ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 38, Number 2, 2008

ON THE NUMBER OF FACTORS OF CONVOLUTIONS OF POLYNOMIALS WITH INTEGER COEFFICIENTS

A.I. BONCIOCAT, N.C. BONCIOCAT AND A. ZAHARESCU

ABSTRACT. We obtain some irreducibility criteria for a class of polynomials of the form $h^{\deg f} \cdot f(g/h)$, where f, g, h are polynomials with integer coefficients, g and h relatively prime, in terms of the prime factorization of the leading coefficient of $h^{\deg f} \cdot f(g/h)$, the degrees of f, g, h, and the size of their coefficients.

1. Introduction. Inspired by earlier work in connection with Hilbert's irreducibility theorem, Cavachi [**3**] investigated the problem of the irreducibility of polynomials of the form $f(X) + pg(X)$, with p prime, $f(X), g(X)$ relatively prime and $\deg f < \deg g$. Given $f(X), g(X) \in \mathbf{Q}[X]$ relatively prime, with $\deg f < \deg g$, an explicit bound B was provided in [**4**] such that for all prime numbers $p > B$, the polynomial $f(X)+pg(X)$ is irreducible over $\mathbf{Q}$. In [**2**], explicit upper bounds have been derived for the number of factors over $\mathbf{Q}$ of a linear combination $n_1 f(X) + n_2 g(X)$, covering also the case $\deg f = \deg g$. In the present paper we consider multiplicative convolutions of polynomials, which offer considerably more flexibility to such irreducibility results, as they include linear combinations and compositions of polynomials. Given two polynomials $g(X) = b_0 + b_1 X + \cdots + b_n X^n$, $h(X) = c_0 + c_1 X + \cdots + c_l X^l \in \mathbf{Z}[X]$, $b_n c_l \neq 0$, by a *multiplicative convolution of g and h* we understand any polynomial of the form

$$\sum_{i=0}^{m} a_i g(X)^i h(X)^{m-i},$$

with $a_0, a_1, \ldots, a_m \in \mathbf{Z}$, $m \geq 1$, $a_0 a_m \neq 0$. If we associate to $a_0, a_1, \ldots, a_m$ the polynomial $f(X) = a_0 + a_1 X + \cdots + a_m X^m$, and

2000 AMS *Mathematics subject classification.* Primary 11C08.
Keywords and phrases. Convolution of polynomials, resultants.
Research partially supported by the CERES Program 4-187/2004 and the CEEX Program CEx05-D11-11/2005 of the Romanian Ministry of Education and Research.
Received by the editors on November 17, 2005, and in revised form on January 17, 2006.

DOI:10.1216/RMJ-2008-38-2-417

assume that $h \neq 0$, then

$$\sum_{i=0}^{m} a_i g(X)^i h(X)^{m-i} = h(X)^m f\left(\frac{g(X)}{h(X)}\right).$$

The irreducibility results we obtain for this kind of convolution will be expressed in terms of the prime factorization of the leading coefficient of the polynomial $h^{\deg f} f(g/h)$, the degrees of f, g, h, and the size of their coefficients. We will treat separately the cases $\deg h < \deg g$ and $\deg h = \deg g$, and will derive irreducibility criteria from more general results on the number of factors of the corresponding convolutions. We use the following notation. Given a polynomial $F(X) = a_0 + \cdots + a_m X^m \in \mathbf{Z}[X]$ of degree $m \geq 0$, we let

$$H(F) = \max\{|a_0|, \ldots, |a_m|\} \quad \text{and} \quad L(F) = \sum_{i=0}^{m} |a_i|,$$

and, if $m > 0$, we let

$$H_1(F) = \max\{|a_0|, \ldots, |a_{m-1}|\} \quad \text{and} \quad L_1(F) = \sum_{i=0}^{m-1} |a_i|.$$

For a nonzero integer n, we denote by $\Omega(n)$ the total number of prime factors of $|n|$ counting multiplicities, $\Omega(\pm 1) = 0$. In the case $\deg h < \deg g$ we prove the following results:

Theorem 1. *Let $f(X) = a_0 + a_1 X + \cdots + a_m X^m$, $g(X) = b_0 + b_1 X + \cdots + b_n X^n$ and $h(X) = c_0 + c_1 X + \cdots + c_l X^l \in \mathbf{Z}[X]$ be polynomials of degree m, n and l respectively, with $m \geq 1$, $n > l$, $a_0 \neq 0$, and g, h relatively prime. Let $\beta = 1 + [H_1(g) + H(h)]/|b_n|$. Assume that d_1 is a positive divisor of a_m and d_2 is a positive divisor of b_n such that*

$$|a_m| > \sum_{i=0}^{m-1} |a_i| \cdot [d_1^n d_2^{mn} L(h(\beta X))]^{m-i}.$$

Then the polynomial $h^m \cdot f(g/h)$ has at most $\Omega(a_m/d_1) + m\Omega(b_n/d_2)$ irreducible factors over $\mathbf{Q}$. The same conclusion holds in the wider range

$$|a_m| > \sum_{i=0}^{m-1} |a_i| \cdot [d_1^{n/m} d_2^n L(h(\beta X))]^{m-i},$$

provided that f is irreducible over $\mathbf{Q}$.

Under the assumption that a_m has a large enough prime factor, we have the following irreducibility criteria.

Corollary 1. *Let $f(X) = a_0 + a_1X + \cdots + a_mX^m$, $g(X) = b_0 + b_1X + \cdots + b_nX^n$ and $h(X) = c_0 + c_1X + \cdots + c_lX^l \in \mathbf{Z}[X]$ be polynomials of degree m, n and l respectively, with $m \geq 1$, $n > l$, $a_0 \neq 0$, f irreducible over $\mathbf{Q}$, and g, h relatively prime. Let $\beta = 1 + [H_1(g) + H(h)]/|b_n|$. If $a_m = pq$ with p a prime satisfying*

$$p > \frac{1}{|q|} \sum_{i=0}^{m-1} |a_i| \cdot [|q|^{n/m} |b_n|^n L(h(\beta X))]^{m-i}.$$

Then the polynomial $h^m \cdot f(g/h)$ is irreducible over $\mathbf{Q}$.

Corollary 2. *Let $f(X) = a_0 + a_1X + \cdots + a_mX^m$, $g(X) = b_0 + b_1X + \cdots + b_nX^n$ and $h(X) = c_0 + c_1X + \cdots + c_lX^l \in \mathbf{Z}[X]$ be polynomials of degree m, n and l respectively, with $m \geq 1$, $n > l$, $a_0 \neq 0$, and g, h relatively prime. Let $\beta = 1 + [H_1(g) + H(h)]/|b_n|$. If $a_m = pq$ with p a prime satisfying*

$$p > \frac{1}{|q|} \max\left\{ \sum_{i=0}^{m-1} |a_i| \cdot |q|^{m-i},\ \sum_{i=0}^{m-1} |a_i| \cdot [|q|^{n/m} |b_n|^n L(h(\beta X))]^{m-i} \right\},$$

then the polynomial $h^m \cdot f(g/h)$ is irreducible over $\mathbf{Q}$.

For the proof of Corollary 2, we first note that if $f(X) = a_0 + a_1X + \cdots + a_mX^m \in \mathbf{Z}[X]$ is a polynomial of degree $m \geq 1$, with $a_0 \neq 0$, and $a_m = pq$ with p a prime satisfying $p > |q|^{m-1} L_1(f(X/|q|))$, then f is irreducible over $\mathbf{Q}$. This follows from Theorem 1 by taking $g(X) = X$ and $h(X) = 1$. On the other hand, if the polynomial f is irreducible over $\mathbf{Q}$ and $a_m = pq$ with

$$p > \frac{1}{|q|} \sum_{i=0}^{m-1} |a_i| \cdot [|q|^{n/m} |b_n|^n L(h(\beta X))]^{m-i},$$

then by Corollary 1, the polynomial $h^m \cdot f(g/h)$ is irreducible over $\mathbf{Q}$. So, if p satisfies the hypothesis of Corollary 2, then both polynomials f and $h^m \cdot f(g/h)$ will be irreducible over $\mathbf{Q}$.

In the case $\deg h = \deg g$, we obtain the following results:

Theorem 2. *Let $f(X) = a_0 + a_1X + \cdots + a_mX^m \in \mathbf{Z}[X]$ be a polynomial of degree $m \geq 1$, $a_0 \neq 0$, and let $g(X) = b_0 + b_1X + \cdots + b_nX^n$ and $h(X) = c_0 + c_1X + \cdots + c_nX^n \in \mathbf{Z}[X]$ be two relatively prime polynomials of degree $n \geq 1$. Let $\alpha = \sum_{i=0}^{m} a_ib_n^ic_n^{m-i}$ and $\beta = 1 + (H_1(g) + H(h)/|b_n|) + (H_1(g)|c_n|/b_n^2)$. Assume $\alpha \neq 0$ and d is a positive divisor of α such that*

$$|a_m| > \sum_{i=0}^{m-1} |a_i| \cdot [d^n L(h(\beta X))]^{m-i}.$$

Then the polynomial $h^m \cdot f(g/h)$ has at most $\Omega(\alpha/d)$ irreducible factors over $\mathbf{Q}$. The same conclusion holds in the wider range

$$|a_m| > \sum_{i=0}^{m-1} |a_i| \cdot [d^{n/m} L(h(\beta X))]^{m-i},$$

provided that f is irreducible over $\mathbf{Q}$.

Corollary 3. *Let $f(X) = a_0 + a_1X + \cdots + a_mX^m \in \mathbf{Z}[X]$ be a polynomial of degree $m \geq 1$, $a_0 \neq 0$, and let $g(X) = b_0 + b_1X + \cdots + b_nX^n$ and $h(X) = c_0 + c_1X + \cdots + c_nX^n \in \mathbf{Z}[X]$ be two relatively prime polynomials of degree $n \geq 1$. Let $\beta = 1 + (H_1(g) + H(h)/|b_n|) + (H_1(g)|c_n|/b_n^2)$, and assume that $\sum_{i=0}^{m} a_ib_n^ic_n^{m-i} = p \cdot q \neq 0$ with p a prime number such that*

$$|a_m| > \sum_{i=0}^{m-1} |a_i| \cdot [|q|^n L(h(\beta X))]^{m-i}.$$

Then the polynomial $h^m \cdot f(g/h)$ is irreducible over $\mathbf{Q}$. The same conclusion holds in the wider range

$$|a_m| > \sum_{i=0}^{m-1} |a_i| \cdot [|q|^{n/m} L(h(\beta X))]^{m-i},$$

provided that f is irreducible over $\mathbf{Q}$.

2. Proof of Theorem 1. For the proof of Theorems 1 and 2 we need the following lemma [**1**], which is a variation of Capelli's theorem.

Lemma 1. *Let K be a field, $f, g, h \in K[X]$, f irreducible over K, g and h relatively prime, and $f(\alpha) = 0$. If*

$$g - \alpha h \underset{K(\alpha)}{\overset{can}{=}} \mathrm{const} \cdot \prod_{i=1}^{r} \phi_i(X)^{e_i},$$

then

$$h^{\deg f} \cdot f(g/h) \underset{K}{\overset{can}{=}} \mathrm{const} \cdot \prod_{i=1}^{r} N_{K(\alpha)/K} \phi_i(X)^{e_i}.$$

In particular, the degree of every irreducible factor of $h^{\deg f} \cdot f(g/h)$ must be a multiple of $\deg f$.

Here $F \underset{K}{\overset{can}{=}} \mathrm{const} \cdot \prod_{i=1}^{r} \phi_i(X)^{e_i}$ means that the ϕ_is are irreducible over K and prime to each other. For the sake of completeness we will give in Section 4 below a proof of the above lemma in the case char $(K) = 0$, which is relevant here.

We now proceed with the proof of Theorem 1. Let $f(X)$, $g(X)$, $h(X)$, d_1 and d_2 be as in the statement of the theorem. Assuming that $h^m \cdot f(g/h)$ has s irreducible factors over $\mathbf{Q}$, it will decompose as $h^m \cdot f(g/h) = F_1 \cdots F_s$, with $F_1, \dots, F_s \in \mathbf{Z}[X]$, and $\deg F_1 \geq 1, \dots, \deg F_s \geq 1$. Let $t_1, \dots, t_s \in \mathbf{Z}$ be the leading coefficients of $F_1, \dots, F_s$, respectively. By comparing the leading coefficients in the equality

$$h^m \cdot f(g/h) = a_0 h^m + \cdots + a_{m-1} g^{m-1} h + a_m g^m = F_1 \cdots F_s,$$

one finds that

$$a_m b_n^m = d_1 d_2^m \cdot \frac{a_m}{d_1} \cdot \left(\frac{b_n}{d_2}\right)^m = t_1 \cdots t_s. \tag{2.1}$$

Assume now that $s > \Omega(a_m/d_1) + m\Omega(b_n/d_2)$. Then, in view of (2.1), it follows that at least one of the t_is, say t_1, will divide $d_1 d_2^m$. In particular, we have

$$|t_1| \le d_1 d_2^m. \tag{2.2}$$

Let $\overline{f} = h^m \cdot f(g/h) - a_m g^m$. Then $h^m \cdot f(g/h) = \overline{f} + a_m g^m$, and since $a_0 \neq 0$, the polynomials $\overline{f}$ and g^m are algebraically relatively prime.

Next, we estimate the resultant $R(g^m, F_1)$. Since g^m and F_1 are also relatively prime, $R(g^m, F_1)$ must be a nonzero integer number, so in particular we have

$$|R(g^m, F_1)| \ge 1. \tag{2.3}$$

Let $r = \deg F_1 \ge 1$, and consider the decomposition of F_1, say

$$F_1(X) = t_1(X - \theta_1) \cdots (X - \theta_r),$$

with $\theta_1, \dots, \theta_r \in \mathbf{C}$. Then

$$|R(g^m, F_1)| = |t_1|^{mn} \prod_{1 \le j \le r} |g^m(\theta_j)|. \tag{2.4}$$

Since each root θ_j of F_1 is also a root of $h^m \cdot f(g/h)$, we have

$$g^m(\theta_j) = -\frac{\overline{f}(\theta_j)}{a_m}, \tag{2.5}$$

and moreover, since $\overline{f}$ and g^m are relatively prime, $\overline{f}(\theta_j) \neq 0$ and $g^m(\theta_j) \neq 0$ for any $j \in \{1, \dots, r\}$. Combining (2.4) and (2.5), we obtain

$$|R(g^m, F_1)| = \frac{|t_1|^{mn}}{|a_m|^r} \cdot \prod_{1 \le j \le r} |\overline{f}(\theta_j)|. \tag{2.6}$$

We now proceed to find an upper bound for $|\overline{f}(\theta_j)|$. In order to do this, we have to find an upper bound for the moduli of the roots of f. It is well known that, if the leading coefficient of a polynomial $f(X) = a_0 + a_1 X + \cdots + a_m X^m$ satisfies $|a_m| > L_1(f)$, then all the roots $\lambda_1,\dots,\lambda_m$ of f must satisfy $|\lambda_i|<1$. Let us fix now an arbitrarily chosen real number $\delta>0$ and assume that $|a_m|/\delta^m > L_1(f(X/\delta))$. Then all the roots $\delta\lambda_1,\dots,\delta\lambda_m$ of $f(X/\delta)$ will verify $|\delta\lambda_i|<1$, so all the λ_is will verify

$$|\lambda_i| < \frac{1}{\delta}. \tag{2.7}$$

Let now $\theta_1,\dots,\theta_{mn}$ be the roots of $h^m\cdot f(g/h)$. Since g and h are relatively prime, one has $h(\theta_j)\neq 0$ and $f(g(\theta_j)/h(\theta_j))=0$ for $j=1,\dots,mn$. Thus, for a given θ_j, there exists $i_j\in\{1,\dots,m\}$ such that $g(\theta_j)/h(\theta_j)=\lambda_{i_j}$, a root of f. By (2.7), we then have

$$\left|\frac{g(\theta_j)}{h(\theta_j)}\right| < \frac{1}{\delta}. \tag{2.8}$$

Recall that $\overline{f}=a_0h^m+a_1gh^{m-1}+\cdots+a_{m-1}g^{m-1}h$. Using (2.8), we derive that

$$|\overline{f}(\theta_j)| = \left|\sum_{i=0}^{m-1} a_i g(\theta_j)^i h(\theta_j)^{m-i}\right| \le |h(\theta_j)|^m\cdot L_1(f(X/\delta)). \tag{2.9}$$

Combining now (2.6), (2.9) and (2.2), we deduce the following upper bound for $|R(g^m,F_1)|$:

$$|R(g^m,F_1)| \le d_1^{mn}d_2^{m^2n}\cdot\left[\frac{|h(\theta_j)|^m L_1(f(X/\delta))}{|a_m|}\right]^r. \tag{2.10}$$

The inequality (2.8) allows us to find also an upper bound for $|h(\theta_j)|$, as follows. By (2.8) we see that

$$\delta|b_0+b_1\theta_j+\cdots+b_n\theta_j^n| < |c_0+c_1\theta_j+\cdots+c_l\theta_j^l|,$$

which further gives

$$\begin{aligned}\delta|b_n||\theta_j|^n &< (|c_0|+\delta|b_0|)+(|c_1|+\delta|b_1|)|\theta_j|+\cdots+(|c_l|+\delta|b_l|)|\theta_j|^l\\ &\quad+\delta|b_{l+1}||\theta_j|^{l+1}+\cdots+\delta|b_{n-1}||\theta_j|^{n-1}\\ &< (H(h)+\delta H_1(g))\cdot(1+|\theta_j|+\cdots+|\theta_j|^{n-1}).\end{aligned}$$

Therefore, we either have $|\theta_j| \leq 1$, or, if not, then we obtain

$$\delta|b_n||\theta_j|^n < (H(h)+\delta H_1(g)) \cdot \frac{|\theta_j|^n - 1}{|\theta_j| - 1} < (H(h)+\delta H_1(g)) \cdot \frac{|\theta_j|^n}{|\theta_j| - 1},$$

which yields

$$|\theta_j| < 1 + \frac{H(h)+\delta H_1(g)}{\delta|b_n|}. \tag{2.11}$$

Denoting by γ the righthand side of (2.11), we find that

$$|h(\theta_j)| < L(h(\gamma X)),$$

which, combined with (2.10), yields

$$|R(g^m, F_1)| \leq d_1^{mn} d_2^{m^2 n} \cdot \left[\frac{L(h(\gamma X))^m L_1(f(X/\delta))}{|a_m|}\right]^r. \tag{2.12}$$

Since $\deg F_1 = r \geq 1$, all we need to prove is that our assumption on the size of $|a_m|$ will imply on one hand $|a_m| > \delta^m L_1(f(X/\delta))$ for a suitable $\delta > 0$, and on the other hand will force

$$d_1^{mn} d_2^{m^2 n} \cdot \frac{L(h(\gamma X))^m L_1(f(X/\delta))}{|a_m|} < 1,$$

or equivalently,

$$|a_m| > d_1^{mn} d_2^{m^2 n} L(h(\gamma X))^m L_1(f(X/\delta)),$$

in order to contradict the fact that $|R(g^m, F_1)| \geq 1$. It will therefore be sufficient to have $|a_m| > \delta^m L_1(f(X/\delta))$ for a $\delta > 0$ as small as possible satisfying $\delta^m \geq d_1^{mn} d_2^{m^2 n} L(h(\gamma X))^m$, that is, $\delta \geq d_1^n d_2^{mn} L(h(\gamma X))$. Recalling the definition of γ, the last inequality reads

$$\delta \geq d_1^n d_2^{mn} \sum_{i=0}^{l} |c_i| \left(1 + \frac{H_1(g)}{|b_n|} + \frac{H(h)}{\delta|b_n|}\right)^i.$$

A suitable candidate for δ is

$$\delta_0 = d_1^n d_2^{mn} \sum_{i=0}^{l} |c_i| \left(1 + \frac{H_1(g)+H(h)}{|b_n|}\right)^i \geq 1,$$

since

$$1+\frac{H_1(g)+H(h)}{|b_n|}\geq 1+\frac{H_1(g)}{|b_n|}+\frac{H(h)}{|b_n|\delta_0}.$$

By the definition of β, δ_0 just found coincides with $d_1^n d_2^{mn}L(h(\beta X))$, which proves that for

$$\begin{aligned}|a_m|&>[d_1^n d_2^{mn}L(h(\beta X))]^m\cdot L_1\left(f\left(\frac{X}{d_1^n d_2^{mn}L(h(\beta X))}\right)\right)\\&=\sum_{i=0}^{m-1}|a_i|\cdot[d_1^n d_2^{mn}L(h(\beta X))]^{m-i},\end{aligned}$$

we actually have $|R(g^m,F_1)|<1$, a contradiction. Therefore, $h^m\cdot f(g/h)$ has at most $\Omega(a_m/d_1)+m\Omega(b_n/d_2)$ factors over $\mathbf{Q}$, and this proves the first part of the theorem.

Assuming now that f is irreducible over $\mathbf{Q}$, the proof goes as in the first part except that, by Lemma 1, the degree of every irreducible factor of $h^m\cdot f(g/h)$ must be a multiple of m, so we must have $\deg(F_1)=r\geq m$. In this case we need to prove that our assumption on the size of $|a_m|$ implies again $|a_m|>\delta^m L_1(f(X/\delta))$ for a suitable $\delta>0$, and at the same time it forces the inequality

$$d_1^n d_2^{mn}\cdot\frac{L(h(\gamma X))^m L_1(f(X/\delta))}{|a_m|}<1,$$

or equivalently,

$$|a_m|>d_1^n d_2^{mn}L(h(\gamma X))^m L_1(f(X/\delta)),$$

which in view of (2.12) will contradict (2.3). It will be therefore sufficient to find a $\delta>0$ such that $\delta^m\geq d_1^n d_2^{mn}L(h(\gamma X))^m$, that is $\delta\geq d_1^{n/m}d_2^n L(h(\gamma X))$, which, recalling the definition of γ, reads

$$\delta\geq d_1^{n/m}d_2^n\sum_{i=0}^{l}|c_i|\left(1+\frac{H_1(g)}{|b_n|}+\frac{H(h)}{\delta|b_n|}\right)^i.$$

A suitable candidate for δ in this case is

$$\delta_1=d_1^{n/m}d_2^n\sum_{i=0}^{l}|c_i|\left(1+\frac{H_1(g)+H(h)}{|b_n|}\right)^i=d_1^{n/m}d_2^n L(h(\beta X))\geq 1,$$

so the contradiction $|R(g^m, F_1)| < 1$ follows now if

$$\begin{aligned}|a_m| &> [d_1^{n/m} d_2^n L(h(\beta X))]^m \cdot L_1\biggl(f\biggl(\frac{X}{d_1^{n/m} d_2^n L(h(\beta X))}\biggr)\biggr)\\ &= \sum_{i=0}^{m-1} |a_i| \cdot [d_1^{n/m} d_2^n L(h(\beta X))]^{m-i}.\end{aligned}$$

This completes the proof of the theorem. □

Remark. Additional information on the coefficients of g and h allows one to obtain sharper bounds than those exhibited in Theorem 1, by searching for sharper estimates for the moduli of the roots of $h^{\deg f} \cdot f(g/h)$. For instance, if $f(X) = a_0 + a_1 X + \cdots + a_m X^m \in \mathbf{Z}[X]$ is a polynomial of degree $m \geq 1$ and d_1 is a positive divisor of a_m such that

$$|a_m| > \sum_{i=0}^{m-1} |a_i| \cdot [d_1^4 + d_1^2]^{(m-i)/2},$$

then the reciprocal polynomial $X^m \cdot f(X + 1/X)$ has at most $\Omega(a_m/d_1)$ irreducible factors over $\mathbf{Q}$. The same conclusion holds in the wider range

$$|a_m| > \sum_{i=0}^{m-1} |a_i| \cdot [d_1^{4/m} + d_1^{2/m}]^{(m-i)/2},$$

provided that f is irreducible over $\mathbf{Q}$. Here $g(X) = X^2 + 1$, $h(X) = X$ and $d_2 = 1$. By (2.8) we easily find that $|h(\theta_j)| = |\theta_j| < (1 + \sqrt{1 + 4\delta^2})/(2\delta)$, so, instead of (2.10), we have

$$|R(g^m, F_1)| \leq d_1^{2m} \cdot \left[\frac{\bigl(1 + \sqrt{1 + 4\delta^2}/2\delta\bigr)^m L_1(f(X/\delta))}{|a_m|}\right]^r.$$

We therefore obtain the contradiction $|R(g^m, F_1)| < 1$ if we have the inequality $|a_m| > \delta^m L_1(f(X/\delta))$, with δ satisfying

$$\delta \geq d_1^2 \cdot \frac{1 + \sqrt{1 + 4\delta^2}}{2\delta},$$

and it follows easily that the latter holds for $\delta \geq \sqrt{d_1^4 + d_1^2}$. Similarly, if f is irreducible over $\mathbf{Q}$, we obtain $|R(g^m, F_1)| < 1$ for $|a_m| > \delta^m L_1(f(X/\delta))$, with $\delta \geq \sqrt{d_1^{4/m} + d_1^{2/m}}$.

3. Proof of Theorem 2. The proof is similar to that of Theorem 1, with some significant differences caused by the fact that in this case all the terms appearing in the convolution contribute to the leading coefficient of $h^{\deg f} \cdot f(g/h)$. Assuming as in the proof of Theorem 1 that $h^m \cdot f(g/h)$ has s irreducible factors over $\mathbf{Q}$, it will decompose as $h^m \cdot f(g/h) = F_1(X) \cdots F_s(X)$, with $F_1(X), \ldots, F_s(X) \in \mathbf{Z}[X]$, and $\deg F_1 \geq 1, \ldots, \deg F_s \geq 1$. Denoting by $t_1, \ldots, t_s \in \mathbf{Z}$ the leading coefficients of $F_1, \ldots, F_s$, respectively and comparing the leading coefficients in the equality $h^m \cdot f(g/h) = F_1 \cdots F_s$, one finds now that $\sum_{i=0}^{m} a_i b_n^i c_n^{m-i} = (\alpha/d) \cdot d = t_1 \cdots t_s$. If we assume that $s > \Omega(\alpha/d)$, it follows that at least one of the t_is, say t_1, will divide d, so in particular we have $|t_1| \leq d$. Using the same notations as in the proof of Theorem 1, one has $|R(g^m, F_1)| \geq 1$, and on the other hand

$$|R(g^m, F_1)| \leq \frac{d^{mn}}{|a_m|^r} \cdot \prod_{1 \leq j \leq r} \left|\overline{f}(\theta_j)\right|. \tag{3.1}$$

As before, we fix an arbitrarily chosen real number $\delta > 0$ and assume that $|a_m|/\delta^m > L_1(f(X/\delta))$. Then all the roots $\lambda_1, \ldots, \lambda_m$ of f will satisfy $|\lambda_i| < 1/\delta$. As a consequence, we obtain

$$\left|\frac{g(\theta_j)}{h(\theta_j)}\right| < \frac{1}{\delta}, \tag{3.2}$$

uniformly for $1 \geq j \geq r$. Recalling now the definition of $\overline{f}$ and using (3.2), we deduce that $|\overline{f}(\theta_j)| \leq |h(\theta_j)|^m \cdot L_1(f(X/\delta))$. Combining this inequality and (3.1), we obtain

$$|R(g^m, F_1)| \leq d^{mn} \cdot \left[\frac{|h(\theta_j)|^m L_1(f(X/\delta))}{|a_m|}\right]^r. \tag{3.3}$$

We then derive an upper bound for $|h(\theta_j)|$ as follows. By (3.2) we find

$$\delta|b_0 + b_1\theta_j + \cdots + b_n\theta_j^n| < |c_0 + c_1\theta_j + \cdots + c_n\theta_j^n|,$$

which further gives

$$(\delta|b_n|-|c_n|)|\theta_j|^n<(H_1(h)+\delta H_1(g))\cdot(1+|\theta_j|+\cdots+|\theta_j|^{n-1}).$$

Let us assume that

$$\delta|b_n|>|c_n|. \tag{3.4}$$

Therefore, we either have $|\theta_j|\le 1$, or if not, we obtain

$$(\delta|b_n|-|c_n|)|\theta_j|^n<(H_1(h)+\delta H_1(g))\cdot\frac{|\theta_j|^n}{|\theta_j|-1},$$

which in view of (3.4) gives

$$|\theta_j|<1+\frac{H_1(h)+\delta H_1(g)}{\delta|b_n|-|c_n|}. \tag{3.5}$$

Denoting by γ the righthand side of (3.5), we obviously have $|h(\theta_j)|<L(h(\gamma X))$ which, combined with (3.3), yields

$$|R(g^m,F_1)|\le d^{mn}\cdot\left[\frac{L(h(\gamma X))^m L_1(f(X/\delta))}{|a_m|}\right]^r. \tag{3.6}$$

Since $\deg F_1=r\ge 1$, all it remains to be proved in this case is that our assumption on the size of $|a_m|$ implies on one hand $|a_m|>\delta^m L_1(f(X/\delta))$ for a suitable $\delta>|c_n|/|b_n|$, and on the other hand, it implies $|a_m|>d^{mn}L(h(\gamma X))^m L_1(f(X/\delta))$, in order to contradict the fact that $|R(g^m,F_1)|\ge 1$. It will be enough to have $|a_m|>\delta^m L_1(f(X/\delta))$ for a $\delta>|c_n|/|b_n|$ satisfying $\delta^m\ge d^{mn}L(h(\gamma X))^m$, that is $\delta\ge d^n L(h(\gamma X))$. This last inequality is equivalent to

$$\delta\ge d^n\sum_{i=0}^{n}|c_i|\left(A+\frac{B}{\delta-(|c_n|/|b_n|)}\right)^i,$$

where $A=1+(H_1(g)/|b_n|)$ and $B=(|c_n|/b_n^2)H_1(g)+(H_1(h)/|b_n|)$. Note that, since g and h are relatively prime, we have $H_1(g)+H_1(h)$

≥ 1. We may therefore choose for δ the value $\delta_0 = d^n \sum_{i=0}^{n} |c_i| \times (A+B)^i \geq 1 + |c_n|/|b_n|$, since

$$\begin{aligned}\delta_0 - \frac{|c_n|}{|b_n|} &= d^n \sum_{i=0}^{n} |c_i| \left(1 + \frac{H_1(g)+H_1(h)}{|b_n|} + \frac{|c_n|}{b_n^2} H_1(g)\right)^i \\ &\quad - \frac{|c_n|}{|b_n|} \\ &\geq |c_n| \cdot \left(1 + \frac{1}{|b_n|}\right)^n - \frac{|c_n|}{|b_n|} \geq |c_n| \geq 1,\end{aligned}$$

which also shows that δ_0 verifies (3.4). By the definition of β, we see that δ_0 coincides with $d^n L(h(\beta X))$, hence for $|a_m| > \sum_{i=0}^{m-1} |a_i| \cdot [d^n L(h(\beta X))]^{m-i}$ we have $|R(g^m, F_1)| < 1$, a contradiction. Thus, $h^m \cdot f(g/h)$ has at most $\Omega(a_m/d_1) + m\Omega(b_n/d_2)$ factors over $\mathbf{Q}$, which completes the proof of the first part of the theorem. For the second part, if f is assumed to be irreducible over $\mathbf{Q}$, then by Lemma 1, the degree of every irreducible factor of $h^m \cdot f(g/h)$ is a multiple of m. Consequently $\deg(F_1) = r \geq m$. In this case we need to show that our assumption on the size of $|a_m|$ implies $|a_m| > \delta^m L_1(f(X/\delta))$ for a suitable $\delta > |c_n|/|b_n|$, and $|a_m| > d^n L(h(\gamma X))^m L_1(f(X/\delta))$, which by (3.6) will contradict the fact that $|R(g^m, F_1)| < 1$. It is enough to find a $\delta > |c_n|/|b_n|$ satisfying $\delta \geq d^{n/m} L(h(\gamma X))$. By the definition of γ, A and B, this inequality states that

$$\delta \geq d^{n/m} \sum_{i=0}^{n} |c_i| \left(A + \frac{B}{\delta - (|c_n|/|b_n|)}\right)^i.$$

We may choose for δ the value $\delta_1 = d^{n/m} \sum_{i=0}^{n} |c_i|(A+B)^i \geq 1 + |c_n|/|b_n|$. Then $|R(g^m, F_1)| < 1$ provided $|a_m| > \sum_{i=0}^{m-1} |a_i| \cdot [d^{n/m} L(h(\beta X))]^{m-i}$, which completes the proof of the theorem.

4. Proof of Lemma 1. We follow the proof of Capelli's theorem from [**5**]. Since $\operatorname{char}(K) = 0$ and f is assumed to be irreducible over K, the zeros α_ν of f are all distinct. Then, since $f(\alpha) = 0$, f will decompose as

$$f(X) = \text{const} \cdot \prod_{\nu=1}^{\deg f} (X - \alpha_\nu),$$

where $\alpha = \alpha_1$, say. Therefore,

$$h(X)^{\deg f} \cdot f\left(g(X)/h(X)\right) = \text{const} \cdot \prod_{\nu=1}^{\deg f} [g(X) - \alpha_\nu h(X)]. \tag{4.1}$$

Denoting by $\phi_i^{(\nu)}$, the polynomial obtained from ϕ_i on replacing α by α_ν, we have $g(X) - \alpha_\nu h(X) = \text{const} \cdot \prod_{i=1}^{r} \phi_i^{(\nu)}(X)^{e_i}$ for each ν, so by (4.1) we obtain

$$h^{\deg f} \cdot f(g/h) \underset{K}{=} \text{const} \cdot \prod_{i=1}^{r} N_{K(\alpha)/K}\phi_i{}^{e_i}.$$

In order to see that this is a canonical decomposition, we first have to prove that the polynomials $N_{K(\alpha)/K}\phi_i(X)$ are irreducible over K. If we assume that $\phi_i(X) \mid I_i(X)$ with I_i irreducible over K, we must also have $\phi_i^{(\nu)}(X) \mid I_i(X)$ for each ν. Then, since $\phi_i(X) \mid [g(X) - \alpha h(X)]$, it follows that

$$\phi_i^{(\nu)}(X) \mid [g(X) - \alpha_\nu h(X)], \tag{4.2}$$

for each ν. We now show that ϕ_i and $\phi_i^{(\nu)}$ are relatively prime. Assuming the contrary, then in view of (4.2) we obtain on one hand $\gcd(\phi_i, \phi_i^{(\nu)}) \mid (\alpha - \alpha_\nu)h$, and on the other hand, $\gcd(\phi_i, \phi_i^{(\nu)}) \mid (\alpha_\nu/\alpha - 1)g$. Since $\alpha \neq \alpha_\nu$, this contradicts the fact that g and h are relatively prime. Therefore, ϕ_i and $\phi_i^{(\nu)}$ are relatively prime, which shows that$N_{K(\alpha)/K}\phi_i(X) \mid I_i(X)$, so $N_{K(\alpha)/K}\phi_i(X)$ is irreducible over K. Now it remains to show that the norms are coprime. Since for $i \neq j$ one has $(\phi_i, \phi_j) = 1$, we obtain by the same argument as above that $(\phi_i, \phi_j^{(\nu)}) = 1$ for all ν. Thus, for $i \neq j$ one has $(\phi_i, N_{K(\alpha)/K}\phi_j) = 1$, and then $(N_{K(\alpha)/K}\phi_i, N_{K(\alpha)/K}\phi_j) = 1$, which completes the proof. □

REFERENCES

1. A.I. Bonciocat and N.C. Bonciocat, *A Capelli type theorem for multiplicative convolutions of polynomials*, Math. Nach., to appear.

2. N.C. Bonciocat, *Upper bounds for the number of factors for a class of polynomials with rational coefficients*, Acta Arith. **113** (2004), 175–187.

3. M. Cavachi, *On a special case of Hilbert's irreducibility theorem*, J. Number Theory **82** (2000), 96–99.

4. M. Cavachi, M. Vâjâitu and A. Zaharescu, *A class of irreducible polynomials*, J. Ramanujan Math. Soc. **17** (2002), 161–172.

5. A. Schinzel, *Polynomials with special regard to reducibility*, in *Encyclopedia of mathematics and its applications*, Cambridge University Press, Cambridge, 2000.

Institute of Mathematics of the Romanian Academy, P.O. Box 1-764,
Bucharest 014700, Romania
Email address: Anca.Bonciocat@imar.ro

Institute of Mathematics of the Romanian Academy, P.O. Box 1-764,
Bucharest 014700, Romania
Email address: Nicolae.Bonciocat@imar.ro

Department of Mathematics, University of Illinois at Urbana-Champaign,
Altgeld Hall, 1409 W. Green Street, Urbana, IL, 61801
Email address: zaharesc@math.uiuc.edu