On the Irreducibility of $0, 1$-Polynomials of the Form $f(x)x^n + g(x)$

Michael Filaseta
Mathematics Department
University of South Carolina
Columbia, SC 29208

Manton Matthews, Jr.
Mathematics Department
University of South Carolina
Columbia, SC 29208

July 28, 2003

The first author expresses his gratitude for support from the National Science Foundation.

1 Introduction

For $f(x) \in \mathbb{C}[x]$ with $f(x) \not\equiv 0$, we define $\tilde{f}(x) = x^{\deg f} f(1/x)$. The polynomial $\tilde{f}$ is called the *reciprocal* of $f(x)$. The constant term of $\tilde{f}$ is always non-zero. If the constant term of f is non-zero, then $\deg \tilde{f} = \deg f$ and the reciprocal of $\tilde{f}$ is f. If $\alpha \neq 0$ is a root of f, then $1/\alpha$ is a root of $\tilde{f}$. If $f(x) = g(x)h(x)$ with $g(x)$ and $h(x)$ in $\mathbb{C}[x]$, then $\tilde{f} = \tilde{g}\tilde{h}$. If $f = \pm \tilde{f}$, then f is called *reciprocal*. If f is not reciprocal, we say that f is *non-reciprocal*. If f is reciprocal and α is a root of f, then $1/\alpha$ is a root of f. The product of reciprocal polynomials is reciprocal so that a non-reciprocal polynomial must have a non-reciprocal irreducible factor. For $f(x) \in \mathbb{Z}[x]$, we refer to the *non-reciprocal part of* $f(x)$ as the polynomial $f(x)$ removed of its irreducible reciprocal factors having a positive leading coefficient. For example, the non-reciprocal part of $3(-x+1)x(x^2+2)$ is $-x(x^2+2)$ (the irreducible reciprocal factors 3 and $x-1$ have been removed from the polynomial $3(-x+1)x(x^2+2)$).

In [2], Filaseta, Ford, and Konyagin established the following result.

Theorem 1. *Let $f(x)$ and $g(x)$ be in $\mathbb{Z}[x]$ with $f(0) \neq 0$, $g(0) \neq 0$, and $\gcd_{\mathbb{Z}}(f(x), g(x)) = 1$. Let r_1 and r_2 denote the number of non-zero terms in $f(x)$ and $g(x)$, respectively. If $n \geq n_0$, where*

$$n_0 = n_0(f,g) = \max\left\{2 \times 5^{2N-1}, 2\max\left\{\deg f, \deg g\right\}\left(5^{N-1} + \frac{1}{4}\right)\right\}$$

and

$$N = 2\,\|f\|^2 + 2\,\|g\|^2 + 2r_1 + 2r_2 - 7,$$

then the non-reciprocal part of $f(x)x^n + g(x)$ is irreducible or identically 1 or -1 unless one of the following holds:

(i) The polynomial $-f(x)g(x)$ is a pth power for some prime p dividing n.

(ii) For either $\varepsilon = 1$ or $\varepsilon = -1$, one of $\varepsilon f(x)$ and $\varepsilon g(x)$ is a 4th power, the other is 4 times a 4th power, and n is divisible by 4.

The work in [2] was motivated by work of Schinzel [3, 4] where a similar result is obtained without an explicit estimate on n_0 (though the methods there do allow for such an estimate).

Theorem 1 is an assertion about the irreducibility of the non-reciprocal part of $F(x) = f(x)x^n + g(x)$. If the non-reciprocal part of $F(x)$ is irreducible and $\gcd(F, \widetilde{F}) = 1$, then $F(x)$ is irreducible. Thus, the above result can be combined with an analysis of $\gcd(F, \widetilde{F})$ to determine information about the irreducibility of $F(x)$.

We remark that the bound n_0 cannot be replaced by a bound that is independent of the size of the coefficients of f and g. To see this, consider an arbitrary integer $k > 1$ and observe that $f(x) = 1$ and $g(x) = x - 2^k - 2$ imply that the non-reciprocal part of $F(x) = f(x)x^n + g(x)$ is reducible for $n = k$ (since $x-2$ is a factor of $F(x)$ and the quotient $F(x)/(x-2)$ is non-reciprocal). Since k is arbitrary, the remark follows.

In this paper, we obtain a result similar to Theorem 1 but restricted to $0,1$-polynomials $f(x)$ and $g(x)$, that is polynomials $f(x)$ and $g(x)$ with each coefficient either 0 or 1. In this case, it is not difficult to check that neither (i) nor (ii) can hold.

Theorem 2. *Let $f(x)$ and $g(x)$ be relatively prime $0,1$-polynomials with $f(0) = g(0) = 1$. If*

$$n > \deg g + 2\max\{\deg f, \deg g\}, \tag{1}$$

then the non-reciprocal part of $f(x)x^n + g(x)$ is irreducible or identically 1.

An interesting aspect of the proof given here is that Theorem 1, even without an explicit value for n_0, will play a crucial role in establishing the bound given in Theorem 2.

2 Proof of Theorem 2

To prove Theorem 2, we make use of the following result that can be found in [1].

Lemma 1. *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 $w(x)$ satisfying $w(x) \neq f(x)$, $w(x) \neq \tilde{f}(x)$, $w\widetilde{w} = f\tilde{f}$, and $w(x)$ is a $0,1$-polynomial with the same number of non-zero terms as $f(x)$.*

Assume (1) holds for some integer n and that the non-reciprocal part of $f(x)x^n + g(x)$ is reducible. Let $w(x)$ be the $0,1$-polynomial that exists by Lemma 1 with $f(x)$ replaced there by $f(x)x^n + g(x)$. In particular,

$$w(x) \neq f(x)x^n + g(x) \quad \text{and} \quad w(x) \neq \tilde{g}(x)x^{n+\deg f-\deg g} + \tilde{f}(x) \tag{2}$$

and

$$w(x)\widetilde{w}(x) = \big(f(x)x^n + g(x)\big)\big(\tilde{g}(x)x^{n+\deg f-\deg g} + \tilde{f}(x)\big). \tag{3}$$

First, consider the case that $\deg f \geq \deg g$. Write $w(x)$ in the form $a(x)x^n + b(x)$ where $a(x)$ and $b(x)$ are $0,1$-polynomials with $b(0) = 1$ (by (3)) and $\deg b(x) < n$. Also, (3) implies that $\deg a(x) = \deg f(x)$ (so that $w(x)$ and $f(x)x^n + g(x)$ have the same degree). Applying (3) again, we obtain

$$\begin{aligned}
&f(x)\tilde{g}(x)x^{2n+\deg f-\deg g} + f(x)\tilde{f}(x)x^n + g(x)\tilde{g}(x)x^{n+\deg f-\deg g} + \tilde{f}(x)g(x) \\
&\quad = \big(f(x)x^n + g(x)\big)\big(\tilde{g}(x)x^{n+\deg f-\deg g} + \tilde{f}(x)\big) \\
&\quad = \big(a(x)x^n + b(x)\big)\big(\tilde{b}(x)x^{n+\deg a-\deg b} + \tilde{a}(x)\big) \\
&\quad = a(x)\tilde{b}(x)x^{2n+\deg a-\deg b} + a(x)\tilde{a}(x)x^n + b(x)\tilde{b}(x)x^{n+\deg a-\deg b} + \tilde{a}(x)b(x).
\end{aligned}$$

The significance of working with $0,1$-polynomials here is that there is no cancellation of terms above. In particular, the expression $\tilde{a}(x)b(x)$ on the right contains a term with degree equal to $\deg b(x)$, which is $< n$, and every term of degree $< n$ on the left also has degree $\leq \deg f + \deg g$. Hence, $\deg b(x) \leq \deg f + \deg g$.

We now consider the case that $\deg f < \deg g$. The somewhat disguised idea will be to work instead with the reciprocal of $f(x)x^n + g(x)$ and proceed as in the case of $\deg f \geq \deg g$. For this purpose, we define $k = n + \deg f - \deg g$ and write $w(x)$ in the form $a(x)x^k + b(x)$ where now $a(x)$ and $b(x)$ are $0,1$-polynomials with $b(0) = 1$, $\deg b(x) < k$, and $\deg a(x) = n + \deg f - k = \deg g$. Instead of the equations above, we use that

$$f(x)\tilde{g}(x)x^{2k+\deg g-\deg f} + f(x)\tilde{f}(x)x^{k+\deg g-\deg f} + g(x)\tilde{g}(x)x^k + \tilde{f}(x)g(x)$$

$$
\begin{aligned}
&= f(x)\tilde{g}(x)x^{2n+\deg f-\deg g} + f(x)\tilde{f}(x)x^n + g(x)\tilde{g}(x)x^{n+\deg f-\deg g} + \tilde{f}(x)g(x) \\
&= \big(f(x)x^n + g(x)\big)\big(\tilde{g}(x)x^{n+\deg f-\deg g} + \tilde{f}(x)\big) \\
&= \big(a(x)x^k + b(x)\big)\big(\tilde{b}(x)x^{k+\deg a-\deg b} + \tilde{a}(x)\big) \\
&= a(x)\tilde{b}(x)x^{2k+\deg a-\deg b} + a(x)\tilde{a}(x)x^k + b(x)\tilde{b}(x)x^{k+\deg a-\deg b} + \tilde{a}(x)b(x).
\end{aligned}
$$

Arguing as before, a term of degree $\deg b(x)$ appears on the right and the only terms of degree $< k$ on the left have degree $\le \deg f + \deg g$, so $\deg b(x) \le \deg f + \deg g$.

Thus, in both of the cases $\deg f \ge \deg g$ and $\deg f < \deg g$, we deduce that $w(x)$ is of the form $a(x)x^m + b(x)$ where $\deg b(x) \le \deg f + \deg g$ and where either $m = n$ and $\deg a = \deg f$ or $m = n + \deg f - \deg g$ and $\deg a = \deg g$. In both cases, $m + \deg a = n + \deg f$. The inequality (1) implies that the product $\tilde{a}(x)b(x)$ consists of terms of degree $< m$ (for either choice of m) and, hence, corresponds to terms in $\tilde{f}(x)g(x)$ on the left-hand sides above of degree $\le \deg f + \deg g$. Therefore, $\tilde{a}(x)b(x)$ has degree $\le \deg f + \deg g$. From (1), we deduce that each of the exponents m and $m + \deg a - \deg b$ is $> \deg f + \deg g$. It follows that

$$\tilde{f}(x)g(x) = \tilde{a}(x)b(x).$$

The possibility that $a(0) = 0$ exists. We consider a non-negative integer ℓ such that $a(x) = a_0(x)x^\ell$ where $a_0(x)$ is a $0,1$-polynomial with $a_0(0) = 1$. Then $\tilde{a} = \tilde{a}_0$ and $\deg a = \ell + \deg \tilde{a}$. Since $\tilde{a}(x)b(x)$ has degree $\deg f + \deg g$, we have $\deg a - \ell + \deg b = \deg f + \deg g$ so that $\deg b = \ell - \deg a + \deg f + \deg g$. We use this to make further comparisons of exponents. For example, to see that the terms in $a(x)\tilde{b}(x)x^{2m+\deg a-\deg b}$ have degrees exceeding the degrees of the terms in $b(x)\tilde{b}(x)x^{m+\deg a-\deg b}$, we can justify instead that

$$m + \ell > 2\big(\ell - \deg a + \deg f + \deg g\big).$$

For the latter, we want $m > \ell + 2\big(\deg f + \deg g - \deg a\big)$, which follows from (1). By comparing coefficients in this manner, we deduce

$$f(x)\tilde{g}(x)x^{2n+\deg f-\deg g} = a(x)\tilde{b}(x)x^{2m+\deg a-\deg b}$$

and, consequently,

$$f(x)\tilde{f}(x)x^n + g(x)\tilde{g}(x)x^{n+\deg f-\deg g} = a(x)\tilde{a}(x)x^m + b(x)\tilde{b}(x)x^{m+\deg a-\deg b}.$$

Recall that n is a fixed integer satisfying (1) for which the non-reciprocal part of $f(x)x^n + g(x)$ is reducible. We now consider an arbitrary positive integer n' satisfying (1) and set $m' = n'$ if $\deg f \ge \deg g$ and $m' = n' + \deg f - \deg g$ if $\deg f < \deg g$. Thus, if $n' = n$, then $m' = m$. We use the polynomials $a(x)$ and $b(x)$ constructed above (corresponding to the case $n' = n$). Multiplying both sides of the equations above by a suitable power of x, we obtain

$$f(x)\tilde{g}(x)x^{2n'+\deg f-\deg g} = a(x)\tilde{b}(x)x^{2m'+\deg a-\deg b}$$

and

$$f(x)\tilde{f}(x)x^{n'} + g(x)\tilde{g}(x)x^{n'+\deg f-\deg g} = a(x)\tilde{a}(x)x^{m'} + b(x)\tilde{b}(x)x^{m'+\deg a-\deg b}.$$

Hence,

$$
\begin{aligned}
&\big(f(x)x^{n'} + g(x)\big)\big(\tilde{g}(x)x^{n'+\deg f-\deg g} + \tilde{f}(x)\big)\\
&= f(x)\tilde{g}(x)x^{2n'+\deg f-\deg g} + f(x)\tilde{f}(x)x^{n'} + g(x)\tilde{g}(x)x^{n'+\deg f-\deg g} + \tilde{f}(x)g(x)\\
&= a(x)\tilde{b}(x)x^{2m'+\deg a-\deg b} + a(x)\tilde{a}(x)x^{m'} + b(x)\tilde{b}(x)x^{m'+\deg a-\deg b} + \tilde{a}(x)b(x)\\
&= \big(a(x)x^{m'} + b(x)\big)\big(\tilde{b}(x)x^{m'+\deg a-\deg b} + \tilde{a}(x)\big).
\end{aligned}
$$

We consider n' sufficiently large with at least $n' \geq n_0(f,g)$, where $n_0(f,g)$ is defined in Theorem 1. Using that $F(x) = f(x)x^{n'} + g(x)$ is a $0,1$-polynomial, we deduce from Theorem 1 that the non-reciprocal part of $F(x)$ is irreducible or identically 1. On the other hand, the polynomial $W(x) = a(x)x^{m'} + b(x)$ satisfies $W\widetilde{W} = F\widetilde{F}$ and $W(x)$ is a $0,1$-polynomial containing the same number of non-zero terms as $F(x)$. By Lemma 1, either $W(x) = F(x)$ or $W(x) = \widetilde{F}(x)$. If $W(x) = F(x)$, then

$$a(x)x^{m'} + b(x) = f(x)x^{n'} + g(x).$$

If $m' = n'$, then $a(x) = f(x)$ and $b(x) = g(x)$, contradicting (2). If $m' \neq n'$, then $m' = n' + \deg f - \deg g$, $\deg g > \deg f$, $a(x) = f(x)x^{\deg g - \deg f}$, and $b(x) = g(x)$, contradicting (2). Similarly, $W(x) = \widetilde{F}(x)$ leads to a contradiction to (2). It follows that our assumption that n exists satisfying (1) and such that the non-reciprocal part of $f(x)x^n + g(x)$ is reducible is incorrect. The theorem follows.

References

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

[2] M. Filaseta, K. Ford, and S. Konyagin, *On an irreducibility theorem of A. Schinzel associated with coverings of the integers*, Illinois J. Math. **44** (2000), 633–643.

[3] A. Schinzel, *On the reducibility of polynomials and in particular of trinomials*, Acta Arith. **11** (1965), 1–34.

[4] A. Schinzel, *Reducibility of polynomials and covering systems of congruences*, Acta Arith. **13** (1967), 91–101.