PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 135, Number 3, March 2007, Pages 677–687
S 0002-9939(06)08526-1
Article electronically published on September 11, 2006

SQUARE-FREE CRITERIA FOR POLYNOMIALS USING NO DERIVATIVES

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

(Communicated by Ken Ono)

ABSTRACT. We provide some square-free criteria for primitive polynomials over unique factorization domains, which do not make use of derivatives or discriminants. Using some ideas of Ostrowski we establish nonvanishing conditions for determinants of matrices with polynomial entries and deduce square-free criteria for polynomials in several variables.

1. INTRODUCTION

In many applications it is desirable to know if a given polynomial is square-free. For instance, a square matrix is diagonalizable if the characteristic polynomial is square-free. One of the most important uses of derivatives in the study of polynomials consists in the investigation of their multiple factors. A fundamental result in this direction is that given two nonconstant polynomials f and g with coefficients in a unique factorization domain of characteristic zero, g irreducible, then g^2 divides f if and only if g divides f and f' (see [16]). An equivalent result is that a polynomial over a unique factorization domain of characteristic zero has a repeated nonconstant factor if and only if its discriminant is zero. It is also well known that if K is a field and F an extension of K, then a polynomial $f \in K[X]$ has $c \in F$ for a multiple root if and only if $f(c) = f'(c) = 0$ (see [6]). For an account on the theory of separable polynomials over commutative rings, the reader is referred to DeMeyer [1], [2], Janusz [5] Nagahara [8], [9], Harrison and McKenzie [4], and McKenzie [7]. Some inconveniences in the use of derivatives over domains of characteristic $p \neq 0$ are due to the fact that the derivative of any polynomial $f \in R[X^p]$ is zero. In this paper we consider primitive polynomials over a unique factorization domain R, and in this framework we first give a square-free criterion for primitive polynomials $f \in R[X]$, which does not make use of derivatives or discriminants. Thus, instead of searching for the common factors of f and its derivative, we fix an arbitrary integer $m \geq 2$ and look for those polynomials g^m with $\deg g = \deg f - 1$, which are not divisible by f. We then obtain some square-free criteria for polynomials over unique factorization domains of characteristic 2, in terms of the prime factorization of their coefficients. By using some ideas of Ostrowski [13], we establish in

Received by the editors September 12, 2005 and, in revised form, October 10, 2005.
2000 *Mathematics Subject Classification.* Primary 11C08, 11C20.
Key words and phrases. Square-free criteria, primitive polynomials, resultants, Frobenius map.
This research was partially supported by the CERES Programs 4-147 and 4-187/2004 of the Romanian Ministry of Education and Research.

the final section some nonvanishing conditions for determinants of matrices with polynomial entries, and then deduce some square-free conditions for polynomials in several variables over fields of characteristic 2, which are expressed only in terms of the degrees of their coefficients.

2. Square-free criteria over unique factorization domains

The square-free criteria for polynomials over unique factorization domains derived in this section are inspired by the following square-free criterion for positive integers: *Let $m \geq 2$ be a fixed, arbitrarily chosen integer. An integer $n > 1$ is square-free if and only if $n \nmid a^m$ for each integer a with $\sqrt{n} \leq a < n$.*

This claim can be proved as follows. Assume n is square-free, that is, $n = p_1 \cdots p_k$ with $k \geq 1$ and $p_1, \ldots, p_k$ distinct primes. Then for every integer a with $\sqrt{n} \leq a < n$, n cannot divide a^m, since this would force n to divide a. Conversely, assume $n = p_1^{n_1} \cdots p_k^{n_k}$ with at least one of the exponents strictly bigger than 1, say $n_1 \geq 2$, and take $a = n/p_1$. The multiplicity of p_1 in the prime decomposition of a^m is $m(n_1 - 1)$, which is at least n_1, since $m \geq 2$ and $n_1 \geq 2$. Therefore n divides a^m, and obviously $\sqrt{n} \leq a < n$. This is the kind of example suggesting the fact that one may search for some information on the factorization of an element x in a domain R, by looking not at the elements dividing x or at the elements that x divides, but rather at those elements of R which are not divisible by x.

Next we present a polynomial analogue of the above result.

Proposition 2.1. *Let R be a unique factorization domain and $f \in R[X]$ a primitive polynomial with $\deg(f) = n \geq 2$. Fix an arbitrarily chosen integer $m \geq 2$. Then the following are equivalent:*

i) *The polynomial f is square-free over R.*

ii) *For every $g \in R[X]$ with $\deg(g) = n - 1$, g^m is not divisible by f.*

Proof. i) $\Rightarrow$ ii) Let $f = p_1 \cdots p_k$, with $p_1, \ldots, p_k \in R[X]$ irreducible and pairwise nonassociated in divisibility. Assume there is a polynomial $g \in R[X]$ with $\deg(g) = n - 1$, such that f divides g^m. Then each one of the p_i's will divide g, and hence f will divide g, which is impossible since $\deg(g) = \deg(f) - 1$.

ii) $\Rightarrow$ i) Assume to the contrary that $f = p_1^{n_1} \cdots p_k^{n_k}$ with $p_1, \ldots, p_k \in R[X]$ irreducible and pairwise nonassociated in divisibility, with at least one of the exponents strictly bigger than 1, say $n_1 \geq 2$. Then, the multiplicity of p_1 in the canonical decomposition of $(f/p_1)^m$ is $m(n_1 - 1)$, which is at least n_1, since $m \geq 2$ and $n_1 \geq 2$. Thus f will divide $(f/p_1)^m$. Now, since $\deg(p_1) \geq 1$, we have $\deg(f/p_1) \leq n - 1$. In case $\deg(p_1) = 1$ we take $g = f/p_1$, while if $\deg(p_1) > 1$ we multiply f/p_1 by a polynomial $h \in R[X]$ with $\deg(h) = \deg(p_1) - 1$, and consider $g = fh/p_1$. In both situations we find g^m divisible by f and $\deg(g) = n - 1$, a contradiction. □

The above criterion is quite flexible, uses no derivatives, and in the case of positive characteristic holds regardless of whether the Frobenius map is surjective or not. Further in positive characteristic one may choose the integer m as the characteristic of R. Now let R be a unique factorization domain of positive characteristic

p. For any polynomial $f = a_0 + a_1X + \cdots + a_nX^n \in R[X]$ of degree $n \geq 2$ denote

$$M = \begin{bmatrix} a_0 & & & & \\ a_1 & a_0 & & & \\ \cdot & a_1 & \cdot & & \\ a_n & \cdot & \cdot & \cdot & \\ & a_n & \cdot & \cdot & \\ & & \cdot & \cdot & a_0 \\ & & & \cdot & a_1 \\ & & & & \cdot \\ & & & & a_n \end{bmatrix},$$

a matrix with $(n-1)p+1$ rows and $(p-1)(n-1)$ columns, where the entries which are not displayed are assumed to be zero. Let $M(n,p)$ be the square matrix obtained from M by omitting the rows whose indices are multiples of p plus 1: $r_1, r_{p+1}, \ldots, r_{(n-1)p+1}$. Then one has the following result.

Corollary 2.2. *Let R be a unique factorization domain of positive characteristic p and $f = a_0 + a_1X + \cdots + a_nX^n \in R[X]$ a primitive polynomial of degree $n \geq 2$. If $\det M(n,p) \neq 0$, then f is square-free over R. Moreover, if the Frobenius map of R is surjective, then f is square-free over R if and only if $\det M(n,p) \neq 0$.*

Proof. Take $m = p$ in Proposition 2.1. Then f has no repeated irreducible factors over R if and only if g^p is not divisible by f, for any polynomial $g \in R[X]$ of degree $n-1$. We regard the equality

$$f(X) \cdot h(X) = g(X)^p \tag{2.1}$$

with

$$g(X) = \sum_{i=0}^{n-1} b_iX^i \in R[X] \quad \text{and} \quad h(X) = \sum_{i=0}^{(p-1)n-p} c_iX^i \in R[X]$$

as a homogeneous system in the indeterminates $c_0, \ldots, c_{(p-1)n-p}$ and $b_0^p, \ldots, b_{n-1}^p$, since $g^p = \sum_{i=0}^{n-1} b_i^p X^{ip}$. The determinant of the system associated to (2.1) is exactly $(-1)^n \det M(n,p)$. Therefore, if $\det M(n,p) \neq 0$, the system will have only the trivial solution, so (2.1) will fail for any pair (g,h) with $\deg g = n-1$ and $\deg h = (p-1)n-p$. If the Frobenius map of R is surjective, then the homogeneous system in the indeterminates $c_0, \ldots, c_{(p-1)n-p}$ and $b_0^p, \ldots, b_{n-1}^p$ may be regarded as a linear one. Therefore, if $\det M(n,p) = 0$, the system associated to (2.1) will have a nontrivial solution in the quotient field of R. Multiplying by a common denominator (which itself is the pth power of some element in R) gives a solution in R for which at least one b_i or one c_i is not zero. If one c_i, say, is not zero, then $h \neq 0$, and hence also $g \neq 0$. Finally, if $\deg g < n-1$, we multiply (2.1) by $\widetilde{g}^p$, where $\widetilde{g} \in R[X]$ can be any polynomial of degree $n-1-\deg g$, thus obtaining a solution for which $\deg g = n-1$ and $\deg h = (p-1)n-p$. Then, according to Proposition 2.1 f must have a repeated nonconstant factor over R, which completes the proof. □

3. Remarks and examples

1) The shape of $M(n,p)$ depends on the residue class of n modulo p. For instance if $p=2$ and $k\geq 1$, after a permutation of the columns we find

$$\det M(2k,2)=\begin{vmatrix} a_1 & & & & a_0 & & & \\ a_3 & a_1 & & & a_2 & a_0 & & \\ \cdot & a_3 & \cdot & & \cdot & a_2 & \cdot & \\ \cdot & \cdot & \cdot & & \cdot & \cdot & \cdot & a_0 \\ a_{2k-1} & \cdot & \cdot & a_1 & a_{2k-2} & \cdot & \cdot & a_2 \\ & a_{2k-1} & \cdot & a_3 & a_{2k} & & \cdot & \cdot \\ & & \cdot & \cdot & & a_{2k} & \cdot & \cdot \\ & & & a_{2k-1} & & & & a_{2k} \end{vmatrix}, \tag{3.1}$$

while

$$\det M(2k+1,2)=\begin{vmatrix} a_1 & & & & a_0 & & & \\ a_3 & a_1 & & & a_2 & a_0 & & \\ \cdot & a_3 & \cdot & & \cdot & a_2 & \cdot & \\ \cdot & \cdot & \cdot & a_1 & \cdot & \cdot & \cdot & a_0 \\ a_{2k+1} & \cdot & \cdot & a_3 & a_{2k} & \cdot & \cdot & a_2 \\ & a_{2k+1} & \cdot & \cdot & & a_{2k} & \cdot & \cdot \\ & & \cdot & \cdot & & & \cdot & \cdot \\ & & & a_{2k+1} & & & & a_{2k} \end{vmatrix}. \tag{3.2}$$

In (3.1) one has k columns with odd subscripts and $k-1$ columns with even subscripts, while in (3.2) there are k columns with odd subscripts and also k columns with even subscripts. For a polynomial $f(X)=a_0+a_1X+\cdots+a_nX^n$ we let

$$f_o(X)=\sum_{i=0}^{\lfloor\frac{n-1}{2}\rfloor} a_{2i+1}X^i \quad\text{and}\quad f_e(X)=\sum_{i=0}^{\lfloor\frac{n}{2}\rfloor} a_{2i}X^i.$$

By (3.1) and (3.2) we see that if $a_na_{n-1}\neq 0$, then $Res(f_o,f_e)=\det M(n,2)$.

2) Let R be a unique factorization domain of characteristic $p>0$ and $f=a_0+a_1X+\cdots+a_nX^n\in R[X]$ a primitive polynomial of degree $n\geq 2$. For a fixed, arbitrarily chosen integer $d\geq 1$ one may take $m=p^d$ in Proposition 2.1 and conclude that f is square-free over R if and only if $f\nmid g^{p^d}$ for all $g\in R[X]$ with $\deg g=\deg f-1$. In this case we may take M to have $(p^d-1)\cdot(n-1)$ columns and define $M_d(n,p)$ as the square matrix obtained from M by removing the rows whose indices are a multiple of p^d plus 1: $r_1,r_{p^d+1},\ldots,r_{(n-1)p^d+1}$. Then, as in Corollary 2.2, f is square-free over R if $\det M_d(n,p)\neq 0$, and moreover, if the Frobenius map of R is surjective, then f is square-free over R if and only if $\det M_d(n,p)\neq 0$.

3) For every $n\geq 2$, $d\geq 1$ and every prime p, $\det M_d(n,p)$ is a homogeneous polynomial of degree $(p^d-1)(n-1)$ in the variables $a_0,a_1,\ldots,a_n$.

Example 3.1. Let R be a unique factorization domain of characteristic 2. Then each of the following polynomials are square-free over R:

i) $f(X)=\sum_{i=0}^{2k}a_iX^i$, f primitive with $k\geq 2$, $a_0a_{2k-1}a_{2k}\neq 0$, $a_1=a_3=\ldots=a_{2k-3}=0$ and arbitrary $a_2,\ldots,a_{2k-2}$;

ii) $f(X)=\sum_{i=0}^{2k+1}a_iX^i$, f primitive with $k\geq 1$, $a_0a_{2k+1}\neq 0$, $a_1=a_3=\ldots=a_{2k-1}=0$ and arbitrary $a_2,\ldots,a_{2k}$;

iii) $f(X)=\sum_{i=0}^{2k+1}a_iX^i$, f primitive with $k\geq 1$, $a_0a_{2k+1}\neq 0$, $a_2=a_4=\ldots=a_{2k}=0$ and arbitrary $a_1,\ldots,a_{2k-1}$.

The following polynomials with integer coefficients are square-free:

iv) $f(x)=\sum_{i=0}^{2k}a_iX^i$, f primitive with $a_0a_{2k}\equiv 1 \bmod 2$ and $a_{2i}\equiv a_{2i+1} \bmod 2$ for $i=0,\ldots,k-1$;

v) $f(x)=\sum_{i=0}^{2k+1}a_iX^i$, f primitive with $a_0a_{2k+1}\equiv 1 \bmod 2$, $a_{2k}\equiv 0 \bmod 2$ and $a_{2i}\equiv a_{2i+1} \bmod 2$ for $i=0,\ldots,k-1$.

For the proof of i) consider the polynomial $Xf(X)$, which is square-free by (3.2) since all the entries above the main diagonal are zero; ii) in this case, if we interchange in (3.2) the blocks of columns with odd and even subscripts, we see that all the entries above the main diagonal are zero; iii) follows by looking again at the polynomial $Xf(X)$, which is now square-free by (3.1), since all the entries below the main diagonal are zero; iv) consider the polynomial $\bar{f}$ obtained by reducing modulo 2 the coefficients of f; if we add the first $k-1$ columns to the corresponding last $k-1$ columns in (3.1), we obtain all the entries in the main diagonal equal to 1 mod 2 and all the entries above the main diagonal equal to 0 mod 2; v) consider again the polynomial $\bar{f}$ obtained by reducing modulo 2 the coefficients of f; the conclusion follows from (3.2) by adding the block of columns with odd subscripts to the one with even subscripts, thus making 1 mod 2 all the entries in the main diagonal, while all the entries above the main diagonal become 0 mod 2.

4) Let $f(X)=\sum_{i=0}^{5}a_iX^i\in\mathbb{Z}[X]$, and consider the question of whether the reduction modulo 3 of the polynomial $f(X)$ is square-free. Then $\det M(5,3)$ equals

$$\begin{aligned}
&a_1^5a_5^3+2a_1^2a_2^3a_4^3+a_0^3a_4^5+2a_0^4a_5^4+2a_1^3a_3^3a_4^2+a_1^3a_3^4a_5+a_1^4a_3^2a_5^2+a_1^2a_2^2a_3^2a_4^2\\
&+2a_1^2a_2^2a_3^3a_5+a_1^3a_2a_4a_3^2a_5+a_1^2a_2a_4^2a_0a_3a_5+2a_1^2a_2a_5^2a_3^2a_0+a_1^3a_3a_4a_5^2a_0\\
&+2a_1^2a_3a_0^2a_5^3+a_1^2a_5^2a_0^2a_4^2+a_0a_2^4a_4^3+2a_0a_2a_5^3a_1^3+2a_0a_2^3a_3^2a_4^2+a_0a_2^3a_3^3a_5\\
&+2a_0a_2^2a_1a_4a_3^2a_5+a_0^2a_2^2a_4^4+2a_0^2a_2^2a_4^2a_3a_5+2a_0^2a_2a_3a_1a_4a_5^2+a_0^2a_2a_5a_1a_4^3\\
&+2a_0^3a_2a_5^2a_4^2+a_0a_1a_3a_2^2a_4^3+2a_0^3a_4^3a_3a_5+2a_0^3a_1a_4a_5^3,
\end{aligned}$$

with coefficients considered modulo 3. Let us assume that $a_0=a_2=a_3=0 \bmod 3$. Then one has $\det M(5,3)=a_1^5a_5^3$. So a polynomial $f(X)=\sum_{i=0}^{5}a_iX^i\in\mathbb{Z}[X]$ is square-free modulo 3, hence also square-free as a polynomial in $\mathbb{Z}[X]$, if

1) $3|a_0$, $3|a_2$, $3|a_3$ and $3\nmid a_1\cdot a_5$.

Assume now $a_0=a_2=a_4=0 \bmod 3$. In this case one obtains

$$\det M(5,3)=a_1^5a_5^3+a_1^3a_3^4a_5+a_1^4a_3^2a_5^2=a_1^3a_5(a_3^2-a_1a_5)^2.$$

Therefore a polynomial $f(X)=\sum_{i=0}^{5}a_iX^i\in\mathbb{Z}[X]$ is square-free modulo 3 in each one of the following cases:

2) $3|a_0$, $3|a_2$, $3|a_4$, $3\nmid a_3$, $a_1\equiv 1 \bmod 3$ and $a_5\equiv 2 \bmod 3$,

3) $3|a_0$, $3|a_2$, $3|a_4$, $3\nmid a_3$, $a_1\equiv 2 \bmod 3$ and $a_5\equiv 1 \bmod 3$.

4. Further square-free criteria

One way to derive bounds for the multiplicities of the factors, in particular square-free criteria for some classes of polynomials over unique factorization domains, is to consider the resultant between two derivatives of different order of a given polynomial, and then make use of certain nonvanishing conditions for determinants. Another way to obtain square-free criteria is to provide certain nonvanishing conditions for determinants, and apply them to the matrix $M(n,p)$. In

this respect, let R be a unique factorization domain and q a prime element of R. For a nonzero element $x \in R$ we shall denote by $\omega_q(x)$ the exponent of q in the prime decomposition of x ($\omega_q(0) = \infty$). The results in this section rely on the following basic lemma.

Lemma 4.1. *Let $n \geq 2$, $A = (a_{ij})$ an $n \times n$ matrix with entries in the unique factorization domain R and σ a permutation of $\{1, 2, \ldots, n\}$. If all the elements of A satisfy*

$$\begin{array}{l} \omega_q(a_{\sigma^{-1}(i)i}) < \omega_q(a_{ji}) \quad \textit{for} \quad j > \sigma^{-1}(i), \\ \omega_q(a_{\sigma^{-1}(i)i}) \leq \omega_q(a_{ji}) \quad \textit{for} \quad j < \sigma^{-1}(i), \end{array} \tag{4.1}$$

then $\det(A) \neq 0$. *The same conclusion holds if we replace* (4.1) *by one of the following three conditions:*

$$\begin{array}{l} \omega_q(a_{\sigma^{-1}(i)i}) \leq \omega_q(a_{ji}) \quad \textit{for} \quad j > \sigma^{-1}(i), \\ \omega_q(a_{\sigma^{-1}(i)i}) < \omega_q(a_{ji}) \quad \textit{for} \quad j < \sigma^{-1}(i), \end{array} \tag{4.2}$$

$$\begin{array}{l} \omega_q(a_{i\sigma(i)}) < \omega_q(a_{ij}) \quad \textit{for} \quad j < \sigma(i), \\ \omega_q(a_{i\sigma(i)}) \leq \omega_q(a_{ij}) \quad \textit{for} \quad j > \sigma(i), \end{array} \tag{4.3}$$

$$\begin{array}{l} \omega_q(a_{i\sigma(i)}) \leq \omega_q(a_{ij}) \quad \textit{for} \quad j < \sigma(i), \\ \omega_q(a_{i\sigma(i)}) < \omega_q(a_{ij}) \quad \textit{for} \quad j > \sigma(i). \end{array} \tag{4.4}$$

Proof. For every permutation τ of $\{1, \ldots, n\}$ with $\tau \neq \sigma$, the corresponding term $x_\tau = a_{1\tau(1)} \cdots a_{n\tau(n)}$ appearing in the formula of $\det(A)$ must contain at least one element $a_{\tau^{-1}(i)i}$ with $\tau^{-1}(i) > \sigma^{-1}(i)$. By (4.1), for such an index i one has $\omega_q(a_{\sigma^{-1}(i)i}) < \omega_q(a_{\tau^{-1}(i)i})$. Since for each one of the remaining indices k we either again have $\tau^{-1}(k) > \sigma^{-1}(k)$ and hence $\omega_q(a_{\sigma^{-1}(k)k}) < \omega_q(a_{\tau^{-1}(k)k})$, or $\tau^{-1}(k) \leq \sigma^{-1}(k)$ and hence $\omega_q(a_{\sigma^{-1}(k)k}) \leq \omega_q(a_{\tau^{-1}(k)k})$, it follows that $\omega_q(x_\sigma) < \omega_q(x_\tau)$. Therefore $\omega_q(x_\sigma) < \omega_q(x_\tau)$ for every $\tau \neq \sigma$, which prevents $\det(A)$ to be zero. The proof is similar if we replace (4.1) with (4.2). In the third case we see that for every permutation $\tau \neq \sigma$, the corresponding term x_τ in the formula of $\det(A)$ must contain at least one element $a_{i\tau(i)}$ with $\tau(i) < \sigma(i)$. By (4.3), for such an index i one has $\omega_q(a_{i\sigma(i)}) < \omega_q(a_{i\tau(i)})$, and for each one of the remaining indices k we either again have $\tau(k) < \sigma(k)$ and hence $\omega_q(a_{k\sigma(k)}) < \omega_q(a_{k\tau(k)})$, or $\sigma(k) \leq \tau(k)$ and hence $\omega_q(a_{k\sigma(k)}) \leq \omega_q(a_{k\tau(k)})$. Therefore $\omega_q(x_\sigma) < \omega_q(x_\tau)$ for every $\tau \neq \sigma$, which as before, prevents $\det(A)$ from vanishing. The proof is similar in the fourth case. □

One may obviously apply Lemma 4.1 to the discriminant of a given polynomial f, and then read the nonvanishing conditions for the discriminant as inequalities between the multiplicities of a given prime q in the canonical decomposition of the coefficients of f. As for our matrix $M(n, p)$, the simplest square-free criteria appear when we consider polynomials over unique factorization domains of characteristic 2 and use Lemma 4.1 with $\sigma = id$.

Proposition 4.2. *Let R be a unique factorization domain of characteristic 2, $f(X) = a_0 + a_1X + \cdots + a_{2k}X^{2k} \in R[X]$ a primitive polynomial of even degree, and q a prime element of R. In each one of the following four situations, the polynomial*

f is square-free over R:

$$\begin{aligned}
&\text{i)} \quad k\geq 2, \quad \omega_q(a_1) < \min_{1\leq i\leq k-1}\omega_q(a_{2i+1}), \quad \omega_q(a_{2k}) \leq \min_{0\leq i\leq k-1}\omega_q(a_{2i}),\\
&\text{ii)} \quad k\geq 2, \quad \omega_q(a_1) \leq \min_{1\leq i\leq k-1}\omega_q(a_{2i+1}), \quad \omega_q(a_{2k}) < \min_{0\leq i\leq k-1}\omega_q(a_{2i}),\\
&\text{iii)} \quad k\geq 3, \quad \omega_q(a_1) < \min_{1\leq i\leq k-2}\omega_q(a_{2i+1}), \quad \omega_q(a_1) \leq \min_{0\leq i\leq k-1}\omega_q(a_{2i}),\\
&\qquad\qquad\quad \omega_q(a_{2k}) < \min_{1\leq i\leq k-1}\omega_q(a_{2i+1}), \quad \omega_q(a_{2k}) \leq \min_{1\leq i\leq k-1}\omega_q(a_{2i}),\\
&\text{iv)} \quad k\geq 3, \quad \omega_q(a_1) \leq \min_{1\leq i\leq k-2}\omega_q(a_{2i+1}), \quad \omega_q(a_1) < \min_{0\leq i\leq k-1}\omega_q(a_{2i}),\\
&\qquad\qquad\quad \omega_q(a_{2k}) \leq \min_{1\leq i\leq k-1}\omega_q(a_{2i+1}), \quad \omega_q(a_{2k}) < \min_{1\leq i\leq k-1}\omega_q(a_{2i}).
\end{aligned}$$

In particular, f is square-free over R in the following cases:

v) $k\geq 2$, $q\nmid a_1\cdot a_{2k}$ *and* $q|a_{2i+1}$ *for* $i=1,\dots,k-1$,
vi) $k\geq 2$, $q\nmid a_1\cdot a_{2k}$ *and* $q|a_{2i}$ *for* $i=0,\dots,k-1$.

Proof. For $\sigma = id.$, the inequalities (4.1)–(4.4) become

$$\omega_q(a_{ii}) < \omega_q(a_{ji}) \text{ for } j>i,\ \omega_q(a_{ii}) \leq \omega_q(a_{ji}) \text{ for } j<i, \tag{4.5}$$

$$\omega_q(a_{ii}) \leq \omega_q(a_{ji}) \text{ for } j>i,\ \omega_q(a_{ii}) < \omega_q(a_{ji}) \text{ for } j<i, \tag{4.6}$$

$$\omega_q(a_{ii}) < \omega_q(a_{ij}) \text{ for } j<i,\ \omega_q(a_{ii}) \leq \omega_q(a_{ij}) \text{ for } j>i, \tag{4.7}$$

$$\omega_q(a_{ii}) \leq \omega_q(a_{ij}) \text{ for } j<i,\ \omega_q(a_{ii}) < \omega_q(a_{ij}) \text{ for } j>i, \tag{4.8}$$

respectively. The conclusion in the cases i)–iv) follows using (3.1) and applying to $M(2k,2)$ the conditions (4.5)–(4.8), respectively. □

For polynomials of odd degree we have the following result.

Proposition 4.3. *Let R be a unique factorization domain of characteristic 2, $f(X)=a_0+a_1X+\cdots+a_{2k+1}X^{2k+1}\in R[X]$ a primitive polynomial of odd degree, and q a prime element of R. In each one of the following four situations, the polynomial f is square-free over R:*

$$\begin{aligned}
&\text{i)} \quad k\geq 1, \quad \omega_q(a_1) < \min_{1\leq i\leq k}\omega_q(a_{2i+1}), \quad \omega_q(a_{2k}) \leq \min_{0\leq i\leq k-1}\omega_q(a_{2i}),\\
&\text{ii)} \quad k\geq 1, \quad \omega_q(a_{2k}) \leq \min_{0\leq i\leq k-1}\omega_q(a_{2i}), \quad \omega_q(a_{2k}) < \min_{0\leq i\leq k-1}\omega_q(a_{2i}),\\
&\text{iii)} \quad k\geq 2, \quad \omega_q(a_1) < \min_{1\leq i\leq k-1}\omega_q(a_{2i+1}), \quad \omega_q(a_1) \leq \min_{0\leq i\leq k-1}\omega_q(a_{2i}),\\
&\qquad\qquad\quad \omega_q(a_{2k}) < \min_{1\leq i\leq k}\omega_q(a_{2i+1}), \quad \omega_q(a_{2k}) \leq \min_{1\leq i\leq k-1}\omega_q(a_{2i}),\\
&\text{iv)} \quad k\geq 2, \quad \omega_q(a_1) \leq \min_{1\leq i\leq k-1}\omega_q(a_{2i+1}), \quad \omega_q(a_1) < \min_{0\leq i\leq k-1}\omega_q(a_{2i}),\\
&\qquad\qquad\quad \omega_q(a_{2k}) \leq \min_{1\leq i\leq k}\omega_q(a_{2i+1}), \quad \omega_q(a_{2k}) < \min_{1\leq i\leq k-1}\omega_q(a_{2i}).
\end{aligned}$$

In particular, f is square-free over R in the following cases:

v) $k\geq 1$, $q\nmid a_1\cdot a_{2k}$ *and* $q|a_{2i+1}$ *for* $i=1,\dots,k$,
vi) $k\geq 1$, $q\nmid a_1\cdot a_{2k}$ *and* $q|a_{2i}$ *for* $i=0,\dots,k-1$.

Proof. The conclusion in the cases i)–iv) follows using (3.2) and applying to $M(2k+1,2)$ the conditions (4.5)–(4.8), respectively. □

5. Square-free criteria for polynomials in several variables

Among the criteria for nonvanishing of determinants, one of the most famous is given by Hadamard's Theorem [3]: *If the elements of an $n\times n$ complex matrix $A=(a_{ij})$ satisfy the inequalities $|a_{ii}|>\sum_{j\neq i}|a_{ij}|$ for each $i=1,\dots,n$, then*

$\det(A) \neq 0$. A complete bibliography of this theorem is contained in [15]. Other conditions for the nonvanishing of a determinant were obtained by Ostrowski in [10]–[14], using only the moduli of the elements of an $n \times n$ complex matrix $A = (a_{ij})$ and some simple combinations of these moduli. The results of Ostrowski use essentially the expressions:

$$\begin{aligned}
&R_i = \sum_{j\neq i} |a_{ij}|, && C_i = \sum_{j\neq i} |a_{ji}|, && i = 1, \dots, n,\\
&R_{i,s} = (\sum_{j\neq i} |a_{ij}|^s)^{1/s}, && C_{i,s} = (\sum_{j\neq i} |a_{ji}|^s)^{1/s}, && i = 1, \dots, n,\\
&m_i = \max_{j\neq i} |a_{ij}| = R_{i,\infty}, && m_i' = \max_{j\neq i} |a_{ji}| = C_{i,\infty}, && i = 1, \dots, n.
\end{aligned}$$

One criterion derived in [13], which generalizes Hadamard's Theorem, is that $\det(A) \neq 0$ if for an arbitrarily chosen fixed α, $0 \leq \alpha \leq 1$, we have

$$|a_{ii}| > R_i^{\alpha} C_i^{1-\alpha}, \qquad i = 1, \dots, n. \tag{5.1}$$

As to $R_{i,s}$ and $C_{i,s}$, the corresponding criterion derived in [12] is that $\det(A) \neq 0$ if

$$\sum_{i=1}^{n} \frac{1}{1 + |a_{ii}|^q / R_{i,p}^q} < 1 \tag{5.2}$$

for a fixed but arbitrary choice of $p \geq 1$ and $q \geq 1$ such that $1/p + 1/q = 1$, and the criterion obtained on replacing $R_{i,p}$ by $C_{i,p}$. For $q = 1$ we have $p = \infty$, and (5.2) becomes

$$\sum_{i=1}^{n} \frac{1}{1 + |a_{ii}|/m_i} < 1.$$

In this final section we adapt the method employed by Ostrowski [13] to prove (5.1), in order to provide nonvanishing conditions for determinants with polynomial entries, and then apply them to the matrix $M(n, p)$ in order to obtain some square-free criteria for polynomials in several variables over a given field. We use the following notation. Let K be a field and $r \geq 1$ a fixed integer. For any index $l \in \{1, \dots, r\}$ and any polynomial $f(X_1, \dots, X_r) \in K[X_1, \dots, X_r]$ we denote by $\deg_{X_l} f$ the degree of f viewed as a polynomial in X_l with coefficients in $K[X_1, \dots, \widehat{X_l}, \dots, X_r]$, where the hat means that the correspondent variable is missing. The correspondent of (5.1) for matrices with polynomial entries is given by the following lemma.

Lemma 5.1. *Let K be a field, $r \geq 1$ a fixed integer and $A = (a_{ij})$ an $n \times n$ matrix with entries in $K[X_1, \dots, X_r]$. Also let α be a fixed, arbitrarily chosen real number with $0 \leq \alpha \leq 1$. If for an index $l \in \{1, \dots, r\}$ the elements a_{ij} satisfy*

$$\deg_{X_l} a_{ii} > \alpha \cdot \max_{j\neq i} \deg_{X_l} a_{ij} + (1 - \alpha) \cdot \max_{j\neq i} \deg_{X_l} a_{ji}, \tag{5.3}$$

for $i, j = 1, \dots, n$, then $\det A \neq 0$.

Proof. It will be sufficient to prove the lemma for $a_{ij} \in K[X]$. The conclusion will then follow by writing X for X_l and by replacing the field K with the field generated by K and the variables $X_1, \dots, X_r$ except for X_l. We introduce a nonarchimedean absolute value $|\cdot|$ on $K(X)$, as follows. We fix a real number $\rho > 1$, and for any polynomial $F(X) \in K[X]$ we define $|F(X)|$ by the equality

$$|F(X)| = \rho^{\deg F(X)}. \tag{5.4}$$

We then extend the absolute value $|\cdot|$ to $K(X)$ by multiplicativity. Thus for any $L(X) \in K(X)$, $L(X) = \frac{F(X)}{G(X)}$, with $F(X), G(X) \in K[X]$, $G(X) \neq 0$, we let $|L(X)| = \frac{|F(X)|}{|G(X)|}$. Let us remark that for any nonzero element u of $K[X]$ one has $|u| \geq 1$, while for the zero polynomial $\mathbf{0} \in K[X]$ we have $|\mathbf{0}| = 0$. We treat separately the cases $\alpha = 0$, $\alpha = 1$ and $0 < \alpha < 1$.

Case 1. $\alpha = 1$. Assume that $\det A = 0$. Then the system

$$\sum_{j=1}^{n} a_{ij}x_j = 0, \qquad i = 1, \ldots, n, \tag{5.5}$$

has a nontrivial solution $(x_1, \ldots, x_n) \in K[X]^n$ of which x_m is a component of maximum absolute value. From the mth equation of (5.5) we obtain

$$|a_{mm}| \cdot |x_m| = |\sum_{j \neq m} a_{mj}x_j| \leq \max_{j \neq m} |a_{mj}| \cdot |x_j| \leq \max_{j \neq m} |a_{mj}| \cdot |x_m|,$$

or, further $|a_{mm}| \leq \max\limits_{j \neq m} |a_{mj}|$, since $|x_m| \neq 0$. Using (5.4), this inequality reads $\deg a_{mm} \leq \max\limits_{j \neq m} \deg a_{mj}$, which contradicts (5.3).

Case 2. $\alpha = 0$. The conclusion follows by the above argument for the transposed of the matrix A.

Case 3. $0 < \alpha < 1$. Let us denote

$$R_i = \max_{j \neq i} |a_{ij}| = \rho^{\max\limits_{j \neq i} \deg a_{ij}} \text{ and } C_i = \max_{j \neq i} |a_{ji}| = \rho^{\max\limits_{j \neq i} \deg a_{ji}},$$

for $i = 1, \ldots, n$. Using this notation, the condition (5.3) reads

$$|a_{ii}| > R_i^{\alpha} C_i^{1-\alpha}, \qquad i = 1, \ldots, n. \tag{5.6}$$

We may obviously assume that none of the products R_iC_i is zero, for otherwise one may rephrase the problem for a matrix of order less than n. Then, if $\det A = 0$, the system (5.5) will have a nontrivial solution $(x_1, \ldots, x_n) \in K[X]^n$. Fix an arbitrary $i \in \{1, \ldots, n\}$. By (5.6) we obtain

$$R_i^{\alpha} C_i^{1-\alpha} \cdot |x_i| \leq |a_{ii}| \cdot |x_i|, \tag{5.7}$$

with strict inequality if $x_i \neq 0$. On the other hand, by the ith equation of (5.5) we derive successively

$$\begin{aligned} |a_{ii}| \cdot |x_i| &\leq \max_{j \neq i} |a_{ij}| \cdot |x_j| = \max_{j \neq i} |a_{ij}|^{\alpha} \cdot |a_{ij}|^{1-\alpha} |x_j| \\ &\leq \max_{j \neq i} |a_{ij}|^{\alpha} \cdot \max_{j \neq i} |a_{ij}|^{1-\alpha} |x_j| = R_i^{\alpha} \cdot \max_{j \neq i} |a_{ij}|^{1-\alpha} |x_j|, \end{aligned}$$

which in view of (5.7) yields $C_i^{1-\alpha} \cdot |x_i| \leq \max\limits_{j \neq i} |a_{ij}|^{1-\alpha} |x_j|$. Therefore, we obtain

$$C_i \cdot |x_i|^{\frac{1}{1-\alpha}} \leq \max_{j \neq i} |a_{ij}| \cdot |x_j|^{\frac{1}{1-\alpha}}, \tag{5.8}$$

with strict inequality if $x_i \neq 0$. By taking the maximum with respect to i in both sides of (5.8), and recalling that at least one of the x_i's is nonzero, one obtains

$$\max_{1 \leq i \leq n} C_i \cdot |x_i|^{\frac{1}{1-\alpha}} < \max_{1 \leq i \leq n} \max_{j \neq i} |a_{ij}| \cdot |x_j|^{\frac{1}{1-\alpha}} = \max_{1 \leq i \leq n} C_i \cdot |x_i|^{\frac{1}{1-\alpha}},$$

a contradiction, and this completes the proof of the lemma. □

Proposition 5.2. *Let K be a field, $char(K) = 2$, $r \geq 2$ a fixed integer and $f(X_1, \ldots, X_r) = a_0 + a_1X_r + \cdots + a_{2k}X_r^{2k}$, $k \geq 2$, with $a_0, \ldots, a_{2k} \in K[X_1, \ldots, X_{r-1}]$, $a_{2k} \neq 0$ and such that $\gcd(a_0, \ldots, a_{2k}) \in K$. Also let α be a fixed, arbitrarily chosen real number with $0 \leq \alpha \leq 1$. If for an index $l \in \{1, \ldots, r-1\}$ one has*

$$\begin{aligned} \deg_{X_l} a_1 &> \alpha \cdot \max_{\substack{0 \leq i \leq 2k-2 \\ i \neq 1}} \deg_{X_l} a_i + (1-\alpha) \cdot \max_{1 \leq i \leq k-1} \deg_{X_l} a_{2i+1}, \\ \deg_{X_l} a_{2k} &> \alpha \cdot \max_{2 \leq i \leq 2k-1} \deg_{X_l} a_i + (1-\alpha) \cdot \max_{0 \leq i \leq k-1} \deg_{X_l} a_{2i}, \end{aligned}$$

then f is square-free over $K[X_1, \ldots, X_{r-1}]$.

Proof. Use (3.1) and apply to $M(2k, 2)$ the conditions (5.3). □

For polynomials of odd degree we have the following result.

Proposition 5.3. *Let K be a field, $char(K) = 2$, $r \geq 2$ a fixed integer and $f(X_1, \ldots, X_r) = a_0 + a_1X_r + \cdots + a_{2k+1}X_r^{2k+1}$, $k \geq 1$, with $a_0, \ldots, a_{2k+1} \in K[X_1, \ldots, X_{r-1}]$, $a_{2k+1} \neq 0$ and such that $\gcd(a_0, \ldots, a_{2k+1}) \in K$. Also let α be a fixed, arbitrarily chosen real number with $0 \leq \alpha \leq 1$. If for an index $l \in \{1, \ldots, r-1\}$ one has*

$$\begin{aligned} \deg_{X_l} a_1 &> \alpha \cdot \max_{\substack{0 \leq i \leq 2k-1 \\ i \neq 1}} \deg_{X_l} a_i + (1-\alpha) \cdot \max_{1 \leq i \leq k} \deg_{X_l} a_{2i+1}, \\ \deg_{X_l} a_{2k} &> \alpha \cdot \max_{\substack{2 \leq i \leq 2k+1 \\ i \neq 2k}} \deg_{X_l} a_i + (1-\alpha) \cdot \max_{0 \leq i \leq k-1} \deg_{X_l} a_{2i}, \end{aligned}$$

then f is square-free over $K[X_1, \ldots, X_{r-1}]$.

Proof. Use (3.2) and apply to $M(2k+1, 2)$ the conditions (5.3). □

References

[1] F. DeMeyer, *Separable polynomials over a commutative ring*, Rocky Mountain J. Math. 2 (1972), no. 2, 299–310. MR0294321 (45:3390)

[2] F. DeMeyer, *Twisted forms of finite étale extensions and separable polynomials*, Int. J. Math. Math. Sci. 26 (2001), no. 8, 467–473. MR1851100 (2002f:13022)

[3] J. Hadamard, *Leçons sur la propagation des ondes,* Paris, 1903, 13–14.

[4] D. K. Harrison and T. Mckenzie, *Towards an arithmetic of polynomials*, Aequationes Math. 43 (1992), no. 1, 21–37. MR1144586 (92m:13008)

[5] G. J. Janusz, *Separable algebras over commutative rings*, Trans. Amer. Math. Soc. 122 (1966), 461–479. MR0210699 (35:1585)

[6] A. I. Kostrikin, *Introduction to Algebra* (translated from Russian) Springer-Verlag, 1982. MR0661256 (83f:00003)

[7] T. McKenzie, *The separable closure of a local ring*, J. Algebra 207 (1998), no. 2, 657–663. MR1644231 (99g:13006)

[8] T. Nagahara, *On separable polynomials over a commutative ring*, Math. J. Okayama Univ. 14 (1969/70), 175–181. MR0289495 (44:6684)

[9] T. Nagahara, *Characterization of separable polynomials over a commutative ring*, Proc. Japan Acad. 46 (1970), 1011–1015. MR0284432 (44:1659)

[10] A. M. Ostrowski, *Mathematische Miszellen. XXIV. Zur relativen Stetigkeit von Wurzeln algebraischer Gleichungen,* Jahresber. Deutsch. Math.-Verein. 58 (1956), Abt.1, 98–102. MR0078327 (17:1175g)

[11] A. M. Ostrowski, *On some conditions for nonvanishing of determinants,* Proc. Amer. Math. Soc. 12 (1961), 268–273. MR0137719 (25:1168)

[12] A. M. Ostrowski, *Sur les conditions générales pour la régularité des matrices,* Rend. Mat. e Appl. ser. V, vol. X (1951), 156–168. MR0049151 (14:125g)
[13] A. M. Ostrowski, *Ueber das Nichtverschwinden einer Klasse von Determinanten und die Lokalisierung der characteristischen Wurzeln von Matrizen,* Compositio Math. 9 (1951), 209–226. MR0045081 (13:524b)
[14] A. M. Ostrowski, *Ueber Determinanten mit überwiegender Hauptdiagonale,* Comm. Math. Helv., Bd. 10 (1937), 69–96. MR1509568
[15] O. Tausski-Todd, *A recurring theorem on determinants,* Amer. Math. Monthly 56 (1949), 672–676. MR0032557 (11:307b)
[16] R. J. Walker, *Algebraic Curves*, Princeton University Press, 1950. MR0033083 (11:387e)

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

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

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

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