PRACTICAL ASPECTS OF TESTING THE IRREDUCIBILITY OF THE NON-RECIPROCAL PART OF A 0, 1-POLYNOMIAL

Michael Filaseta
Dept. Mathematics, University of South Carolina, Columbia, South Carolina
filaseta@math.sc.edu

Received: 10/14/18, Accepted: 8/22/19, Published: 4/27/20

Abstract

We establish a general result concerning the irreducibility of the non-reciprocal part of $0,1$-polynomials and illustrate it with a few examples. We also use the result to show that if the gaps in consecutive elements of a sequence of positive integers increases to infinity, then when the first n of these positive integers are used as successive exponents for a $0,1$-polynomial, the non-reciprocal part of the polynomial is irreducible provided only that n is sufficiently large.

1. Introduction

A $0,1$-*polynomial* is a polynomial in which each term has coefficient 1. Thus, for example,

$$f(x) = x^{2002} + x^{1999} + x^{1996} + x^{1993} + x^{1990} + 1$$

is a $0,1$-polynomial. If $g(x)$ is a non-zero polynomial in $\mathbb{Z}[x]$, we define $\tilde{g}(x) = x^{\deg g} g(1/x)$ to be the *reciprocal of* $g(x)$. A polynomial $g(x) \in \mathbb{Z}[x]$ is said to be *reciprocal* if $g(x)$ is non-zero and $g(x) = \pm\tilde{g}(x)$. This corresponds to saying that if α is a root of $g(x)$, then $\alpha \neq 0$ and $1/\alpha$ is a root of $g(x)$. We will refer to the *reciprocal part of a polynomial* $h(x) \in \mathbb{Z}[x]$ as the product of the irreducible reciprocal factors of $h(x)$ which have a positive leading coefficient, where here and elsewhere irreducibility is in $\mathbb{Z}[x]$. The *non-reciprocal part of a polynomial* $h(x) \in \mathbb{Z}[x]$ is defined as $h(x)$ divided by its reciprocal part. Observe that if the non-reciprocal part of a polynomial $h(x)$ is irreducible, then one obtains that $h(x)$ is irreducible if and only if $\gcd(h(x), \tilde{h}(x)) = 1$ as the latter implies the reciprocal part of $h(x)$ is 1. A driving motivation then for establishing the irreducibility of the non-reciprocal part of a non-reciprocal polynomial is that it reduces determining the irreducibility of the polynomial to computing a greatest common divisor of two polynomials. This idea has been used in [2] to establish a quick method for determining whether a non-reciprocal $0,1$-polynomial is irreducible and, in a more general context, in

[3] for determining whether an arbitrary non-reciprocal polynomial in $\mathbb{Z}[x]$ is irreducible. One can often obtain information about the factorization of polynomials in $\mathbb{Z}[x]$ as well. As an example, the methods in [2] quickly lead to the example $f(x)$ above having an irreducible non-reciprocal part. A computation shows $\gcd(f(x), \tilde{f}(x)) = x^2 + 1$. Thus, $f(x)$ is in fact $x^2 + 1$ times an irreducible polynomial.

The reciprocal part of a polynomial $h(x) \in \mathbb{Z}[x]$ divides $\gcd(h(x), \tilde{h}(x))$ in $\mathbb{Q}[x]$. On the other hand, examples like $h(x) = (x^3 + x + 1)(x^3 + x^2 + 1)$ show that $\gcd(h(x), \tilde{h}(x))$ can contain some irreducible non-reciprocal factors of $h(x)$. We will justify in the next section, nevertheless, that $0, 1$-polynomials $h(x)$ have the interesting property that the reciprocal part of $h(x)$ is simply $\gcd(h(x), \tilde{h}(x))$ so that in this case the non-reciprocal part of $h(x)$ is $h(x)/\gcd(h(x), \tilde{h}(x))$.

In this paper, we focus on results related to the irreducibility of the non-reciprocal part of $0, 1$-polynomials. Such polynomials are easier to tackle (see Theorem 4) allowing us to obtain some interesting results. For example, we will show that the non-reciprocal parts of the polynomials with $n + 1$ terms given by

$$\begin{gathered} 1 + x + x^4 + x^9 + \cdots + x^{n^2}, \\ 1 + x + x^2 + x^4 + x^8 + \cdots + x^{2^{n-1}}, \\ 1 + x^{f_2} + x^{f_3} + x^{f_4} + \cdots + x^{f_{n+1}}, \end{gathered} \tag{1}$$

where $f_0 = 0$, $f_1 = 1$, and $f_{n+1} = f_n + f_{n-1}$ for $n \geq 1$ are the Fibonacci numbers, are irreducible if $n \geq 2$, $n \geq 3$ and $n \geq 4$, respectively. These polynomials are just examples, and the methods we describe can be used in a very general context. Nevertheless, we delve into these specific examples a little further and determine a possible complete factorization of these polynomials; the author is reluctant to call these possible factorizations conjectures only because the data is somewhat limited, but nevertheless includes information on polynomials with degrees considerably larger than what direct computations using existing factoring routines allow.

This paper was motivated by considering a variation of the following result from [1].

Theorem 1. *Let n be a positive integer, and let $a_0, a_1, \ldots, a_n$ be integers satisfying $0 = a_0 < a_1 < \cdots < a_n$. There exists an absolute constant $C > 1$ such that if $a_{j+1} > Ca_j$ for each $j \in \{1, 2, \ldots, n-1\}$, then the non-reciprocal part of $f(x) = \sum_{j=0}^{n} x^{a_j}$ is either irreducible or identically one. Furthermore, if C' denotes the infimum of such C, then*

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

This result is asserting that if the exponents on a $0, 1$-polynomial increase fast enough, then its non-reciprocal part is irreducible. The lower bound on C' above,

however, exists solely because of examples with few terms which have a reducible non-reciprocal part. It seemed likely to the author that a considerably stronger result should be possible if one starts with an infinite sequence $a_0, a_1, \ldots$ with $0 = a_0 < a_1 < \cdots$ and only wants the non-reciprocal part of $f_n(x) = \sum_{j=0}^{n} x^{a_j}$ to be irreducible or identically 1 for large enough n. With this in mind, we will establish the following, which neither implies nor is implied by Theorem 1.

Theorem 2. *Let $a_0, a_1, a_2, \ldots$ be a sequence satisfying $0 = a_0 < a_1 < a_2 < \cdots$,*

$$a_{k+1} - a_k \leq a_{k+2} - a_{k+1} \leq a_{k+3} - a_{k+2} \leq \cdots \quad \text{for some } k \in \mathbb{Z}^+,$$

and

$$\lim_{j\to\infty} (a_j - a_{j-1}) = \infty. \tag{2}$$

Then there is an N, depending on the sequence, such that for all $n \geq N$, the non-reciprocal part of $\sum_{j=0}^{n} x^{a_j}$ is irreducible.

The proof is constructive, so the value of N can be determined based on sufficient knowledge of the sequence a_j. Also, observe that Theorem 2 implies that the three examples in (1) each have an irreducible non-reciprocal part if n is sufficiently large. On the other hand, Theorem 1 only applies to the irreducibility of the non-reciprocal part of the second example in (1) (though it was noted already in [1] that the irreducibility of the non-reciprocal part of the third example follows with some extra effort).

2. Preliminary Observations

In the introduction, we indicated that if $h(x)$ is a $0,1$-polynomial, then the reciprocal part of $h(x)$ is $\gcd(h(x), \tilde{h}(x))$ and the non-reciprocal part of $h(x)$ is given by $h(x)/\gcd(h(x), \tilde{h}(x))$. This does not appear to have been noticed before. However, the following related result can be found in [2].

Lemma 1. *Let $f(x)$ be a reciprocal $0,1$-polynomial. Then $f(x)$ is not divisible by a non-reciprocal polynomial in $\mathbb{Z}[x]$.*

We show here that the following is a consequence of this lemma from which the comments on $h(x)$ above follow.

Theorem 3. *Let $f(x)$ be a non-zero $0,1$-polynomial. Then the reciprocal part of $f(x)$ is equal to $\gcd\big(f(x), \tilde{f}(x)\big)$.*

Proof. We will use that every factor $w(x)$ in $\mathbb{Z}[x]$ of a $0,1$-polynomial $f(x)$ satisfying $f(0) = 1$ is a monic polynomial with constant term 1 or the negative of such a monic polynomial; this holds since otherwise $w(x)$ has a positive real root which is

impossible since the non-zero coefficients of the multiple $f(x)$ of $w(x)$ are positive. In particular, if $w(x)$ is also reciprocal, then $\widetilde{w}(x) = w(x)$.

Let $g(x) = \gcd\big(f(x), \tilde{f}(x)\big)$. The definition of $\tilde{f}(x)$ implies $\tilde{f}(0) = 1$. Since $g(x)$ is a monic polynomial in $\mathbb{Z}[x]$, we deduce that $g(0) = 1$. If $w(x) \in \mathbb{Z}[x]$ is an irreducible reciprocal polynomial for which $w(x)^k$ divides $f(x)$, then we can write

$$f(x) = w(x)^k f_0(x),$$

for some $f_0(x) \in \mathbb{Z}[x]$. Note that there is a nonnegative integer s and a $0,1$-polynomial $f_1(x)$ with $f_1(0) = 1$ such that $f(x) = x^s f_1(x)$. The definition of a reciprocal polynomial implies that $w(x)$ is not x. Thus, $w(x)$ divides $f_1(x)$. From the comments above, we deduce $\widetilde{w}(x) = w(x)$. The definition of reciprocal now implies

$$\tilde{f}(x) = \widetilde{w}(x)^k \tilde{f}_0(x) = w(x)^k \tilde{f}_0(x).$$

Therefore, $w(x)^k$ divides $\tilde{f}(x)$, and we deduce that $g(x)$ is divisible by the reciprocal part of $f(x)$.

Now, assume that there is a non-reciprocal polynomial $w(x)$ such that $w(x)$ divides $g(x)$. Then $w(x)$ divides both $f(x)$ and $\tilde{f}(x)$. Let m be an integer exceeding $\deg f$. Set $F(x) = f(x)x^m + \tilde{f}(x)$. Then one checks that $\widetilde{F}(x) = F(x)$ so that $F(x)$ is a reciprocal $0,1$-polynomial. Since $w(x)$ divides both $f(x)$ and $\tilde{f}(x)$, we see that $F(x)$ has the non-reciprocal factor $w(x)$. This contradicts Lemma 1. Hence, $g(x)$ does not have any irreducible non-reciprocal factors, and the theorem follows. □

Another observation we make is that although our interest is in $0,1$-polynomials in this paper, we will be interested in their non-reciprocal parts and these can be rather different in appearance from the $0,1$-polynomials themselves. For example, the polynomial we started with in the introduction was a $0,1$-polynomial of degree 2002 with 6 terms. Its non-reciprocal part is a polynomial with over 1000 terms and has coefficients which are 1 and coefficients which are -1. To elaborate on this observation, we show that there are polynomials $f(x)$ where the non-reciprocal part of $f(x)$ has many more terms than $f(x)$ and has maximal coefficient any prescribed positive integer one wants (or minimal coefficient any prescribed negative integer). For integers m and k satisfying $m > k \geq 1$, set

$$\begin{aligned} f_{m,k}(x) &= \sum_{j=0}^{k-1} x^{2m+2j+1} + x^{m+k-1} + x^{m+k-2} + \sum_{j=0}^{k-1} x^{2j} \\ &= x^{m+k-1} + x^{m+k-2} + \sum_{j=0}^{k-1} x^{2j}(x^{2m+1} + 1). \end{aligned}$$

By factoring out $x+1$ from the first two terms on the right and from each summand

on the right, we see that $f_{m,k}(x) = (x+1)\, g_{m,k}(x)$, where

$$g_{m,k}(x) = x^{m+k-2} + \sum_{t=0}^{2m+2k-2} (-1)^t \min\left\{ \left\lfloor \frac{t}{2} \right\rfloor + 1, \left\lfloor \frac{2m+2k-t}{2} \right\rfloor, k \right\} x^t.$$

As any reciprocal factor of $f_{m,k}(x)$ must also be a reciprocal factor of $\tilde{f}_{m,k}(x)$, we deduce from

$$\tilde{f}_{m,k}(x) - f_{m,k}(x) = x^{m+k-2}(x-1)(x+1)^2,$$

that the only possible irreducible reciprocal factors of $f_{m,k}(x)$ are $x-1$ and $x+1$. Since $f_{m,k}(x)$ only has positive coefficients, $f_{m,k}(1) \neq 0$. Furthermore, one can check that

$$f'_{m,k}(-1) = k(2m+1) + (-1)^{m+k} \neq 0.$$

Hence, the non-reciprocal part of $f_{m,k}(x)$ is $g_{m,k}(x)$. For fixed k and m large with $m+k$ odd, one sees that the maximum coefficient of $g_{m,k}(x)$ is k and the minimum coefficient is $-k$. Furthermore, $f_{m,k}(x)$ has $2k+2$ terms and $g_{m,k}(x)$ has $2m+2k-1$ terms. As k is an arbitrary positive integer and m can be an arbitrarily large positive integer, $g_{m,k}(x)$ can have many more terms than $f_{m,k}(x)$.

3. Background and a General Result

Our main source of information comes from a result in [1] based on an idea of Ljunggren [5]. The basic idea is that if $f(x) \in \mathbb{Z}[x]$ factors as a product of two non-reciprocal polynomials $u(x)$ and $v(x)$ in $\mathbb{Z}[x]$, then one can consider the polynomial $w(x) = u(x)\tilde{v}(x)$ and it will have the same Euclidean norm as $f(x)$. In other words, the sum of the squares of the coefficients of $f(x)$ will equal the sum of the squares of the coefficients of $w(x)$. In the case that $f(x)$ is a $0,1$-polynomial, with some further arguments, one gets the following (see [1]).

Theorem 4. *Let $f(x)$ be a $0,1$-polynomial with $f(0) = 1$. Then the non-reciprocal part of $f(x)$ is reducible if and only if there exists a $0,1$-polynomial $w(x)$ with the same number of non-zero terms as $f(x)$ satisfying $w(x) \neq f(x)$, $w(x) \neq \tilde{f}(x)$ and*

$$w(x)\widetilde{w}(x) = f(x)\tilde{f}(x). \tag{3}$$

Let n be an integer which is at least 2, and let $a_0, a_1, \ldots, a_n$ be integers satisfying $0 = a_0 < a_1 < \cdots < a_n$. Let $f(x) = \sum_{j=0}^{n} x^{a_j}$. To apply the above theorem, we write

$$w(x) = \sum_{j=0}^{n} x^{k_j},$$

where k_j are nonnegative integers satisfying $k_0 < k_1 < \cdots < k_n$. Condition (3) implies $k_0 = 0$ and $k_n = a_n$. We imagine expanding the right and left sides of (3).

On the right, the non-constant term of least degree will have degree a_1 or $a_n - a_{n-1}$. We consider the case that $a_n - a_{n-1} > a_1$ so that this least degree is a_1. As the non-constant term of least degree on the left of (3) is either a term in $w(x)$ or a term in $\widetilde{w}(x)$ and since we can interchange the roles of $w(x)$ and $\widetilde{w}(x)$ in Theorem 4, we can suppose that $w(x)$ is of the form $1 + x^{a_1} + \cdots + x^{a_n}$, where the $n-2$ terms between x^{a_1} and x^{a_n} are still to be determined. Observe also that $a_n - a_{n-1} > a_1$ implies that $f(x)$ is not reciprocal. This then implies that the non-reciprocal part of $f(x)$ is not a constant. With regard to Theorem 4, we deduce that if the non-reciprocal part of $f(x)$ is not reducible, then it is irreducible.

We are ready now to state our main new apparatus for obtaining the consequences mentioned in the introduction.

Theorem 5. *Let n be an integer which is at least 2, and let $a_0, a_1, \ldots, a_n$ be integers satisfying $0 = a_0 < a_1 < \cdots < a_n$. Let $f(x) = \sum_{j=0}^{n} x^{a_j}$. Let $w(x) = 1 + x^{a_1} + \cdots + x^{a_n}$ be as in Theorem 4, where the terms between x^{a_1} and x^{a_n} are unknowns. Suppose, for some integers $i \in [1, k-1]$, $s \in [1, k-i]$, $k \in [i+s, n)$ and $\ell \in [k+1, n]$, that each of the following holds.*

(i) We have the element relations

$$\begin{aligned} a_i &\notin \{a_n - a_v : k+2 \le v \le n-1\}, \\ a_{i+s} &\notin \{a_n - a_{v'} : k+2 \le v' \le n-1\}, \\ a_{i+s} &\notin \{a_{u'} - a_{k'} : k+1 \le k' < u' \le \ell - 1\}, \\ a_{i+s} - a_i &\notin \{a_{u'} - a_u : 0 \le u < u' \le i+s-1\}. \end{aligned}$$

(ii) The inequalities

$$\begin{aligned} a_{k+1} - a_k &\le a_{k+2} - a_{k+1} \le \cdots \le a_\ell - a_{\ell-1}, \\ a_n - a_{n-1} &> \max\{a_1, a_{i+s} - a_i + a_{i-1}\}, \\ a_{k+2} - a_{k+1} &> \max\{a_i, a_{i+s} - a_i + a_{i-1}\}. \end{aligned}$$

are satisfied.

(iii) The polynomial $w(x)$ is $w_0(x)$ plus a $0,1$-polynomial, where

$$w_0(x) = 1 + x^{a_1} + \cdots + x^{a_{k-1}} + x^{a_k} + x^{a_\ell} + x^{a_{\ell+1}} + \cdots + x^{a_{n-1}} + x^{a_n},$$

and $w_0(x)$ and $\widetilde{w}_0(x)$ contain all the terms of $w(x)$ and $\widetilde{w}(x)$ up to and including degree a_k, respectively.

Then the non-reciprocal part of $f(x)$ is irreducible.

The choices of subscripts in the sets in (i) are somewhat arbitrary but agree with the notation used in the proof we present. The conditions (i), (ii) and (iii) in Theorem 5 may appear cumbersome. To help understand them, we illustrate how to use the result before proving it by presenting a proof of Theorem 2 and some examples.

Proof of Theorem 2. We establish the theorem by showing that, for n sufficiently large, $f(x) = \sum_{j=0}^{n} x^{a_j}$ satisfies the conditions in Theorem 5. Fix an $i \geq 1$. For any positive integer s, the largest element of the set $\{a_{u'} - a_u : 0 \leq u < u' \leq i+s-1\}$ is $a_{i+s-1} - a_0 = a_{i+s-1}$. By (2), for s sufficiently large, we have $a_{i+s} - a_{i+s-1} > a_i$. This will ensure that the fourth condition in (i) is satisfied. Fix such an $s \geq 1$. Similarly, the conditions in the theorem imply that, for $k \geq i+s$ sufficiently large, we have

$$a_{i+s} < a_{k+1} - a_k \leq a_{k+2} - a_{k+1} \leq a_{k+3} - a_{k+2} \leq \cdots .$$

Fix such a k. Now, for $\ell = n \geq k+1$, we see that all the conditions in (i) and (ii) of Theorem 5 are satisfied.

We are left with showing that, for $\ell = n$ sufficiently large, condition (iii) of Theorem 5 holds, where i, s, and k are fixed as above. By (2), there is a positive integer $k_2 > k$ such that

$$a_{k'+1} - a_{k'} > a_k \quad \text{for all } k' \geq k_2.$$

Let k_3 be a positive integer for which

$$a_{k_3} > a_{k_2} + a_{k_2-1}.$$

We take n large enough so that

$$a_n - a_{n-1} > a_{k_3+1}.$$

This implies then that the terms of $\tilde{f}(x)$ other than the constant term have degree greater than a_{k_3+1}. Thus, the terms of $f(x)\tilde{f}(x)$ of degree less than or equal to a_{k_3+1} are given by

$$f_0(x) = 1 + x^{a_1} + \cdots + x^{a_{k_3+1}}.$$

Let $w(x) = 1 + x^{a_1} + \cdots + x^{a_n}$ be as in Theorem 5, and assume $w(x)$ is not of the form written in (iii). We write $w(x) = w_1(x) + w_2(x) + w_3(x)$, where $w_1(x)$ contains all the terms of $w(x)$ of degree less than or equal to a_{k_2}, $w_3(x)$ contains all the terms of $w(x)$ of degree at least $a_n - a_{k_2}$, and $w_2(x)$ contains all the remaining terms of $w(x)$. Observe that the terms of $\widetilde{w}(x)$ of degree up to a_{k_2} correspond to the terms of $\widetilde{w}_3(x) = x^{a_n} w_3(1/x)$. Since the terms of $f(x)\tilde{f}(x) = w(x)\widetilde{w}(x)$ of degree up to a_{k_2} have degree a_j for some $j \leq k_2$, each term of $w_1(x)$ and $\widetilde{w}_3(x)$ must be of this form. Since, by assumption, $w(x)$ is not of the form written in (iii), there is a term $x^{a_{j_1}}$ in $\widetilde{w}_3(x)$ with $2 \leq j_1 \leq k$. Fix such a $j_1 \leq k$. Let $j_2 \leq k_2$ be maximal such

that $x^{a_{j_2}}$ is a term in $w(x)$, and let $j_3 \leq k_2$ be maximal such that $x^{a_{j_3}}$ is a term in $\widetilde{w}(x)$. Observe that $j_2 \neq j_3$ since otherwise $f(x)\tilde{f}(x) = w(x)\widetilde{w}(x)$ would have a term $2x^{a_{j_2}}$ contradicting the value of $f_0(x)$ above. Thus,

$$a_{j_2} + a_{j_3} \leq a_{k_2} + a_{k_2-1} < a_{k_3}.$$

Therefore, there is a j (for example, one can take $j = k_3$) such that the term x^{a_j} in $f_0(x)$ does not appear in the product $w_1(x)\widetilde{w}_3(x)$. Let j' be the minimal such j. From the definitions of $w_1(x)$, $w_3(x)$ and $f_0(x)$, we see that $k_2 < j' \leq k_3$. Also, $x^{a_{j'}}$ is the term in $f(x)\tilde{f}(x) - w_1(x)\widetilde{w}_3(x) = w(x)\widetilde{w}(x) - w_1(x)\widetilde{w}_3(x)$ of least degree. By considering the term in $w(x)$ of least degree exceeding a_{k_2} and the term in $\widetilde{w}(x)$ of least degree exceeding a_{k_2}, we see that $x^{a_{j'}}$ is a term in $w(x)$ or a term in $\widetilde{w}(x)$.

If $x^{a_{j'}}$ is a term in $w(x)$, then $w(x)\widetilde{w}(x)$ contains terms with degrees $a_{j'}$ and $a_{j'} + a_{j_1}$. These two degrees are greater than a_{k_2}, at most $a_{k_3} + a_k$, and differ by at most a_k. Since $k_3 > k_2$, we see that $a_{k_3} + a_k < a_{k_3+1}$. Since the terms of $f(x)\tilde{f}(x) = w(x)\widetilde{w}(x)$ of degree at most a_{k_3+1} are given by $f_0(x)$ which has no two terms with degrees greater than a_{k_2} and degrees differing by at most a_k, we obtain a contradiction.

If $x^{a_{j'}}$ is a term in $\widetilde{w}(x)$, then $w(x)\widetilde{w}(x)$ contains terms with degrees $a_{j'}$ and $a_{j'} + a_1$. These degrees are greater than a_{k_2}, at most $a_{k_3} + a_1 < a_{k_3+1}$, and differ by a_1. Again, this contradicts that the terms of $f(x)\tilde{f}(x) = w(x)\widetilde{w}(x)$ of degree at most a_{k_3+1} are given by $f_0(x)$.

Hence, our assumption that $w(x)$ is not of the form written in (iii) is contradicted for $\ell = n$ sufficiently large. Furthermore, the inequality $a_n - a_{n-1} > a_{k_3+1} > a_k$ and the value of $f_0(x)$ ensure that $\widetilde{w}(x)$ has no terms besides 1 of degree less than or equal to a_k. Thus, (iii) and the corollary follow. □

The value of N in Theorem 2 can in general be determined by following the steps of the arguments above. Given a particular sequence a_j, the following idea can also be used often to show that condition (iii) in Theorem 5 holds. Suppose that we have found i, s, and k, and we want to show that, for $\ell = n$ sufficiently large, the condition in (iii) holds. The idea is to adjust k first so that also

$$1 + x^{a_1} + \cdots + x^{a_k}$$

is irreducible and, if possible, $a_{k+1} > a_k + a_{k-1}$. Then we can also show that condition (iii) holds in this situation by simply taking n as before so that the conditions in (i) and (ii) hold but also so that

$$a_n - a_{n-1} > a_k + a_{k-1}.$$

To see this, observe that with this condition the smallest non-constant degree term of $\tilde{f}(x)$ is of degree larger than $a_k + a_{k-1}$. Since $a_{k+1} > a_k + a_{k-1}$, the terms of

$f(x)\tilde{f}(x)$ of degree no more than $a_k + a_{k-1}$ are given by

$$1 + x^{a_1} + \cdots + x^{a_k}.$$

Recall Theorem 4 implies $f(x)\tilde{f}(x) = w(x)\widetilde{w}(x)$ and both $f(x)$ and $w(x)$ are $0,1$-polynomials with $n+1$ terms and constant term 1. It follows that each term in $w(x)$ and $\widetilde{w}(x)$ of degree at most $a_k + a_{k-1}$ is of the form x^{a_j} for some $j \in \{0, 1, \ldots, k\}$. For each $j \in \{1, \ldots, k\}$, since the coefficient of x^{a_j} in $f(x)\tilde{f}(x)$ is 1, at most one of $w(x)$ and $\widetilde{w}(x)$ will contain the term x^{a_j}. Write

$$w(x) = w_1(x) + x^{a_k + a_{k-1} + 1} w_2(x) \quad \text{and} \quad \widetilde{w}(x) = w_3(x) + x^{a_k + a_{k-1} + 1} w_4(x),$$

where the $w_j(x)$ are $0,1$-polynomials with $\deg w_1 \le a_k$ and $\deg w_3 \le a_k$. In fact, we necessarily have $\deg w_1 + \deg w_3 \le a_k + a_{k-1}$. Since $f(x)\tilde{f}(x) = w(x)\widetilde{w}(x)$ and $w(x)\widetilde{w}(x)$ is $w_1(x)w_3(x)$ plus terms of degree more than $a_k + a_{k-1}$, we deduce that

$$w_1(x)w_3(x) = 1 + x^{a_1} + \cdots + x^{a_k}.$$

Since x^{a_1} is a term of $w(x)$, we have $\deg w_1(x) \ge a_1 > 0$. The irreducibility of $1 + x^{a_1} + \cdots + x^{a_k}$ now implies that $w_3(x) = 1$ and (iii) holds with $\ell = n$.

The above illustrates then some rather general situations where Theorem 5 can be applied. To further demonstrate the usefulness of this theorem and the above idea, we turn to a few examples before giving the proof of the theorem.

Example 1. For n a positive integer, define

$$f_n(x) = 1 + x + x^4 + x^9 + \cdots + x^{n^2}.$$

Thus, $a_j = j^2$ for $j \in \{0, 1, 2, \ldots\}$. We follow the discussion above. We first choose $i = 1$, then $s = 1$ and then $k = i + s = 2$. For $\ell = n$ and $n \ge 3$, one can see then that all the conditions in (i) and (ii) are satisfied. The polynomial $1 + x + x^4$ is irreducible, and for $n \ge 4$ we have

$$a_n - a_{n-1} \ge a_4 - a_3 = 16 - 9 = 7 > 5 = a_2 + a_1 = a_k + a_{k-1}.$$

Furthermore, $a_{k+1} = a_3 = 9 > 5 = a_k + a_{k-1}$. Hence, as shown above, Theorem 5 (iii) also holds, and we deduce that the non-reciprocal part of $f_n(x)$ is irreducible for $n \ge 4$. One can check directly that the non-reciprocal part of $f_n(x)$ is irreducible for $n \in \{2, 3\}$ as well. We note that $f_n(x)$ is not irreducible for all n. In fact, $x + 1$ is a factor for all odd n since $f_n(-1)$ is easily seen to be 0 for such n.

Computationally, it appears that $f_n(x)$ in Example 1 is irreducible if $n \ge 2$ is even and is the product of

$$P_n(x) = \Bigg(\prod_{\substack{d \mid (n+1) \\ d \equiv 2 \pmod 4}} \Phi_d(x) \Bigg) \Bigg(\prod_{\substack{d \mid (2n),\, d > 2 \\ d \equiv 2 \pmod 4}} \Phi_d(x) \Bigg)$$

and an irreducible polynomial if $n \geq 3$ is odd, where $\Phi_n(x)$ denotes the n^{th} cyclotomic polynomial. We sketch here an explanation for why $P_n(x)$ divides $f_n(x)$ when n is odd. First, one can show that $P_n(x)$ can be rewritten as

$$P_n(x) = \frac{(x^m+1)(x^n+1)}{x+1},$$

where m is the largest odd divisor of $n+1$. Since n and $n+1$ are relatively prime, it is not hard to see that $x+1$ is the only common factor of x^m+1 and x^n+1. Thus, it suffices to show that each of x^m+1 and x^n+1 divides $f_n(x)$. Let ζ be a root of x^n+1. Then $\zeta^n = -1$ and $\zeta^{2n} = 1$. Since n is odd, for each integer j, we have

$$\zeta^{(n-j)^2} = \left(\zeta^n\right)^n \left(\zeta^{2n}\right)^{-j} \zeta^{j^2} = -\zeta^{j^2}.$$

This is enough to see that $f_n(x)$ is divisible by x^n+1. Let ξ denote a root of x^m+1 so that $\xi^m = -1$ and $\xi^{2m} = 1$. As m is odd, one checks here that for integers u and v, we have

$$\xi^{(um+v)^2} = \left(\xi^{m^2}\right)^{u^2} \xi^{v^2} = (-1)^u \xi^{v^2} = \left(\xi^{m^2}\right)^u \xi^{v^2}.$$

Then $f_n(\xi)$ can be written as

$$(1+\xi+\xi^4+\cdots+\xi^{(m-1)^2})\left(1+\left(\xi^{m^2}\right)+\left(\xi^{m^2}\right)^2+\cdots+\left(\xi^{m^2}\right)^{(n+1-m)/m}\right).$$

As noted above, each of the expressions $\left(\xi^{m^2}\right)^u$ is $(-1)^u$. Also, $(n+1-m)/m$ is odd, so $f_n(\xi) = 0$ and $f_n(x)$ is divisible by x^m+1. Thus, $P_n(x)$ divides $f_n(x)$. Given that the non-reciprocal part of $f_n(x)$ is irreducible, we can and have verified that $f_n(x)/P_n(x)$ is irreducible for $4 \leq a_n \leq 250000$ (that is, for $2 \leq n \leq 500$) by showing for such n that

$$\gcd(f_n(x), \tilde{f}_n(x)) = \begin{cases} 1 & \text{if } n \equiv 0 \pmod 2 \\ P_n(x) & \text{if } n \equiv 1 \pmod 2. \end{cases}$$

Example 2. For n a positive integer, define

$$f_n(x) = 1 + x + x^2 + x^4 + x^8 + \cdots + x^{2^{n-1}}.$$

Thus, $a_0 = 0$ and $a_j = 2^{j-1}$ for $j \geq 1$. We choose $i = 1$, then $s = 2$ and then $k = 4$. Conditions (i) and (ii) of Theorem 5 are satisfied then for $\ell = n \geq 6$. One checks that $a_n - a_{n-1} \geq a_{k+1} > a_k + a_{k-1}$ and $f_4(x)$ is irreducible and that the non-reciprocal part of $f_n(x)$ is irreducible for all $n \in \{3,4,5\}$. Hence, Theorem 5 implies that the non-reciprocal part of $f_n(x)$ is irreducible for all $n \geq 3$.

It may be interesting to know more about these polynomials. One can check computationally as with the first example above up to degree 250000 or more, but this is not much information to go on since $f_{19}(x)$ already has degree over 250000.

The polynomials $f_n(x)$ up to degree 1048576 (that is, for $3 \le n \le 21$) were verified as irreducible except for the cases where $n \in \{4, 10, 12, 18\}$; in other words, we verified that $\gcd\left(f_n(x), \tilde{f}_n(x)\right) = 1$ for $3 \le n \le 21$ with $n \notin \{4, 10, 12, 18\}$. In the case that $n \in \{4, 10, 12, 18\}$, we have $f_n(x)$ is $\Phi_{n+1}(x)$ times an irreducible polynomial. The polynomial $f_n(x)$ has $n+1$ terms and in these cases $n+1$ is a prime and 2 is a primitive root modulo that prime causing the exponents of $f_n(x)$ modulo $n+1$ to be $0, 1, 2, \ldots, n$. Hence, $\Phi_{n+1}(x)$ is indeed a divisor of $f_n(x)$ when $n+1$ is a prime with 2 as a primitive root. Based on this small sampling, it appears that $f_n(x)$ is irreducible unless $n+1 \ge 5$ is a prime with 2 as a primitive root, and in the latter case $f_n(x)$ is $\Phi_{n+1}(x)$ times an irreducible polynomial. We verified using the test for divisibility by a cyclotomic polynomial given in [4] that $f_n(x)$ does not have a cyclotomic divisor unless $n+1$ is a prime and 2 is primitive root modulo $n+1$ in the extended range $n \le 36$ (so for all $f_n(x)$ of degree no more than 5×10^{10}).

Example 3. For n a positive integer, let f_n be the sequence of Fibonacci numbers, so $f_0 = 0$, $f_1 = 1$, and $f_n = f_{n-1} + f_{n-2}$ for $n \ge 2$. We consider the 0, 1-polynomials $F_n(x)$ formed by using the set of distinct Fibonacci numbers in order as exponents. Thus, $F_0(x) = 1$ and

$$F_n(x) = 1 + x^{f_2} + x^{f_3} + x^{f_4} + \cdots + x^{f_{n+1}} \quad \text{for } n \ge 1.$$

In the notation of Theorem 5, we can write

$$a_j = \begin{cases} 0 & \text{if } j = 0 \\ f_{j+1} & \text{if } j \ge 1. \end{cases}$$

Set $i = 1$ and $s = 3$. We cannot appeal to the idea explained before Example 1 since the condition $a_{k+1} > a_k + a_{k-1}$ will not be satisfied for $k \ge i + s = 4$. We argue that we can take $k = 5$ nonetheless. For this argument, we take $\ell = n \ge 8$ so that

$$a_n - a_{n-1} \ge a_8 - a_7 = f_9 - f_8 = 34 - 21 = 13.$$

One checks that the conditions of (i) and (ii) all hold. Given $a_n - a_{n-1} \ge 13$, the only term of $\tilde{f}(x)$ of degree less than 13 is the term 1, and hence the only terms of $f(x)\tilde{f}(x)$ of degree less than 13 are given by

$$1 + x + x^2 + x^3 + x^5 + x^8.$$

Starting with

$$w(x) = 1 + x^{a_1} + \cdots + x^{a_n},$$

where the missing terms are unknowns, we want to argue first that x^2 must be a term in $w(x)$. If it is not, then $\widetilde{w}(x)$ contains the terms in $1 + x^2$. The term x in $w(x)$ times the term x^2 in $\widetilde{w}(x)$ accounts for the term x^3 in $f(x)\tilde{f}(x)$. We see then

that x^5 must be a term in $w(x)$ or $\widetilde{w}(x)$ so that $f(x)\tilde{f}(x) = w(x)\widetilde{w}(x)$. But if x^5 is a term in $w(x)$, then $w(x)\widetilde{w}(x)$ has a term of degree $5+2=7$, contradicting that $f(x)\tilde{f}(x)$ has no such term; and if x^5 is a term in $\widetilde{w}(x)$, then $w(x)\widetilde{w}(x)$ has a term of degree $1+5=6$, contradicting that $f(x)\tilde{f}(x)$ has no term of degree 6. Therefore, we must have that x^2 is a term in $w(x)$ and not $\widetilde{w}(x)$. Next, we see that x^3 must be a term in $w(x)$ or $\widetilde{w}(x)$. If x^3 is a term in $\widetilde{w}(x)$, then $w(x)\widetilde{w}(x)$ has a term of degree $1+3=4$, contradicting that $f(x)\tilde{f}(x)$ has no such term. Hence, x^3 must be a term in $w(x)$. Now, we see that x^5 is a term in $w(x)$ or $\widetilde{w}(x)$. If x^5 is a term in $\widetilde{w}(x)$, then $w(x)\widetilde{w}(x)$ has a term of degree $1+5=6$, contradicting that $f(x)\tilde{f}(x)$ has no such term. Similarly, x^8 cannot be a term of $\widetilde{w}(x)$ since otherwise x^9 would be a term in $f(x)\tilde{f}(x) = w(x)\widetilde{w}(x)$ and it is not. Thus, $w(x)$ includes all the terms in $1+x+x^2+x^3+x^5+x^8$ and no others of degree less than 13 and the only term of $\widetilde{w}(x)$ of degree less than 13 is the term 1. This establishes (iii) in Theorem 5. After checking $n \in \{4,5,6,7\}$ directly, we deduce that the non-reciprocal part of $F_n(x)$ is irreducible for all $n \geq 4$.

By computing $\gcd(F_n(x), \widetilde{F}_n(x))$, we verified that $F_n(x)$ is irreducible in $\mathbb{Z}[x]$ for $n \leq 27$ (so for $\deg F_n \leq 317811$) except for $n \in \{5,8,11\}$. For $n=5$, the polynomial $F_n(x)$ is $x+1$ times an irreducible polynomial. For $n \in \{8,11\}$, the polynomial $F_n(x)$ is x^2+x+1 times an irreducible polynomial. We further checked using the approach in [4] that for $n \notin \{5,8,11\}$ and $n \leq 49$ (so for $\deg F_n \leq 10^{10}$) that $F_n(x)$ has no cyclotomic factor. Thus, it appears as if $F_n(x)$ is irreducible for $n \geq 12$; but as indicated in the introduction, this is not based on a lot of evidence.

4. The Proof of Theorem 5

We apply Theorem 4. We want to show that necessarily $w(x) = f(x)$ and do so by induction on $k+n-\ell$. As $w_0(x)$ has $k+n-\ell+2$ terms and $w(x)$ has $n+1$ terms, we will be done if $k+n-\ell = n-1$ or, in other words, if $\ell = k+1$. So we suppose $\ell > k+1$. Conditions (i) and (ii) of the theorem are stated in such a way that if i, s, and n are fixed, then the conditions remain valid if we increase k or decrease ℓ. The idea behind the inductive argument is to show that we can either increase k or decrease ℓ and maintain condition (iii) of the theorem. Thus, starting with $\ell \geq k+2$, we can increase $k+n-\ell \leq n-2$ until eventually $k+n-\ell = n-1$ or, equivalently, $\ell = k+1$, and our argument will be complete.

A rough sketch of the argument is as follows. If we multiply the term $x^{a_{k+1}}$ in $f(x)$ with the constant term 1 in $\tilde{f}(x)$, we see that $f(x)\tilde{f}(x) - w_0(x)\widetilde{w}_0(x)$ has a term of degree a_{k+1} (explained in more detail in the next paragraph). Let cx^t, with $c \neq 0$, be the term in

$$f(x)\tilde{f}(x) - w_0(x)\widetilde{w}_0(x) = w(x)\widetilde{w}(x) - w_0(x)\widetilde{w}_0(x)$$

of smallest degree. We show that $c \in \{1,2\}$ and $t = \min\{a_{k+1}, a_n - a_{\ell-1}\}$. After that, we will show that if $t \neq a_{k+1}$, then $c = 1$, the expression $x^{a_{\ell-1}}$ is a term in $w(x)$, and there are no terms of $w(x)$ with degree in the interval $(a_{\ell-1}, a_\ell)$. In this case, we can replace $w_0(x)$ with

$$1 + x^{a_1} + \cdots + x^{a_k} + x^{a_{\ell-1}} + x^{a_\ell} + \cdots + x^{a_{n-1}} + x^{a_n}.$$

Finally, we will show that if $t = a_{k+1}$, then the term $x^{a_{k+1}}$ is a term in $w(x)$, there are no terms of $w(x)$ with degree in the interval (a_k, a_{k+1}), and $\widetilde{w}(x)$ has no terms of degree less than a_{k+1} other than those given by $\widetilde{w}_0(x)$. Furthermore, in this case, $x^{a_{k+1}}$ is a term in $\widetilde{w}(x)$ if and only if $c = 2$ and $a_n - a_{\ell-1} = a_{k+1}$. Here, we can replace $w_0(x)$ with either

$$1 + x^{a_1} + \cdots + x^{a_k} + x^{a_{k+1}} + x^{a_\ell} + \cdots + x^{a_{n-1}} + x^{a_n}$$

or

$$1 + x^{a_1} + \cdots + x^{a_k} + x^{a_{k+1}} + x^{a_{\ell-1}} + x^{a_\ell} + \cdots + x^{a_{n-1}} + x^{a_n}.$$

If $\ell = k+2$ and $a_n - a_{\ell-1} = a_{k+1}$, then $w_0(x)$ takes the first of these two forms. The theorem will then follow by induction on $k + n - \ell$ as described.

Observe that the terms of $f(x)\tilde{f}(x)$ obtained from multiplying a term x^{a_u} in $f(x)$ with $u \leq k$ or $u \geq \ell$ and a term $x^{a_n - a_v}$ in $\tilde{f}(x)$ with $v \leq k$ or $v \geq \ell$ correspond to terms that appear in $w_0(x)\widetilde{w}_0(x)$. Hence, these terms cancel in the difference $f(x)\tilde{f}(x) - w_0(x)\widetilde{w}_0(x)$. Thus, the terms in $f(x)\tilde{f}(x) - w_0(x)\widetilde{w}_0(x)$ are those with exponents of the form $a_u + a_n - a_v$ where either $k < u < \ell$ or $k < v < \ell$. The smallest of these exponents t is $a_{k+1} + a_n - a_n = a_{k+1}$ or $a_0 + a_n - a_{\ell-1} = a_n - a_{\ell-1}$. The corresponding coefficient of the term with this least exponent will be 1 if $a_{k+1} \neq a_n - a_{\ell-1}$ and will be 2 if $a_{k+1} = a_n - a_{\ell-1}$. This establishes the first part that we set out to show.

Suppose now that $t \neq a_{k+1}$. By the above analysis, $t = a_n - a_{\ell-1} < a_{k+1}$ and $c = 1$. Since x^t is the term in $w(x)\widetilde{w}(x) - w_0(x)\widetilde{w}_0(x)$ of minimal degree, we deduce that x^t is a term in $w(x) - w_0(x)$ or a term in $\widetilde{w}(x) - \widetilde{w}_0(x)$. Assume that x^t is a term in $w(x) - w_0(x)$. Since $a_n - t = a_{\ell-1}$, we deduce that $x^{a_{\ell-1}}$ is a term in $\widetilde{w}(x) - \widetilde{w}_0(x)$ and, hence, there is a term in $w(x)\widetilde{w}(x) - w_0(x)\widetilde{w}_0(x)$ of degree $a_k + a_{\ell-1}$. Since $f(x)\tilde{f}(x) = w(x)\widetilde{w}(x)$, we obtain that there is a term in $f(x)\tilde{f}(x) - w_0(x)\widetilde{w}_0(x)$ of degree $a_k + a_{\ell-1}$. Recall that the exponents of terms in $f(x)\tilde{f}(x) - w_0(x)\widetilde{w}_0(x)$ are of the form $a_u + a_n - a_v$ with either $k < u < \ell$ or $k < v < \ell$. So there exist such u and v satisfying

$$a_u + a_n - a_v = a_k + a_{\ell-1}. \tag{4}$$

Since x^t is a term in $f(x)\tilde{f}(x) - w_0(x)\widetilde{w}_0(x)$, we obtain from (iii) and (4) that

$$t > a_k \implies a_n - a_{\ell-1} > a_k \implies a_n > a_k + a_{\ell-1}$$

$$\implies a_v - a_u > 0 \implies v > u.$$

Since at least one of u and v exceeds k, we see that $v > k$. The inequality $a_n - a_{\ell-1} < a_{k+1}$ and (4) give that

$$a_n + a_k - a_{k+1} < a_{\ell-1} + a_{k+1} + a_k - a_{k+1} = a_{\ell-1} + a_k = a_u + a_n - a_v.$$

Therefore,

$$a_{k+1} - a_k > a_v - a_u > 0.$$

Since $v > k$ and (ii) holds, we obtain a contradiction. Hence, x^t is not a term in $w(x) - w_0(x)$, and we must have that x^t is a term in $\widetilde{w}(x) - \widetilde{w}_0(x)$. Since $t = a_n - a_{\ell-1}$, we obtain that $x^{a_{\ell-1}}$ is a term in $w(x)$. The minimality of t ensures that $\widetilde{w}(x)$ has no terms with degree in $(a_n - a_\ell, a_n - a_{\ell-1})$. Therefore, $w(x)$ has no terms of degree in $(a_{\ell-1}, a_\ell)$. This establishes what we wanted in the case $t \neq a_{k+1}$.

Now, we suppose $t = a_{k+1}$. The minimality of t implies that $w(x)$ has no terms with degree in (a_k, a_{k+1}) and $\widetilde{w}(x)$ has no terms of degree less than a_{k+1} other than those in $\widetilde{w}_0(x)$. As before, either x^t is a term in $w(x) - w_0(x)$ or x^t is a term in $\widetilde{w}(x) - \widetilde{w}_0(x)$. If $c = 2$, then, as noted before, we have $a_{k+1} = a_n - a_{\ell-1}$. In this case, $x^t = x^{a_{k+1}}$ is a term in $w(x)$ and $x^t = x^{a_n - a_{\ell-1}}$ is a term in $\widetilde{w}(x)$, and we obtain what we want. We consider now $c = 1$. Then $x^t = x^{a_{k+1}}$ is a term in exactly one of $w(x)$ and $\widetilde{w}(x)$. We want to prove the former, so we assume that x^t is a term in $\widetilde{w}(x)$ and hence in $\widetilde{w}(x) - \widetilde{w}_0(x)$. Then $w(x)\widetilde{w}(x) - w_0(x)\widetilde{w}_0(x)$ has a term of degree $t + a_i = a_{k+1} + a_i$, where i is as stated in the theorem. Since $f(x)\tilde{f}(x) = w(x)\widetilde{w}(x)$, we obtain in this case that there exist nonnegative integers u and v with either $k < u < \ell$ or $k < v < \ell$ and such that

$$a_u + a_n - a_v = a_{k+1} + a_i. \tag{5}$$

Note that $n \geq \ell > k + 1$ so that (ii) implies

$$a_n - a_{k+1} \geq a_{k+2} - a_{k+1} > a_i.$$

Hence, $a_n > a_{k+1} + a_i$ and (5) gives us that $a_v > a_u$. Therefore, $v > u$, which implies $v > k$ since at least one of u or v exceeds k. We consider cases depending on whether $a_n - a_v = a_{k+1}$, $a_n - a_v > a_{k+1}$ or $a_n - a_v < a_{k+1}$.

First, consider the case that $a_n - a_v = a_{k+1}$. In this case, $u = i < k$ from (5), so that $k < v < \ell$. We have that $f(x)$ has a term $x^{a_{k+1}}$ and $\tilde{f}(x)$ has a term $x^{a_n - a_v} = x^{a_{k+1}}$. Therefore, $2x^{a_{k+1}} = 2x^t$ will appear as a term in $f(x)\tilde{f}(x) - w_0(x)\widetilde{w}_0(x)$. As $c = 1$, we obtain a contradiction.

Next, consider the case that $a_n - a_v > a_{k+1}$. We deduce from (5) that $a_u < a_i$ with $i < k$. Thus, $u \leq i - 1$, $k < v < \ell$ and $a_n - a_v = a_{k+1} + a_i - a_u$. From the definition of s in the theorem, we have $i + s \leq k$. Hence, there is a term in $w(x)\widetilde{w}(x) - w_0(x)\widetilde{w}_0(x)$ of degree $t + a_{i+s} = a_{k+1} + a_{i+s}$. Since $f(x)\tilde{f}(x) = w(x)\widetilde{w}(x)$, we obtain in this case that there exist nonnegative integers u' and v' with either $k < u' < \ell$ or $k < v' < \ell$ and such that

$$a_{u'} + a_n - a_{v'} = a_{k+1} + a_{i+s}. \tag{6}$$

If $v' = n$, then $k < u' < \ell$ and $a_{u'} - a_{k+1} = a_{i+s}$, contradicting the third condition in (i) with $k' = k+1$. Thus, $v' < n$, and from (ii) we have

$$a_n - a_{v'} \geq a_n - a_{n-1} > a_{i+s} - a_i + a_{i-1}$$

so that (6) gives us $a_{u'} - a_{k+1} < a_i - a_{i-1}$. From (ii), we obtain

$$u' \leq k+1. \tag{7}$$

We consider three subcases depending on whether $a_n - a_{v'} = a_{k+1}$, $a_n - a_{v'} > a_{k+1}$ or $a_n - a_{v'} < a_{k+1}$.

The first subcase $a_n - a_{v'} = a_{k+1}$ is handled in the same way that we dealt with $a_n - a_v = a_{k+1}$. We obtain from $a_n - a_{v'} = a_{k+1}$ that $u' = i+s \leq k$, $k < v' < \ell$ and $2x^{a_{k+1}}$ is a term in $f(x)\tilde{f}(x) - w_0(x)\widetilde{w}_0(x)$, giving $c = 2$ and a contradiction.

For the second subcase where $a_n - a_{v'} > a_{k+1}$, we deduce from (6) that $a_{u'} < a_{i+s}$ so that $0 \leq u' \leq i+s-1 < k$ and $k < v' < \ell$. From (6) and $a_n - a_v = a_{k+1} + a_i - a_u$, we obtain

$$a_{i+s} - a_i \leq a_{i+s} - a_i + a_u = a_v - a_{v'} + a_{u'} \leq a_v - a_{v'} + a_{i+s-1}. \tag{8}$$

Since also $u \leq i-1$, we have

$$a_{i+s} - a_i + a_{i-1} \geq a_{i+s} - a_i + a_u = a_v - a_{v'} + a_{u'} \geq a_v - a_{v'}. \tag{9}$$

Recall $k < v < \ell$ and $k < v' < \ell$. If $v' > v$, then (8) implies

$$a_{v'} - a_v \leq a_i + a_{i+s-1} - a_{i+s} < a_i,$$

contradicting (ii). If $v' = v$, then (8) implies $a_{i+s} - a_i = a_{u'} - a_u$, contradicting $u' \leq i+s-1$ and (i). If $v' < v$, then (9) immediately contradicts (ii).

For the last subcase $a_n - a_{v'} < a_{k+1}$, the term $x^{a_n - a_{v'}}$ appears in $\widetilde{w}_0(x)$ since $\widetilde{w}_0(x)$ contains all the terms of $\tilde{f}(x)$ of degree less than a_{k+1}. Consequently, $x^{a_{v'}}$ is a term in $w_0(x)$. Since $t = a_{k+1}$, condition (iii) in the theorem implies that all the terms in $w(x)$ of degree less than a_{k+1} and all the terms in $w(x)$ of degree more than $a_n - a_{k+1}$ appear in $w_0(x)$. Since x^t is a term in $w(x)\widetilde{w}(x) - w_0(x)\widetilde{w}_0(x)$, we must have $a_n - a_{k+1} \geq a_{k+1}$ so that $a_{v'} > a_{k+1}$. As $x^{a_{v'}}$ is a term in $w_0(x)$, we deduce $v' \geq \ell$. We return to using that $x^{a_n - a_{v'}}$ is a term in $\widetilde{w}_0(x)$. Since (6) came from taking the product of a term $x^{a_{u'}}$ in $f(x)$ and a term $x^{a_n - a_{v'}}$ in $\tilde{f}(x)$ which appears in the difference $f(x)\tilde{f}(x) - w_0(x)\widetilde{w}_0(x)$, we deduce that $u' \geq k+1$. Recall (7). Thus, $u' = k+1$. From (6), we deduce $a_n - a_{v'} = a_{i+s}$ which contradicts (i). Therefore, the case $a_n - a_v > a_{k+1}$ is complete.

We are left with considering the case that $a_n - a_v < a_{k+1}$ in (5). As in the last subcase above, the term $x^{a_n - a_v}$ appears in $\widetilde{w}_0(x)$ since $\widetilde{w}_0(x)$ contains all the terms of $\tilde{f}(x)$ of degree less than a_{k+1}. Also, as in the last subcase, we have x^{a_v} is a term

in $w_0(x)$, and $a_v > a_n - a_{k+1} \geq a_{k+1}$ so that $v \geq \ell$. Alternatively, we showed after (5) that $v > k$ so x^{a_v} being a term in $w_0(x)$ implies $v \geq \ell$. Since (5) came from taking the product of a term x^{a_u} in $f(x)$ and a term $x^{a_n - a_v}$ in $\tilde{f}(x)$ which appears in the difference $f(x)\tilde{f}(x) - w_0(x)\widetilde{w}_0(x)$, we deduce that $k+1 \leq u < \ell$. From (5), we have

$$a_u - a_{k+1} = a_i - (a_n - a_v) \leq a_i.$$

If $u > k+1$, we obtain a contradiction to (ii). If $u = k+1$, we deduce $a_n - a_v = a_i$ which contradicts (i).

Our assumption that $x^t = x^{a_{k+1}}$ is a term in $\widetilde{w}(x) - \widetilde{w}_0(x)$ led to (5). We are left then with considering the case that this assumption does not hold. But in this case, $x^{a_{k+1}}$ is a term in $w(x) - w_0(x)$, giving us what we set out to establish and finishing the proof.

Acknowledgment. The author is grateful to the anonymous referee for her or his comments.

References

[1] M. Filaseta, On the factorization of polynomials with small Euclidean norm, In *Number Theory in Progress, Vol. 1* (Zakopane-Kościelisko, 1997), pp. 143–163, de Gruyter, Berlin, 1999.

[2] M. Filaseta and D. B. Meade, Irreducibility testing of lacunary $0,1$-polynomials, *J. Algorithms* **55** (2005), 21–28.

[3] M. Filaseta, A. Granville and A. Schinzel, Irreducibility and greatest common divisor algorithms for sparse polynomials, *Number Theory and Polynomials* (ed. James McKee and Chris Smyth), LMS Lecture Note Series 352, Cambridge Univ. Press, 2008, pp. 155–176.

[4] M. Filaseta and A. Schinzel, On testing the divisibility of lacunary polynomials by cyclotomic polynomials, *Math. Comp.* **73** (2004), 957–965.

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