On the factorization of lacunary polynomials

H. W. Lenstra, Jr.

To Andrzej Schinzel

Abstract. Descartes's rule of signs implies that the number of non-vanishing real zeroes of a non-zero polynomial f in one variable with real coefficients is at most $2k$, if $k+1$ is the number of non-zero terms of f. In this paper the following non-archimedean analogue is obtained. Let p be a prime number, L a field that is a finite extension of the field of p-adic numbers, and k a positive integer. Then there exists a positive integer $B = B(k, L)$ with the following property: if $f \in L[X]$ has at most $k+1$ non-zero terms, and $f \neq 0$, then f has at most B non-vanishing zeroes in L, counting multiplicities. For example, if L is the field of 2-adic numbers, and $k = 2$, then one can take $B = 6$. As a consequence, it is shown that for any three positive integers m, k, and d there exists a positive integer $A = A(m, k, d)$ with the following property. Suppose that K is an algebraic number field of degree at most m over the field of rational numbers, that $f \in K[X]$ is a non-zero polynomial with at most $k+1$ non-zero terms, and that $g \in K[X]$ is a factor of f such that each irreducible factor of g has degree at most d and such that $g(0) \neq 0$. Then the degree of g is at most A. The value for A given by the proof satisfies $A(m, k, d) = O(k^2 \cdot 2^{md} \cdot md \cdot \log(2mdk))$, the O-constant being absolute and effectively computable.

1991 Mathematics Subject Classification: Primary 11R09, 11S05.

Key words: lacunary polynomial, p-adic numbers, Descartes's rule of signs.

Acknowledgements. The author was supported by NSF under grant No. DMS 92-24205. He thanks J.A. Csirik, M. Filaseta, B. Poonen, A. Schinzel, R. Tijdeman, and J.D. Vaaler for helpful advice.

1. Introduction

Let $\mathbf{Q}$ denote the field of rational numbers, and for a ring R, write $R[X]$ for the ring of polynomials in one variable X over R.

Theorem 1. *For any three positive integers m, k, and d there exists a positive integer $A = A(m, k, d)$ with the following property. Suppose that K is an algebraic number field of degree at most m over $\mathbf{Q}$, that $f \in K[X]$ is a non-zero polynomial* *with at most $k+1$ non-zero terms, and that $g \in K[X]$ is a factor of f such that each irreducible factor of g has degree at most d and such that $g(0) \neq 0$. Then the degree of g is at most A.*

Note that the bound A is independent of the coefficients and the degree of f.

With $d = 1$, the theorem implies a bound $A = A([K : \mathbf{Q}], k, 1)$ on the number of non-vanishing zeroes in K of any non-zero polynomial in $K[X]$ with at most $k+1$ non-zero terms. If K can be embedded in the field $\mathbf{R}$ of real numbers, then $2k$ is such a bound, by Descartes's rule of signs (see [10, Section 109]); in particular, one can take $A(1, k, 1) = 2k$. My proof in the general case, which is given in Section 5, invokes the following non-archimedean analogue of Descartes's rule of signs. For a prime number p, let $\mathbf{Q}_p$ denote the field of p-adic numbers.

Theorem 2. *For any positive integer k and any field L that is a finite extension of $\mathbf{Q}_p$ for some prime number p, there exists a positive integer $B = B(k, L)$ with the following property. Let $f \in L[X]$ be a non-zero polynomial with at most $k+1$ non-zero terms and with $f(0) \neq 0$. Then f has at most B zeroes in L, counted with multiplicities.*

B. Poonen [7] has shown that this result can be extended to fields of Laurent series over finite fields if the zeroes are not counted with multiplicities. I do not know whether there exist generalizations to systems of equations in several variables, as in [3].

The proof of Theorem 2 is given in Section 4. It depends on a result that is even valid for algebraically closed fields. Let an *exponential valuation* on a field be defined as in [11, Section 1-3].

Theorem 3. *For every prime number p, every positive integer k, and every positive real number r there exists a positive integer $C = C(p, k, r)$ with the following property. Let E be a field of characteristic zero with an exponential valuation $\nu : E \to \mathbf{R} \cup \{\infty\}$ satisfying $\nu(p) = 1$, and let $f \in E[X]$ be a non-zero polynomial with at most $k+1$ non-zero terms. Then f has at most C zeroes $x \in E$ with $\nu(x-1) \geq r$, counted with multiplicities.*

The theorem is reminiscent of the following observation of Hajós (see [2; 6, Lemma 1]): if E is a field of characteristic zero, and $f \in E[X]$ is a non-zero polynomial with at most $k+1$ non-zero terms, then no non-vanishing zero of f has multiplicity greater than k. My proof of Theorem 3, which is given in Section 3, may be viewed as a refinement of Hajós's argument. It makes use of a property of binomial coefficients that is proved in Section 2.

Hajós's result easily implies a result analogous to Theorem 3 for fields with an exponential valuation that have a residue class field of characteristic zero; in this case one can take $C = k$, and the condition $\nu(x-1) \geq r$ can simply be replaced by $\nu(x-1) > 0$. In the case of Theorem 3, polynomials like $X^{p^N} - 1$ show that the bound C necessarily depends on r. I do not know a valid variant of Theorem 3 that applies to algebraically closed fields of non-zero characteristic.

In Section 6 we extend, by a specialization argument, Theorem 1 to a more general class of fields and to polynomials in several variables.

Explicit values for A, B, and C are given in Propositions 8.1, 7.2, and 7.1, respectively. They satisfy

$$\begin{aligned} A(m,k,d) &= O\big(k^2 \cdot 2^{md} \cdot md \cdot \log(2mdk)\big), \\ B(k,L) &= O\big(k^2 \cdot p^{f_L} \cdot e_L \cdot \log(2e_L k)\big), \\ C(p,k,r) &= O\Big(k + \frac{k \cdot \log\big(k/(r\log p)\big)}{r \log p}\Big), \end{aligned}$$

where e_L and f_L denote the ramification index and the residue class field degree of L over $\mathbf{Q}_p$, respectively, and where the O-constants are absolute. These estimates give a fair impression of the order of magnitude of the best bounds that may be obtained by my method, for many values of the arguments; at the same time, my bounds are certainly open to numerical improvement.

From Theorem 1 and the value for A just given one can deduce a lower bound for the largest degree of an irreducible factor of f, and an upper bound for the number of irreducible factors of f. These bounds depend only on k, on the degree $[K:\mathbf{Q}]$ of K, and on the degree n of f. They are quite weak; in fact, for fixed k and $[K:\mathbf{Q}]$ they are roughly proportional to $\log n$ and $n/\log n$, respectively. On the other hand, they are completely independent of the coefficients of f and the discriminant of K.

It is an interesting problem to establish lower bounds for any values of A, B, and C that make the conclusions of the theorems valid. Is the best value for $B(k,L)$ computable from k and reasonable data—such as a defining polynomial—specifying L? It is not hard to show that the answer is affirmative if $k=1$. For the rest, I have not attempted to go beyond the case $k=2$ and $L=\mathbf{Q}_2$, which is treated in Section 9; it turns out that the largest number of non-vanishing zeroes that a "trinomial" $f \in \mathbf{Q}_2[X]$ can have in $\mathbf{Q}_2$ equals 6 (see Proposition 9.2).

Cucker, Koiran, and Smale [1] exhibited a polynomial time algorithm that computes all integer zeroes of a sparsely encoded polynomial $f \in \mathbf{Z}[X]$, where $\mathbf{Z}$ denotes the ring of integers. The present paper was originally inspired by one of the problems that they raise, namely that of computing the *rational* zeroes of f in polynomial time as well. This can indeed be done, and in fact there is a polynomial time algorithm that determines all low degree irreducible factors of a sparsely encoded polynomial in one variable with coefficients in an algebraic number field. This result is obtained in [5], by means of techniques different from those employed here.

Whenever, in the remainder of this paper, zeroes of a polynomial are counted, then it is understood that they are counted with multiplicities. If p is a prime number, then ord_p denotes the unique exponential valuation $\mathbf{Q} \to \mathbf{R} \cup \{\infty\}$ for which $\mathrm{ord}_p\, p = 1$. If R is a ring with 1, then R^* denotes its group of units.

If n is a non-negative integer, and t belongs to some $\mathbf{Q}$-algebra, then we write $\binom{t}{n} = \prod_{i=0}^{n-1} \frac{t-i}{n-i}$; this equals 1 if $n = 0$.

2. Interpolating binomial coefficients

For two non-negative integers k and n, define $d_k(n)$ to be the least common multiple of all integers that can be written as the product of at most k pairwise distinct positive integers that are at most n. Taking empty products to be 1, we have $d_k(n) = 1$ if $k = 0$ or $n = 0$. Clearly, $d_k(n)$ divides $n!$, with equality if $n \le k$. (In fact, it is not hard to show that one has $d_k(n) = n!$ if and only if $n \le 2k + 1$, a result that will not be needed.) We have

$$(2.1) \qquad m \cdot d_{k-1}(m-1) \text{ divides } d_k(n) \qquad \text{if } 1 \le m \le n,\ k \ge 1.$$

This is immediate from the definition.

Proposition 2.2. *Let k and n be non-negative integers, and let $T \subset \mathbf{Z}$ be a set of cardinality $k+1$. Then there exists a polynomial $h \in \mathbf{Z}[X]$ such that for each $t \in T$ one has $h(t) = d_k(n) \cdot \binom{t}{n}$.*

Remark. With $d_k(n)$ replaced by $n!$, the conclusion of the proposition is trivial. This trivial result is strong enough to imply Theorem 3 in the case that $r > 1/(p-1)$, which suffices for the proofs of Theorems 2 and 1.

Proof. We proceed by induction on k. If $k = 0$ then $T = \{t\}$ for some integer t, and the constant polynomial $h = \binom{t}{n}$ has the required property, since $d_0(n) = 1$. Next let $k > 0$. Let an element $u \in T$ be chosen. The formal identity $(1+X)^t = (1+X)^u \cdot (1+X)^{t-u}$ shows that for each $t \in \mathbf{Z}$ we have

$$\binom{t}{n} = \sum_{m=0}^{n} \binom{u}{n-m}\binom{t-u}{m}.$$

Using that $\binom{t-u}{m} = \frac{t-u}{m} \cdot \binom{t-u-1}{m-1}$ for $m > 0$, we obtain

$$\binom{t}{n} = \binom{u}{n} + (t-u) \cdot \sum_{m=1}^{n} \frac{1}{m}\binom{u}{n-m}\binom{t-u-1}{m-1}.$$

Applying the induction hypothesis with $k-1$, $m-1$, and $\{t-u-1 : t \in T,\ t \ne u\}$ in the roles of k, n, and T, respectively, we find that for each $m \in \{1, 2, \ldots, n\}$ there exists $h_m \in \mathbf{Z}[X]$ such that for each $t \in T$, $t \ne u$, one has $\binom{t-u-1}{m-1} = h_m(t-u-1)/d_{k-1}(m-1)$. Therefore we have

$$\binom{t}{n} = \binom{u}{n} + (t-u) \cdot \sum_{m=1}^{n} \frac{1}{m \cdot d_{k-1}(m-1)}\binom{u}{n-m} h_m(t-u-1)$$

for each $t \in T$; this time we can include $t = u$, because of the factor $t - u$. Multiplying by $d_k(n)$ we obtain $d_k(n) \cdot \binom{t}{n} = h(t)$ for each $t \in T$, where

$$h = d_k(n) \cdot \binom{u}{n} + (X - u) \cdot \sum_{m=1}^{n} \frac{d_k(n)}{m \cdot d_{k-1}(m-1)} \binom{u}{n-m} h_m(X - u - 1).$$

By (2.1), the polynomial h belongs to $\mathbf{Z}[X]$. This proves 2.2.

Corollary 2.3. *Let k and n be non-negative integers with $n > k$, and let $T \subset \mathbf{Z}$ be a set of cardinality $k+1$. Then there exist rational numbers $c_0, c_1, \ldots, c_k$ such that for each i the denominator of c_i divides $d_k(n)/i!$ and such that for each $t \in T$ one has $\binom{t}{n} = \sum_{i=0}^{k} c_i \binom{t}{i}$.*

Note that $d_k(n)/i!$ is actually an integer, for $0 \le i \le k < n$.

Proof. Let h be as in Proposition 2.2. Replacing h by its remainder upon division by $\prod_{t \in T}(X - t)$, we may assume that $\deg h \le k$. (In fact, if h has been recursively constructed as in the proof of 2.2, then it already satisfies this condition.) Since $i!\binom{X}{i}$ is an ith degree polynomial in $\mathbf{Z}[X]$ with leading coefficient 1, for each $i \ge 0$, we can write $h = \sum_{i=0}^{k} l_i i! \binom{X}{i}$ with $l_i \in \mathbf{Z}$. Now the numbers $c_i = l_i i!/d_k(n)$ have the required properties. This proves 2.3.

Proposition 2.4. *Let p be a prime number, and let k, n be integers with $k \ge 0$ and $n \ge 1$. Then we have*

$$\operatorname{ord}_p d_k(n) \le k \cdot \left[\frac{\log n}{\log p}\right],$$

where $[x]$ denotes the largest integer not exceeding x.

Proof. From the definition of $d_k(n)$ one sees that the largest power of p dividing $d_k(n)$ divides some product of at most k positive integers that are at most n. Each of these integers has at most $[\log n / \log p]$ factors of p, so their product has at most $k \cdot [\log n / \log p]$ factors of p. This proves 2.4.

Algorithm. Let p be a prime number, and let k and n be non-negative integers. To compute $\operatorname{ord}_p d_k(n)$, one determines the least non-negative integer j for which $[n/p^{j+1}] \le k$; then one has

$$\operatorname{ord}_p d_k(n) = jk + \operatorname{ord}_p([n/p^j]!).$$

This computation is conveniently carried out in base p; then one obtains $[n/p^j]$ by deleting the p-adically most significant j digits of n, and if s denotes the sum of the remaining digits then one has $\operatorname{ord}_p([n/p^j]!) = ([n/p^j] - s)/(p-1)$. The elementary correctness proof of this method is left to the reader.

For example, with $p=2$, $k=25$, $n=181$ one has in base 2:

$$k=11001,\quad n=10110101,\quad j=10\,(=p),\quad [n/p^j]=101101,\quad s=100,$$
$$\mathrm{ord}_p([n/p^j]!)=101001,\quad \mathrm{ord}_p\, d_k(n)=10\cdot 11001+101001=1011011,$$

and the conclusion is that $\mathrm{ord}_2\, d_{25}(181)=91$.

3. Zeroes close to 1

We prove Theorem 3. For p, k, and r as in the statement of the theorem, we define

$$C(p,k,r)=\max\bigl\{m\geq 0 : mr-\mathrm{ord}_p\, d_k(m)\leq \max\{ir-\mathrm{ord}_p(i!) : 0\leq i\leq k\}\bigr\},$$

with $d_k(m)$ as defined in Section 1. If p, k, and r are fixed, then $\max\{ir-\mathrm{ord}_p(i!) : 0\leq i\leq k\}$ is constant, and $mr-\mathrm{ord}_p\, d_k(m)$ tends to infinity with m; this follows from 2.4 and the hypothesis that $r>0$. Therefore $C(p,k,r)$ is well-defined, and we have $C(p,k,r)\geq k$ since $d_k(k)=k!$.

We shall, with p, k, and r as above, prove that $C=C(p,k,r)$ satisfies the conclusion of the theorem. To do this, let E, ν, and f be as in the theorem. Replacing E by an algebraic closure and extending ν we may, without loss of generality, assume that E is algebraically closed.

Write $f=\sum_{t\in T} a_t X^t$, where T is a set consisting of $k+1$ non-negative integers, and $a_t\in E$ for $t\in T$. Define $g\in E[X]$ and $b_i\in E$, for $i\geq 0$, by

$$g=f(1+X)=\sum_{i\geq 0} b_i X^i.$$

Then we have

$$b_i=\sum_{t\in T} a_t\binom{t}{i}\qquad \text{for } i\geq 0.$$

Since $f\neq 0$ we have $g\neq 0$, so not all b_i vanish.

Denote by n the number of zeroes x of f in E satisfying $\nu(x-1)\geq r$. This is the same as the number of zeroes y of g in E satisfying $\nu(y)\geq r$. Since E is algebraically closed, that number can, by the theory of Newton polygons (see [11, Section 3-1]), be expressed in terms of r and the valuations of the coefficients b_i of g, as follows:

$$n=\max\bigl\{m\geq 0 : \nu(b_m)+mr=\min\{\nu(b_i)+ir : i\geq 0\}\bigr\}.$$

It follows that we have

$$\nu(b_n)+nr\leq \nu(b_i)+ir\qquad \text{for all } i\geq 0.$$

Since not all b_i vanish, this implies that $\nu(b_n)\neq\infty$.

If $n\leq k$, then we have $n\leq C$, as required. Suppose next that $n>k$. By 2.3, there are rational numbers c_0, c_1, $\ldots$, c_k, with the denominator of c_i dividing

$d_k(n)/i!$, such that for each $t \in T$ one has

$$\binom{t}{n} = \sum_{i=0}^{k} c_i \binom{t}{i}.$$

Multiplying by a_t and summing over $t \in T$ we find that

$$b_n = \sum_{i=0}^{k} c_i b_i.$$

Therefore we have

$$\nu(b_n) \geq \min\{\nu(c_i) + \nu(b_i) : 0 \leq i \leq k\}.$$

The bound on the denominator of c_i and the normalization $\nu(p) = 1$ imply that $\nu(c_i) \geq \mathrm{ord}_p(i!) - \mathrm{ord}_p\, d_k(n)$. Also, we have $\nu(b_i) \geq \nu(b_n) + nr - ir$. Therefore we find that

$$\nu(b_n) \geq \min\{\mathrm{ord}_p(i!) - \mathrm{ord}_p\, d_k(n) + \nu(b_n) + nr - ir : 0 \leq i \leq k\}.$$

Since $\nu(b_n) \neq \infty$, this implies that

$$nr - \mathrm{ord}_p\, d_k(n) \leq \max\{ir - \mathrm{ord}_p(i!) : 0 \leq i \leq k\}.$$

Therefore we have $n \leq C$, as required. This proves Theorem 3.

Remark. If $d_k(n)$ is replaced by $n!$ in this proof (cf. the Remark in Section 2), then it is still valid for $r > 1/(p-1)$, but not for $r \leq 1/(p-1)$. This follows from $\mathrm{ord}_p(n!) = n/(p-1) + o(n)$ for $n \to \infty$.

4. Local fields

We prove Theorem 2. Let L be as in the theorem. Then L has a discrete valuation ν with a finite residue class field. Let ν be normalized such that $\nu(p) = 1$ for some prime number p, and let e be the unique positive integer for which $\nu(L^*) = \frac{1}{e}\mathbf{Z}$. We write $\mathcal{O}$ for the valuation ring $\{x \in L : \nu(x) \geq 0\}$, and P for the maximal ideal $\{x \in L : \nu(x) > 0\} = \{x \in L : \nu(x) \geq 1/e\}$ of $\mathcal{O}$. We denote by q the cardinality of the finite residue class field $\mathcal{O}/P$. Let $C = C(p, k, 1/e)$ be as in Theorem 3. We shall show that $B = k \cdot (q-1) \cdot C$ satisfies the conclusion of Theorem 2.

Let $f \in L[X]$ be any non-zero polynomial with at most $k+1$ non-zero terms. Theorem 3 implies that f has at most C zeroes in $1 + P$. Applying this result to $f(uX)$, for $u \in \mathcal{O}^*$, we see that f has at most C zeroes in any coset $u + P \in (\mathcal{O}/P)^*$. Summing this over the $q-1$ elements of $(\mathcal{O}/P)^*$, we derive that f has at most $(q-1) \cdot C$ zeroes in $\mathcal{O}^*$. Applying this result to $f(aX)$, for $a \in L^*$, we find that f has at most $(q-1) \cdot C$ zeroes in any coset $a\mathcal{O}^* \in L^*/\mathcal{O}^*$; or, equivalently, that f has at most $(q-1) \cdot C$ zeroes $x \in L^*$ for which $\nu(x)$ assumes a given finite value. Since by the theory of Newton polygons we have $\#\{\nu(x) : x \in L^*,\ f(x) = 0\} \leq k$ (see also [8, Lemma 2.1]), we can now conclude that f has at most $k \cdot (q-1) \cdot C$ zeroes in L^*. If we restrict, as in Theorem 2, to polynomials with $f(0) \neq 0$, then this is also an upper bound for the number of zeroes of f in L. This proves Theorem 2.

Remark. If the conclusion of Theorem 3 is available only for $r > 1/(p-1)$ (cf. the Remark in Section 3), then the preceding proof still works if one replaces the cosets $u + P \in (\mathcal{O}/P)^*$ by $u + P^l \in (\mathcal{O}/P^l)^*$, where $l/e > 1/(p-1)$; then the factor $q-1$ needs to be replaced by the order $(q-1) \cdot q^{l-1}$ of $(\mathcal{O}/P^l)^*$, and the conclusion is that one can take $B(k, L) = k \cdot (q-1) \cdot q^{l-1} \cdot C(p, k, l/e)$.

5. Number fields

We prove Theorem 1. Let m, k, and d be as in Theorem 1. Let p be any prime number, for example $p = 2$, and let $\bar{\mathbf{Q}}_p$ be an algebraic closure of $\mathbf{Q}_p$. By [4, Chap. II, Prop. 14], the field $\mathbf{Q}_p$ has only finitely many extensions of degree at most dm in $\bar{\mathbf{Q}}_p$. Let L be the composite of all these extensions; it is of finite degree over $\mathbf{Q}_p$. We shall show that $A = B(k, L)$ satisfies the conclusion of the theorem.

Let K, f, and g be as in Theorem 1. We may embed K as a subfield in $\bar{\mathbf{Q}}_p$. Then $K \cdot \mathbf{Q}_p$ has degree at most m over $\mathbf{Q}_p$. Hence any zero of f in $\bar{\mathbf{Q}}_p$ that has degree at most d over K lies in an extension of degree at most dm of $\mathbf{Q}_p$, and therefore in L. Thus, the number of zeroes of f in $\bar{\mathbf{Q}}_p^*$ that have degree at most d over K is bounded by $B(k, L)$. This implies that the degree of g is at most $B(k, L)$, as required. This proves Theorem 1.

6. A generalization

For a ring R and a positive integer n, we denote by $R[X_1, \ldots, X_n]$ the polynomial ring in n variables $X_1, \ldots, X_n$ over R. A polynomial in one variable is called *monic* if it has leading coefficient 1.

Proposition 6.1. *Let m, k, d be positive integers, and let $A = A(m, k, d)$ be any positive integer for which the conclusion of Theorem 1 is true. Suppose that K is a field that is of degree at most m over a purely transcendental field extension K_0 of $\mathbf{Q}$, that n is a positive integer, and that $f \in K[X_1, \ldots, X_n]$ is a non-zero polynomial with at most $k+1$ terms. Let $g \in K[X_1, \ldots, X_n]$ be a factor of f such that for each $i \in \{1, 2, \ldots, n\}$, every irreducible factor of g has degree at most d in X_i, and g is not divisible by X_i. Then, for each $i \in \{1, 2, \ldots, n\}$, the degree of g in X_i is at most A.*

Proof. We know the result to be true if $K_0 = \mathbf{Q}$ and $n = 1$. We first extend this to the case $K_0 = \mathbf{Q}(t : t \in T)$ for some collection T that is algebraically independent over $\mathbf{Q}$, still for $n = 1$. Let K_0 be such, let $K = K_0(u)$ be of degree l over K_0, and let f, $g \in K[X]$ be as in the statement of 6.1. Without loss of generality we assume that f and g are monic. Let $R_0 \subset K_0$ be a subring of the form $R_0 = \mathbf{Q}[t : t \in T][1/r]$, where $r \in \mathbf{Q}[t : t \in T]$ is a non-zero element that is chosen in such a manner that R_0 contains the coefficients of the following elements of K, when expressed on the K_0-basis $(u^i)_{i=0}^{l-1}$ of K: the coefficients of f; the coefficients of the monic irreducible factors of g; the inverse of $g(0)$; and u^l. Then $R = \sum_{i=0}^{l-1} R_0 \cdot u^i$ is a subring of K that is isomorphic to $R_0[U]/(h)$ for some monic polynomial $h = \sum_{i=0}^{l} h_i U^i \in R_0[U]$, and one has f, $g \in R[X]$. Next, one chooses rational numbers a_t, for $t \in T$, such that $(a_t)_{t\in T}$ is not a zero of r, and one defines $\varphi : R_0 \to \mathbf{Q}$ by substituting a_t for t. Adjoining a zero of $\sum_i \varphi(h_i)U^i$, one can extend φ to a ring homomorphism from R to some algebraic number field K_1 of degree at most l over $\mathbf{Q}$. The induced map $R[X] \to K_1[X]$ sending X to X maps f to a monic polynomial $f_1 \in K_1[X]$ with at most $k+1$ non-zero terms, and g to a factor g_1 of f_1 that has the same degree as g, that can be written as the product of polynomials of degree at most d, and that satisfies $g_1(0) \neq 0$. Hence by what we know about K_1, the degree of g is at most A. This proves the case $n = 1$ of 6.1.

For general n, let the notation again be as in 6.1, and let $i \in \{1, 2, \ldots, n\}$. View f and g as polynomials in a single variable X_i with coefficients in the field $K(X_j | j \neq i)$ of fractions of the polynomial ring in the remaining variables; this field is of degree at most m over the field $K_0(X_j | j \neq i)$, which is purely transcendental over $\mathbf{Q}$. In $K(X_j | j \neq i)[X_i]$, the polynomial g is a product of polynomials of degree at most d, and it is not divisible by X_i. Hence by what we know about the case $n = 1$, the degree of g is at most A. This proves 6.1.

7. Explicit bounds: the local case

Proposition 7.1. *Let $C(p, k, r)$ be as defined in Section 3, and write*

$$c = \frac{\exp 1}{(\exp 1) - 1}, \qquad v = \max\{i - \big(\operatorname{ord}_p(i!)\big)/r : 0 \leq i \leq k\}, \qquad w = \frac{k}{r \log p}.$$

Then we have

$$C(p, k, r) \leq c \cdot (v + w \log w) \leq c \cdot k \cdot \Big(1 + \frac{\log\big(k/(r \log p)\big)}{r \log p}\Big).$$

We note that $c \doteq 1.58197671$.

Proof. The last inequality follows from the fact that $v \leq k$. We prove the first inequality. By the definition of $C(p, k, r)$, it suffices to show that

$$m - \frac{\operatorname{ord}_p d_k(m)}{r} > v \qquad \text{for all } m > c \cdot (v + w \log w).$$

The function $1-(\log x)/x$ of a positive variable x assumes its minimum $1/c$ at $x=\exp 1$. Hence for all $x>0$ we have $x \geq (\log x)+x/c$. Now let m be an integer, $m > c\cdot(v+w\log w)$; we have $m>1$, since $v\geq 1$ and $w\log w \geq -\exp(-1)$. Taking $x=m/w$ and applying 2.4 we find that

$$\begin{aligned} m = w\cdot x &\geq w\cdot \log x + \frac{wx}{c} = w\log m - w\log w + \frac{m}{c} \\ &> w\log m + v = \frac{k\log m}{r\log p} + v \geq \frac{\operatorname{ord}_p d_k(m)}{r} + v, \end{aligned}$$

as required. This proves 7.1.

Let p be a prime number, and let L be a finite field extension of $\mathbf{Q}_p$. Denote by e_L and f_L the ramification index and the residue class field degree of L over $\mathbf{Q}_p$, respectively. For a positive integer k we define

$$B(k,L) = k\cdot(p^{f_L}-1)\cdot C(p,k,1/e_L),$$

with $C(p,k,1/e_L)$ as defined in Section 3.

Proposition 7.2. *With $B(k,L)$ as just defined, the conclusion of Theorem 2 is valid. Moreover, with c as in 7.1 and e_L and f_L as just defined, we have*

$$B(k,L) \leq c\cdot k^2\cdot(p^{f_L}-1)\cdot\Big(1+\frac{e_L\cdot\log(e_L k/\log p)}{\log p}\Big).$$

Proof. This is clear from Section 4 and 7.1.

Example: $k=1$. One can show that $C(p,1,1/e_L) = s_L\cdot e_L+1$, where $s_L = \max\{s\in\mathbf{Z} : s\cdot e_L+1\geq p^s\}$, so one has $B(1,L) = (p^{f_L}-1)\cdot(s_L\cdot e_L+1)$. The smallest value for B that makes the conclusion of Theorem 2 valid with $k=1$ is equal to the number of roots of unity in L, which is of the form $(p^{f_L}-1)\cdot p^{r_L}$, where r_L is a non-negative integer for which $(p-1)\cdot p^{r_L-1}$ divides e_L.

8. Explicit bounds: the global case

For positive integers m, k, and d, we define

$$A(m,k,d) = k\cdot\sum_{j=1}^{md}(2^j-1)\cdot C\Big(2,k,\frac{1}{[md/j]md}\Big),$$

where $[x]$ denotes the greatest integer not exceeding x, and the function C is as defined in Section 3.

Proposition 8.1. *With $A(m,k,d)$ as just defined, the conclusion of Theorem* 1 *is valid. Moreover, we have*

$$A(m,k,d) < \frac{c}{\log 2} \cdot k^2 \cdot (md+10) \cdot 2^{md+1} \cdot \log\Big(\frac{kmd}{\log 2}\Big),$$

where c is as in 7.1.

We note that $c/\log 2 \doteq 2.28230995$.

The proof of 8.1 requires a more refined approach than the one taken in Section 5.

We denote by $\bar{\mathbf{Q}}_2$ an algebraic closure of the field $\mathbf{Q}_2$ of 2-adic numbers, and by $\nu : \bar{\mathbf{Q}}_2 \to \mathbf{Q} \cup \{\infty\}$ the extension of the natural exponential valuation on $\mathbf{Q}_2$, normalized so that $\nu(2) = 1$. We fix a group homomorphism $\mathbf{Q} \to \bar{\mathbf{Q}}_2^*$, written $r \mapsto 2^r$, with the property that $2^1 = 2$; to construct such a group homomorphism, one chooses inductively $2^{1/n!}$ to be an nth root of $2^{1/(n-1)!}$, and one defines $2^{a/n!}$ to be the ath power of $2^{1/n!}$, for $a \in \mathbf{Z}$. We have $\nu(2^r) = r$ for each $r \in \mathbf{Q}$. For positive integers j and e, we define the subgroups U_e and T_j of $\bar{\mathbf{Q}}_2^*$ by

$$U_e = \{x : \nu(x-1) \geq 1/e\}, \qquad T_j = \{\zeta : \zeta^{2^j-1} = 1\}.$$

We have $U_e \subset U_{e'}$ if $e \leq e'$, and $T_j \subset T_{j'}$ if j divides j'.

Lemma 8.2. *Let k, j, and e be positive integers, and let $f \in \bar{\mathbf{Q}}_2[X]$ be a non-zero polynomial having $k+1$ non-zero terms. Then f has at most $k \cdot (2^j - 1) \cdot C(2,k,1/e)$ zeroes in the subgroup $2^{\mathbf{Q}} \cdot T_j \cdot U_e$ of $\bar{\mathbf{Q}}_2^*$.*

Proof. This is done by a straightforward extension of the argument of Section 4: one knows from Theorem 3 that f has at most $C(2,k,1/e)$ zeroes in U_e, and one deduces that the same is true for any coset of U_e; next one observes that T_j has order $2^j - 1$, and one derives that f has at most $(2^j-1) \cdot C(2,k,1/e)$ zeroes in each coset $2^r \cdot T_j \cdot U_e$ of $T_j \cdot U_e$; and one concludes the proof using the fact that ν assumes at most k different values r at the zeroes of f in $\bar{\mathbf{Q}}_2^*$. This proves 8.2.

Lemma 8.3. *Let n be a positive integer, and let L be an extension of $\mathbf{Q}_2$ of degree at most n inside $\bar{\mathbf{Q}}_2$. Then there exists an integer $j \in \{1, 2, \ldots, n\}$ such that $L^* \subset 2^{\mathbf{Q}} \cdot T_j \cdot U_{[n/j]n}$.*

Proof. Let f_L and e_L be as in Section 7, and put $M = L(2^{1/e_L})$. We claim that $j = f_M$, the residue class field degree of M over $\mathbf{Q}_2$, has the stated properties. To prove this, denote by e' and f' the ramification index and residue class field degree of M over L. Then we have $e'f' = [M:L] \leq e_L$, and therefore

$$f_M \leq e' \cdot f_M = e' \cdot f' \cdot f_L \leq e_L \cdot f_L = [L:\mathbf{Q}_2] \leq n.$$

This proves, first, that $j = f_M$ does belong to $\{1, 2, \ldots, n\}$, and secondly, that $e' \leq [n/f_M] = [n/j]$. Hence the ramification index e_M of M over $\mathbf{Q}_2$ satisfies $e_M = e' \cdot e_L \leq [n/j] \cdot n$. Therefore each $x \in M$ with $\nu(x-1) > 0$ belongs to

$U_{[n/j]n}$. From $j = f_M$ it follows that $T_j \subset M^*$, and that T_j is in fact a system of representatives for the group of units of the residue class field of M (see [9, Chap. 2, Prop. 8(iii)]). It follows that the kernel of $\nu : M^* \to \mathbf{Q}$ is contained in $T_j \cdot U_{[n/j]n}$. Now, in order to prove that $L^* \subset 2^{\mathbf{Q}} \cdot T_j \cdot U_{[n/j]n}$, let x belong to L^*. Then $\nu(x) = r$ for some $r \in \frac{1}{e_L}\mathbf{Z}$, so the element $x \cdot 2^{-r}$, which does belong to M^*, is in the kernel of ν. Therefore we have $x \in 2^r \cdot T_j \cdot U_{[n/j]n} \subset 2^{\mathbf{Q}} \cdot T_j \cdot U_{[n/j]n}$, as required. This proves 8.3.

One can show that the integer e' occurring in the proof above is a power of 2. This observation may be used to improve our value for $A(m, k, d)$, but it will not change its order of magnitude.

We turn to the proof of 8.1. Let m, k, d be positive integers, and let K, f, g be as in Theorem 1. We may assume that K is a subfield of $\bar{\mathbf{Q}}_2$. Then every zero of g in $\bar{\mathbf{Q}}_2$ lies in an extension of degree at most $n = md$ of $\mathbf{Q}_2$, so by Lemma 8.3 also in $\bigcup_{j=1}^{n}(2^{\mathbf{Q}} \cdot T_j \cdot U_{[n/j]n})$. From Lemma 8.2 it now follows that the number of zeroes of g in $\bar{\mathbf{Q}}_2$ is at most

$$\sum_{j=1}^{n} k \cdot (2^j - 1) \cdot C\bigl(2, k, 1/([n/j]n)\bigr) = A(m, k, d).$$

Hence $A(m, k, d)$ is an upper bound for the degree of g. This proves the first assertion of 8.1. We prove the second assertion. From 7.1 we obtain

$$A(m, k, d) \le c \cdot k^2 \cdot \sum_{j=1}^{n} (2^j - 1) \cdot \Bigl(1 + \frac{[n/j]n \cdot \log\bigl([n/j]nk/\log 2\bigr)}{\log 2}\Bigr),$$

where we still write $n = md$. For $[n/2] < j \le n$ we have $[n/j] = 1$, and for $1 \le j \le [n/2]$ we have $[n/j] \le n$ and $\log\bigl([n/j]nk/\log 2\bigr) \le 2\log(nk/\log 2)$. This leads to

$$\begin{aligned} A(m, k, d) &< c \cdot k^2 \cdot \Bigl(2^{n+1} + 2^{n+1} \cdot \frac{n \cdot \log(nk/\log 2)}{\log 2} + 2^{[n/2]+1} \cdot \frac{n^2 \cdot 2\log(nk/\log 2)}{\log 2}\Bigr) \\ &\le c \cdot k^2 \cdot 2^{n+1} \cdot \frac{(n + 10) \cdot \log(nk/\log 2)}{\log 2}, \end{aligned}$$

the second inequality being obtained by a routine argument. This proves 8.1.

9. Two-adic trinomials

In this section we determine how many zeroes a polynomial of the form

(9.1) $\quad f = a + bX^t + cX^u \quad$ with $a \in \mathbf{Q}_2^*,\ b,\ c \in \mathbf{Q}_2,\ t,\ u \in \mathbf{Z},\ 0 < t < u,$

may have in $\mathbf{Q}_2$; here we still count zeroes with their multiplicities. We let the function C be as defined in Section 3, and we write ν for the natural exponential valuation on $\mathbf{Q}_2$.

According to the first assertion of 7.2, with $k = 2$, $p = 2$, $L = \mathbf{Q}_2$, $e_L = 1$, and $f_L = 1$, an upper bound for the number of zeroes of any f as in (9.1) in $\mathbf{Q}_2$ is given by $2 \cdot C(2,2,1)$, which by a direct computation is found to be 8. (The second assertion of 7.2 gives the upper bound 16.0018.) The following result shows that the best upper bound is 6.

Proposition 9.2.
(a) *Let f be as in* (9.1)*. Then the number of zeroes of f in $\mathbf{Q}_2$ equals* 0, 1, 2, 3, 4, *or* 6, *and if it equals* 4 *or* 6 *then t and u are both even.*
(b) *For any $n \in \{0,1,2,3,4,6\}$ there exists f as in* (9.1)*, with $b \neq 0$ and $c \neq 0$, such that the number of zeroes of f in $\mathbf{Q}_2$ equals n.*

In the proof we use a variant of 2.2. We write $\mathbf{Z}_p$ for the ring of p-adic integers.

Proposition 9.3. *Let p be a prime number, n a non-negative integer, and T a finite non-empty subset of $\mathbf{Z}$. Write $T_j = \{t \in T : (t \bmod p) = j\}$ for each $j \in \mathbf{Z}/p\mathbf{Z}$, and put $k = \max\{\#T_j : j \in \mathbf{Z}/p\mathbf{Z}\} - 1$. Then there exists a polynomial $h \in \mathbf{Z}_p[X]$ such that for each $t \in T$ one has $h(t) = d_k(n) \cdot \binom{t}{n}$.*

Proof. Let $j \in \mathbf{Z}/p\mathbf{Z}$ be such that T_j is non-empty, and put $k(j) = \#T_j - 1$. Applying 2.2 to T_j, we obtain a polynomial $h_j \in \mathbf{Z}[X]$ with the property that for each $t \in T_j$ one has $h_j(t) = d_{k(j)}(n) \cdot \binom{t}{n}$. Next define

$$g_j = 1 - \prod_{t \in T_j} \left(1 - \prod_{u \in T,\, u \notin T_j} \frac{X - u}{t - u}\right).$$

We have $g_j \in \mathbf{Z}_p[X]$, since none of the denominators $t - u$ is divisible by p. Also, we have $g_j(t) = 1$ for $t \in T_j$ and $g_j(u) = 0$ for $u \in T$, $u \notin T_j$.

It is now straightforward to verify that the polynomial

$$h = \sum_j g_j \cdot h_j \cdot d_k(n)/d_{k(j)}(n)$$

has the properties stated in 9.3; note that for each j we have $d_k(n)/d_{k(j)}(n) \in \mathbf{Z}$, since $k(j) \leq k$. This proves 9.3.

Proof of 9.2. (a) Let f be as in (9.1). Let it first be assumed that t or u is odd; in this case 9.2(a) asserts that f has at most 3 zeroes in $\mathbf{Q}_2$. To prove this, we observe that $T = \{0, t, u\}$ contains integers of both parities, so when we apply 9.3 we can take $k = 1$ (as opposed to $k = 2$ when we apply 2.2). With this improvement, the argument given in Section 3 shows that the number of zeroes of f in $\mathbf{Z}_2^* = 1+2\mathbf{Z}_2$ is at most $C(2,1,1) = 2$ (as opposed to $C(2,2,1) = 4$). If ν assumes at most 1 value at the set of zeroes of f in $\mathbf{Q}_2$, then the argument of Section 4 now implies that f has at most 2 zeroes in $\mathbf{Q}_2$. Assume therefore that ν assumes at least 2 values at the zeroes of f in $\mathbf{Q}_2$. Let r and s be zeroes of f in $\mathbf{Q}_2$ with $\nu(r) > \nu(s)$. By the theory of Newton polygons, each zero of f in $\mathbf{Q}_2$ is in $r \cdot \mathbf{Z}_2^*$ or in $s \cdot \mathbf{Z}_2^*$, and the polynomials $f(rX)$ and $f(sX)$ have the shape

$$f(rX) = (a' + b'X^t + c'X^u) \cdot d', \quad \text{with } a',\, b' \in \mathbf{Z}_2^*,\ c' \in 2\mathbf{Z}_2,\ d' \in \mathbf{Q}_2^*,$$
$$f(sX) = (a'' + b''X^t + c''X^u) \cdot d'', \quad \text{with } a'' \in 2\mathbf{Z}_2,\ b'',\, c'' \in \mathbf{Z}_2^*,\ d'' \in \mathbf{Q}_2^*.$$

Each of these polynomials has 1 as a zero and has at most 2 zeroes in $\mathbf{Z}_2^*$. If t is odd, then 1 is a simple zero of the reduction of $f(rX)/d'$ modulo 2, so by Hensel's lemma (see [11, Cor. 2-2-6]) it is the unique zero of $f(rX)$ in $\mathbf{Z}_2^* = 1 + 2\mathbf{Z}_2$. If t is even then u is odd, and 1 is a simple zero of the reduction of $f(sX)/d''$ modulo 2, so by Hensel's lemma it is the unique zero of $f(sX)$ in $\mathbf{Z}_2^*$. In either case, one of the two polynomials has a unique zero in $\mathbf{Z}_2^*$, and the other at most 2. Therefore f has at most 3 zeroes in $\mathbf{Q}_2$, as asserted.

Next assume that t and u are even. We can write $t = t_0 2^l$ and $u = u_0 2^l$, where l is a positive integer and t_0 or u_0 is odd. Then we have $f = f_0(X^{2^l})$, where $f_0 = a + bX^{t_0} + cX^{u_0}$, and the zeroes of f are the 2^lth roots of the zeroes of f_0. By the above, f_0 has at most 3 zeroes in $\mathbf{Q}_2$; and since $\mathbf{Q}_2$ contains exactly 2 roots of unity, each of these zeroes that has a 2^lth root in $\mathbf{Q}_2$ has exactly 2 of them. Hence the number of zeroes of f in $\mathbf{Q}_2$ equals 0, 2, 4, or 6. This proves (a).

(b) One easily verifies that the polynomials

$$X^2 + X + 1, \quad X^3 + X^2 - 2, \quad X^2 - 5X + 4, \quad X^4 - 5X^2 + 4$$

have exactly 0, 1, 2, 4 zeroes in $\mathbf{Q}_2$, respectively. (They have in fact the same property over $\mathbf{Q}$ and $\mathbf{R}$.) Next consider the polynomial

$$f = 3X^5 + X - 4.$$

One has

$$\frac{f(8X+1)}{128} = 768X^5 + 480X^4 + 120X^3 + 15X^2 + X \equiv X \cdot (X - 1) \bmod 2.$$

By Hensel's lemma, $f(8X+1)$ has two zeroes in $\mathbf{Z}_2$, so f has two zeroes in $1+8\mathbf{Z}_2$. Also, one has

$$\frac{f(4X)}{4} = 3 \cdot 2^8 \cdot X^5 + X - 1 \equiv X - 1 \bmod 8,$$

so $f(4X)$ has a zero in $\mathbf{Z}_2$ that is 1 mod 8, and f has a zero in $2^2 \cdot (1+8\mathbf{Z}_2)$. This shows that f has at least 3 zeroes in $\mathbf{Q}_2$, and by (a) it has no others. Since each element of $1+8\mathbf{Z}_2$ is a square in $\mathbf{Q}_2$, each of the 3 zeroes of f has two square roots in $\mathbf{Q}_2$. Therefore the polynomial $3X^{10} + X^2 - 4$ has exactly 6 zeroes in $\mathbf{Q}_2$. This proves 9.2.

Remark. The arguments used in the proof of 9.2 lead to the following general result. Let the hypotheses and the notation be as in 7.2, and define

$$B'(k, L) = w_L \cdot (p^{f_L} - 1) \cdot \big(1 + (k-1) \cdot C(p, k-1, 1/e_L)\big),$$

where w_L denotes the number of roots of unity in L that have p-power order. Then the conclusion of Theorem 2 is valid with $B'(k, L)$ in the place of $B(k, L)$. For $k = 1$, we have $B'(1, L) = w_L \cdot (p^{f_L} - 1)$, which is the number of *all* roots of unity in L; it follows that for $k = 1$ the bound $B'(k, L)$ cannot be improved. If $k > 1$, then one has $B'(k, L) < B(k, L)$ for all L with $w_L = 1$; but if $w_L > 1$, then one has $B'(k, L) > B(k, L)$ for all k exceeding a bound that depends on L.

References

[1] Cucker, F., Koiran, P., Smale, S., A polynomial time algorithm for diophantine equations in one variable. J. Symbolic Comput., to appear.

[2] Hajós, G., [Solution to problem 41] (in Hungarian). Mat. Lapok 4 (1953), 40–41.

[3] Khovanskiĭ, A.G., Fewnomials. Amer. Math. Soc., Providence 1991.

[4] Lang, S., Algebraic number theory. 2nd ed. Springer, New York 1994.

[5] Lenstra, H.W., Jr., Finding small degree factors of lacunary polynomials. This volume, 267–276.

[6] Montgomery, H.L., Schinzel, A., Some arithmetic properties of polynomials in several variables. In: Transcendence theory: advances and applications (ed. by A. Baker, D.W. Masser), Chapter 13, 195–203. Academic Press, London 1977.

[7] Poonen, B., Zeros of sparse polynomials over local fields of characteristic p. Math. Res. Lett., to appear.

[8] Schacher, M., Straus, E.G., Some applications of a non-Archimedean analogue of Descartes' rule of signs. Acta Arith. 25 (1974), 353–357.

[9] Serre, J-P., Corps locaux. Hermann, Paris 1962.

[10] Weber, H., Lehrbuch der Algebra, vol. I. 2nd ed. Vieweg, Braunschweig 1912.

[11] Weiss, E., Algebraic number theory. McGraw-Hill, New York 1963.