier, *Double transitivity of Galois groups of trinomials*, Acta Arith. **82** (1997), no. 1, 1–15. MR1475762 ↑1

[CMS99] ———, *Galois groups of trinomials*, J. Algebra **222** (1999), no. 2, 561–573. MR1734229 ↑1

[DFV13] E. Dobrowolski, M. Filaseta, and A. F. Vincent, *The non-cyclotomic part of* $f(x)x^n + g(x)$ *and roots of reciprocal polynomials off the unit circle*, Int. J. Number Theory **9** (2013), no. 7, 1865–1877. MR3130155 ↑1, 1

[Fil99] Michael Filaseta, *On the factorization of polynomials with small Euclidean norm*, Number theory in progress, Vol. 1 (Zakopane-Kościelisko, 1997), de Gruyter, Berlin, 1999, pp. 143–163. MR1689504 ↑7.7

[FFN06] Michael Filaseta, Carrie Finch, and Charles Nicol, *On three questions concerning* $0, 1$*-polynomials*, J. Théor. Nombres Bordeaux **18** (2006), no. 2, 357–370 (English, with English and French summaries). MR2289429 ↑7.7

[FFK00] M. Filaseta, K. Ford, and S. Konyagin, *On an irreducibility theorem of A. Schinzel associated with coverings of the integers*, Illinois J. Math. **44** (2000), no. 3, 633–643. MR1772434 ↑1, 1

[FM04] Michael Filaseta and Manton Matthews Jr., *On the irreducibility of* $0, 1$*-polynomials of the form* $f(x)x^n + g(x)$, Colloq. Math. **99** (2004), no. 1, 1–5, DOI 10.4064/cm99-1-1. MR2084532 ↑1, 1

[Har12] Joshua Harrington, *On the factorization of the trinomials* $x^n + cx^{n-1} + d$, Int. J. Number Theory **8** (2012), no. 6, 1513–1518. MR2965763 ↑7.5

[HVW13] Joshua Harrington, Andrew Vincent, and Daniel White, *The factorization of* $f(x)x^n + g(x)$ *with* $f(x)$ *monic and of degree* ≤ 2, J. Théor. Nombres Bordeaux **25** (2013), no. 3, 565–578 (English, with English and French summaries). MR3179677 ↑1

[HS00] Marc Hindry and Joseph H. Silverman, *Diophantine geometry*, Graduate Texts in Mathematics, vol. 201, Springer-Verlag, New York, 2000. An introduction. MR1745599 ↑2, 2

[Lju60] Wilhelm Ljunggren, *On the irreducibility of certain trinomials and quadrinomials*, Math. Scand. **8** (1960), 65–70. MR0124313 ↑1

[MO] MathOverflow, *Is* $x^{2k+1} - 7x^2 + 1$ *irreducible?*. https://mathoverflow.net/questions/258914. ↑1

[MRW08] Michael J. Mossinghoff, Georges Rhin, and Qiang Wu, *Minimal Mahler measures*, Experiment. Math. **17** (2008), no. 4, 451–458. MR2484429 ↑2

[MS96] A. Movahhedi and A. Salinier, *The primitivity of the Galois group of a trinomial*, J. London Math. Soc. (2) **53** (1996), no. 3, 433–440. MR1396708 ↑1

[Osa87] Hiroyuki Osada, *The Galois groups of the polynomials* $X^n + aX^l + b$, J. Number Theory **25** (1987), no. 2, 230–238. MR873881 ↑1

[Per07] Oskar Perron, *Neue Kriterien für die Irreduzibilität algebraischer Gleichungen*, J. Reine Angew. Math. **132** (1907), 288–307 (German). MR1580727 ↑7.3

[Pra04] Victor V. Prasolov, *Polynomials*, Algorithms and Computation in Mathematics, vol. 11, Springer-Verlag, Berlin, 2004. Translated from the 2001 Russian second edition by Dimitry Leites. MR2082772 ↑1, 1, 7.3

[Sch67] A. Schinzel, *Reducibility of polynomials and covering systems of congruences*, Acta Arith. **13** (1967/1968), 91–101. MR0219515 ↑1

[Sch69] ———, *Reducibility of lacunary polynomials. I*, Acta Arith. **16** (1969/1970), 123–159, DOI 10.4064/aa-16-2-123-160. MR0252362 ↑1

[Sch00] ———, *Polynomials with special regard to reducibility*, Encyclopedia of Mathematics and its Applications, vol. 77, Cambridge University Press, Cambridge, 2000. With an appendix by Umberto Zannier. MR1770638 ↑1, 1, 1, 2, 4.6

[Sel56] Ernst S. Selmer, *On the irreducibility of certain trinomials*, Math. Scand. **4** (1956), 287–302. MR0085223 ↑3

[Smy71] C. J. Smyth, *On the product of the conjugates outside the unit circle of an algebraic integer*, Bull. London Math. Soc. **3** (1971), 169–175, DOI 10.1112/blms/3.2.169. MR0289451 ↑2, 2

[Vou96] Paul Voutier, *An effective lower bound for the height of algebraic numbers*, Acta Arith. **74** (1996), no. 1, 81–95, DOI 10.4064/aa-74-1-81-95. MR1367580 ↑2

ETH Inst. für Theoretische Studien, Clausiusstrasse 47, 8092 Zürich, Switzerland

E-mail address: william.sawin@math.ethz.ch

URL: http://williamsawin.com/

Raymond and Beverly Sackler School of Mathematical Sciences, Tel-Aviv University, Tel-Aviv, Israel

E-mail address: markshus@mail.tau.ac.il

Mathematisches Institut, Universität Bayreuth, 95440 Bayreuth, Germany.

E-mail address: Michael.Stoll@uni-bayreuth.de

URL: http://www.mathe2.uni-bayreuth.de/stoll/