On the factorization of polynomials with small Euclidean norm

Michael Filaseta

Dedicated to Andrzej Schinzel on the occasion of his 60th birthday

1. Introduction

Throughout this paper, we refer to the *non-cyclotomic* part of a polynomial $f(x) \in \mathbb{Z}[x]$ as $f(x)$ with its cyclotomic factors removed. More specifically, if $\pm g_1(x), \ldots, \pm g_r(x)$ are non-cyclotomic irreducible polynomials in $\mathbb{Z}[x]$ and $g_{r+1}(x), \ldots, g_s(x)$ are cyclotomic polynomials such that $f(x) = g_1(x) \cdots g_r(x) \times$ $\times g_{r+1}(x) \cdot \cdots \cdot g_s(x)$, then $g_1(x) \cdots g_r(x)$ is the non-cyclotomic part of $f(x)$. We refer to a polynomial $f(x) \in \mathbb{Z}[x]$ of degree n as *reciprocal* if $f(x) = \pm x^n f(1/x)$. We refer to $x^n f(1/x)$ as *the reciprocal* of $f(x)$. Analogous to our first definition, we refer to the *non-reciprocal* part of $f(x) \in \mathbb{Z}[x]$ as $f(x)$ with the irreducible reciprocal factors having positive leading coefficient removed. Here and throughout this paper we refer to irreducibility over the integers so that the irreducible polynomials under consideration have integer coefficients and content one. Observe that a reciprocal polynomial may be equal to its non-reciprocal part as is the case, for example, with $x^6 + x^5 + x^4 + 3x^3 + x^2 + x + 1$ which factors as a product of two non-reciprocal irreducible polynomials.

In 1956, E.S. Selmer [8] investigated the irreducibility over the rationals of the trinomials $x^n + \varepsilon_1 x^a + \varepsilon_2$ where $n > a > 0$ and each $\varepsilon_j \in \{-1, 1\}$. He obtained complete solutions in the case $a = 1$ and partial results for $a > 1$. In 1960, W. Ljunggren [2] extended Selmer's work to deal generally with the case when $a \geq 1$. In addition, he studied the quadrinomials $x^n + \varepsilon_1 x^b + \varepsilon_2 x^a + \varepsilon_3$ where each $\varepsilon_j \in \{-1, 1\}$ and $n > b > a > 0$. There was a correctable error in Ljunggren's work involving the omission of certain cases; this was noted in 1985 by W.H. Mills [3] who filled in the gaps of Ljunggren's arguments. It was established that the non-cyclotomic parts of the trinomials above are irreducible or, in the case that every factor is cyclotomic, identically 1. (Throughout this paper we view the polynomials ± 1 as neither reducible nor irreducible.) In the case of quadrinomials, the analo-

The author gratefully acknowledges support by NSF Grant DMS-9400937 and NSA Grant MDA904-97-1-0035.

gous result does not hold, but W.H. Mills classified those quadrinomials above for which the non-cyclotomic part is reducible.

Recently, in [1], Solan and the author showed that if $f(x) = x^n + x^c + x^b + x^a + 1$ where $n > c > b > a > 0$, then the non-reciprocal part of $f(x)$ is either irreducible or identically one. It is unknown whether the same result holds if "non-reciprocal" is replaced by "non-cyclotomic". The example

$$x^{11} + x^8 + x^6 + x^2 + x + 1 = (x^5 - x^3 + 1)(x^4 + x + 1)(x^2 + 1) \tag{1}$$

shows that the result of Solan and the author cannot be extended to six terms.

A natural question is: can such results be generalized? In 1969, A. Schinzel [4] published a remarkable paper which leads to an affirmative answer to this question. A consequence (not an obvious one) of his even more general results is the following:

Theorem 1 (Schinzel). *Let r be a positive integer, and fix non-zero integers $a_0, \dots, a_r$. Let $F(x_1, \dots, x_r) = a_r x_r + \cdots + a_1 x_1 + a_0$. Then there exist two finite sets S and T of matrices satisfying:*

(i) *Each matrix in S or T is an $r \times \rho$ matrix with integer entries and of rank ρ for some $\rho \le r$.*

(ii) *The matrices in S and T are computable.*

(iii) *For every set of positive integers $d_1, \dots, d_r$ with $d_1 < d_2 < \cdots < d_r$, the non-reciprocal part of $F(x^{d_1}, \dots, x^{d_r})$ is reducible if and only if there is an $r \times \rho$ matrix $N = (v_{ij})$ in S and integers $v_1, \dots, v_\rho$ satisfying*

$$\begin{pmatrix} d_1 \\ d_2 \\ \vdots \\ d_r \end{pmatrix} = N \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_\rho \end{pmatrix}$$

but there is no $r \times \rho'$ matrix M in T with $\rho' < \rho$ and no integers $v'_1, \dots, v'_{\rho'}$ satisfying

$$\begin{pmatrix} d_1 \\ d_2 \\ \vdots \\ d_r \end{pmatrix} = M \begin{pmatrix} v'_1 \\ v'_2 \\ \vdots \\ v'_{\rho'} \end{pmatrix}.$$

Moreover, Schinzel's results imply that the polynomials $F(x^{d_1}, \dots, x^{d_r})$ with reducible non-reciprocal part can be factored as a product of polynomials with non-reciprocal irreducible parts where the factors can be described explicitly in terms of the matrix N occurring in (iii). Finally, we note that Schinzel also dealt with the case that $F(x_1, \dots, x_r)$ is non-linear.

We emphasize the consequence stated above of Schinzel's result as it describes one of the main objectives of this paper. We will be interested in showing how to classify all polynomials $f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{Z}[x]$ with a fixed value of the

Euclidean norm $\|f\| = (\sum_{j=0}^{n} a_j^2)^{1/2}$ for which the non-reciprocal part of $f(x)$ is irreducible. The above theorem indicates that an algorithm exists for doing this, or more precisely for classifying the polynomials $f(x)$ having a fixed Euclidean norm and for which the non-reciprocal part of $f(x)$ is reducible. However, our approach will not be to use the above theorem directly. Instead we base our approach on the work of Ljunggren [2]. Certain aspects of Schinzel's own work (cf. [4, 5]) make use of Ljunggren's ideas, and much of what we do here will bear similarities to these aspects of Schinzel's work.

As an example of the type of result we can obtain by our methods, we establish an explicit theorem in the case that $f(x)$ is a polynomial of the form $x^n + x^d + x^c + x^b + x^a + 1$. To describe the result, we recall the example given in (1). From one example, we can obtain others as follows. Take any zero or more of the non-reciprocal irreducible factors with positive leading coefficient of a given example $f(x)$, and consider the product of the reciprocals of these factors with the remaining irreducible factors of $f(x)$. As we shall see in Section 3 (see Lemma 3), the product obtained will have the same Euclidean norm as $f(x)$ and, in the case that $f(x)$ is a polynomial with each coefficient either 0 or 1, the product obtained will also be a polynomial with each coefficient either 0 or 1. For example, from (1), we obtain (1) itself together with the examples

$$(x^5 - x^2 + 1)(x^4 + x + 1)(x^2 + 1) = x^{11} + x^9 + x^7 + x^6 + x + 1,$$
$$(x^5 - x^3 + 1)(x^4 + x^3 + 1)(x^2 + 1) = x^{11} + x^{10} + x^5 + x^4 + x^2 + 1,$$

and

$$(x^5 - x^2 + 1)(x^4 + x^3 + 1)(x^2 + 1) = x^{11} + x^{10} + x^9 + x^5 + x^3 + 1,$$

each of which has a reducible non-reciprocal part. To simplify the statement of our next result, we refer to examples obtained from a given example as described above as being *variations* of the given example.

Theorem 2. *Let a, b, c, d, and n be positive integers satisfying $a < b < c < d < n$, and let $f(x) = x^n + x^d + x^c + x^b + x^a + 1$. Then the non-reciprocal part of $f(x)$ is reducible if and only if $f(x)$ is a variation (as described above) of*

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

where s and t denote arbitrary distinct positive integers.

The two factors given for $f(x)$ above are such that their non-reciprocal parts are irreducible so that there are four variations of $f(x)$. That the two factors of $f(x)$ have irreducible non-reciprocal parts follows from our approach, but in fact something stronger holds as the results of Ljunggren and Mills mentioned earlier imply the non-cyclotomic parts of these factors are irreducible as well. Observe that (1) is the case $s = 1$ and $t = 2$ above.

It is of some interest to relate the above theorem to Schinzel's theorem. In Schinzel's theorem, we take $r = 5$, $F(x_1, x_2, x_3, x_4, x_5) = x_5 + x_4 + x_3 + x_2 + x_1 + 1$,

$d_1 = a$, $d_2 = b$, $d_3 = c$, $d_4 = d$, $d_5 = n$, $v_1 = s$, and $v_2 = t$. According to the above theorem, a matrix equation as in the first part of (iii) of Schinzel's theorem is

$$\begin{pmatrix} a \\ b \\ c \\ d \\ n \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 2 & 2 \\ 4 & 2 \\ 5 & 3 \end{pmatrix} \begin{pmatrix} s \\ t \end{pmatrix}.$$

In the case of this $F(x_1, x_2, x_3, x_4, x_5)$, the set S in Schinzel's theorem includes the 5×2 matrix in the above display, the matrix obtained by interchanging its columns, as well as other matrices obtained by considering variations of the factorization given in Theorem 2; the set T is the empty set.

The remainder of the paper is organized as follows. In the next section, we explain a method which, given $F(x_1, \dots, x_r) = a_r x_r + \dots + a_1 x_1 + a_0$ as in Theorem 1, classifies the positive integers $d_1, \dots, d_r$ for which the non-reciprocal part of $F(x^{d_1}, \dots, x^{d_r})$ is reducible. In Section 3, we show how to use a modification of this approach to establish Theorem 2. We clarify here that our proof is computational and relies on numerous cases that we resolved using MAPLE, a symbolic package. In Section 4, we use the ideas from Sections 2 and 3 to establish the following results.

Theorem 3. *Let $f(x)$ be an irreducible non-reciprocal polynomial having each coefficient either 0 or 1 and constant term 1. Then for each positive integer ℓ, the polynomial $f(x^\ell)$ is irreducible.*

This theorem will be obtained without the use of Capelli's theorem (cf. [7]), and it would be of some interest to know an alternative argument based on Capelli's theorem. Equivalently, it is easy to see that if α is a root of an $f(x)$ satisfying the conditions in Theorem 3, then Theorem 3 implies that for every positive integer ℓ the polynomial $x^\ell - \alpha$ does not factor in $\mathbb{Q}(\alpha)[x]$; we ask for a direct argument for establishing the irreducibility of $x^\ell - \alpha$ in $\mathbb{Q}(\alpha)[x]$. In addition, it would be of interest to know whether "non-reciprocal" can be replaced by "non-cyclotomic" in the statement of Theorem 3.

Our next result shows that if a polynomial with coefficients 0 and 1 is sufficiently lacunary, then its non-reciprocal part must be irreducible or identically one.

Theorem 4. *Let $f(x) = \sum_{j=0}^{r} x^{d_j}$ be such that $0 = d_0 < d_1 < \dots < d_r$. Then there exists an absolute constant $C > 0$ such that if $d_{j+1} > C d_j$ for each $j \in \{1, 2, \dots, r-1\}$, then the non-reciprocal part of $f(x)$ is either irreducible or identically one. Furthermore, if C' denotes the infimum of such C, then*

$$\frac{1+\sqrt{3}}{2} \le C' \le \frac{1+\sqrt{5}}{2}.$$

It would be of interest to know the precise value of C'. If the d_j are defined to be the Fibonacci numbers beginning with $d_1 = 1$ and $d_2 = 2$, then Theorem 4 does not apply; however, a modification of the approach can be used to show that the non-reciprocal part of $f(x) = \sum_{j=0}^{r} x^{d_j}$ is irreducible for all r and this choice of d_j. We note that this $f(x)$ is not always irreducible but conjecture that it is irreducible unless $r \in \{3, 5, 8, 11\}$.

We also note that our approach can be used to prove the existence of a bound on the number of non-reciprocal irreducible factors of a polynomial $f(x)$ that depends only on $||f||$ and not on $\deg f$. That such bounds exist was first noticed by Schinzel in [4]. A very nice estimate of this sort (which is considerably stronger than what we can obtain here) was given later by Schinzel in [5, p. 234].

Finally, we mention that Douglas Meade and the author have used ideas in this paper to write MAPLE programs which (i) determine whether a given polynomial $f(x)$ having each coefficient 0 or 1 is irreducible and (ii) determine whether the non-reciprocal part of such an $f(x)$ is irreducible. The programs work best when $f(x)$ is non-reciprocal, lacunary, and contains a small number of coefficients (say < 50) which are one. The results in this paper are used to aid with (ii) and can be applied to random polynomials of degree as large as 10^{100000}. An additional step for (i) is used to determine whether $f(x)$ has a reciprocal factor. This can be done by checking whether $\gcd(f(x), x^{\deg f} f(1/x)) = 1$, but unfortunately computing the greatest common divisor by the Euclidean algorithm can take on the order of $O(\deg f)$ steps. We modify this slightly by considering computations modulo primes, but determining whether $\gcd(f(x), x^{\deg f} f(1/x)) = 1$ is still the most costly part of the program. For (i), our program can readily handle polynomials of degree ≤ 20000. The results of this paper, therefore, raise the question of whether an efficient algorithm can be found for determining if a given lacunary polynomial has a reciprocal factor (in particular, to handle lacunary polynomials with coefficients 0 and 1 and degree say $\leq 10^{100}$). More details including running times and comparisons with MAPLE's built-in irreducibility test will be given in a subsequent paper. In addition, we currently have an interactive version of the program available on the World Wide Web through the URL

`http://www.math.sc.edu/~filaseta/irreduc.html`

2. The general approach

We suppose initially that we are given a specific polynomial $f(x) \in \mathbb{Z}[x]$ of degree n, and we wish to determine whether its non-reciprocal part is irreducible. The case when $f(0) = 0$ can be dealt with by setting $g(x) = f(x)/x$. Note that x is not reciprocal. If $g(0) = 0$, then the non-reciprocal part of $f(x)$ is reducible (it's divisible by x^2). If $g(x)$ is not reciprocal, then $g(x)$ must have a non-reciprocal factor so that here also the non-reciprocal part of $f(x)$ is reducible. Thus, we are left with considering the case where $g(0) \neq 0$ and $g(x)$ is reciprocal. In this case, $g(x)$ is divisible by a non-reciprocal polynomial if and only if the non-reciprocal part of $g(x)$ is reducible (since a reciprocal polynomial cannot be divisible by exactly one non-reciprocal irreducible polynomial). Thus, if $f(0) = 0$, then to determine whether the non-reciprocal part of $f(x)$ is irreducible, we are left with considering whether the non-reciprocal part of another polynomial $g(x) \in \mathbb{Z}[x]$ is irreducible where $g(0) \neq 0$. We may therefore suppose in what follows that $f(0) \neq 0$, and we do so.

We refer to the reciprocal of $f(x)$ as $\tilde{f}(x)$ (and likewise for other polynomials). We begin with an idea of Ljunggren [2]. We suppose for the moment that the non-reciprocal part of $f(x)$ is reducible. It follows (cf. [1]) that there are non-reciprocal polynomials $u(x)$ and $v(x)$ in $\mathbb{Z}[x]$ such that $f(x) = u(x)v(x)$. Ljunggren observed that we can obtain important information about the non-reciprocal part of $f(x)$ by considering the polynomial $w(x) = u(x)\tilde{v}(x)$. The condition $f(0) \neq 0$ implies that each of $f(x)$, $\tilde{f}(x)$, $w(x)$, and $\widetilde{w}(x)$ has non-zero constant term and degree n. This implies $f(x) = \tilde{\tilde{f}}(x)$ with a similar equation holding for $w(x)$, $u(x)$, and $v(x)$. Note that the coefficient of x^n in $f(x)\tilde{f}(x)$ is $\|f\|^2$ and the coefficient of x^n in $w(x)\widetilde{w}(x)$ is $\|w\|^2$. Of significance here is that

$$f(x)\tilde{f}(x) = u(x)v(x)\tilde{u}(x)\tilde{v}(x) = w(x)\widetilde{w}(x). \tag{2}$$

We deduce then that $\|f\| = \|w\|$. In [2], Ljunggren considered the case when $f(x)$ has four non-zero coefficients each of which is ± 1. In this case, (2) implies $\|w\| = 2$ which in turn implies that $w(x)$ has exactly four non-zero coefficients each of which is ± 1. To obtain his results, Ljunggren proceeded to do a case analysis to show that if $w(x)$ satisfies $w(x)\widetilde{w}(x) = f(x)\tilde{f}(x)$, then $w(x) = \pm f(x)$ or $w(x) = \pm \tilde{f}(x)$. This implies $v(x)$ or $u(x)$, respectively, must be reciprocal, giving a contradiction. In this section, we show in the general situation of $f(x) \in \mathbb{Z}[x]$, a similar analysis can always be done.

We write

$$f(x) = \sum_{j=0}^{r} a_j x^{d_j} \quad \text{and} \quad w(x) = \sum_{j=0}^{s} b_j x^{k_j}, \tag{3}$$

where we view the a_j's and d_j's as given integers and the b_j's and k_j's as unknown integers with

$$\begin{aligned} &0 = d_0 < d_1 < \ldots < d_{r-1} < d_r = n \qquad \text{and} \\ &0 = k_0 < k_1 < \ldots < k_{s-1} < k_s = n \end{aligned} \tag{4}$$

(so our use of "unknown" is misleading in the case of k_0 and k_s). We also suppose that each a_j and b_j is non-zero.

Lemma 1. *The non-reciprocal part of $f(x)$ is reducible if and only if there exists $w(x)$ different from $\pm f(x)$ and $\pm\tilde{f}(x)$ such that $w(x)\widetilde{w}(x) = f(x)\tilde{f}(x)$.*

Proof. If the non-reciprocal part of $f(x)$ is reducible, then we have already seen that there exists $w(x)$ satisfying (2). Observe that $u(x)$ and $v(x)$ being non-reciprocal and the definition of $w(x)$ above implies that $w(x)$ is different from both $\pm f(x)$ and $\pm\tilde{f}(x)$.

Now, suppose we know there exists $w(x)$ different from $\pm f(x)$ and $\pm \tilde{f}(x)$ such that $w(x)\widetilde{w}(x) = f(x)\tilde{f}(x)$, and assume the non-reciprocal part of $f(x)$ is irreducible or identically ± 1. We write $f(x) = g(x)h(x)$ where each irreducible factor of $g(x)$ is non-reciprocal and each irreducible factor of $h(x)$ is reciprocal. By assumption, $g(x)$ has at most one irreducible factor. Observe that $f(x)\tilde{f}(x) = \pm g(x)\tilde{g}(x)h^2(x)$. Using $w(x)\widetilde{w}(x) = f(x)\tilde{f}(x)$, it is easy to see that $w(x) = \pm g(x)h(x) = \pm f(x)$ or $w(x) = \pm \tilde{g}(x)h(x) = \pm \tilde{f}(x)$, a contradiction. The lemma now follows. □

Given Lemma 1, our goal now is to determine whether there exists $w(x)$ different from $\pm f(x)$ and $\pm \tilde{f}(x)$ such that $w(x)\widetilde{w}(x) = f(x)\tilde{f}(x)$. As noted earlier, we have $\|f\| = \|w\|$. We immediately deduce that $\sum_{j=0}^{s} |b_j| \le \|f\|^2$. We count the number of ways of taking $\|f\|^2 + 1$ ones and dividing them into $\|f\|^2 + 1$ ordered containers so that the number of ones in the containers are $|b_0|, |b_1|, \dots, |b_s|$, and $\|f\|^2 + 1 - \sum_{j=0}^{s} |b_j|$, with any remaining $\|f\|^2 - s - 1$ containers being empty. Allowing for the $2^{s+1} \le 2^{\|f\|^2}$ signs for $b_0, \dots, b_s$, we obtain that the number of different possibilities for s together with the $(s+1)$-tuple $(b_0, b_1, \dots, b_s)$ is bounded by

$$2^{\|f\|^2} \times \binom{2\|f\|^2 + 1}{\|f\|^2} \le 2^{3\|f\|^2}.$$

Observe that this bound is independent of the degree n of the given polynomial $f(x)$.

Our goal now is to determine the possible values for the $(s+1)$-tuple $(k_0, k_1, \dots \dots, k_s)$. We do this by solving a system of linear equations in the unknowns $k_0, k_1, \dots, k_s$. We obtain these equations by expanding the left and right sides of (2) and comparing exponents. The exponents appearing on the left side depend only on $f(x)$ and, hence, are fixed. The exponents appearing on the right side are linear combinations in the unknowns k_j. Equation (2) implies that these exponents must be the same. The idea is to consider every possible matching of the exponents on the left side with the right side. Each matching of exponents corresponds to a system of equations which we attempt to solve. If a solution $(k_0, k_1, \dots, k_s)$ exists, we consider the various possibilities for $(b_0, b_1, \dots, b_s)$ discussed above and form polynomials $w(x)$. If we determine a $w(x)$ different from $\pm f(x)$ and $\pm \tilde{f}(x)$ satisfying (2), then Lemma 1 implies that the non-reciprocal part of $f(x)$ is reducible. If after considering all possible $(k_0, k_1, \dots, k_s)$ and $(b_0, b_1, \dots, b_s)$ as just described, there is no such $w(x)$, then Lemma 1 implies the non-reciprocal part of $f(x)$ is irreducible or ± 1.

When comparing exponents on the left and right side of (2), we need to be careful as cancellation of terms can occur. To be more precise, the complete set of exponents on the right side can be written as

$$E = \{n - k_j + k_i : 0 \le i, j \le s\}.$$

A particular solution for $(k_0, k_1, \dots, k_s)$ that we seek may cause two or more elements from E to be the same. Then depending on $(b_0, b_1, \dots, b_s)$, these equal elements from E may not be equal to any of the exponents appearing on the left side of (2) (as the sum of the coefficients corresponding to these powers of x may be zero). As suggested by these remarks, we must also account for the possibility that a solution $(k_0, k_1, \ldots, k_s)$ causes some elements of E to be equal.

We proceed as follows. We observe that for (2) to hold, each element of E must either be equal to an exponent which appears on the left side of (2) or must be equal to a second expression from E. We consider every possible system of equations, each system consisting of equations formed by setting an element of E equal to either an exponent appearing on the left side of (2) or a second element from E. We do this in such a way that (i) each element of E occurs in such an equation at least once, (ii) every exponent on the left side of (2) is used exactly once, and (iii) the equations $n - k_s + k_0 = 0$ and $n - k_0 + k_s = 2n$ are used. We only allow equations of the form $n - k_j + k_i = n - k_v + k_u$ if $(i, j) \neq (u, v)$. We modify the systems slightly by replacing the two equations in (iii) with $k_0 = 0$ and $k_s = n$. Observe that if $e_1, e_2, \ldots, e_t$ are elements of E which are equal to the same exponent m appearing on the left of (2), then (ii) can hold by considering the equations $e_1 = m, e_2 = e_1, \ldots, e_t = e_1$. Also, $k_0 = 0$ and $k_s = n$ are necessary for (4) to hold and they imply that the equations in (iii) hold.

We do not seek to obtain systems of equations with *every* solution $(k_0, k_1, \ldots$ $\ldots, k_s)$ of a system corresponding to some solution of (2); but we do want each solution of (2) to correspond to a solution of at least one of these systems of equations. In particular, if we have a system of equations as above which contains each equation in a second such system of equations, we do not need to consider the first system of equations (any choice of $(k_0, k_1, \ldots, k_s)$ satisfying the first system will also satisfy the second).

Now, suppose we have a system of equations as above. One of the following three possibilities may occur: (i′) the system has a unique solution (in $\mathbb{R}^{s+1}$), (ii′) the system has no solutions, or (iii′) the system has infinitely many solutions. From our point of view, the cases (i′) and (ii′) are ideal. If (i′) occurs, then we go through each possibility for $(b_0, b_1, \ldots, b_s)$, form polynomials $w(x)$, and see if each such $w(x)$ is different from $\pm f(x)$ and $\pm \tilde{f}(x)$ and satisfies (2). If (ii′) occurs, then there is no $w(x)$ corresponding to the system of equations under consideration. We have some difficulty if (iii′) occurs because then we seemingly must determine those solutions $(k_0, k_1, \ldots, k_s)$ satisfying (4) and then consider each such solution as a possible list of exponents for $w(x)$. To alleviate this situation, we will show that each system satisfying (iii′) cannot correspond to an appropriate list of exponents for $w(x)$. More specifically, we show that if (iii′) holds and $k_0, k_1, \ldots, k_s$ is a solution to the system, then it cannot be the case that the k_j are distinct (so (4) cannot hold). This follows as a consequence of the matrix B in [4, p. 133; 6, p. 291] having rank ℓ as established there; we give an alternative approach here (which nevertheless bears some similarities to the Remark of [4, p. 134]).

Lemma 2. *Let s and t be positive integers. Suppose a system of linear equations in the variables $x_0, \ldots, x_s$ is of the form*

$$\alpha_{i0} x_0 + \alpha_{i1} x_1 + \ldots + \alpha_{is} x_s = \beta_i \qquad \textit{for } 1 \le i \le t,$$

where the α_{ij} *and* β_i *are all in* $\mathbb{Z}$. *Suppose further that the system of equations has infinitely many solutions* $(x_0, \dots, x_s) \in \mathbb{R}^{s+1}$. *If the system has at least one solution* $(x_0, \dots, x_s) \in \mathbb{Z}^{s+1}$ *with* $x_0, x_1, \dots, x_s$ *distinct, then the system has infinitely many such solutions.*

The proof of the lemma can be modified to show that if there is at least one solution $(x_0, \dots, x_s) \in \mathbb{R}^{s+1}$ with $x_0, x_1, \dots, x_s$ distinct, then the system has infinitely many solutions $(x_0, \dots, x_s) \in \mathbb{Q}^{s+1}$ with $x_0, x_1, \dots, x_s$ distinct. However, it is possible that distinct solutions exist in $\mathbb{Q}^{s+1}$ but not in $\mathbb{Z}^{s+1}$. It would be possible to work with a version of the lemma dealing with distinct rational solutions rather than distinct integer solutions, but the lemma as stated will make the arguments more direct.

Before proving the lemma, we show that it gives us what we want. Suppose we have a system of equations as constructed above for which (iii′) occurs. We view the variables as $x_0, x_1, \dots, x_s$, and suppose further that there is a solution $(k_0, k_1, \dots, k_s)$ to our system that satisfies (2) and (4). In particular, (4) and Lemma 2 imply that the system has infinitely many solutions in distinct integers. Then there must be a solution $(k'_0, k'_1, \dots, k'_s)$ consisting of distinct integers with either $\min_{0\le j\le s}\{k'_j\} < 0$ or $\max_{0\le j\le s}\{k'_j\} > n$. We fix such a solution and define u and v by $k'_u = \min_{0\le j\le s}\{k'_j\}$ and $k'_v = \max_{0\le j\le s}\{k'_j\}$. Note that since $k'_0, k'_1, \dots, k'_s$ are distinct, u and v are uniquely determined. Also, either $k'_u < 0$ or $k'_v > n$. Since our system under consideration requires $k'_0 = 0$ and $k'_s = n$, the definition of u and v implies $k'_u \le 0$ and $k'_v \ge n$. We deduce that $k'_v - k'_u \ge n + 1$. This means that $n - k'_v + k'_u \le -1$. On the other hand, our system of equations includes an equation either of the form $n - x_v + x_u = n - x_j + x_i$ with $(u, v) \ne (i, j)$ or of the form $n - x_v + x_u = m$ for some exponent m appearing on the left of (2). The former cannot happen as it would imply $n - k'_v + k'_u = n - k'_j + k'_i$ which is impossible as $k'_0, k'_1, \dots, k'_s$ being distinct and the definition of u and v imply $n - k'_v + k'_u < n - k'_j + k'_i$ whenever $(u, v) \ne (i, j)$. On the other hand, $n - k'_v + k'_u \le -1$ and so it cannot be an exponent on the left side of (2). Thus, we have a contradiction. This implies each system as in (iii′) cannot have a solution $(k_0, k_1, \dots, k_s)$ satisfying (2) and (4) as promised.

Proof of Lemma 2. Consider the $t \times (s + 1)$ matrix $A = (\alpha_{i,j-1})$, and let ρ be the rank of A. Then there are ρ linearly independent rows of A which, together with the corresponding values of β_i, determine the solution set of the equations. By rearranging the equations if necessary, we may suppose the first ρ rows of A are linearly independent. By Gaussian elimination, we can solve for some ρ of the unknowns $x_0, \dots, x_s$ in terms of the others. We may suppose these ρ unknowns are $x_0, \dots, x_{\rho-1}$ and do so. Considering the first ρ rows and ρ columns of A, we obtain a $\rho \times \rho$ matrix B with non-zero determinant. Set $D = |\det B| \ge 1$. It is not difficult to see that the general solution to the system of equations can be written in the form

$$x_i = \frac{1}{D}\Big(c_i + \sum_{j=\rho}^{s} b_{ij}x_j\Big) \qquad \text{for } 0 \le i \le \rho - 1. \tag{5}$$

Here, $B\vec{u} = \vec{v}$ where $\vec{u}$ is the column vector with $(i+1)$st entry c_i/D and $\vec{v}$ is the column vector with ith entry β_i; and for $j \in \{\rho, \ldots, s\}$ we have $B\vec{u}_j = \vec{v}_j$ where $\vec{u}_j$ is the column vector with $(i+1)$st entry b_{ij}/D and $\vec{v}_j$ is the column vector consisting of the first ρ elements in the jth column of A. Cramer's Rule guarantees that each c_i and b_{ij} is in $\mathbb{Z}$.

We fix a solution $(k_0, k_1, \ldots, k_s)$ consisting of distinct integers (such a solution exists by the conditions in the lemma). We choose positive integers $\ell_\rho, \ell_{\rho+1}, \ldots, \ell_s$ inductively satisfying the inequality

$$\ell_m > 2 \max_{0 \le i \le s} \{|k_i|\} + 2 \max_{0 \le i \le s} \Big\{ \sum_{j=\rho}^{m-1} |b_{ij}|\ell_i \Big\} + 2D \max_{\rho \le i \le m-1} \{\ell_i\} \tag{6}$$

for $m = \rho, \rho+1, \ldots, s$. We define $k_i' = k_i + \ell_i D$ for $\rho \le i \le s$. For $0 \le i \le \rho - 1$, k_i' is defined using (5) so that $(k_0', \ldots, k_s')$ is a solution to our system of equations. Thus,

$$k_i' = \frac{1}{D}\Big(c_i + \sum_{j=\rho}^{s} b_{ij} k_j'\Big) = k_i + \sum_{j=\rho}^{s} b_{ij}\ell_j \qquad \text{for } 0 \le i \le \rho - 1.$$

Clearly, each $k_i' \in \mathbb{Z}$. Considering each of the cases $i \ge \rho$, $i < \rho \le j$, and $j < \rho$ separately and using (6), it is not difficult to establish that $k_i' \ne k_j'$ whenever $0 \le i < j \le s$. The lemma then follows. □

The above describes our approach for establishing whether the non-reciprocal part of a given $f(x) \in \mathbb{Z}[x]$ is irreducible. It is an easy matter to obtain some estimate for the total number of numbers s, coefficient vectors $(b_0, b_1, \ldots, b_s)$, and exponent vectors $(k_0, k_1, \ldots, k_s)$ that we need consider in the above approach. We obtained the upper bound

$$\exp(4\|f\|^2(\|f\|^2 + 2)\log\|f\|).$$

The details are omitted.

We consider next a polynomial $f(x)$ with variable exponents. More precisely, we consider $f(x) = a_r x_r^{d_r} + \ldots + a_1 x_1^{d_1} + a_0$, and analogous to Theorem 1 we seek to describe the r-tuples $(d_1, \ldots, d_r)$ for which the non-reciprocal part of $f(x)$ is reducible. The strategy we proceed with is the same as before. We want to determine when a polynomial $w(x)$ exists satisfying (2), (3), and (4) that is different from $\pm f(x)$ and $\pm \tilde{f}(x)$. We deal with the possibilities for the coefficients of $w(x)$ as before, and we consider various systems of equations with the unknowns being the exponents $k_0, k_1, \ldots, k_s$ appearing in $w(x)$. The condition (ii) needs to be modified as we do not know which exponents on the left side of (2) are equal or are cancelled (appear with coefficient zero). We therefore modify the situation by considering every possibility for equal exponents and cancelled exponents on the left. With each fixed possibility, we proceed as before with now condition (ii) an acceptable one (we use every distinct exponent which appears on the left with the given possibility for equal exponents we are considering and we ignore those exponents being cancelled). By the comments above concerning (iii′), we need only consider the systems where there is a unique solution for the exponents $k_0, k_1, \ldots, k_s$ in terms of $d_1, \ldots, d_r$. Once we determine a possible list of exponents for $w(x)$, we go through each possibility for the coefficients and compare both sides of (2). At this point, the coefficients have been made explicit and the only unknowns are $d_1, \ldots, d_r$. We go through a new collection of systems of equations in these unknowns determined by considering possible matchings of the exponents (from comparing the left and right sides of (2) and allowing for possible cancellation of terms on both sides). This time the possibility of having a system with infinitely many solutions is of no concern to us; this will occur as it apparently does in the case of Theorem 2. By Lemma 1, if we find a solution set that gives us both (2) and (4) with $w(x)$ different from $\pm f(x)$ and $\pm \tilde{f}(x)$, we have a classification of $f(x)$ of the form $a_r x_r^{d_r} + \ldots + a_1 x_1^{d_1} + a_0$ giving polynomials with reducible non-reciprocal part. Once we have completed going through the systems of equations and all possible coefficients, every possible $f(x)$ of this form with reducible non-reciprocal part will fall into one of the classifications obtained.

In the next section, we outline the proof of Theorem 2 and indicate some ideas which will reduce the number of computations discussed above in order to obtain such a result. There are some simplifications that are particular to the study of polynomials having each coefficient either 0 or 1, but some of the ideas can be used in the more general setting.

3. The proof of Theorem 2

In the previous section, we considered fixed integers $a_0, a_1, \ldots, a_r$ and described a method for resolving when the polynomial $f(x) = a_r x_r^{d_r} + \ldots + a_1 x_1^{d_1} + a_0$ has irreducible non-reciprocal part. In this section, we focus on the special case when $a_0 = a_1 = \ldots = a_r = 1$, though some of our comments will apply to the more general situation. In particular, we describe the proof of Theorem 2. We begin by showing that whenever every $a_j = 1$, the coefficients in the polynomial $w(x)$ can be described precisely.

Lemma 3. *Let $f(x)$ and $w(x)$ satisfy (2), (3), and (4). If $a_j = 1$ for every $j \in \{0, 1, \ldots, r\}$ and $b_s > 0$, then $s = r$ and $b_j = 1$ for every $j \in \{0, 1, \ldots, r\}$.*

Proof. As discussed earlier, equation (2) implies $||f|| = ||w||$. Therefore,

$$\sum_{j=0}^{r} a_j^2 = \sum_{j=0}^{s} b_j^2.$$

Also, since $\tilde{f}(1) = f(1)$ and $\widetilde{w}(1) = w(1)$, (2) implies $f(1)^2 = w(1)^2$. Since $a_j = 1$ for each j, we obtain

$$\Big(\sum_{j=0}^{s} b_j\Big)^2 \le \Big(\sum_{j=0}^{s} b_j^2\Big)^2 = \Big(\sum_{j=0}^{r} a_j^2\Big)^2 = \Big(\sum_{j=0}^{r} a_j\Big)^2 = \Big(\sum_{j=0}^{s} b_j\Big)^2.$$

We deduce that equality holds in the inequality above which, given that $b_s > 0$, can only occur if every $b_j = 1$. Since $\|f\| = \|w\|$, we obtain the condition $s = r$. $\square$

The condition $b_s > 0$ is of no real importance. We can replace any $w(x)$ satisfying (2) with $-w(x)$ and the conditions (2), (3), and (4) will remain valid. Thus, given Lemma 1, we are left with determining whether there is a polynomial $w(x)$, different from $\pm f(x)$ and $\pm \tilde{f}(x)$, satisfying (2), (3), and (4) with $s = r$ and $b_j = 1$ for every $j \in \{0, 1, \dots, r\}$.

For more general polynomials $f(x)$, there are some modifications of the technique described in Section 2 that we will want to make use of in this section. In comparing exponents on the left and right of (2), we need not compare the complete set of exponents. Each side of (2) is a reciprocal polynomial of degree $2n$ so that it is only necessary to compare the exponents of the terms of degree $\le n$. In the case of $f(x)$ as in Lemma 3, we will be only considering $w(x)$ with $r+1$ non-zero coefficients each of value 1. This will imply that the coefficients of x^n on both sides of (2) are the same. Hence, in this case, we need only compare those terms of degree $< n$ in (2).

Now, we turn to another modification of the technique described in Section 2 that can be used when considering a general polynomial $f(x)$. We will make use of the following result.

Lemma 4. *Let m be a positive integer. Let $f_1, f_2, \dots, f_m$ be arbitrary real numbers with at least one non-zero. Then there exist distinct integers $x_1, x_2, \dots, x_m$ satisfying*

$$f_1 x_1 + f_2 x_2 + \ldots + f_m x_m \ge 0 \quad \textit{and} \quad 0 < x_1 < x_2 < \ldots < x_m \tag{7}$$

if and only if for some $k \in \{1, 2, \dots, m\}$ the sum $\sum_{j=k}^m f_j$ is positive.

Proof. Suppose first that there is a $k \in \{1, 2, \dots, m\}$ for which $\sum_{j=k}^m f_j > 0$. Let m' be a positive integer satisfying

$$m' > m\Big(\sum_{j=1}^m |f_j|\Big) \Big/ \Big(\sum_{j=k}^m f_j\Big).$$

Then it follows that

$$\begin{aligned} f_1 + 2f_2 + \ldots + (k-1)f_{k-1} + m' f_k + (m'+1) f_{k+1} + \ldots + (m'+m-k) f_m \\ \ge m'(f_k + f_{k+1} + \ldots + f_m) - \max\{k-1, m-k\} \sum_{j=1}^m |f_j|. \end{aligned}$$

The choice of m' implies the last expression above is positive. Hence, to obtain (7), we can take $x_j = j$ for $1 \le j \le k-1$ and $x_j = m' + j - k$ for $k \le j \le m$ where m' is a sufficiently large positive integer.

Now, suppose we know there exist distinct positive integers $x_1, x_2, \dots, x_m$ satisfying (7) and we want to show $\sum_{j=k}^m f_j > 0$ for some $k \in \{1, 2, \dots, m\}$. Assume to the contrary that $\sum_{j=k}^{m} f_j \le 0$ for every $k \in \{1, 2, \ldots, m\}$. Observe that

$$\begin{aligned}(8) \qquad \sum_{j=1}^{m} f_j x_j = x_1 \sum_{j=1}^{m} f_j + (x_2 - x_1) \sum_{j=2}^{m} f_j \\ + (x_3 - x_2) \sum_{j=3}^{m} f_j + \ldots + (x_m - x_{m-1}) \sum_{j=m}^{m} f_j.\end{aligned}$$

Each sum on the right is ≤ 0 by assumption and each of the expressions x_1 and $x_j - x_{j-1}$ for $2 \le j \le m$ is positive by (7). Therefore, we deduce that $\sum_{j=1}^{m} f_j x_j \le 0$. We have a contradiction to (7) unless equality holds. On the other hand, equality holds only if each sum in (8) is equal to 0. It is easy to see that the condition that at least one f_j is non-zero implies that at least one of the sums in (8) is non-zero. Again, we obtain a contradiction. It follows that for some $k \in \{1, 2, \ldots, m\}$ we must have $\sum_{j=k}^{m} f_j > 0$. $\square$

The purpose of Lemma 4 is to enable us to reduce the number of systems of equations we need to consider when comparing exponents on the left and right of (2). This is achieved by using Lemma 4 to determine what the least possible exponents can be on the left and right of (2). Then we go through the different possibilities for the least exponents being equal to one another. Once we determine an equation by comparing two least exponents, we obtain information from this equation and plug the information into the list of exponents on the left and right of (2). We combine and cancel terms with equal exponents that the one equation has produced, and we repeat the process of finding the least possible exponents, forming an equation, plugging in the information the equation gives, and combining like terms. We repeat the process until we obtain a situation where (2) holds and we can use Lemma 1 or until we obtain a contradiction. The latter can occur if there is one possible least exponent determined by Lemma 4 occurring on only one side of (2) (so a term occurs only on one side of (2) and equality cannot hold). If no contradiction occurs and we determine a situation where (2) occurs but $w(x)$ is one of $\pm f(x)$ and $\pm \tilde{f}(x)$, we continue by going through other possibilities for equations that have occurred earlier. This is the "idea" behind our use of Lemma 4; we turn now to some specifics by applying our approach to obtain Theorem 2.

As is evident in the statement of Lemma 3, an advantage of considering polynomials $f(x)$ with coefficients just 0 and 1 is that we may suppose the polynomial $w(x)$ will also have coefficients which are just 0 and 1. This helps directly with analyzing the exponents in (2) as now all the non-zero coefficients appearing in the factors on the left and right are positive so that no cancellation of terms can occur when we expand the left and right side of (2). We still need to concern ourselves with the possibility of terms combining, but we need not concern ourselves with the possibility that some terms combine to give a coefficient of value 0.

To prove Theorem 2, we made use of MAPLE (Version V, Release 4), a symbolic package, to deal with the various cases and systems of equations we needed to consider. We expand the left and right side of (2) using (3) with $s = r = 5$, $a_0 = a_1 = \ldots = a_5 = 1$, and $b_0 = b_1 = \ldots = b_5 = 1$. We also use the notation of the statement of Theorem 2 in discussing the exponents of $f(x)$. The exponents of interest to us are those which are $< n$, and for the left side of (2) the list of these exponents is:

$$0, \quad a, \quad b, \quad c, \quad d, \quad n-d, \quad n-d+a, \quad n-d+b, \quad n-d+c,$$
$$n-c, \quad n-c+a, \quad n-c+b, \quad n-b, \quad n-b+a, \quad n-a.$$

The list for the exponents $< n$ on the right is identical except with k_1, k_2, k_3, and k_4 in place of a, b, c, and d, respectively. Observe that, in (2) and Lemma 1, the roles of $w(x)$ and $\widetilde{w}(x)$ are interchangeable. In other words, if necessary we may work with $\widetilde{w}(x)$ instead of $w(x)$. By doing this if necessary we may suppose that $k_1 \le n-k_4$ and do so. Similarly, as the non-reciprocal part of $f(x)$ is irreducible if and only if the non-reciprocal part of $\tilde{f}(x)$ is irreducible, we may suppose $a \le n-d$ and do so.

We now use the inequalities in (4) to determine the least possible five exponents on the left and right of (2) (after it is expanded). On the left, the least two exponents are 0 and a; the latter holds as we know $a \le n-d$ and we are making no claims that there is only one exponent having the value of a. The next three least exponents have thirteen possibilities which we list as triples, the elements of each triple being listed from least to greatest. These triples are:

$$(b,c,d), \quad (b,c,n-d), \quad (b,n-d,c), \quad (b,n-d,n-c), \quad (b,n-d,n-d+a),$$
$$(n-d,b,c), \quad (n-d,b,n-d+a), \quad (n-d,b,n-c), \quad (n-d,n-d+a,b),$$
$$(n-d,n-d+a,n-c), \quad (n-d,n-c,b), \quad (n-d,n-c,n-d+a), \quad (n-d,n-c,n-b).$$

The triples can be determined by using Lemma 4 or by direct considerations of the exponents. An analogous situation exists for the least five exponents on the right of (2) with a, b, c, and d replaced by k_1, k_2, k_3, and k_4. In particular, the second least exponent on the right is k_1 so that we deduce by comparing second least exponents that $k_1 = a$.

We use the 13 orderings of the least five exponents on the left of (2) and the 13 orderings of the least five exponents on the right to begin our comparison of the exponents appearing in (2). We thus consider the 169 possibilities for what these least five exponents on both sides can be. There are some observations that would enable us to reduce the number of possibilities to consider, but there is no reason to elaborate here on this (from a computational point of view, the 169 possibilities are not hard to handle).

With each of these 169 possibilities we consider a corresponding system of equations. There is no reason to consider the least two exponents appearing on the left and right given that we already have determined that $k_1 = a$ so that these exponents are the same. Thus, we are only using the triples listed above and the corresponding triples for the exponents on the right. For example, if we take the first possibility listed for a triple on the left, namely (b,c,d), with the possibility on the right corresponding to the fifth triple listed, namely $(k_2, n-k_4, n-k_4+k_1)$, we get the equations $k_2 = b$, $n-k_4 = c$, and $n-k_4+k_1 = d$. There is one more initial equation we consider before attempting to solve the system of equations. We sum the exponents on the left side of (2) which are $< n$ and equate this to the sum of the exponents $< n$ on the right side of (2). We obtain $10n + 3k_1 + k_2 - k_3 - 3k_4 = 10n + 3a + b - c - 3d$. This equation is of value largely because it is an equation we can use independent of which of the 169 cases we consider. We make the substitution $k_1 = a$ to simplify any of the equations obtained thus far. In this example that means we are left with the following equations:

$$(9) \qquad k_2 = b, \quad n - k_4 = c, \quad n - k_4 + a = d, \quad \text{and} \quad k_2 - k_3 - 3k_4 = b - c - 3d.$$

We now have four equations (three of which depend on which of the 169 cases we are considering) that form our initial system of equations.

By our previous remarks, we know that if we consider enough such equations (arising from comparing both sides of (2)) that we can ignore the system if no solution or infinitely many solutions exist for k_2, k_3, and k_4. In fact, the four equations obtained above in each of the 169 cases were sufficient for determining a unique solution for k_2, k_3, and k_4. It still may be the case when further equations are considered the system becomes inconsistent; but regardless we know with these four equations (one set of equations for each of 169 cases) if a solution exists when we extend the system to include more equations by comparing further exponents arising in (2), then the values for k_2, k_3, and k_4 must agree with that obtained from these four equations. Using MAPLE to analyze each of the 169 cases of four equations obtained above, we attempt to solve the four equations for the variables k_2, k_3, k_4, as well as n. Our hope was that since we had four linear equations, with any luck we should be able to solve for four of the variables. As it turns out, it is not always possible to solve, from these four equations, for k_2, k_3, k_4, and n in terms of the remaining unknowns a, b, c, and d. It is not difficult to see in fact that no such solution exists when considering the equations given in (9). In such situations, we attempt to solve the four equations for k_2, k_3, k_4, and d in terms of the remaining unknowns. In the case of (9), we deduce that

$$(10) \qquad k_2 = b, \quad k_3 = -3n + 7c + 3a, \quad k_4 = n - c, \quad \text{and} \quad d = c + a.$$

In general, however, it is not always possible to solve the four equations for k_2, k_3, k_4, and n or for k_2, k_3, k_4, and d. In each of these cases it is possible to solve for k_2, k_3, k_4, and c (as we determined simply by performing the computations).

Rather than directly considering further equations arising from comparing exponents in (2), we first substitute the knowledge learned thus far into (2). In the example we have been following, we consider the exponents we obtain in (2) after substituting for k_2, k_3, k_4, and d using the equations in (10). We then cancel the terms which occur on both sides. In our example, we are then left with the exponents

$$(11) \qquad n - a, \quad n - c, \quad n - c + a, \quad n - c + b, \quad n - c - a, \quad \text{and} \quad n - c - a + b$$

on the left and the exponents

$$(12) \qquad c + b, \quad 4n - 7c - 2a, \quad 4n - 7c - 3a,$$
$$4n - 7c - 3a + b, \quad -3n + 7c + 3a, \quad \text{and} \quad -3n + 8c + 3a$$

on the right. In general, we allow for possible duplication of exponents in each of these lists.

Next, we determine the possible least elements that occur as exponents remaining on the left and right of (2). This is done by applying Lemma 4. In our example, we use Lemma 4 to determine that the only possible least exponent appearing in (11) is $n - c - a$. It is reasonable to ask why one should use Lemma 4 here when it is clear by inspection that $n-c-a$ is the least exponent. To clarify the situation, we did not do these computations by hand. We programmed MAPLE to perform the computations so that once we started the program we were only left to intervene after we received examples of $w(x)$ satisfying (2) and different from $\pm f(x)$ and $\pm \tilde{f}(x)$. We clarify what the output was below. Lemma 4 was used as a method for programming MAPLE to compare a list of exponents such as those given in (11) and (12). In the case of (12), Lemma 4 was used to determine that the least exponent is one of $c+b$, $4n-7c-3a$, and $-3n+7c+3a$. To help explain the use of Lemma 4, suppose we are given the two exponents $4n - 7c - 3a$ and $-3n+7c+3a$ and we want to know if the inequality $4n-7c-3a \le -3n+7c+3a$ can hold given that $0 < a < c < n$. We rewrite the inequality as $-7n+14c+6a \ge 0$. According to Lemma 4, this inequality is possible since $-7+14 > 0$. Observe that Lemma 4 also implies that $-3n + 7c + 3a \le 4n - 7c - 3a$ can hold. Thus, the list of minimal possible exponents in each of (11) and (12) is made by comparing every pair of exponents in each list using Lemma 4. At this point, we have two lists for the possible minimal exponent, one for the left side of (2) and one for the right side. We do not stop the comparison of the exponents here. It is possible that these two lists of minimal possible exponents have some inconsistencies. More specifically, we check to determine whether or not each element from one list can actually be at least as small as each element from the other list. Again this comparison can be done using Lemma 4. In the example, this comparison does not reduce the sizes of the lists of minimal exponents we obtain. Observe that if the least exponent remaining on one side of (2) is determined to be strictly less than the least exponent remaining on the other side of (2) (i.e., if each exponent in the latter list cannot be less than or equal to some exponent in the former list), then we can stop the case under consideration for the exponents on the left and right of (2) will not be equal.

The least exponent remaining on the left of (2) must equal the least exponent remaining on the right of (2). This gives us another equation or, more precisely, a list of possible equations. In the example, we deduce that one of the equations $n - c - a = c + b$, $n - c - a = 4n - 7c - 3a$, and $n - c - a = -3n + 7c + 3a$ must hold. We consider each of these possibilities, solving the equation for one variable in terms of the others. For example, for the last of these possibilities $n - c - a = -3n + 7c + 3a$ we might get $a = n - 2c$ (I say "might" as I do not claim that MAPLE will be consistent with which variable it solves for). We now repeat the process described in the last two paragraphs. We substitute the new information (in the example, $a = n-2c$) into the list of remaining exponents on the left and right of (2) (in the example, into (11) and (12)), allowing for repetitions, and cancelling like exponents. In our example, the substitution $a = n - 2c$ into

(11) and (12) leads to the same list of exponents remaining on the left and right of (2), namely c, $2c$, $c+b$, $n-c$, $2n-3c$, and $n-c+b$. In this case, substituting the information obtained from the equations considered thus far we deduce that $w(x) = 1 + x^a + x^b + x^c + x^{a+c} + x^{a+2c} = f(x)$. Since $w(x) = f(x)$, no output is produced here and we continue with the last unresolved case (using one of the equations $n-c-a = c+b$ and $n-c-a = 4n-7c-3a$ if they have not been resolved yet). If after substituting into the remaining exponents in (2) there are still exponents remaining, we determine values for the least remaining exponent on both sides of (2) as before. We equate these and obtain an additional equation (or a list of equations to consider), plugging in the information obtained from such an equation back into the list of remaining exponents in (2). This process is repeated as long as necessary. In every case, it turned out that after the initial substitution and cancellation of terms that led to (11) and (12) in the example above, at most three additional substitutions were necessary (in other words, each system of equations consisted of ≤ 8 equations). A particular case ended whenever the list of equations we were considering had no solutions or had a solution leading to the cancellation of all the exponents in (2). In the former situation, we simply considered the most recent equation we had not yet considered and formed a new system of equations. In the latter case, to avoid printing out unnecessary output, we checked whether any of the following occurred: $w(x) = f(x)$, $w(x) = \tilde{f}(x)$, 0 was an exponent obtained, the inequalities $a \le b \le c \le d \le n$ (using Lemma 4) do not hold, and the inequalities $a \le k_2 \le k_3 \le k_4 \le n$ (using Lemma 4) do not hold. In any of these cases, no output was printed. Otherwise, the exponents for $f(x)$ and $w(x)$ were printed.

We now are left with interpreting the output. There were six different values for the pair $(f(x), w(x))$ that were given. One was given by

$$f(x) = 1+x^a+x^{2a}+x^{6a}+x^{8a}+x^{11a} \quad \text{and} \quad w(x) = 1+x^a+x^{6a}+x^{7a}+x^{9a}+x^{11a}.$$

This corresponds to the case $s = a$ and $t = 2a$ in the statement of Theorem 2. Another value for $f(x)$ and $w(x)$ corresponded to these same two polynomials with the role of $f(x)$ and $w(x)$ interchanged. We note that when $a = 1$ these two polynomials correspond to two of the four variations of (1) spelled out in the introduction. The other two variations of (1) did not occur as we imposed the conditions $a \le n-d$ and $k_1 \le n-k_4$ (we used this to deduce that $k_1 = a$). Recall that there is no harm in doing this as some variation of a given $f(x)$ with reducible non-reciprocal part will always arise even with these conditions. A third output obtained was with $f(x)$ as in the statement of Theorem 2, with $s = a$ and $t = b$, and $w(x) = 1 + x^a + x^{4a+b} + x^{3a+2b} + x^{5a+2b} + x^{5a+3b}$. We note that the factorization given in the statement of the theorem was done without the aid of computer. The computations however indicate that this $f(x)$ has only two irreducible non-reciprocal factors since otherwise there would have been more than one $w(x)$ obtained corresponding to this $f(x)$, and there was not. A forth output obtained was with $f(x)$ as in the statement of Theorem 2, with $s = b$ and $t = a$, and $w(x) = 1 + x^a + x^{2a+b} + x^{a+2b} + x^{3a+4b} + x^{3a+5b}$. Note that these last two outputs are the reason why we require only s and t in the statement of the theorem to be distinct and impose no condition on which of s and t is larger (though this is clear also from other considerations). The fifth and sixth outputs obtained were

$$f(x) = 1 + x^a + x^b + x^{-3a+2b} + x^{-5a+4b} + x^{-7a+5b} \quad \text{and}$$
$$w(x) = 1 + x^a + x^{-2a+b} + x^{-2a+2b} + x^{-6a+4b} + x^{-7a+5b},$$

and

$$f(x) = 1 + x^a + x^b + x^{-5a+2b} + x^{-3a+2b} + x^{-7a+3b} \quad \text{and}$$
$$w(x) = 1 + x^a + x^{-4a+b} + x^{-6a+2b} + x^{-4a+2b} + x^{-7a+3b},$$

respectively. In the fifth case, the substitution $a = t$ and $b = s + 2t$ leads to $w(x)$ being of the form given for $f(x)$ in the statement of the theorem; this implies that the $f(x)$ given in the fifth case is a variation of the $f(x)$ stated in the theorem. The substitution is justified as the exponents are listed in increasing order above (as obtained in the program) so that $0 < c - b = (-3a + 2b) - b = b - 3a$ which implies $b - 2a > a$; in other words, $a = t$ and $b = s + 2t$ is possible for some distinct positive integers s and t as in the theorem. Similarly, if we consider the substitution $a = s$ and $b = t + 4s$ in the sixth example, we deduce that the $f(x)$ obtained there is a variation of the $f(x)$ stated in the theorem. This completes the proof of the theorem.

4. Proofs of Theorem 3 and Theorem 4

We establish here the remaining results stated in the introduction.

Proof of Theorem 3. Fix $f(x)$ and ℓ as in the theorem. Observe that if α and $1/\alpha$ are roots of $f(x^\ell)$, then α^ℓ and $1/\alpha^\ell$ are roots of $f(x)$. Since $f(x)$ is irreducible and non-reciprocal, it is not possible for a number β and its reciprocal $1/\beta$ to both be roots of $f(x)$ (one should consider the possibility that $\beta = 1/\beta$ here, but then $f(x)$ is reciprocal). We deduce that $f(x^\ell)$ has no irreducible reciprocal factors.

Consider $f(x)$ as in (3). Set $g(x) = f(x^\ell)$. Suppose $w(x) = \sum_{j=0}^{s} b_j x^{k_j} \in \mathbb{Z}[x]$ with $0 = k_0 < k_1 < \ldots < k_s = \ell d_r$ and $w(x)\widetilde{w}(x) = g(x)\tilde{g}(x)$. We show that $w(x)$ must be one of $\pm g(x)$ and $\pm\tilde{g}(x)$. Once this has been established, Lemma 1 implies the theorem holds. Observe that each exponent in $g(x)\tilde{g}(x)$ is a multiple of ℓ. From Lemma 3, it follows in particular that $w(x)$ has non-negative coefficients. This implies that each power x^{k_j} occurring in $w(x)$ appears with a non-zero coefficient in the expansion of $w(x)\widetilde{w}(x)$. The equality $w(x)\widetilde{w}(x) = g(x)\tilde{g}(x)$ now implies that for each $j \in \{0, 1, \ldots, r\}$ there is an integer k'_j such that $k_j = \ell k'_j$. We deduce that $h(x)\tilde{h}(x) = f(x)\tilde{f}(x)$ where $h(x) = \sum_{j=0}^{s} b_j x^{k'_j}$. Lemma 1 now implies that $h(x) = \pm f(x)$ or $h(x) = \pm\tilde{f}(x)$. These in turn imply that $w(x)$ must be one of $\pm g(x)$ and $\pm\tilde{g}(x)$, and the theorem follows. □

Proof of Theorem 4. We show first that $C = (1+\sqrt{5})/2$ satisfies the conditions in the theorem. By the theorems of Ljunggren [2] mentioned in the introduction, the non-reciprocal part of $f(x)$ is irreducible or identically one whenever $r \le 3$. The theorem of Solan and the author [1] also mentioned there implies the same if $r = 4$. Since $2/(-1+\sqrt{5}) = (1+\sqrt{5})/2$, we obtain

$$\begin{aligned} d_{j+1} &> d_j + \left(\frac{1+\sqrt{5}}{2} - 1\right) d_j \\ &= d_j + \left(\frac{-1+\sqrt{5}}{2}\right) d_j > d_j + d_{j-1} \qquad \text{for each } j \ge 2. \end{aligned} \tag{14}$$

Theorem 2 and (14) imply the non-reciprocal part of $f(x)$ is irreducible if $r = 5$ since in the case that the non-reciprocal part of $f(x)$ is reducible in Theorem 2 we have

$$d_5 = 5s + 3t < (4s + 2t) + (2s + 2t) = d_4 + d_3$$

with a similar argument holding for each of the three other variations $f(x)$ can have in Theorem 2.

We consider now the case that $r \ge 6$. As before we consider $w(x)$ with (2), (3), and (4) holding and apply Lemma 3 so that we may take $s = r$ and each $b_j = 1$. By considering $\widetilde{w}(x)$ instead of $w(x)$, we may suppose that $k_1 \le n - k_{r-1}$ and do so. From (14), we deduce that

$$n - d_j + d_i = d_r - d_j + d_i > d_{r-2} \qquad \text{if } j \ne r.$$

It follows that the $r-1$ least exponents on the left of (2) are $0, d_1, d_2, \dots, d_{r-2}$. The condition $k_1 \le n - k_{r-1}$ implies that the least non-zero exponent on the right of (2) is k_1. Therefore, $k_1 = d_1$. Define ℓ to be the greatest positive integer $\le r$ for which $k_\ell = d_\ell$.

Assume $\ell \le r-3$. Let m denote the least non-zero exponent of $\widetilde{w}(x)$. Observe that m occurs as an exponent on the right of (2) and must be different from $d_0, d_1, \dots, d_\ell$. Since the smallest exponent on the left of (2) which is greater than d_ℓ is $d_{\ell+1}$, we obtain that $m \ge d_{\ell+1}$. On the other hand, $m > d_{\ell+1}$ is impossible since otherwise the exponent $d_{\ell+1}$ cannot occur on the right of (2). It follows that $m = d_{\ell+1}$. Observe now that (14) implies

$$d_{\ell+1} < m + d_1 < d_{\ell+2}.$$

Since $m + d_1$ is an exponent appearing on the right of (2) and since the $r-1$ least exponents on the left of (2) are $0, d_1, d_2, \dots, d_{r-2}$, we deduce that $\ell \ge r-3$. Hence, $\ell = r-3$.

We now show that $\ell = r-3$ is impossible. We consider the exponents on the left and right of (2) which are in the interval $(d_{r-2}, d_{r-2} + d_{r-3}]$. Observe that

$$n - d_j + d_i = d_r - d_j + d_i > d_{r-1} > d_{r-2} + d_{r-3} \qquad \text{if } j \le r-2.$$

If $j = r$ and $0 \le i \le r$, then $n - d_j + d_i = d_i \notin (d_{r-2}, d_{r-2} + d_{r-3}]$. Also, if $j = r-1$ and $i \ge r-3$, then $n - d_j + d_i \ge d_r - d_{r-1} + d_{r-3} > d_{r-2} + d_{r-3}$. Hence, the only possible exponents on the left of (2) which can be in $(d_{r-2}, d_{r-2} + d_{r-3}]$ are the

$r-3$ numbers $n-d_{r-1}+d_i$ with $0 \le i \le r-4$. The least exponents for $w(x)$ and $\widetilde{w}(x)$ are given by

$$w(x) = 1 + x^{d_1} + \ldots + x^{d_{r-3}} + \ldots \quad \text{and} \quad \widetilde{w}(x) = 1 + x^{d_{r-2}} + \ldots,$$

where the exponents beyond the last exponent in each of these two expressions are unknowns (but greater than the exponents shown). It follows that the exponents on the right of (2) in the interval $(d_{r-2}, d_{r-2}+d_{r-3}]$ include the $r-3$ numbers $d_{r-2}+d_j$ for $1 \le j \le r-3$. As the right side of (2) contains at least these $r-3$ numbers in $(d_{r-2}, d_{r-2}+d_{r-3}]$ and the left side of (2) contains at most the $r-3$ numbers indicated earlier, we deduce that each side contains exactly the $r-3$ exponents indicated in $(d_{r-2}, d_{r-2}+d_{r-3}]$. By ordering these lists of $r-3$ exponents on the left and right of (2) from least to greatest, we obtain

$$d_r - d_{r-1} = d_{r-2}+d_1, \;\; d_r - d_{r-1}+d_1 = d_{r-2}+d_2, \;\; d_r - d_{r-1}+d_2 = d_{r-2}+d_3, \;\; \ldots.$$

Since $r \ge 6$, we deduce that $r-3 \ge 3$ so that there are ≥ 3 equations above as shown. By considering the first and third equations, we obtain $d_3 = d_2 + d_1$, a contradiction to (14).

We now know that $\ell \ge r-2$. Still denoting by m the least non-zero exponent of $\widetilde{w}(x)$, we now have

$$w(x) = 1 + x^{d_1} + \ldots + x^{d_{r-2}} + \ldots \quad \text{and} \quad \widetilde{w}(x) = 1 + x^m + \ldots.$$

The smallest exponent $> d_{r-2}$ on the left of (2) is either d_{r-1} or $n-d_{r-1}$. Note that $m > d_{r-2}$. The missing terms for $w(x)$ above are x^{n-m} and x^n. It follows that the smallest exponent $> d_{r-2}$ on the right of (2) is either m or $n-m$. Hence, one of d_{r-1} and $n-d_{r-1}$ must equal one of m and $n-m$. Therefore, $m = d_{r-1}$ or $m = n-d_{r-1}$. If $m = n - d_{r-1}$, then $n-m = d_{r-1}$ so that $w(x) = f(x)$. Now, suppose $m = d_{r-1}$. Since $w(x) = \widetilde{\widetilde{w}}(x)$, we deduce that

$$w(x) = 1 + x^{d_1} + \ldots + x^{d_{r-2}} + x^{n-d_{r-1}} + x^n$$

and

$$\widetilde{w}(x) = 1 + x^{d_{r-1}} + x^{n-d_{r-2}} + \ldots + x^{n-d_1} + x^n.$$

Expanding both sides of (2), deleting like exponents, and comparing exponents $< n$, we are left with the exponents $n-d_{r-1}+d_j$ for $1 \le j \le r-2$ on the left and the exponents $d_{r-1}+d_j$ for $1 \le j \le r-2$ on the right. Comparing the least of these, we deduce $n-d_{r-1}+d_1 = d_{r-1}+d_1$. Hence, $n = 2d_{r-1}$. It follows that $n-d_{r-1} = d_{r-1}$. Therefore, $w(x) = f(x)$ in this case as well. By applying Lemma 1, we now deduce that the non-reciprocal part of $f(x)$ is irreducible or identically one.

To complete the proof of the theorem, it remains to show that if $C < (1+\sqrt{3})/2$, then there is an $f(x)$ as in the theorem satisfying the condition $d_{j+1} > Cd_j$ for $1 \le j \le r-1$ but with reducible non-reciprocal part. To construct such an $f(x)$, we use Theorem 2. Specifically, we take s to be a sufficiently large integer (depending on C) and t to be the integer satisfying $s\sqrt{3} < t < (s\sqrt{3})+1$. One checks directly that $f(x)$ has the desired property, completing the proof of the theorem. $\square$

Acknowledgments. This paper benefited from helpful discussions with several people. The author thanks Brian Hipp, Ralph Howard, Douglas Meade, Robert Murphy, Andrzej Schinzel, and Ognian Trifonov for such conversations.

References

[1] Filaseta, M., Solan, I., An extension of a theorem of Ljunggren. Math. Scand., to appear.

[2] Ljunggren, W., On the irreducibility of certain trinomials and quadrinomials. Math. Scand. 8 (1960), 65–70.

[3] Mills, W.H., The factorization of certain quadrinomials. Math. Scand. 57 (1985), 44–50.

[4] Schinzel, A., Reducibility of lacunary polynomials I. Acta Arith. 16 (1969/70), 123–159.

[5] — Reducibility of lacunary polynomials III. Acta Arith. 34 (1978), 227–266.

[6] — Reducibility of lacunary polynomials VI. Acta Arith. 47 (1986), 277–293.

[7] — Selected topics on polynomials. Univ. of Michigan Press, Ann Arbor 1982.

[8] Selmer, E., On the irreducibility of certain trinomials. Math. Scand. 4 (1956), 287–302.

Mathematics Department
University of South Carolina
Columbia, SC 29208
filaseta@math.sc.edu