**International Journal of Pure and Applied Mathematics**

**Volume 23 No. 2 2005, 179-193**

# REDUCIBILITY OF FOUR TERM POLYNOMIALS

Amarisa Chantanasiri[1], Vichian Laohakosol[2] §

[1]Department of Mathematics
Chulalongkorn University
Bangkok, 10330, THAILAND
e-mail: um_amarisa@yahoo.com

[2]Department of Mathematics
Kasetsart University
Bangkok, 10900, THAILAND
e-mail: fscivil@ku.ac.th

**Abstract:** Continuing on an old work of Ostrowski in 1975-1976, the reducibility of polynomials with four terms is investigated. For such polynomials whose corresponding baric polygons are quadrangles, it is shown by elementary means that one of the two remaining reduced polynomials has neither linear nor quadratic factors.

**AMS Subject Classification:** 12D05, 11C08
**Key Words:** polynomials, reducibility, baric polyhedra

## 1. Introduction

Let $m \geq 1$ and $x_1, \ldots, x_m$ be independent variables. A *product of powers* (denoted by $PP$) of these variables is an expression of the form

$$P := x_1^{\alpha_1} \ldots x_m^{\alpha_m}. \tag{1}$$

Such $PP$ is called *rational* if all $\alpha_\mu \in \mathbb{Z}$, and a rational $PP$ with all $\alpha_\mu \geq 0$ is called *integer*. The $PP$ (1) with all $\alpha_\mu \in \mathbb{Q}$ is called *algebraic*. The set of algebraic $PP$'s is denoted by $[x_1, \ldots, x_m]$. Let $K$ be a field. Define an algebraic

Received: June 16, 2005 

§Correspondence author

polynomial as a finite sum $F := \sum_\nu c_\nu P_\nu$, where $c_\nu \in K \setminus \{0\}$ and $P_\nu$ are distinct algebraic $PP$'s. If all $PP$'s in $F$ are rational (respectively, integer), we call $F$ rational (respectively, integer). *From now on, by polynomial we mean algebraic polynomial over a field $K$, unless otherwise specified.*

A polynomial which is not a monomial, i.e. contains at least two different $PP$'s, is called *proper*. Let $F$ be a polynomial with coefficients from $K$. We say that $F$ is *reducible* with respect to $K$ if $F = GH$, where $G$ and $H$ are proper polynomials with coefficients from $K$, while it is called *irreducible* (with respect to $K$) otherwise. For a proper polynomial $F$ with coefficients from $K$, which is irreducible with respect to $K$, it can happen that there exists an algebraic extension $K^*$ of $K$ such that $F$ has a proper factor with coefficients from $K^*$. In this case, we say that $F$ becomes reducible with respect to $K^*$. But if there does not exist any algebraic extension of $K$ in which $F$ becomes reducible, $F$ is called *absolutely irreducible*.

We say that $PP$'s $P_1, \ldots, P_k$ are *algebraically independent* over a field $K$ if there is no nonzero rational polynomial $F(y_1, \ldots, y_k)$ with coefficients from $K$ such that $F(P_1, \ldots, P_k) = 0$, and we say that they are algebraically dependent over $K$ otherwise.

In 1975-1976, A. Ostrowski (see [1], [2]) published a deep, general and extensive research on multiplication and factorization of polynomials based principally on the generalized notions of highest and lowest terms of a polynomial, called general mappings, $\Lambda$, of a polynomial into an extreme aggregate of its terms. The first part of Ostrowski's works discusses all possible orderings, $\Omega$, in the set of $PP$'s under a very general set of postulates, which contains the usual lexicographical principle as a special case. A one-to-one correspondence between $\Omega$ and $\Lambda$ is established and all realizations of postulates defining $\Omega$ are investigated using the ideas of weight functions and the baric polyhedron of a polynomial. The second part of Ostrowski's works contains applications of the results in the first part to the problem of reducibility of polynomials. In particular, the cases of two and three term polynomials are completely determined, while that of four term polynomials discussion is only carried out for the case of the baric polygon being a triangle.

The main objective of this article is to investigate the reducibility of four term polynomials. For these polynomials, their corresponding baric polygons are either triangles or quadrangles. In the triangle case, Ostrowski's list of reducible polynomials misses out one possibility and we make complete the classification in the first part of Section 3. The latter part of Section 3 treats the case of quadrangle where we show by elementary means that one of the remaining two reduced polynomials has neither linear nor quadratic factors.

## 2. Preliminaries

In this section, we recall two basic notions, weight function and baric polyhedron, and describe Ostrowski's reducibility results for the case of two and three term polynomials. A function $W : [x_1, \dots, x_m] \to \mathbb{R}$ is called a *weight function* if for $P_1$ and $P_2$ from $[x_1, \dots, x_m]$, we have

$$W(P_1P_2) = W(P_1) + W(P_2).$$

Examples of weight functions are:

1) The weight function given by the *dimension*: $W(x_1) = \cdots = W(x_m) = 1$.

2) The weight function given by the *degree* in $x_1$: $W(x_1) = 1,\ W(x_2) = \cdots = W(x_m) = 0$.

3) The weight function given by the *classical weight in the theory of symmetric functions*: $W(x_1) = 1,\ W(x_2) = 2, \dots,\ W(x_m) = m$.

If we have a finite set of points $A_1, \dots, A_N$ in $\mathbb{R}^m$, then the *smallest* convex polyhedron which contains $A_1, \dots, A_N$ is the set of all points representable in the form $A = \sum_{\nu=1}^{N} t_\nu A_\nu$, where $t_1, \dots, t_N \geq 0$ and $t_1 + \cdots + t_N = 1$. This polyhedron will be denoted by $\langle A_1, \dots, A_N \rangle$. Any $PP$ of the form (1) corresponds to a representative point, $A \in \mathbb{R}^m$ with coordinates $(\alpha_1, ..., \alpha_m)$. We also define $A$ to be the *representative point* of $cP$ with $c \in K \setminus \{0\}$. Then in this way $n$ terms of $F$ correspond to $n$ different points $A_1, \dots, A_n$. The polyhedron, $C_F := \langle A_1, \dots, A_n \rangle$, is called the *baric polyhedron* of the polynomial $F$.

The next lemma, analogous to the classical Eisenstein-Schönemann Theorem, plays a crucial role in irreducibility consideration. Its proof can be found in [2].

**Lemma 1.** *Let $J$ be the set of all integer polynomials in $x_1, \dots, x_m$ with coefficients from a field $K$. Consider a weight function $W(F)$ such that $W(x_\nu) > 0$ $\big(\nu = 1, \dots, m\big)$. Let $z$ be a variable which is independent of $J$. Consider the polynomial*

$$Z := \varphi + \sum_{\pi=1}^{p} \psi_\pi z^{\pi k} + \chi z^n,$$

*where $n > pk \geq 2$, $\varphi, \chi$ and $\psi_\pi$ $\big(\pi \in \{1, \dots, p\}\big)$ are polynomials from $J$ and $\varphi\chi \neq 0$. Assume that $W(\varphi) > \max\{W(\chi), W(\psi_1), \dots, W(\psi_p)\}$, the polynomial $\varphi$ has no multiple factors and $\gcd(\varphi, \chi, \psi_1, \dots, \psi_p) = 1$. Suppose that $Z$ is a product of two polynomials depending on $z$:*

$$Z = FG,\ F = f_0 + f_1 z^{u_1} + \cdots + f_s z^{u_s}, \quad 0 < u_1 < \cdots < u_s,\ s \geq 1,$$

$$G = g_0 + g_1 z^{v_1} + \cdots + g_t z^{v_t}, \quad 0 < v_1 < \cdots < v_t,\ t \geq 1,$$

*where* $f_\sigma, g_\tau \in J \setminus \{0\}$ $\big(\sigma \in \{0, \ldots, s\},\ \tau \in \{0, \ldots, t\}\big)$. *Then* $\gcd(\varphi, \psi_1, \ldots, \psi_p) = 1$, *all exponents* $u_\sigma, v_\tau$ *are divisible by* $k$, *and therefore* $n$ *is also divisible by* $k$.

The following complete reducibility characterizations of two and three term polynomials are due to Ostrowski [2].

**Two-term polynomials.** A rational polynomial with two distinct terms $ax_1^{u_1} \ldots x_m^{u_m} + bx_1^{v_1} \ldots x_m^{v_m},\ ab \neq 0$ is absolutely irreducible in the domain of rational polynomials $\Longleftrightarrow \gcd(u_1 - v_1, \ldots, u_m - v_m) = 1$.

**Three-term polynomials.** A rational polynomial with three distinct terms $aP_1 + bP_2 + cP_3,\ abc \neq 0$ is absolutely irreducible, even in the domain of algebraic polynomials, if $P_2/P_1, P_3/P_1$ are algebraically independent. If $P_2/P_1, P_3/P_1$ are not algebraically independent and $P_1, P_2, P_3$ are algebraic (respectively, rational) $PP$'s, then $aP_1 + bP_2 + cP_3$ is reducible in the domain of algebraic (respectively, rational) polynomials.

## 3. Four Term Polynomials

Consider the general algebraic polynomial with four distinct terms,

$$aP_1 + bP_2 + \gamma P_3 + dP_4, \quad ab\gamma d \neq 0. \tag{2}$$

There are three cases to distinguish according to the number of algebraically independent elements among the quotients

$$P_2/P_1, \quad P_3/P_1, \quad P_4/P_1. \tag{3}$$

The cases, where there are three or one algebraically independent quotients are settled by Ostrowski [2] with results as stated in the next two lemmas.

**Proposition 1.** *If all quotients* (3) *are algebraically independent, then the polynomial* (2) *is always absolutely irreducible in the domain of algebraic polynomials.*

**Proposition 2.** *If there is only one algebraically independent quotient in* (3), *the polynomial* (2) *is always reducible in the domain of algebraic polynomials, and if all quotients* (3) *are rational* $PP$*'s,* (2) *is reducible even in the domain of rational polynomials.*

For the rest of this paper, we treat the case that *there are exactly two algebraically independent quotients*. Let

$$P_1 := x_1^{\alpha_1} \dots x_m^{\alpha_m},\ P_2 := x_1^{\beta_1} \dots x_m^{\beta_m},\ P_3 := x_1^{\gamma_1} \dots x_m^{\gamma_m},\ P_4 := x_1^{\delta_1} \dots x_m^{\delta_m},$$

and let their corresponding representative points be

$$X_1 := (\alpha_1, \dots, \alpha_m), \quad X_2 := (\beta_1, \dots, \beta_m),$$

$$X_3 := (\gamma_1, \dots, \gamma_m), \quad X_4 := (\delta_1, \dots, \delta_m),$$

respectively. Since there are exactly two algebraically independent quotients, $X_1, X_2, X_3, X_4$ all lie in the same plane but are not collinear. This implies that the corresponding baric diagram is either a triangle or a quadrangle. To simplify discussion, we first perform a few suitable change of variables. Dividing the polynomial in (2) by $aP_1$ brings it to the form

$$Z := 1 + a'P_1' + b'P_2' + \gamma'P_3', \tag{4}$$

which amounts to bringing the point $X_1$ into the origin, and its corresponding term in $aP_1+bP_2+\gamma P_3+dP_4$ becomes 1. We assume, without loss of generality, that $P_1', P_2'$ are independent. We introduce $y_1 := P_1'$ and $y_2 := P_2'$ as new variables so that $P_3' = P_1'^{\alpha} P_2'^{\beta} = y_1^{\alpha} y_2^{\beta}$, where $\alpha, \beta \in \mathbb{Q}$. Then $Z = 1 + a'y_1 + b'y_2 + \gamma' y_1^{\alpha} y_2^{\beta}$. Since the baric polygon of $Z$ is either a triangle or a quadrangle, $\alpha, \beta$ must both be positive.

Take $y'_1 := a'y_1$ and $y'_2 := b'y_2$. Then $Z = 1 + y'_1 + y'_2 + c{y'_1}^{\alpha}{y'_2}^{\beta}$, where $c := \frac{\gamma'}{a'^{\alpha} b'^{\beta}}$. Let $M$ be a common denominator of $\alpha$ and $\beta$, $p := M\alpha$ and $q := M\beta$. So $p, q \in \mathbb{N}$. Then putting $y'_1 =: x'^M$ and $y'_2 =: y'^M$, we obtain $Z$ in the form

$$Z = 1 + x'^M + y'^M + cx'^p y'^q \quad (c \neq 0,\ p, q \in \mathbb{N}). \tag{5}$$

### 3.1. Baric Triangles

If the baric polygon of $Z$ in (5) is a triangle, we must have $p + q \leq M$. Since $p, q > 0$, it follows that $p, q < M$ Suppose that $Z$ is reducible in the domain of integer polynomials. If we apply Lemma 1, replacing there $z$ with $x'$, $n$ with $M$ and $k$ with $p$, we obtain in the notations of Lemma 1 that $\varphi = 1+y'^M$, $\psi_1 = cy'^q$ and $\chi = 1$. Thus if we use the degree in $y'$ as weight, all conditions of Lemma 1 are satisfied. It follows that $\frac{M}{p} \in \mathbb{Z}^+$. Similarly, $\frac{M}{q} \in \mathbb{Z}^+$. Also, we have that the factors of $Z$ are polynomials in $x'^p$ and $y'^q$. Since $p, q \neq M$, $\frac{M}{p}, \frac{M}{q} \geq 2$.

Introduce $x := x'^p$ and $y := y'^q$ as new variables. Let $m := \frac{M}{p}$ and $n := \frac{M}{q}$. Then we have to consider the reducible polynomials of the shape

$$Z = 1 + x^m + y^n + cxy \quad (c \neq 0,\ m, n \geq 2). \tag{6}$$

Without loss of generality, we can assume that in (6), $m \geq n$.

If $m \geq 5$ or $(m = 4,\ n = 3)$ or $(m = 3,\ n = 2)$, Ostrowski [2], applying arguments based on Puiseux expansion, showed that $Z$ in (6) is irreducible. For $m = 4$, Ostrowski's analysis is incomplete, i.e. he only discussed the case $n = 4$, showing that $Z$ is reducible only when $c = \pm 2\sqrt{2}, \pm 2\sqrt{2}i$ with all possible decompositions taking the forms

$$\begin{aligned}
x^4 + y^4 - 2\sqrt{2}xy + 1 &= (x^2 - i\sqrt{2}xy - y^2 + i)(x^2 + i\sqrt{2}xy - y^2 - i),\\
x^4 + y^4 - 2\sqrt{2}ixy + 1 &= (x^2 + \sqrt{2}xy + y^2 + i)(x^2 - \sqrt{2}xy + y^2 - i),\\
x^4 + y^4 + 2\sqrt{2}xy + 1 &= (x^2 - i\sqrt{2}xy - y^2 - i)(x^2 + i\sqrt{2}xy - y^2 + i),\\
x^4 + y^4 + 2\sqrt{2}ixy + 1 &= (x^2 + \sqrt{2}xy + y^2 - i)(x^2 - \sqrt{2}xy + y^2 + i).
\end{aligned}$$

It is easily seen that each factor in the above decompositions is irreducible. To make complete Ostrowski's result, we record here the fact that in the remaining case $m = 4, n = 2$, $Z$ is reducible only for the same values of $c$ as above with all possible decompositions taking the form

$$\begin{aligned}
x^4 + y^2 - 2\sqrt{2}ixy + 1 &= (x^2 + \sqrt{2}x + iy + 1)(x^2 - \sqrt{2}x - iy + 1),\\
x^4 + y^2 + 2\sqrt{2}ixy + 1 &= (x^2 - \sqrt{2}x + iy + 1)(x^2 + \sqrt{2}x - iy + 1),\\
x^4 + y^2 - 2\sqrt{2}xy + 1 &= (x^2 - \sqrt{2}ix + iy - 1)(x^2 + \sqrt{2}ix - iy - 1),\\
x^4 + y^2 + 2\sqrt{2}xy + 1 &= (x^2 + \sqrt{2}ix + iy - 1)(x^2 - \sqrt{2}ix - iy - 1).
\end{aligned}$$

For $m \leq 3$, Ostrowski found the following exhaustive list of all reducible polynomials with their decompositions.

$$\begin{aligned}
x^3 + y^3 + 1 - 3xy &= (x + y + 1)(x + e^{2\pi i/3}y + e^{4\pi i/3})(x + e^{4\pi i/3}y + e^{2\pi i/3}),\\
x^3 + y^3 + 1 - 3e^{2\pi i/3}xy &= (x + y + e^{2\pi i/3})(x + e^{2\pi i/3}y + 1)(x + e^{4\pi i/3}y + e^{4\pi i/3}),\\
x^3 + y^3 + 1 - 3e^{4\pi i/3}xy &= (x + y + e^{4\pi i/3})(x + e^{2\pi i/3}y + e^{2\pi i/3})(x + e^{4\pi i/3}y + 1),\\
x^2 + y^2 + 1 - 2xy &= (x - y + i)(x - y - i),\\
x^2 + y^2 + 1 + 2xy &= (x + y + i)(x + y - i).
\end{aligned}$$

To sum up, for the polynomial $Z$ in (4) with $P_1'$ and $P_2'$ in (4) algebraically independent and $P_3' = P_1'^{\alpha} P_2'^{\beta},\ \alpha, \beta > 0,\ \alpha + \beta \leq 1$, the inequalities on $\alpha$ and $\beta$ signify that the baric polyhedron of $Z$ is a triangle. We have found that $Z$ in

(6) can be only reducible if $m = n = 4$; $m = 4,\ n = 2$; $m = n = 3$; $m = n = 2$, that is, $\alpha = \beta = \frac{1}{4}$; $\alpha = \frac{1}{4},\ \beta = \frac{1}{2}$; $\alpha = \beta = \frac{1}{3}$; $\alpha = \beta = \frac{1}{2}$. For the coefficients $a', b', \gamma'$, we obtain the condition $\gamma' = ca'^{\alpha}b'^{\beta} = ca'^{1/m}b'^{1/n}$, where the values of $c$ corresponding to the four cases of $m, n$ are given above. If all these conditions are satisfied, then $Z$ is reducible in the domain of algebraic polynomials. If we consider the irreducibility of $Z$ in the domain of rational polynomials, we have to add the condition that $P_1'^{1/m}$ and $P_2'^{1/n}$ are rational since $x = (a'P_1')^{1/m}$ and $y = (b'P_2')^{1/n}$.

### 3.2. Baric Quadrangles

We consider now a general four term polynomial with a baric plane quadrangle. We have $Z = 1 + aP_1 + bP_2 + \gamma P_3$, where $P_1$ and $P_2$ correspond to the two summits of the baric quadrangle adjacent to the summit at the origin. As before, $P_3 = P_1{}^{\alpha}P_2{}^{\beta}$, where $\alpha, \beta \in \mathbb{Q}$. Introducing $\xi := aP_1$ and $\eta := bP_2$ as new variables, our polynomial can be written as $1 + \xi + \eta + c\,\xi^{\alpha}\eta^{\beta}$, where $c \neq 0$, whose baric quadrangle is in the first quadrant with $\alpha, \beta > 0$ and $\alpha + \beta > 1$. Let $n$ be a common denominator of $\alpha$ and $\beta$, $p := n\alpha$ and $q := n\beta$. So $p, q \in \mathbb{Z}^+$. We may, without loss of generality, choose $n$ such that $p, q \geq 2$. Putting $\xi =: x^n$ and $\eta =: y^n$, we obtain

$$Z := 1 + x^n + y^n + cx^p y^q \quad (c \neq 0,\ p, q \in \mathbb{Z}^+,\ p + q > n). \tag{7}$$

To investigate reducibility in the domain of algebraic polynomials, we can choose $n$ such that $Z$ becomes reducible in the domain of rational and even integer polynomials. In fact, letting $n$ be a common denominator of $\alpha,\ \beta$ and all exponents in the factors of $Z$, we can restrict ourselves to the consideration of the reducibility of (7) in the domain of integer polynomials.

For the case that $p = n$ or $q = n$, without loss of generality, assume $p = n$. Ostrowski proved that:

(i) $Z$ in (7) is reducible if and only if $c = \exp(1 - (2\lambda + 1)q/n)\pi i$.

(ii) If $p < n$ and $q < n$, then $Z$ in (7) is always irreducible.

From now on, because we can interchange $x$ with $y$, we assume that $p > n$ and $q \neq n$. Observe that if $q < n$, then the form (7) can be somewhat simplified. In this case, we can apply Lemma 1, replacing there $z$ with $x$ and $n$ with $p$, we obtain in the notations of Lemma 1 that $\varphi = 1 + y^n,\ \psi_1 = 1$ and $\chi = cy^q$. Thus if we use the degree in $y$ as weight, all conditions of Lemma 1 are satisfied. It follows that $p$ is divisible by $n$. Then $p = nr$ for some $r \in \mathbb{N}$. Since $p \neq n$, $r > 1$. By changing the notations, we can reduce (7) to the form

$$Z = 1 + x + y^n + cx^p y^q \quad (c \neq 0,\ 1 < q < n,\ p > 1). \tag{8}$$

We pick up here where Ostrowski left off.

**Theorem 1.** *If $Z$ in (8) is reducible, then the factors of $Z$ cannot be independent of $x$.*

*Proof.* Suppose that $Z = F(y)G(x,y)$, where $F(y)$ and $G(x,y)$ are proper integer polynomials. Then we have $1 + x + y^n + cx^py^q = F(y)G(x,y)$, so the degree of $G(x,y)$ in $x$ is $p$. Since $p \geq 2$, we can write $G(x,y) = G_2(x,y)x^2 + G_1(y)x + G_0(y)$, where $G_2(x,y), G_1(y), G_0(y)$ are integer polynomials and the degree of $G_2(x,y)$ in $x$ is $p-2$. So $1 + x + y^n + cx^py^q = F(y)G_2(x,y)x^2 + F(y)G_1(y)x + F(y)G_0(y)$. Comparing the coefficients of $x$ on both sides, we have $1 = F(y)G_1(y)$, which is impossible since $F(y)$ is proper. □

**Theorem 2.** *$Z$ in (8) does not have a linear factor in $x$.*

*Proof.* Suppose that $x - \frac{F(y)}{G(y)}$ is a linear factor of $Z$. For ease of writing, for the rest of the proof, we drop the dependence of $y$ in $F(y)$ and $G(y)$. Without loss of generality, we can assume that $F$ is monic and $\gcd_y(F,G) = 1$. Replacing $x$ with $\frac{F}{G}$ in (8), we obtain $0 = G^p + FG^{p-1} + y^nG^p + cy^qF^p$. Then $G \,|\, y^q$, so we can write $G = ay^g$ where $g \leq q$. Thus

$$0 = (ay^g)^p + F(ay^g)^{p-1} + y^n(ay^g)^p + cy^qF^p. \tag{9}$$

Suppose that $g > 1$. Since $\gcd_y\big(F,G\big) = 1$, $y \nmid F$. It follows from (9) that $q = g(p-1)$. Dividing (9) by $y^q$, we obtain $0 = a^py^g + a^{p-1}F + a^py^{n+g} + cF^p$. Then $-\frac{a^p}{c}(y^{n+g} + y^g) = \left\{F^{p-1} + \frac{a^{p-1}}{c}\right\}F$. Since $F$ is monic, $-\frac{a^p}{c} = 1$. Write $F = y^f + b_{f-1}y^{f-1} + b_{f-2}y^{f-2} + \cdots + b_1y + b_0$. Since $y \nmid F$, $b_0 \neq 0$, we have

$$\begin{aligned}
y^{n+g} + y^g &= \left[(y^f + b_{f-1}y^{f-1} + b_{f-2}y^{f-2} + \cdots + b_1y + b_0)^{p-1} + \frac{a^{p-1}}{c}\right] \\
&\qquad \times \left[y^f + b_{f-1}y^{f-1} + b_{f-2}y^{f-2} + \cdots + b_1y + b_0\right] \\
&= \left(y^{fp} + \binom{p-1}{1}y^{f(p-1)}(b_{f-1}y^{f-1} + b_{f-2}y^{f-2} + \cdots + b_1y + b_0)\right. \\
&\quad + \binom{p-1}{2}y^{f(p-2)}(b_{f-1}y^{f-1} + b_{f-2}y^{f-2} + \cdots + b_1y + b_0)^2 + \cdots \\
&\qquad + \binom{p-1}{p-2}y^{2f}(b_{f-1}y^{f-1} + b_{f-2}y^{f-2} + \cdots + b_1y + b_0)^{p-2} \\
&\qquad \left. + y^f(b_{f-1}y^{f-1} + b_{f-2}y^{f-2} + \cdots + b_1y + b_0)^{p-1} + \frac{a^{p-1}}{c}y^f\right)
\end{aligned}$$

$$+ b_{f-1}y^{fp-1} + \binom{p-1}{1} b_{f-1}y^{f(p-1)-1}(b_{f-1}y^{f-1} + b_{f-2}y^{f-2} + \cdots + b_1y + b_0) + \cdots + b_{f-2}y^{fp-2} + \cdots .$$

The highest degrees on both sides being equal, we get $n+g = fp$, and since $(n+g)-g \geq 3$, comparing the coefficients of $y^{fp-1}$ and $y^{fp-2}$, we have $b_{f-1} = 0$ and $b_{f-2} = 0$, respectively. Continue comparing descending coefficients and assume $0 = b_{f-1} = b_{f-2} = ... = b_{j+1}$ with $0 \leq j \leq f-3$. Then

$$\begin{aligned} y^{n+g} + y^g &= \left[(y^f + b_jy^j + b_{j-1}y^{j-1} + \cdots + b_1y + b_0)^{p-1} + \frac{a^{p-1}}{c}\right] \\ &\quad \times \left[y^f + b_jy^j + b_{j-1}y^{j-1} + \cdots + b_1y + b_0\right] \\ &= y^{fp} + \left(\binom{p-1}{1} + 1\right) b_jy^{f(p-1)+j} + \cdots . \end{aligned}$$

For $j > g - f(p-1)$, comparing the coefficients of $y^{f(p-1)+j}$, we have $b_j = 0$. Let $j_* := g - f(p-1)$. Comparing the coefficients of $y^{f(p-1)+j_*}$ on both sides, we have $b_{j_*} \neq 0$. Thus

$$\begin{aligned} y^{n+g} + y^g &= \left[(y^f + b_{j_*}y^{j_*} + \cdots + b_2y^2 + b_1y + b_0)^{p-1} + \frac{a^{p-1}}{c}\right] \\ &\quad \times \left[y^f + b_{j_*}y^{j_*} + \cdots + b_2y^2 + b_1y + b_0\right] \\ &= \left[(y^f + b_{j_*}y^{j_*} + \cdots + b_2y^2)^{p-1} + \binom{p-1}{1}(y^f + b_{j_*}y^{j_*} + \cdots + b_2y^2)^{p-2}(b_1y + b_0)\right. \\ &\quad + \cdots + \binom{p-1}{p-2}(y^f + b_{j_*}y^{j_*} + \cdots + b_2y^2)(b_1y + b_0)^{p-2} + (b_1y)^{p-1} \\ &\quad \left. + \binom{p-1}{1}(b_1y)^{p-2}b_0 + \cdots + \binom{p-1}{p-2}(b_1y)b_0^{p-2} + b_0^{p-1} + \frac{a^{p-1}}{c}\right] \\ &\quad \times \left[y^f + b_{j_*}y^{j_*} + \cdots + b_2y^2 + b_1y + b_0\right]. \end{aligned}$$

Comparing the coefficients of $y^0$ on both sides, we have $b_0^{p-1} + \frac{a^{p-1}}{c} = 0$ because $b_0 \neq 0$. Comparing the coefficients of $y^1$ on both sides, we have $b_1 = 0$. For $2 \leq i \leq f$, we obtain

$$y^{n+g} + y^g = \left[(y^f + \cdots + b_{i+1}y^{i+1} + b_iy^i + b_0)^{p-1} + \frac{a^{p-1}}{c}\right]$$

$$\times \left[y^f + \cdots + b_{i+1}y^{i+1} + b_iy^i + b_0\right]$$

$$= \left[(y^f + \cdots + b_{i+1}y^{i+1})^{p-1} + \binom{p-1}{1}(y^f + \cdots + b_{i+1}y^{i+1})^{p-2}(b_iy^i + b_0) + ...\right.$$

$$+ \binom{p-1}{p-2}(y^f + \cdots + b_{i+1}y^{i+1})(b_iy^i + b_0)^{p-2} + (b_iy^i)^{p-1} + \binom{p-1}{1}(b_iy^i)^{p-2}b_0$$

$$\left. + \cdots + \binom{p-1}{p-2}(b_iy^i)b_0^{p-2} + b_0^{p-1} + \frac{a^{p-1}}{c}\right]\left[y^f + \cdots + b_{i+1}y^{i+1} + b_iy^i + b_0\right].$$

Comparing the coefficients of $y^0$ on both sides, we have $b_0^{p-1} + \frac{a^{p-1}}{c} = 0$. If $i < g$, comparing the coefficients of $y^i$ on both sides, we have $b_i = 0$. Note that $j_* = g - f(p-1) < g$, so $b_{j_*} = 0$, which is a contradiction and this implies $g = 0$.

Thus $G = a$, and (9) becomes $0 = a^p + Fa^{p-1} + y^n a^p + cy^q F^p$. Then $y^qF^p + \frac{a^{p-1}}{c}F = -\frac{a^p}{c}(y^n + 1)$. Since $F$ is monic, $-\frac{a^p}{c} = 1$. Write $F = y^f + b_{f-1}y^{f-1} + b_{f-2}y^{f-2} + \cdots + b_1y + b_0$. Thus

$$y^n + 1 = y^q(y^f + b_{f-1}y^{f-1} + b_{f-2}y^{f-2} + \cdots + b_1y + b_0)^p$$
$$+\frac{a^{p-1}}{c}(y^f + b_{f-1}y^{f-1} + b_{f-2}y^{f-2} + \cdots + b_1y + b_0).$$

Comparing the coefficients of $y^0$ on both sides, we have $\frac{a^{p-1}}{c}b_0 = 1$, so $b_0 \neq 0$. Comparing the coefficients of $y^1$ on both sides, we have $\frac{a^{p-1}}{c}b_1 = 0$, so $b_1 = 0$. For $2 \leq i \leq f$, we obtain

$$y^n = y^q(y^f + \cdots + b_{i+1}y^{i+1} + b_iy^i + b_0)^p + \frac{a^{p-1}}{c}(y^f + \cdots + b_{i+1}y^{i+1} + b_iy^i).$$

Since $q < n$, it follows that $y^q|(y^f + \cdots + b_{i+1}y^{i+1} + b_iy^i)$. Then $f \geq q$ and $b_i = 0$ for all $i < q$.

— If $f = q$, then $y^n = y^q(y^q + b_0)^p + \frac{a^{p-1}}{c}y^q$. Dividing both sides by $y^q$, we obtain $y^{n-q} = (y^q + b_0)^p + \frac{a^{p-1}}{c}$. Since $p > 1$, it follows that $b_0 = 0$, which is a contradiction.

— If $f > q$, then

$$y^n = y^q(y^f + b_{f-1}y^{f-1} + \cdots + b_qy^q + b_0)^p + \frac{a^{p-1}}{c}(y^f + b_{f-1}y^{f-1} + \cdots + b_qy^q)$$
$$= y^q\left[(y^{fp} + \binom{p}{1}y^{f(p-1)}(b_{f-1}y^{f-1} + \cdots + b_qy^q + b_0)\right.$$

$$+\binom{p}{2}y^{f(p-2)}(b_{f-1}y^{f-1}+\cdots+b_qy^q+b_0)^2+\cdots$$
$$+\binom{p}{p-1}y^f(b_{f-1}y^{f-1}+\cdots+b_qy^q+b_0)^{p-1}+(b_{f-1}y^{f-1}+\cdots+b_qy^q+b_0)^p\Big]$$
$$+\frac{a^{p-1}}{c}(y^f+b_{f-1}y^{f-1}+\cdots+b_qy^q).$$

Comparing the coefficients of $y^q$ on both sides, we have $b_0^p+\frac{a^{p-1}}{c}b_q=0$, which yields, since $b_0\neq 0$, $b_q\neq 0$. Comparing the coefficients of $y^{fp+q-1}$ on both sides, we have $b_{f-1}=0$. Assuming $0=b_{f-1}=...=b_{j+1}$ with $q+1\leq j\leq f-2$, we get

$$y^n=\ y^q(y^f+b_jy^j+\cdots+b_qy^q+b_0)^p+\frac{a^{p-1}}{c}(y^f+b_jy^j+\cdots+b_qy^q)=$$
$$y^q\Big[(y^{fp}+\binom{p}{1}y^{f(p-1)}(b_jy^j+\cdots+b_qy^q+b_0)+\binom{p}{2}y^{f(p-2)}(b_jy^j+\cdots+b_qy^q+b_0)^2$$
$$+\cdots+\binom{p}{p-1}y^f(b_jy^j+\cdots+b_qy^q+b_0)^{p-1}+(b_jy^j+\cdots+b_qy^q+b_0)^p\Big]$$
$$+\frac{a^{p-1}}{c}(y^f+b_jy^j+\cdots+b_qy^q).$$

Comparing the coefficients of $y^{f(p-1)+j+q}$ on both sides, we have $b_j=0$. Then $F=y^f+b_qy^q+b_0$. Using this and comparing the coefficients of $y^{f(p-1)+2q}$ on both sides, we have $\binom{p}{1}b_q=0$, so $b_q=0$, which is a contradiction. □

**Theorem 3.** *$Z$ in (8) with $p\geq 4$ does not have a quadratic factor in $x$.*

*Proof.* Suppose that we have the decomposition

$$1+x+y^n+cx^py^q=\big(D_{p-2}(y)x^{p-2}+D_{p-3}(y)x^{p-3}+\cdots$$
$$+D_1(y)x+D_0(y)\big)\big(A(y)x^2+B(y)x+C(y)\big). \tag{10}$$

To simplify notation, from now on we simply write $D_{p-2},D_{p-3},...,D_0,A,B,C$. Comparing the coefficients of $x^p,x^{p-1},x^{p-2},...,x^3,x^2,x^1,x^0$ on both sides, we obtain respectively

$$cy^q=AD_{p-2}, \tag{11}$$
$$0=AD_{p-3}+BD_{p-2}, \tag{12}$$
$$0=AD_{p-4}+BD_{p-3}+CD_{p-2}, \tag{13}$$
$$0=AD_{p-5}+BD_{p-4}+CD_{p-3}, \tag{14}$$

$$\vdots$$

$$0 = AD_1 + BD_2 + CD_3, \tag{15}$$

$$0 = AD_0 + BD_1 + CD_2, \tag{16}$$

$$1 = BD_0 + CD_1, \tag{17}$$

$$1 + y^n = CD_0. \tag{18}$$

By (11), we can write $A = \alpha y^a$ and $D_{p-2} = \frac{c}{\alpha}\, y^{q-a}$, where $\alpha \neq 0$ and $0 \leq a \leq q$.

If $q = a > 0$, then $y \nmid D_{p-2}$. By (12), $y \mid B$. By (13), $y \mid C$. By (18), $y \mid (1+y^n)$, which is impossible.

If $a = 0$, then $y \nmid A$. By (12), $y \mid D_{p-3}$. By (13), $y \mid D_{p-4}$. Continuing, we have $y \mid D_0$. By (18), $y \mid (1 + y^n)$, which is impossible.

From now on, we assume that $0 < a < q$

Replacing $A = \alpha y^a$ and $D_{p-2} = \frac{c}{\alpha}\, y^{q-a}$ in (12), we get $D_{p-3} = -\frac{c}{\alpha^2}$ $y^{q-2a}B$. By (13), (14), we have respectively

$$D_{p-4} = \frac{c}{\alpha^3}\, y^{q-3a}B^2 - \frac{c}{\alpha^2}\, y^{q-2a}C, \quad D_{p-5} = -\frac{c}{\alpha^4}\, y^{q-4a}B^3 + \frac{2c}{\alpha^3}\, y^{q-3a}BC.$$

In general, for $k \geq 2$, we have

$$D_{p-k} = \frac{(-1)^k\, c}{\alpha^{k-1}}\, y^{q-(k-1)a}B^{k-2} + \frac{(-1)^{k+1}(k-3)c}{\alpha^{k-2}} y^{q-(k-2)a}B^{k-4}C + \cdots + E_k(y),$$

where

$$E_k := E_k(y) = \begin{cases} \frac{(-1)^r rc}{\alpha^{r+1}}\, y^{q-(r+1)a}BC^{r-1}, & \text{if } \ k = 2r+1, \\ (-1)^{r+1}\frac{c}{\alpha^r}\, y^{q-ra}C^{r-1}, & \text{if } k = 2r. \end{cases}$$

Thus from (15), (16), (17) and (18), we get

$$D_1 = \frac{(-1)^{p-1}\, c}{\alpha^{p-2}} y^{q-(p-2)a}B^{p-3} + \frac{(-1)^p(p-4)c}{\alpha^{p-3}} y^{q-(p-3)a}B^{p-5}C + \cdots + E_{p-1}\,, \tag{19}$$

$$D_0 = \frac{(-1)^p\, c}{\alpha^{p-1}} y^{q-(p-1)a}B^{p-2} + \frac{(-1)^{p+1}(p-3)c}{\alpha^{p-2}} y^{q-(p-2)a}B^{p-4}C + \cdots + E_p\,, \tag{20}$$

$$1 = \frac{(-1)^p\ c}{\alpha^{p-1}} y^{q-(p-1)a} B^{p-1} + \frac{(-1)^{p+1}(p-2)c}{\alpha^{p-2}} y^{q-(p-2)a} B^{p-3} C + ...+ \begin{cases} \frac{(-1)^{\frac{p-1}{2}} \frac{p-1}{2} c}{\alpha^{\frac{p+1}{2}}} y^{q-\frac{p+1}{2}a} B^2 C^{\frac{p-3}{2}} + \frac{(-1)^{\frac{p+1}{2}} c}{\alpha^{\frac{p-1}{2}}} y^{q-\frac{p-1}{2}a} C^{\frac{p-1}{2}}, & \text{if } p \text{ is odd,} \\ \text{const. } y^{q-\frac{p}{2}a} B C^{\frac{p-2}{2}}, & \text{if } p \text{ is even,} \end{cases} \tag{21}$$

$$1 + y^n = \frac{(-1)^p\ c}{\alpha^{p-1}} y^{q-(p-1)a} B^{p-2} C + \frac{(-1)^{p+1}(p-3)c}{\alpha^{p-2}} y^{q-(p-2)a} B^{p-4} C^2 + ...+ \begin{cases} \frac{(-1)^{\frac{p-1}{2}} \frac{p-1}{2} c}{\alpha^{\frac{p+1}{2}}} y^{q-\frac{p+1}{2}a} B C^{\frac{p-1}{2}}, & \text{if } p \text{ is odd,} \\ \text{const. } y^{q-\frac{p}{2}a} C^{\frac{p}{2}}, & \text{if } p \text{ is even.} \end{cases} \tag{22}$$

Here and throughout the rest of the proof constant denotes complex constant which may change step from step. Now distinguish all possible cases according to possible values of $q$.

*Case* $q > (p-1)a$. By (20), $y \mid D_0$. It follows from (18) that $y \mid (1 + y^n)$, which is impossible.

*Case* $(p-2)a \le q < (p-1)a$. It follows from (20) that $y \mid B$, and from (19) that $y \mid D_1$, which contradicts (17)

*Case* $q < (p-2)a$. By (20), $y \mid B$. Let $B = y^b \mathcal{B}(y)$, where $b \ge 1$ and $y \nmid \mathcal{B}(y)$. If $y \mid D_1$, by (17), $y \mid 1$, which is impossible. Thus $y \nmid D_1$. By (18), $y \nmid C$ and $y \nmid D_0$. Substituting for $B$ in (19), (20) and (21), we get, respectively

$$y^{(p-2)a-q} D_1 = \frac{(-1)^{p-1}\ c}{\alpha^{p-2}}\, y^{(p-3)b} \mathcal{B}^{p-3} + \frac{(-1)^p (p-4)c}{\alpha^{p-3}}\, y^{a+(p-5)b} \mathcal{B}^{p-5} C + \cdots + \begin{cases} \frac{(p-2)c}{2\alpha^{\frac{p}{2}}}\, y^{\frac{p-4}{2}a+b} \mathcal{B} C^{\frac{p-4}{2}}, & \text{if } p \text{ is even,} \\ \frac{(-1)^{\frac{p+1}{2}} c}{\alpha^{\frac{p-1}{2}}}\, y^{\frac{p-3}{2}a} C^{\frac{p-3}{2}}, & \text{if } p \text{ is odd,} \end{cases} \tag{23}$$

$$y^{(p-1)a-q} D_0 = \frac{(-1)^p\ c}{\alpha^{p-1}}\, y^{(p-2)b} \mathcal{B}^{p-2} + \frac{(-1)^{p+1}(p-3)c}{\alpha^{p-2}}\, y^{a+(p-4)b} \mathcal{B}^{p-4} C + \cdots + \begin{cases} \frac{(-1)^{\frac{p+2}{2}} c}{\alpha^{\frac{p}{2}}}\, y^{\frac{p-2}{2}a} C^{\frac{p-2}{2}}, & \text{if } p \text{ is even,} \\ \frac{(p-1)c}{2\alpha^{\frac{p+1}{2}}}\, y^{\frac{p-3}{2}a+b} \mathcal{B} C^{\frac{p-3}{2}}, & \text{if } p \text{ is odd,} \end{cases} \tag{24}$$

$$1 = \frac{(-1)^p\ c}{\alpha^{p-1}} y^{q-(p-1)(a-b)} \mathcal{B}^{p-1} + const. y^{q-(p-2)a+(p-3)b} \mathcal{B}^{p-3} C + ...+$$

$$\begin{cases} \text{const. } y^{q-\frac{p+1}{2}a+2b}\mathcal{B}^2C^{\frac{p-3}{2}} + const.y^{q-\frac{p-1}{2}a}C^{\frac{p-1}{2}}, & \text{if } p \text{ is odd,} \\ \text{const. } y^{q-\frac{p}{2}a+b}\mathcal{B}C^{\frac{p-2}{2}}, & \text{if } p \text{ is even.} \end{cases} \tag{25}$$

— If $2b < a$, comparing the degree of the monomial $y$-factor in (23) and (24), we have $(p-2)a-q = (p-3)b$ and $(p-1)a-q = (p-2)b$. Thus $(p-2)a-(p-3)b = q = (p-1)a-(p-2)b$, i.e. $b = a$, a contradiction.

— If $2b > a$, we distinguish two separate sub-cases.

— $p$ even. Comparing the degree of the monomial $y$-factor in (23) and (24), we have $(p-2)a-q = \frac{p-4}{2}a+b$ and $(p-1)a-q = \frac{p-2}{2}a$. Thus $(p-2)a-\frac{p-4}{2}a+b = q = (p-1)a-\frac{p-2}{2}a$ yielding $b = 0$, a contradiction.

— $p$ odd. Comparing the degree of the monomial $y$-factor in (23) and (24), we get $(p-2)a-q = \frac{p-3}{2}a$ and $(p-1)a-q = b+\frac{p-3}{2}$. Thus $(p-2)a-\frac{p-3}{2}a = q = (p-1)a-b-\frac{p-3}{2}a$ yielding $b = a$ and $q = \frac{p-1}{2}a$.

— If $2b = a$, and $p$ is even, from (25) we see that each term on the right hand side has a monomial $y$-factor of the same degree $q-(p-1)(a-b) = q-(p-1)b$. If $q-(p-1)b > 0$, then $y$ divides the right hand side but not the left hand side, which is impossible. If $q-(p-1)b \leq 0$, multiplying through by $y^{(p-1)b-q}$, we see that $\mathcal{B} \mid y^{(p-1)b-q}$ which forces $\mathcal{B}$ to be a constant. Thus comparing the degree of y in (24) and (25), we get $(p-1)2b-q+\deg\ D_0 = \frac{p-2}{2}\deg\ C+(p-2)b$ and $(p-1)b-q = \frac{p-2}{2}\deg\ C$, implying $\deg\ D_0 = -b$, which is impossible.

*Case* $q = (p-1)a$. If $p$ is even, then (21) shows that $B \mid 1$ and so $B$ is a constant. But then the left hand side of (21) is a constant, while on the right hand side each term is of different degree in $y$ with the last term having the highest degree which is impossible.

We are now left with three remaining cases:

X) $q = \frac{p-1}{2}a,\ b = a > 0,\ p$ odd;

Y) $q < (p-2)a,\ 2b = a > 0,\ p$ odd;

Z) $q = (p-1)a,\ p$ odd.

For odd $p > 4$,the equation (21) can be written as

$$\begin{aligned} \frac{(-1)^p\alpha^{p-1}}{c}y^{(p-1)a-q} &= B^{p-1}-(p-2)B^{p-3}\left(\alpha y^aC\right) \\ &\quad + \text{const. } B^{p-5}\left(\alpha y^aC\right)^2+...+(-1)^{\frac{p+1}{2}}\frac{p-1}{2}B^2\left(\alpha y^aC\right)^{\frac{p-3}{2}} \\ &\quad + (-1)^{\frac{p-1}{2}}B^0\left(\alpha y^aC\right)^{\frac{p-1}{2}}. \end{aligned}$$

Note that the expression on the right hand side can be factored so that

$$\frac{(-1)^p\alpha^{p-1}}{c}y^{(p-1)a-q} = (B^2-r_1\alpha y^aC)(B^2-r_2\alpha y^aC)...(B^2-r_{\frac{p-1}{2}}\ \alpha y^aC),$$

where the roots $r_1, ..., r_{\frac{p-1}{2}}$ are complex numbers. We claim that there exist at least two distinct roots. For otherwise, all roots are equal to $r$, say. Considering the sum and product of all these roots we must have $r = \frac{2(p-2)}{p-1}$ and $r^{\frac{p-1}{2}} = 1$, which are not compatible. Taking two distinct factors, say corresponding to $r_1 \neq r_2$, we deduce that there are nonnegative integers $\mu_1 \leq \mu_2$ satisfying

$$B^2 - r_1 \alpha y^a C = \text{const. } y^{\mu_1} \quad \text{and} \quad B^2 - r_2 \alpha y^a C = \text{const. } y^{\mu_2}.$$

Solving the two equations yields

$$(r_1 - r_2)\alpha y^a C = \text{const. } y^{\mu_2} - \text{const. } y^{\mu_1} \tag{26}$$

$$(r_1 - r_2)B^2 = \text{const. } y^{\mu_2} - \text{const. } y^{\mu_1}. \tag{27}$$

— If $\mu_1 = \mu_2$, then since $y \nmid C$, (26) yields $a = \mu_1 = \mu_2$ and so $C = \text{const.}$, and similarly (27) yields $2b = \mu_1 = \mu_2 = a$ and so $\mathcal{B}^2 = \text{const.}$ Substituting these values into (22), we get $y^{pb-q}(1 + y^n) = \text{const.}$, which is a contradiction.

— If $\mu_1 < \mu_2$, then as in the previous case $a = 2b = \mu_1 < \mu_2$, and so (27) yields $\mathcal{B}^2 = \text{const.} + \text{const. } y^{\mu_2 - \mu_1}$. Since the first *const.* does not vanish as $y \nmid \mathcal{B}$, this last relation is a contradiction because the left hand side, if not a constant, contains at least three distinct terms. The theorem is finally proved. □

## References

[1] A.M. Ostrowski, On the multiplication and factorization of polynomials, I. Lexicographic orderings and extreme aggregates of terms, *Aequationes Math.*, **13** (1975), 201-228.

[2] A.M. Ostrowski, On the multiplication and factorization of polynomials, II. Irreducibility discussion, *Aequationes Math.*, **14** (1976), 1-32.