Sharp bounds for the number of roots of univariate fewnomials

Martín Avendaño[a,1], Teresa Krick[b,2]

[a] *Texas A&M University, Department of Mathematics*
Milner Bldg. 023, College Station, TX 77843-3368, USA
Email: `avendano@math.tamu.edu`
[b] *Departamento de Matemática, FCEyN, Universidad de Buenos Aires and CONICET,*
Ciudad Universitaria, –1428– Buenos Aires, Argentina
Email: `krick@dm.uba.ar`

Abstract

Let K be a field and $t \geq 0$. Denote by $B_{\mathrm{m}}(t, K)$ the supremum of the number of roots in K^*, counted with multiplicities, that can have a non-zero polynomial in $K[x]$ with at most $t + 1$ monomial terms. We prove, using an unified approach based on Vandermonde determinants, that $B_{\mathrm{m}}(t, L) \leq t^2 B_{\mathrm{m}}(t, K)$ for any local field L with a non-archimedean valuation $v : L \to \mathbb{R} \cup \{\infty\}$ such that $v|_{\mathbb{Z}_{\neq 0}} \equiv 0$ and residue field K, and that $B_{\mathrm{m}}(t, K) \leq (t^2 - t + 1)(p^f - 1)$ for any finite extension $K/\mathbb{Q}_p$ with residual class degree f and ramification index e, assuming that $p > t + e$. For any finite extension $K/\mathbb{Q}_p$, for p odd, we also show the lower bound $B_{\mathrm{m}}(t, K) \geq (2t - 1)(p^f - 1)$, which gives the sharp estimation $B_{\mathrm{m}}(2, K) = 3(p^f - 1)$ for trinomials when $p > 2 + e$.

Keywords: Lacunary polynomials, Root counting, Local fields, Generalized Vandermonde determinants.
2008 MSC: 11S05, 13F30

1. Introduction

Definition 1.1. *Let K be a field and let $t \geq 0$. We denote by $B_1(t, K)$ and $B_{\mathrm{m}}(t, K)$ the supremum of the number of roots in K^*, counted without/with*

---

multiplicities respectively, that can have a non-zero polynomial in $K[x]$ with at most $t + 1$ monomial terms.

Since a monomial can not have non-zero roots, we have $B_1(0, K) = B_\mathrm{m}(0, K) = 0$ for any field K. For this reason, we restrict our attention to the case $t \geq 1$. Note also that $B_1(t, K) \leq B_\mathrm{m}(t, K)$ for any field K and any $t \geq 0$. Moreover, if K is a field of characteristic zero, it can be shown (by taking derivatives) that any root in K^* of a polynomial with $t+1$ non-zero terms has multiplicity at most t, hence $B_\mathrm{m}(t, K) \leq t\, B_1(t, K)$, although we do not even know whether $B_\mathrm{m}(t, K)$ might be greater than $B_1(t, K)$ in this case. When K is a field of characteristic $p \neq 0$, the binomials $x^{p^n} - 1 = (x - 1)^{p^n} \in K[x]$, which have the root $x = 1$ with multiplicity p^n, show that $B_\mathrm{m}(t, K) = \infty$ for any $t \geq 1$. Similarly, for any algebraically closed field K and $t \geq 1$, we have $B_1(t, K) = B_\mathrm{m}(t, K) = \infty$, since the binomials $x^d - 1$ have d different roots in K^* for any positive integer d not divisible by the characteristic of K.

For the field of real numbers $\mathbb{R}$, it is well-known by Descartes' rule of signs that $B_1(t, \mathbb{R}) \leq B_\mathrm{m}(t, \mathbb{R}) \leq 2t$. Furthermore, the equality holds since this upper bound is attained by the polynomials $(x^2 - 1^2)(x^2 - 2^2) \cdots (x^2 - t^2) \in \mathbb{R}[x]$, that have exactly $t + 1$ non-zero terms and $2t$ simple real roots. This result extends straightforwardly to any ordered field by the corresponding generalization of Descartes'rule of signs (and since the same example stays valid), see for instance in [4, Prop. 1.2.14]:

Theorem 1.2. *Let K be an ordered field. Then*

$$B_1(t, K) = B_\mathrm{m}(t, K) = 2t.$$

Here we give a different proof of this theorem, based on generalized Vandermonde determinants, in order to introduce the technique used in the proof of our main results.

Recall that if K is an ordered field, then also the field of formal power series $K((u))$ and the field of Puiseux series $K\{\{u\}\} = \bigcup_{n \geq 1} K((u^{1/n}))$ are ordered (by saying that a power series is positive if and only if its first non-zero coefficient, i.e. the one with minimum power of u, is positive). Also the field of rational functions $K(u)$ can be ordered by embedding it into $K((u))$. Theorem 1.2 implies that $B_1(t, K\{\{u\}\}) = B_\mathrm{m}(t, K\{\{u\}\}) = 2t$ for any ordered field K.

For other fields, the situation can be dramatically different. For instance, B. Poonen showed in [10, Thm. 1], that in the case $K = \mathbb{F}_q$, we

have $B_1(t, \mathbb{F}_q\{\{u\}\}) = q^t$. In the case of a field K of characteristic zero, next result gives a bound for $B_1(t, K\{\{u\}\})$ and $B_{\mathrm{m}}(t, K\{\{u\}\})$ in terms of $B_1(t, K)$ and $B_{\mathrm{m}}(t, K)$.

Theorem 1.3. *Let L be a local field with a valuation $v : L \to \mathbb{R} \cup \{\infty\}$ such that $v(n \cdot 1_L) = 0$ for all $n \in \mathbb{Z} \setminus \{0\}$, and let K be its residue field. Then*

$$B_1(t, L) \leq t^2\, B_1(t, K) \quad and \quad B_{\mathrm{m}}(t, L) \leq t^2\, B_{\mathrm{m}}(t, K).$$

Note that the assumption $v(n \cdot 1_L) = 0$ for all $n \in \mathbb{Z} \setminus \{0\}$ implies that L is a field of characteristic zero, because otherwise we would obtain a contradiction in $v(\mathrm{char}(L) \cdot 1_L) = v(0) = \infty$. Also, by construction of the residue field, we have that $v(\mathrm{char}(K) \cdot 1_L) > 0$, and hence K is also implied to be of characteristic zero. Theorem 1.3 can be applied to the fields $L = K((u))$ or $L = K\{\{u\}\}$, as long as a bound for $B_1(t, K)$ or $B_{\mathrm{m}}(t, K)$ is provided. The valuation on L used in this case is the trivial one, i.e. $v|_{K^*} = 0$ and $v(u) = 1$. Unfortunately, the bound obtained is not sharp in general. For instance, the case $K = \mathbb{R}$ give us $B_1(t, \mathbb{R}\{\{u\}\}) \leq B_{\mathrm{m}}(t, \mathbb{R}\{\{u\}\}) \leq 2t^3$, while the sharpest bound is $2t$.

Theorem 1.3 can not be applied to the field $\mathbb{Q}_p$ of p-adic numbers (nor to any finite extension $K/\mathbb{Q}_p$), since its residue field has non-zero characteristic. In the case of a finite extension K of $\mathbb{Q}_p$ with ramification index e and residue class degree f, H.W. Lenstra proved in [7, Prop. 7.2] that

$$B_{\mathrm{m}}(t, K) \leq c\, t^2\, (p^f - 1)\, (1 + e\log(e\, t / \log(p)) / \log(p)),$$

$c = e/(e - 1) \approx 1.58197671$. Our following result improves Lenstra's for prime numbers p large enough with respect to the number of non-zero terms.

Theorem 1.4. *Let $K/\mathbb{Q}_p$ be a finite extension, with ramification index e and residue class degree f. Assume that $p > e + t$. Then*

$$B_{\mathrm{m}}(t, K) \leq (t^2 - t + 1)\, (p^f - 1).$$

The previous bound is sharp for binomials (i.e. $t = 1$), since the polynomial $x^{p^f} - x \in K[x]$ has $p^f - 1$ roots in K^*. It is also sharp for trinomials (i.e. $t = 2$) when $p > 2 + e$, thanks to the following explicit example, see Section 4.

Example 1.5. *Let p be an odd prime number and let $K/\mathbb{Q}_p$ be a finite extension with residue field of cardinality q. Then, the trinomial*

$$f(x) = x^{(q-1)(1+q^{q-1})} - (1 + q^{q-1})x^{q-1} + q^{q-1} \in K[x]$$

has at least $3(q - 1)$ roots in K^* counted with multiplicities.

In [3], the authors define the class of regular polynomials in $K[x]$, where K is a local field with respect to a discrete valuation with residue field of cardinality $q < +\infty$, and prove that the polynomials in this class can not have more than $t(q-1)$ roots in K^*, counted with multiplicities [3, Cor. 4.6]. Moreover, this bound is sharp for regular polynomials, since explicit examples (with all simple roots) are presented. This implies the lower bound $B_{\mathrm{m}}(t, K) \geq B_1(t, K) \geq t(q-1)$. Note that in particular, this lower bound holds for any finite extension $K/\mathbb{Q}_p$. The following result improves it in this case by a factor of almost 2.

Theorem 1.6. *Let p be an odd prime number and let $K/\mathbb{Q}_p$ be a finite extension with residue field of cardinality q. Then $B_1(t, K) \geq (2t-1)(q-1)$.*

The previous results also complement another result by Lenstra, where the sharp estimate $B_{\mathrm{m}}(2, \mathbb{Q}_2) = 6$ is shown [7, Prop. 9.2]. He also asks for the exact value of $B_{\mathrm{m}}(2, \mathbb{Q}_p)$ for other primes p. As a consequence of Theorems 1.4 and 1.6 and Example 1.5 we derive that

$$B_1(2, \mathbb{Q}_p) = B_{\mathrm{m}}(2, \mathbb{Q}_p) = 3(p-1)$$

for any prime $p \geq 5$, thus leaving the case $p = 3$ as the only remaining open question. For $t = 3$, we are also closing the gap to

$$5(p-1) \leq B_1(3, \mathbb{Q}_p) \leq B_{\mathrm{m}}(3, \mathbb{Q}_p) \leq 7(p-1)$$

for any prime $p \geq 5$. Moreover, for any $(t+1)$-nomial over $\mathbb{Q}_p$ with $p > t+1$ we deduce

$$(2t-1)(p-1) \leq B_1(t, \mathbb{Q}_p) \leq B_{\mathrm{m}}(t, \mathbb{Q}_p) \leq (t^2 - t + 1)(p-1).$$

A deeper analysis for the case $t = 3$ may give a hint of whether the sharp bound for $(t+1)$-nomials is linear or quadratic in t. Our feeling is that it should be quadratic although we do not have yet any evidence to support it.

2. Generalized confluent Vandermonde determinants

Definition 2.1. *Let $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_t) \in \mathbb{N}^t$ and for $s \in N$, $(x_0, \ldots, x_{s-1})$ be a group of s variables. The* generalized Vandermonde matrix *associated to α is defined as*

$$M_{\boldsymbol{\alpha}}(x_0, \ldots, x_{s-1}) = \begin{pmatrix} 1 & x_0^{\alpha_1} & \cdots & x_0^{\alpha_t} \\ \vdots & \vdots & & \vdots \\ 1 & x_{s-1}^{\alpha_1} & \cdots & x_{s-1}^{\alpha_t} \end{pmatrix} \in \mathbb{Z}[x_0, \ldots, x_{s-1}]^{s \times (t+1)}.$$

When $s = t + 1$, the polynomial

$$V_{\boldsymbol{\alpha}}(x_0, \ldots, x_t) = \det(M_{\boldsymbol{\alpha}}(x_0, \ldots, x_t)) \in \mathbb{Z}[x_0, \ldots, x_t]$$

is called a generalized Vandermonde determinant.

We note that when $\mathbf{st} = (1, 2, \ldots, t)$, then $V_{\mathbf{st}}(x_0, \ldots, x_t)$ corresponds to the standard Vandermonde determinant.

The basic properties of generalized Vandermonde determinants are summarized in the following well-known proposition, see for instance [6, Thm. 5] or [9].

Proposition 2.2. *Let $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_t)$ with $0 < \alpha_1 < \cdots < \alpha_t$. Then*

(a) $V_{\mathbf{st}}(x_0, \ldots, x_t) = \displaystyle\prod_{0 \leq i < j \leq t} (x_j - x_i)$.

(b) $V_{\boldsymbol{\alpha}} = V_{\mathbf{st}} P_{\boldsymbol{\alpha}}$ *for some non-zero $P_{\boldsymbol{\alpha}} \in \mathbb{Z}[x_0, \ldots, x_t]$.*

(c) $V_{\boldsymbol{\alpha}}$ *and $P_{\boldsymbol{\alpha}}$ are homogeneous polynomials of degree $|\boldsymbol{\alpha}|$ and $|\boldsymbol{\alpha}| - t(t+1)/2$ respectively.*

(d) *The coefficients of $P_{\boldsymbol{\alpha}}$ are all non-negative.*

We show now, before dealing with multiplicities, how Proposition 2.2 immediately implies $B_1(t, K) \leq 2t$ for ordered fields.

Proof of Theorem 1.2 (first part). Suppose that $B_1(t, K) > 2t$. Then there exists a non-zero polynomial $f = a_0 + a_1 x^{\alpha_1} + \cdots + a_t x^{\alpha_t} \in K[x]$ with strictly more than $2t$ different roots. Therefore at least $t + 1$ of these roots, say $r_0, \ldots, r_t$, are all strictly positive or strictly negative. The equalities $f(r_i) = 0$ for $0 \leq i \leq t$ translate into the matrix identity

$$M_{\boldsymbol{\alpha}}(r_0, \ldots, r_t) \cdot \begin{pmatrix} a_0 \\ \vdots \\ a_t \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

and since $f \neq 0$, we conclude that $V_{\boldsymbol{\alpha}}(r_0, \ldots, r_t) = 0$. However, by Proposition 2.2(**d**),

$$V_{\boldsymbol{\alpha}}(r_0, \ldots, r_t) = V_{\mathbf{st}}(r_0, \ldots, r_t) \, P_{\boldsymbol{\alpha}}(r_0, \ldots, r_t) \neq 0$$

since $V_{\mathbf{st}}(r_0, \ldots, r_t) \neq 0$ and $P_{\boldsymbol{\alpha}}(r_0, \ldots, r_t)$ is strictly positive or negative according to the sign of the r_i's. Contradiction! $\qquad\square$

In order to deal with multiple roots, we need a more general version of Definition 2.1 and Proposition 2.2.

Definition 2.3. *Let $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_t) \in \mathbb{N}^t$, $(x_0, \ldots, x_m)$ be a group of $m+1$ variables for $m \geq 0$, and $\boldsymbol{s} = (s_0, \ldots, s_m) \in \mathbb{N}^{m+1}$. The* generalized confluent Vandermonde matrix *associated to $\boldsymbol{\alpha}$ and $\boldsymbol{s}$ is defined as*

$$M_{\boldsymbol{\alpha}}^{\boldsymbol{s}}(x_0, \ldots, x_m) = \begin{array}{c} \overset{\longleftarrow \quad t+1 \quad \longrightarrow}{\left(\begin{array}{c} \overline{M_{\boldsymbol{\alpha}}^{s_0}(x_0)} \\ \vdots \\ M_{\boldsymbol{\alpha}}^{s_{m-1}}(x_{m-1}) \end{array} \right)} \end{array} \begin{array}{c} s_0 \\ \vdots \\ s_m \end{array} \quad \in \mathbb{Z}[x_0, \ldots, x_m]^{|\boldsymbol{s}| \times (t+1)}$$

where for $0 \leq i \leq m$,

$$M_{\boldsymbol{\alpha}}^{s_i}(x_i) = \begin{pmatrix} 1 & x_i^{\alpha_1} & \cdots & x_i^{\alpha_t} \\ 0 & \alpha_1 x_i^{\alpha_1 - 1} & \cdots & \alpha_t x_i^{\alpha_t - 1} \\ \vdots & \vdots & & \vdots \\ 0 & \binom{\alpha_1}{s_i-1} x_i^{\alpha_1 - s_i + 1} & \cdots & \binom{\alpha_t}{s_i-1} x_i^{\alpha_t - s_i + 1} \end{pmatrix} \in \mathbb{Z}[x_i]^{s_i \times (t+1)}.$$

When $|\boldsymbol{s}| = t + 1$, the polynomial

$$V_{\boldsymbol{\alpha}}^{\boldsymbol{s}}(x_0, \ldots, x_m) = \det(M_{\boldsymbol{\alpha}}^{\boldsymbol{s}}(x_0, \ldots, x_m)) \in \mathbb{Z}[x_0, \ldots, x_m]$$

is called a generalized confluent Vandermonde determinant.

Note that the matrix $M_{\boldsymbol{\alpha}}(x_0, \ldots, x_{s-1})$ of Definition 2.1 corresponds to the matrix $M_{\boldsymbol{\alpha}}^{\mathbf{1}}(x_0, \ldots, x_{s-1})$ with $\mathbf{1} = (1, \ldots, 1) \in \mathbb{N}^s$.

Next result generalizes Proposition 2.2 to these more general matrices.

Proposition 2.4. *Let $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_t)$ with $0 < \alpha_1 < \cdots < \alpha_t$ and let $\mathbf{st} = (1, 2, \ldots, t)$. Let $\boldsymbol{s} = (s_0, \ldots, s_m) \in \mathbb{N}^{m+1}$ with $|\boldsymbol{s}| = t + 1$. Then*

(a) $V_{\mathbf{st}}^{\boldsymbol{s}}(x_0, \ldots, x_m) = \displaystyle\prod_{0 \leq i < j \leq m} (x_j - x_i)^{s_i s_j}.$

(b) $V_{\boldsymbol{\alpha}}^{\boldsymbol{s}} = V_{\mathbf{st}}^{\boldsymbol{s}} P_{\boldsymbol{\alpha}}^{\boldsymbol{s}}$ *for some $P_{\boldsymbol{\alpha}}^{\boldsymbol{s}} \in \mathbb{Z}[x_0, \ldots, x_m]$.*

(c) $V_{\boldsymbol{\alpha}}^{\boldsymbol{s}}$ *and $P_{\boldsymbol{\alpha}}^{\boldsymbol{s}}$ are homogeneous polynomials of degree $|\boldsymbol{\alpha}| - \sum_{i=0}^{m} s_i(s_i-1)/2$ and $|\boldsymbol{\alpha}| - t(t+1)/2$ respectively.*

(d) *The coefficients of $P_{\boldsymbol{\alpha}}^{\boldsymbol{s}}$ are all non-negative.*

Proof. Set

$$\hat{s} = (s_0, \ldots, s_{k-1}, s_k + 1, s_{k+1}, \ldots, s_m) \in \mathbb{N}^{m+1},$$

$$\bar{s} = (s_0, \ldots, s_{k-1}, s_k, 1, s_{k+1}, \ldots, s_m) \in \mathbb{N}^{m+2}.$$

The proofs will be inductive, assuming the properties hold for $\bar{s}$ and proving them for $\hat{s}$, noting that the case $s = (1, 1, \ldots, 1) \in \mathbb{N}^{t+1}$ corresponds to Proposition 2.2. They are based on the following identity of polynomials.

$$V_{\alpha}^{\hat{s}}(x_0, \ldots, x_m) = \left. \frac{V_{\alpha}^{\bar{s}}(x_0, \ldots, x_k, x_k + \delta, x_{k+1}, \ldots, x_m)}{\delta^{s_k}} \right|_{\delta=0} \tag{1}$$

To prove Identity (1), we perform row operations on $M_{\alpha}^{\bar{s}}(\ldots, x_k, x_k + \delta, \ldots)$. More precisely, we will only operate on the subblock A of this matrix corresponding to $M_{\alpha}^{s_k}(x_k)$ and $M_{\alpha}^1(x_k + \delta)$.

$$A = \left(\frac{M_{\alpha}^{s_k}(x_k)}{M_{\alpha}^1(x_k + \delta)} \right) = \begin{pmatrix} 1 & x_k^{\alpha_1} & \cdots & x_k^{\alpha_t} \\ 0 & \alpha_1 x_k^{\alpha_1 - 1} & \cdots & \alpha_t x_k^{\alpha_t - 1} \\ \vdots & \vdots & & \vdots \\ 0 & \binom{\alpha_1}{s_k - 1} x_k^{\alpha_1 - s_k + 1} & \cdots & \binom{\alpha_t}{s_k - 1} x_k^{\alpha_t - s_k + 1} \\ \hline 1 & (x_k + \delta)^{\alpha_1} & \cdots & (x_k + \delta)^{\alpha_t} \end{pmatrix}$$

Expanding the last row and subtracting the first s_k rows multiplied by δ^{i-1} from the last one, we get

$$B = \begin{pmatrix} 1 & x_k^{\alpha_1} & \cdots & x_k^{\alpha_t} \\ 0 & \alpha_1 x_k^{\alpha_1 - 1} & \cdots & \alpha_t x_k^{\alpha_t - 1} \\ \vdots & \vdots & & \vdots \\ 0 & \binom{\alpha_1}{s_k - 1} x_k^{\alpha_1 - s_k + 1} & \cdots & \binom{\alpha_t}{s_k - 1} x_k^{\alpha_t - s_k + 1} \\ 0 & \sum_{i \geq s_k} \binom{\alpha_1}{i} \delta^i x_k^{\alpha_1 - i} & \cdots & \sum_{i \geq s_k} \binom{\alpha_t}{i} \delta^i x_k^{\alpha_t - i} \end{pmatrix}$$

Now we compute the determinant $V_{\alpha}^{\bar{s}}(\ldots, x_k, x_k + \delta, \ldots)$ using the block B instead of A. The last row of B shows that it is divisible by δ^{s_k}. Moreover, dividing by δ^{s_k} and then specializing it into $\delta = 0$ corresponds to keeping only the term in δ^{s_k} in the last row of B, thus reducing to the determinant of the matrix $M_{\alpha}^{\hat{s}}(x_0, \ldots, x_m)$. This concludes the proof of Identity (1).

(a) See also [1] or [5, Thm. 2.4].
Assume it holds for $\bar{s}$. Then

$$V_{\mathrm{st}}^{\bar{s}}(\ldots, x_k, x_k + \delta, \ldots) = \prod_{0 \leq i < j \leq m} (x_j - x_i)^{s_i s_j} \prod_{0 \leq i \leq k} (x_k + \delta - x_i)^{s_i} \prod_{k < j \leq m} (x_j - (x_k + \delta))^{s_j}$$

$$= \delta^{s_k} \prod_{0 \leq i < j \leq m} (x_j - x_i)^{s_i s_j} \prod_{0 \leq i < k} (x_k + \delta - x_i)^{s_i} \prod_{k < j \leq m} (x_j - (x_k + \delta))^{s_j}$$

Therefore, by Identity (1),

$$V_{\mathbf{st}}^{\hat{\mathbf{s}}}(x_0,\dots,x_m) = \prod_{0\le i<j\le m}(x_j-x_i)^{s_i s_j}\prod_{0\le i<k}(x_k-x_i)^{s_i}\prod_{k<j\le m}(x_j-x_k)^{s_j}$$

$$= \prod_{0\le i<j\le m;\, i,j\ne k}(x_j-x_i)^{s_i s_j}\prod_{0\le i<k}(x_k-x_i)^{s_i(s_k+1)}\prod_{k<j\le m}(x_j-x_k)^{s_j(s_k+1)},$$

proving that it holds for $\hat{\mathbf{s}}$.

(b) Assume it holds for $\bar{\mathbf{s}}$. Then, by Identity (1) and the inductive hypothesis, we get

$$V_{\boldsymbol{\alpha}}^{\hat{\mathbf{s}}}(x_0,\dots,x_m) = \left.\frac{V_{\mathbf{st}}^{\bar{\mathbf{s}}}(\dots,x_k,x_k+\delta,\dots)P_{\boldsymbol{\alpha}}^{\bar{\mathbf{s}}}(\dots,x_k,x_k+\delta,\dots)}{\delta^{s_k}}\right|_{\delta=0}$$

which by the previous item and Identity (1) again gives

$$V_{\boldsymbol{\alpha}}^{\hat{\mathbf{s}}}(x_0,\dots,x_m) = V_{\mathbf{st}}^{\hat{\mathbf{s}}}(x_0,\dots,x_m)P_{\boldsymbol{\alpha}}^{\bar{\mathbf{s}}}(x_0,\dots,x_k,x_k,\dots,x_m).$$

We conclude by setting $P_{\boldsymbol{\alpha}}^{\hat{\mathbf{s}}}(x_0,\dots,x_m) = P_{\boldsymbol{\alpha}}^{\bar{\mathbf{s}}}(x_0,\dots,x_k,x_k,\dots,x_m)$, which belongs to $\mathbb{Z}[x_0,\dots,x_m]$ since $P_{\boldsymbol{\alpha}}^{\bar{\mathbf{s}}}$ has integer coefficients.

(c) The proof of item **(b)** shows that the polynomials $P_{\boldsymbol{\alpha}}^{\mathbf{s}}$ are homogeneous and of the same degree, independent from $\mathbf{s}$, than the polynomial $P_{\boldsymbol{\alpha}}$ of Proposition 2.2. We compute the degree of $V_{\mathbf{st}}^{\mathbf{s}}$ using item **(a)**:

$$\deg(V_{\mathbf{st}}^{\mathbf{s}}) = \sum_{0\le i<j\le m}s_i s_j = \frac{1}{2}\left(|\mathbf{s}|^2 - \sum_{i=0}^{m}s_i^2\right) = \frac{1}{2}\left(|\mathbf{s}|^2 - |\mathbf{s}| - \sum_{i=0}^{m}s_i(s_i-1)\right)$$

$$= \frac{t(t+1)}{2} - \frac{1}{2}\sum_{i=0}^{m}s_i(s_i-1).$$

Therefore, by **(b)**, $V_{\boldsymbol{\alpha}}^{\mathbf{s}}$ is a homogeneous polynomial and

$$\deg(V_{\boldsymbol{\alpha}}^{\mathbf{s}}) = \deg(V_{\mathbf{st}}^{\mathbf{s}}) + \deg(P_{\boldsymbol{\alpha}}^{\mathbf{s}}) = |\boldsymbol{\alpha}| - \sum_{i=0}^{m}s_i(s_i-1)/2.$$

(d) The proof of Item **(b)** also shows that if we assume that the polynomial $P_{\boldsymbol{\alpha}}^{\bar{\mathbf{s}}}$ has non-negative coefficients, then $P_{\boldsymbol{\alpha}}^{\hat{\mathbf{s}}}$ has non-negative coefficients as well. $\qquad\square$

At this point, we have all the ingredients to prove that $B_{\mathrm{m}}(t,K) \le 2t$ for ordered fields.

Proof of Theorem 1.2 (second part). Suppose that $B_m(t, K) > 2t$. Then there exists a non-zero polynomial $f = a_0 + a_1 x^{\alpha_1} + \cdots + a_t x^{\alpha_t} \in K[x]$ with strictly more than $2t$ roots counted with multiplicities. Choose, for some $m \geq 0$, $m + 1$ of these roots, different, say $r_0, \ldots, r_m$, all strictly positive or strictly negative satisfying that for some $s_i \leq \text{mult}(f; r_i)$, $s_0 + \cdots + s_m = t + 1$ holds, and set $\boldsymbol{s} = (s_0, \ldots, s_m)$. Note that since $\text{char}(K) = 0$, the equalities

$$f(r_i) = \cdots = f^{(s_i - 1)}(r_i) = 0 \quad \text{for } 0 \leq i \leq m$$

translate into the matrix identity

$$M_{\boldsymbol{\alpha}}^{\boldsymbol{s}}(r_0, \ldots, r_m) \cdot \begin{pmatrix} a_0 \\ \vdots \\ a_t \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}.$$

This is because the k-th row of $M_{\boldsymbol{\alpha}}^{s_i}(r_i)$ times $(a_0, \ldots, a_t)^t$ equals $\frac{f^{(k-1)}(r_i)}{(k-1)!}$. Since $f \neq 0$, we conclude that $V_{\boldsymbol{\alpha}}^{\boldsymbol{s}}(r_0, \ldots, r_m) = 0$. However, by Proposition 2.4(**d**),

$$V_{\boldsymbol{\alpha}}^{\boldsymbol{s}}(r_0, \ldots, r_m) = V_{\text{st}}^{\boldsymbol{s}}(r_0, \ldots, r_m) \, P_{\boldsymbol{\alpha}}^{\boldsymbol{s}}(r_0, \ldots, r_m) \neq 0$$

since $V_{\text{st}}^{\boldsymbol{s}}(r_0, \ldots, r_m) \neq 0$ and $P_{\boldsymbol{\alpha}}^{\boldsymbol{s}}(r_0, \ldots, r_m)$ is strictly positive or negative according to the sign of the r_i's. Contradiction! $\quad\square$

Note that the proof of Proposition 2.4(**b**) shows inductively that

$$P_{\boldsymbol{\alpha}}^{\boldsymbol{s}}(x_0, \ldots, x_m) = P_{\boldsymbol{\alpha}}(\underbrace{x_0, \ldots, x_0}_{s_0}, \underbrace{x_1, \ldots, x_1}_{s_1}, \ldots, \underbrace{x_m, \ldots, x_m}_{s_m}). \qquad (2)$$

This observation is useful for the proof of next result, which will be used in Section 3.

Lemma 2.5. *Let* $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_t)$ *with* $0 < \alpha_1 < \cdots < \alpha_t$ *and let* $\boldsymbol{s} = (s_0, \ldots, s_m) \in \mathbb{N}^{m+1}$. *Then*

$$P_{\boldsymbol{\alpha}}^{\boldsymbol{s}}(1 + x_0, \ldots, 1 + x_m) = \sum_{1 \leq \beta_1 < \cdots < \beta_t} \det \begin{pmatrix} \binom{\alpha_1}{\beta_1} & \cdots & \binom{\alpha_1}{\beta_t} \\ \vdots & & \vdots \\ \binom{\alpha_t}{\beta_1} & \cdots & \binom{\alpha_t}{\beta_t} \end{pmatrix} P_{\boldsymbol{\beta}}^{\boldsymbol{s}}(x_0, \ldots, x_m)$$

where $\boldsymbol{\beta} = (\beta_1, \ldots, \beta_t)$. *The same formula holds when replacing* P *by* V.

Proof. First we prove the identity for $V_{\boldsymbol{\alpha}}$.

$$V_{\boldsymbol{\alpha}}(1+x_0,\ldots,1+x_t) = \det \begin{pmatrix} 1 & (1+x_0)^{\alpha_1} & \cdots & (1+x_0)^{\alpha_t} \\ 1 & (1+x_1)^{\alpha_1} & \cdots & (1+x_1)^{\alpha_t} \\ \vdots & \vdots & & \vdots \\ 1 & (1+x_t)^{\alpha_1} & \cdots & (1+x_t)^{\alpha_t} \end{pmatrix}$$

$$= \det \begin{pmatrix} 1 & \sum_{\beta_1\geq 0}\binom{\alpha_1}{\beta_1}x_0^{\beta_1} & \cdots & \sum_{\beta_t\geq 0}\binom{\alpha_t}{\beta_t}x_0^{\beta_t} \\ 1 & \sum_{\beta_1\geq 0}\binom{\alpha_1}{\beta_1}x_1^{\beta_1} & \cdots & \sum_{\beta_t\geq 0}\binom{\alpha_t}{\beta_t}x_1^{\beta_t} \\ \vdots & \vdots & & \vdots \\ 1 & \sum_{\beta_1\geq 0}\binom{\alpha_1}{\beta_1}x_t^{\beta_1} & \cdots & \sum_{\beta_t\geq 0}\binom{\alpha_t}{\beta_t}x_t^{\beta_t} \end{pmatrix}$$

$$= \sum_{\beta_1,\ldots,\beta_t\geq 1} \binom{\alpha_1}{\beta_1}\cdots\binom{\alpha_t}{\beta_t} \det \begin{pmatrix} 1 & x_0^{\beta_1} & \cdots & x_0^{\beta_t} \\ 1 & x_1^{\beta_1} & \cdots & x_1^{\beta_t} \\ \vdots & \vdots & & \vdots \\ 1 & x_t^{\beta_1} & \cdots & x_t^{\beta_t} \end{pmatrix}$$

Reducing our sum to $\beta_1,\ldots,\beta_t$ pairwise different, and using the definition of determinant in the last line, we get

$$V_{\boldsymbol{\alpha}}(1+x_0,\ldots,1+x_t) =$$

$$= \sum_{\substack{1\leq\beta_1<\cdots<\beta_t \\ \sigma\in\mathrm{Perm}\{1,\ldots,t\}}} \binom{\alpha_1}{\beta_{\sigma(1)}}\cdots\binom{\alpha_t}{\beta_{\sigma(t)}} \det \begin{pmatrix} 1 & x_0^{\beta_{\sigma(1)}} & \cdots & x_0^{\beta_{\sigma(t)}} \\ 1 & x_1^{\beta_{\sigma(1)}} & \cdots & x_1^{\beta_{\sigma(t)}} \\ \vdots & \vdots & & \vdots \\ 1 & x_t^{\beta_{\sigma(1)}} & \cdots & x_t^{\beta_{\sigma(t)}} \end{pmatrix}$$

$$= \sum_{\substack{1\leq\beta_1<\cdots<\beta_t \\ \sigma\in\mathrm{Perm}\{1,\ldots,t\}}} (-1)^{|\sigma|}\binom{\alpha_1}{\beta_{\sigma(1)}}\cdots\binom{\alpha_t}{\beta_{\sigma(t)}} \det \begin{pmatrix} 1 & x_0^{\beta_1} & \cdots & x_0^{\beta_t} \\ 1 & x_1^{\beta_1} & \cdots & x_1^{\beta_t} \\ \vdots & \vdots & & \vdots \\ 1 & x_t^{\beta_1} & \cdots & x_t^{\beta_t} \end{pmatrix}$$

$$= \sum_{1\leq\beta_1<\cdots<\beta_t} \det \begin{pmatrix} \binom{\alpha_1}{\beta_1} & \cdots & \binom{\alpha_1}{\beta_t} \\ \vdots & & \vdots \\ \binom{\alpha_t}{\beta_1} & \cdots & \binom{\alpha_t}{\beta_t} \end{pmatrix} V_{\boldsymbol{\beta}}(x_0,\ldots,x_t).$$

Now note that by Proposition 2.4(**a**),

$$V_{\mathbf{st}}^{\boldsymbol{s}}(1+x_0,\ldots,1+x_m) = V_{\mathbf{st}}^{\boldsymbol{s}}(x_0,\ldots,x_m).$$

Therefore, the identity holds for $P_{\boldsymbol{\alpha}}$ by Proposition 2.2(**b**). Next, Identity (2) implies that the identity holds for $P_{\boldsymbol{\alpha}}^{\boldsymbol{s}}$, and finally the identity for $V_{\boldsymbol{\alpha}}^{\boldsymbol{s}}$ follows from Proposition 2.4(**b**). $\qquad\square$

Lemma 2.5 motivates the need of working with determinants of matrices whose terms are binomial coefficients. The following notation and results show that they share many properties with the generalized Vandermonde determinants.

Notation 2.6. *Let $\boldsymbol{\beta} = (\beta_1, \ldots, \beta_t) \in \mathbb{Z}_{\geq 0}^t$. We set*

$$W_{\boldsymbol{\beta}}(x_1, \ldots, x_t) = \det \begin{pmatrix} \binom{x_1}{\beta_1} & \cdots & \binom{x_1}{\beta_t} \\ \vdots & & \vdots \\ \binom{x_t}{\beta_1} & \cdots & \binom{x_t}{\beta_t} \end{pmatrix} \in \mathbb{Q}[x_1, \ldots, x_t]$$

where $\binom{x}{\beta} = x(x-1)\cdots(x-\beta+1)/\beta!$.

Lemma 2.7. *Let $1 \leq \beta_1 < \cdots < \beta_t$ and let $\mathbf{st} = (1, 2, \ldots, t)$. Then*

(a) $\beta_1! \cdots \beta_t! \, W_{\boldsymbol{\beta}}(x_1, \ldots, x_t) \in \mathbb{Z}[x_1, \ldots, x_t]$.

(b) $1!2! \cdots t! \, W_{\mathbf{st}}(x_1, \ldots, x_t) = x_1 \cdots x_t \displaystyle\prod_{1 \leq i < j \leq t} (x_j - x_i)$.

(c) $\beta_1! \cdots \beta_t! \, W_{\boldsymbol{\beta}} = 1!2! \cdots t! \, W_{\mathbf{st}} \, Q_{\boldsymbol{\beta}}$ *for some non-zero $Q_{\boldsymbol{\beta}} \in \mathbb{Z}[x_1, \ldots, x_t]$.*

(d) $\deg(W_{\boldsymbol{\beta}}) = |\boldsymbol{\beta}|$ *and* $\deg(Q_{\boldsymbol{\beta}}) = |\boldsymbol{\beta}| - t(t+1)/2$.

Proof. **(a)** Multiply the j-th column of the matrix by $\beta_j!$.

(b) We need to prove that

$$\det \begin{pmatrix} \binom{x_1}{1} & \cdots & \binom{x_1}{t} \\ \vdots & & \vdots \\ \binom{x_t}{1} & \cdots & \binom{x_t}{t} \end{pmatrix} = \frac{x_1 \cdots x_t \prod_{1 \leq i < j \leq t}(x_j - x_i)}{1!2! \cdots t!}.$$

Taking x_i as a common factor in the i-th row and $1/j!$ as a common factor in the j-th column, this determinant equals

$$\frac{x_1 \cdots x_t}{1!2! \cdots t!} \det \begin{pmatrix} 1 & x_1 - 1 & (x_1 - 1)(x_1 - 2) & \cdots & (x_1 - 1)\cdots(x_1 - t + 1) \\ 1 & x_2 - 1 & (x_2 - 1)(x_2 - 2) & \cdots & (x_2 - 1)\cdots(x_2 - t + 1) \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & x_t - 1 & (x_t - 1)(x_t - 2) & \cdots & (x_t - 1)\cdots(x_t - t + 1) \end{pmatrix}.$$

It is clear that adding the first to the second column, we get $(x_1, \ldots, x_t)^t$ in the second column. Next, adding a combination of the first and the new

second column to the third, we get $(x_1^2, \ldots, x_t^2)^t$ in the third column, etc. Therefore our determinant equals

$$\frac{x_1 \cdots x_t}{1!2! \cdots t!} \det \begin{pmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{t-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{t-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & x_t & x_t^2 & \cdots & x_t^{t-1} \end{pmatrix}$$

which shows the statement.

(c) The polynomial $W_{\boldsymbol{\beta}}(x_1, \ldots, x_t)$ is divisible by $x_1 \cdots x_t$, since setting $x_i = 0$ in the matrix that defines it yields a column of zeros. Similarly, it is divisible by the binomials $x_j - x_i$, since setting $x_i = x_j$ would produce two identical columns. Since the polynomial $\beta_1! \cdots \beta_t! W_{\boldsymbol{\beta}} \in \mathbb{Z}[x_1, \ldots, x_t]$ of item (a) is divisible by all these coprime and monic factors, the quotient $Q_{\boldsymbol{\beta}}$ has integer coefficients.

(d) Since the degree of the j-th column of the matrix defining $W_{\boldsymbol{\beta}}$ equals β_j, then $\deg(W_{\boldsymbol{\beta}}) \le |\boldsymbol{\beta}|$. Moreover, a simple inspection shows that the monomial $x_1^{\beta_1} \cdots x_t^{\beta_t}$ can not be canceled. This means that $\deg(W_{\boldsymbol{\beta}}) = |\boldsymbol{\beta}|$, and therefore, by item (c), we conclude $\deg(Q_{\boldsymbol{\beta}}) = |\boldsymbol{\beta}| - t(t+1)/2$. $\square$

Observation 2.8. *When $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_t) \in \mathbb{Z}_{\ge 0}^t$, then $W_{\boldsymbol{\beta}}(\boldsymbol{\alpha}) \in \mathbb{Z}$, since in this case, all the entries of the matrix defining it are integer numbers.*

3. Local fields

Throughout this section we assume that L is a local field of characteristic zero with respect to the non-archimedean valuation $v : L \to \mathbb{R} \cup \{\infty\}$. The ring of integers $A = \{x \in L : v(x) \ge 0\}$ is a local ring with maximal ideal $\mathfrak{M} = \{x \in L : v(x) > 0\}$. The residue field of L is the quotient $K = A/\mathfrak{M}$.

Definition 3.1. *Let $t \ge 0$. We denote by $D_1(t, L)$ and $D_m(t, L)$ the supremum of the number of roots in $1 + \mathfrak{M}$, counted without/with multiplicities respectively, that can have a non-zero polynomial in $L[x]$ with at most $t + 1$ non-zero terms.*

Next example, which shows that the bound $D_1(t, L) = \infty$ can be reached, was suggested to us by the referee: take $L = \overline{\mathbb{Q}_p}$ and $f = x^{p^n} - 1$. The set of solutions of this polynomial is the cyclic group of order p^n, which is indeed contained in $1 + \mathfrak{M}$, since by Fermat's theorem, $r^{p-1} \in 1 + \mathfrak{M}$ for such a root, and $p - 1$ is prime to p.

Note that $D_1(t, L) \leq D_{\mathrm{m}}(t, L) \leq t\,D_1(t, L)$, since in characteristic zero the roots of a polynomial with $t+1$ terms can not have multiplicity greater than t.

Proposition 3.2. *Let L be a field with a valuation $v : L \to \mathbb{R} \cup \{\infty\}$, with residue field K. Then*

$$B_1(t, L) \leq t\,B_1(t, K)\,D_1(t, L) \quad and \quad B_{\mathrm{m}}(t, L) \leq t\,B_1(t, K)\,D_{\mathrm{m}}(t, L).$$

Proof. Let $f \in L[x]$ be a non-zero polynomial with at most $t + 1$ terms. The theory of Newton polygons (see [11, Prop. 3.1.1]) shows that the set $V = \{v(r) : f(r) = 0,\ r \in L^*\}$ corresponds to slopes of the segments of the Newton polygon $NP(f)$ of f and thus has at most t elements. Take $v \in V$ and let $r_0 \in L^*$ such that $v(r_0) = v$. Every root r of f with $v(r) = v$ corresponds to the root r/r_0 of $g(x) := f(x\,r_0)$ with $v(r/r_0) = 0$, with the same multiplicity.

Therefore we only need to prove that g has at most $B_1(t, K)D_1(t, L)$ (resp. $B_1(t, K)D_{\mathrm{m}}(t, L)$) roots with valuation zero counted without (resp. with) multiplicities.

By dividing g by its coefficient with minimum valuation, we can assume, without loss of generality, that $g \in A[x]$ and that not all coefficients of g belong to $\mathfrak{M}$. Let $\bar{g} \in K[x]$ be the non-zero polynomial obtained by reducing the coefficients of g modulo $\mathfrak{M}$. Then, by Definition 1.1, the set $W = \{\bar{r} \in K^* : \bar{g}(\bar{r}) = 0\} = \{\bar{r}_1, \ldots, \bar{r}_m\}$ has $m \leq B_1(t, K)$ elements, each of them represented by some $r_i \in A \setminus \mathfrak{M}$.

Each root $r \in L$ of g with valuation zero belongs to some coset $r_i + \mathfrak{M}$, and each root of g in $r_i + \mathfrak{M}$ corresponds to a root of $h_i(x) := g(x\,r_i)$ in $1 + \mathfrak{M}$. Since h_i has at most $D_1(t, L)$ (resp. $D_{\mathrm{m}}(t, L)$) roots in $1 + \mathfrak{M}$ counted without (resp. with) multiplicities, then g has at most $mD_1(t, L)$ (resp. $mD_{\mathrm{m}}(t, L)$) roots in L with valuation zero counted without (resp. with) multiplicites. $\quad\square$

Now we derive Theorem 1.3 as an immediate consequence of Lemma 3.2 above and Proposition 3.3 below.

Proposition 3.3. *Let L be a local field with a non-archimedean valuation $v : L \to \mathbb{R} \cup \{\infty\}$ such that $v(n \cdot 1_L) = 0$ for all $n \in \mathbb{Z} \setminus \{0\}$. Then $D_1(t, L) \leq D_{\mathrm{m}}(t, L) \leq t$.*

Proof. The proof goes as the proof of Theorem 1.2. Let A be the ring of integers of L and let $\mathfrak{M}$ be the maximal ideal of A. As we pointed out in the introduction, the assumption on v implies that L has characteristic zero.

Suppose that $D_m(t, L) > t$. Then there exists a non-zero polynomial $f = a_0 + a_1 x^{\alpha_1} + \cdots + a_t x^{\alpha_t} \in L[x]$ with strictly more than t roots in $1 + \mathfrak{M}$ counted with multiplicities. Choose, for some $m \geq 0$, $m + 1$ of these roots, different, say $r_0, \ldots, r_m$, satisfying that for some $s_i \leq \operatorname{mult}(f; r_i)$, $s_0 + \cdots + s_m = t + 1$ holds, and set $\boldsymbol{s} = (s_0, \ldots, s_m)$. The equalities

$$f(r_i) = \cdots = f^{(s_i - 1)}(r_i) = 0 \ \text{ for } 0 \leq i \leq m$$

translate into the matrix identity

$$M_{\boldsymbol{\alpha}}^{\boldsymbol{s}}(r_0, \ldots, r_m) \cdot \begin{pmatrix} a_0 \\ \vdots \\ a_t \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Therefore, since $f \neq 0$, we conclude that $V_{\boldsymbol{\alpha}}^{\boldsymbol{s}}(r_0, \ldots, r_m) = 0$. This implies, by Proposition 2.4(**a-b**), that $P_{\boldsymbol{\alpha}}^{\boldsymbol{s}}(r_0, \ldots, r_m) = 0$. Write $r_i = 1 + x_i$ with $x_i \in \mathfrak{M}$ for $0 \leq i \leq m$. Then, applying Lemma 2.5 and using Notation 2.6,

$$P_{\boldsymbol{\alpha}}^{\boldsymbol{s}}(1 + x_0, \ldots, 1 + x_m) = \sum_{1 \leq \beta_1 < \cdots < \beta_t} W_{\boldsymbol{\beta}}(\boldsymbol{\alpha}) \, P_{\boldsymbol{\beta}}^{\boldsymbol{s}}(x_0, \ldots, x_m).$$

Let us show that the term corresponding to $\boldsymbol{\beta} = \mathbf{st} = (1, 2, \ldots, t)$ in the right-hand side is a non-zero integer: $W_{\mathbf{st}}(\boldsymbol{\alpha}) \in \mathbb{Z}$ by Observation 2.8, and is non-zero by Proposition 2.7(**b**) since $r_i \neq r_j$; also $P_{\mathbf{st}}^{\boldsymbol{s}} = 1_L$ by definition. Therefore by assumption it has valuation zero. The remaining non-zero terms have positive valuation since in that case $W_{\boldsymbol{\beta}}(\boldsymbol{\alpha})$ is a non-zero integer number, and $P_{\boldsymbol{\beta}}^{\boldsymbol{s}}(x_0, \ldots, x_s)$ has positive valuation since $v(x_i) > 0$ and $P_{\boldsymbol{\beta}}^{\boldsymbol{s}}$ is, according to Proposition 2.4(**b-c**), a homogeneous polynomial of positive degree with integer coefficients. Therefore $v(P_{\boldsymbol{\alpha}}^{\boldsymbol{s}}(r_0, \ldots, r_s)) = 0$ which implies $P_{\boldsymbol{\alpha}}^{\boldsymbol{s}}(r_0, \ldots, r_s)$ is a unit in A, and in particular $\neq 0$. This contradicts the assumption $D_m(t, L) > t$. $\qquad \square$

Proof of Theorem 1.3.

$$\begin{aligned} B_1(t, L) &\leq t \, B_1(t, K) \, D_1(t, L) && \text{by Lemma 3.2} \\ &\leq t^2 \, B_1(t, K) && \text{by Proposition 3.3.} \end{aligned}$$

The same proof holds for $B_m(t, L)$. $\qquad \square$

Our next aim is to prove Theorem 1.4. We do it following the same lines of the proof of Theorem 1.3, i.e. proving first in Proposition 3.8 below that $D_1(t, L) \leq D_m(t, L) \leq t$ using Lemma 2.5 (which will require the

14

extra assumption $p > e + t$), and then using Proposition 3.7 below, that improves Proposition 3.2 (if we used Proposition 3.2 we would conclude that $B_1(t, L) \leq B_{\mathrm{m}}(t, L) \leq t^2(q - 1)$ instead).

In what follows, K is assumed to be a finite extension of $\mathbb{Q}_p$ for an odd prime number p, with ramification index e and residue class degree f, A is its ring of integers and $\mathfrak{M}$ its maximal ideal. The valuation $v : K \to \mathbb{R} \cup \{\infty\}$ of K extends the standard p-adic valuation v_p of $\mathbb{Q}_p$. It satisfies $v(p) = 1$ and its group of values is $v(K^\times) = \frac{1}{e}\mathbb{Z}$. The ideal $\mathfrak{M}$ of A is principal, generated by an element $\pi \in A$ with valuation $v(\pi) = 1/e$. The residue field $\mathbb{F}_q \approx A/\mathfrak{M}$ is a finite field of cardinality $q = p^f$. We finally define the "first digit" of any $x \in K^*$ to be the first digit in its expansion, i.e. corresponding to $\pi^{-ev(x)}x \ \in A/\mathfrak{M}$.

We will need the following lemma, which actual proof, simpler than our previous one, was suggested by the referee.

Lemma 3.4. *Assume that $p - 1 \nmid e$. Then 1 is the only p-th root of unity in K.*

Proof. Let ξ_p be a primitive p-root of unity. The prime p is totally ramified in $\mathbb{Q}(\xi_p)$, see e.g. [8], and therefore the extension $\mathbb{Q}_p(\xi_p)/\mathbb{Q}_p$ has degree $p-1$. If $K/\mathbb{Q}_p$ is a finite extension such that $\xi_p \in K$, we have $\mathbb{Q}_p(\xi_p) \subset K$ and by the multiplicativity of the ramification degree, $p - 1 \mid e$. $\qquad\square$

We also need Hensel's lemma in its Newton method version, see [11, Prop. 3.1.2]:

Lemma 3.5 (Newton's method)**.** *Let K be a complete field with respect to a discrete non-archimedian valuation v and let A be its valuation ring. Let $f \in A[x]$ be a non-zero polynomial and let $r_0 \in A$ be such that $v(f(r_0)) > 2v(f'(r_0))$. Then, there exists a unique $r \in A$ such that $f(r) = 0$ and $v(r - r_0) \geq v(f(r_0)) - v(f'(r_0)) > v(f'(r_0))$.*

Any $r_0 \in A$ satisfying the hypothesis of Lemma 3.5 is called an *approximate root* of f. The corresponding root $r \in A$ of f can be obtained as the limit $r = \lim_{n \to \infty} r_n$ of the sequence given by Newton's iteration $r_{n+1} = r_n - f(r_n)/f'(r_n)$. We also have that $v(f'(r)) = v(f'(r_0)) \neq \infty$ and therefore r is always a simple root of f.

Lemma 3.6. *Under the same notations of Lemma 3.5, let*

$$f = a_t x^{\alpha_t} + \cdots + a_1 x^{\alpha_1} + a_0 \in K[x] \quad with \ \ 0 < \alpha_1 < \cdots < \alpha_t.$$

Assume that $p \nmid \alpha_{i+1} - \alpha_i$ for some i, $0 \leq i \leq t-1$, and that the segment defined by $(\alpha_i, v(a_i))$ and $(\alpha_{i+1}, v(a_{i+1}))$ is one of the segments of the Newton polygon $NP(f)$ of f. Let $-m_i := (v(a_{i+1}) - v(a_i))/(\alpha_{i+1} - \alpha_i)$ denote its slope. Then, the roots of f in K^* that have valuation m_i are all simple and are in one-to-one correspondence with the roots of the binomial

$$g_i = a_i x^{\alpha_i} + a_{i+1} x^{\alpha_{i+1}}.$$

Moreover, the number of roots of g_i in K^* equals $\gcd(q-1, \alpha_{i+1} - \alpha_i)$ when $e\, m_i \in \mathbb{Z}$ and the first digit of a_{i+1}/a_i is a $(\alpha_{i+1} - \alpha_i)$-th power in $A/\mathfrak{M}$, or zero otherwise. In particular, the number of roots of f in K^* with valuation m_i is bounded by $q-1$.

Proof. Note that any non-zero root of g_i has necessarily valuation m_i. If $e\, m_i \notin \mathbb{Z}$ then there are no elements in K^* with valuation m_i, i.e. no roots in K^* of f or g_i with valuation m_i. Let us then assume that $e\, m_i \in \mathbb{Z}$.

By making the change of variables $x \leftarrow \pi^{e m_i} x$ in f and g_i we can reduce the proof to the case $m_i = 0$, i.e. $v(a_i) = v(a_{i+1})$ and $v(a_j) > v(a_i)$ for all $j \neq i, i+1$. By dividing f by a_{i+1}, we can then reduce the proof to the case $f \in A[x]$, $a_{i+1} = 1$ and $v(a_i) = 0$. In particular if $g = a_i x^{\alpha_i} + x^{\alpha_{i+1}}$ then $f - g \in \mathfrak{M}[x]$.

In this case we will show that the roots of f with valuation zero are approximate roots of g and viceversa.

Let $r \in K^*$ be such that $f(r) = 0$ and $v(r) = 0$. Then $g(r) = f(r) - (f - g)(r) \in \mathfrak{M}$, i.e. $v(g(r)) > 0$. Besides, since $p \nmid \alpha_{i+1} - \alpha_i$, then

$$g'(r) = \underbrace{(\alpha_{i+1} - \alpha_i) r^{\alpha_{i+1}-1}}_{v(\cdot)=0} + \underbrace{\alpha_i r^{-1} g(r)}_{v(\cdot)>0}$$

has valuation zero. This means that $v(g(r)) > 2v(g'(r))$ and by Lemma 3.5, r is an approximate root of g.

Now let $r \in K^*$ be such that $g(r) = 0$, i.e. $r^{\alpha_{i+1}-\alpha_i} = -a_i$ and therefore, since $v(a_i) = 0$, $v(r) = 0$. Therefore, like above, $v(g'(r)) = 0$. Also $f(r) = (f - g)(r) + g(r)$ implies $f(r) \in \mathfrak{M}$, i.e. $v(f(r)) > 0$. Besides,

$$f'(r) = \underbrace{(f - g)'(r)}_{v(\cdot)>0} + \underbrace{g'(r)}_{v(\cdot)=0}$$

has valuation zero. Therefore r is an approximate root of f. This shows that there are the same number of roots, that are all simple.

16

If the first digit of a_i is not an $(\alpha_{i+1} - \alpha_i)$-th power in $A/\mathfrak{M}$, then clearly the binomial $g(x)$ has no roots (not even modulo $\mathfrak{M}$). When it is a power, then the number of roots of g modulo $\mathfrak{M}$ is exactly $\gcd(q - 1, \alpha_{i+1} - \alpha_i)$ since there are exactly that many $(\alpha_{i+1} - \alpha_i)$-th roots of unity in $\mathbb{F}_q$ (the multiplicative group $\mathbb{F}_q^\times$ is cyclic with $q - 1$ elements). Since $p \nmid \alpha_{i+1} - \alpha_i$, each of these roots lifts via Hensel lemma to a unique root of g in K^*. $\qquad\square$

Proposition 3.7. *Let p be an odd prime number and let K be a finite extension of $\mathbb{Q}_p$ with ramification index e and residue class degree f, such that $p - 1 > e$, and set $q = p^f$. Then*

$$B_1(t, K) \leq \big((t - 1)D_1(t, K) + 1\big)(q - 1) \quad and$$
$$B_\mathrm{m}(t, K) \leq \big((t - 1)D_\mathrm{m}(t, K) + 1\big)(q - 1).$$

Proof. We proceed as in the proof of Proposition 3.2, grouping the roots by valuation and by first digit. Let $f = a_0 + a_1 x^{\alpha_1} + \cdots + a_t x^{\alpha_t} \in K[x]$, with $0 =: \alpha_0 < \alpha_1 < \cdots < \alpha_t$, be a non-zero polynomial with at most $t + 1$ monomials. The Newton polygon $NP(f)$ of f has at most t segments.

If the number of segments is bounded by $t - 1$, then we immediately get the bounds

$$B_1(t, K) \leq (t - 1)D_1(t, K)(q - 1) \quad \text{and} \quad B_\mathrm{m}(t, K) \leq (t - 1)D_\mathrm{m}(t, K)(q - 1),$$

since $B_1(t, \mathbb{F}_q) \leq q - 1$, which are stronger than the bounds that we have to show.

Therefore we can assume that $NP(f)$ has exactly t segments. In particular, $NP(f)$ consists of the segments $(\alpha_i, v(a_i)) - (\alpha_{i+1}, v(a_{i+1}))$ for $0 \leq i \leq t - 1$. If $p \mid \alpha_{i+1} - \alpha_i$ for $0 \leq i \leq t - 1$ then $p \mid \alpha_i$ for $1 \leq i \leq t$ and therefore $f(x) = g(x^p)$ where $g = a_0 + a_1 x^{\alpha_1/p} + \cdots + a_t x^{\alpha_t/p}$. The roots of f are the p-th roots of the roots of g. Since by Lemma 3.4 there is only one p-th root of unity in K, each root of g gives at most one root of f, with the same multiplicities.

Hence we can reduce to the case where at least one of the segments of $NP(f)$ satisfies $p \nmid \alpha_{i+1} - \alpha_i$.

In this case Lemma 3.6 implies that there are at most $(q - 1)$ roots of f in K^* with the valuation associated to this segment, necessarily simple. For the valuations corresponding to the remaining $t - 1$ segments, we have at most $(t - 1)D_1(t, K)(q - 1)$ and $(t - 1)D_\mathrm{m}(t, K)(q - 1)$ roots of f counted without/with multiplicities. This concludes the proof. $\qquad\square$

As a consequence of Proposition 3.7, we get the sharp bound $B_1(1, K) = q-1$ for any finite extension $K/\mathbb{Q}_p$ with p odd and residue field of q elements. The lower bound is attained by the polynomial $x^{q-1} - 1 \in K[x]$.

Proposition 2.7 allows us to prove the last result needed in the proof of Theorem 1.4.

Proposition 3.8. *Let $K/\mathbb{Q}_p$ be a finite extension with ramification index e and residue class degree f. Assume that $p > e + t$. Then*

$$D_1(t, K) \leq D_{\mathrm{m}}(t, K) \leq t.$$

Proof. As in the proof of Proposition 3.3, it is enough to show that given $\boldsymbol{\alpha}$ and $\boldsymbol{s}$ s.t. $|\boldsymbol{s}| = t+1$, $P_{\boldsymbol{\alpha}}^{\boldsymbol{s}}(r_0, \ldots, r_m) \neq 0$ for any distinct $r_0, \ldots, r_m \in 1 + \mathfrak{M}$. Write $r_i = 1 + x_i$ with $x_i \in \mathfrak{M}$ for $0 \leq i \leq m$, then by Lemma 2.5 and using Notation 2.6,

$$P_{\boldsymbol{\alpha}}^{\boldsymbol{s}}(1 + x_0, \ldots, 1 + x_m) = \sum_{1 \leq \beta_1 < \cdots < \beta_t} W_{\boldsymbol{\beta}}(\boldsymbol{\alpha}) \, P_{\boldsymbol{\beta}}^{\boldsymbol{s}}(x_0, \ldots, x_m).$$

The term of the right-hand side corresponding to $\boldsymbol{\beta} = \mathbf{st} = (1, \ldots, t)$ is equal to $W_{\mathbf{st}}(\boldsymbol{\alpha})$, since $P_{\mathbf{st}}^{\boldsymbol{s}} = 1$, and is a non-zero integer number by Lemma 2.7**(b)** and Observation 2.8.

We show that the remaining non-zero terms for $\boldsymbol{\beta} \neq \mathbf{st}$ have valuation strictly greater than $v(W_{\mathbf{st}}(\boldsymbol{\alpha}))$: By Lemma 2.7**(c)**, their ratio satisfies

$$\frac{W_{\boldsymbol{\beta}}(\boldsymbol{\alpha}) \, P_{\boldsymbol{\beta}}^{\boldsymbol{s}}(x_0, \ldots, x_m)}{W_{\mathbf{st}}(\boldsymbol{\alpha})} = \frac{1! 2! \cdots t!}{\beta_1! \cdots \beta_t!} \, Q_{\boldsymbol{\beta}}(\boldsymbol{\alpha}) \, P_{\boldsymbol{\beta}}^{\boldsymbol{s}}(x_0, \ldots, x_m),$$

where $Q_{\boldsymbol{\beta}}(\boldsymbol{\alpha}) \in \mathbb{Z} \setminus \{0\}$. Since $P_{\boldsymbol{\beta}}^{\boldsymbol{s}}$ is homogeneous of degree $|\boldsymbol{\beta}| - t(t+1)/2$ and $v(x_i) \geq 1/e$ for $0 \leq i \leq s$, then

$$v\left(\frac{W_{\boldsymbol{\beta}}(\boldsymbol{\alpha}) \, P_{\boldsymbol{\beta}}^{\boldsymbol{s}}(x_0, \ldots, x_m)}{W_{\mathbf{st}}(\boldsymbol{\alpha})}\right) \geq \frac{|\boldsymbol{\beta}| - t(t+1)/2}{e} + v_p(1! 2! \cdots t!) - v_p(\beta_1! \cdots \beta_t!).$$

Our assumption $p > e + t$ implies that $v_p(1! 2! \cdots t!) = 0$, so we can write

$$v\left(\frac{W_{\boldsymbol{\beta}}(\boldsymbol{\alpha}) \, P_{\boldsymbol{\beta}}^{\boldsymbol{s}}(x_0, \ldots, x_m)}{W_{\mathbf{st}}(\boldsymbol{\alpha})}\right) \geq \frac{1}{e} \sum_{i=1}^{t} \left(\beta_i - i - e v_p(\beta_i!)\right).$$

Since $1 \leq \beta_1 < \cdots < \beta_t$ with $\boldsymbol{\beta} \neq \mathbf{st}$, then $\beta_i \geq i$ for $1 \leq i \leq t$ and there exists j s.t. $\beta_j > j$. We consider three cases:

18

- if $\beta_i < p$, then $\beta_i - i - ev_p(\beta_i!) = \beta_i - i \geq 0$.

- if $p \leq \beta_i < 2p$, then $\beta_i - i - ev_p(\beta_i!) \geq \beta_i - i - e \geq p - t - e > 0$.

- if $\beta_i \geq 2p$, then $\beta_i - i - ev_p(\beta_i!) \geq \beta_i - i - \frac{e\beta_i}{p-1} \geq 2p(1 - \frac{e}{p-1}) - t > 2(p - 1 - e) - t \geq t > 0$.

In all the cases we have $\beta_i - i - ev_p(\beta_i!) \geq 0$. Moreover, when $\beta_j > j$, then $\beta_j - j - ev_p(\beta_j!) > 0$. This proves that

$$v\left(W_{\boldsymbol{\beta}}(\boldsymbol{\alpha})\, P_{\boldsymbol{\beta}}^{\boldsymbol{s}}(x_0, \ldots, x_m)\right) - v\left(W_{\mathbf{st}}(\boldsymbol{\alpha})\right) > 0$$

for any $\boldsymbol{\beta} \neq \mathbf{st}$. In particular, $v\left(P_{\boldsymbol{\alpha}}^{\boldsymbol{s}}(r_0, \ldots, r_m)\right) = v\left(W_{\mathbf{st}}(\boldsymbol{\alpha})\right)$ which implies that $P_{\boldsymbol{\alpha}}^{\boldsymbol{s}}(r_0, \ldots, r_m) \neq 0$ as desired. $\qquad\square$

Proof of Theorem 1.4.

$$\begin{aligned}
B_{\mathrm{m}}(t, K) &\leq \left((t-1)D_{\mathrm{m}}(t, K) + 1\right)(q - 1) && \text{by Proposition 3.7} \\
&\leq \left((t-1)t + 1\right)(q - 1) && \text{by Proposition 3.8}
\end{aligned}$$

$\qquad\square$

In [7], H.W. Lenstra introduced another technique to produce upper bounds for $D_{\mathrm{m}}(t, L)$. For two non-negative integers t and m, he defines $d_t(m)$ to be the least common multiple of all integers that can be written as the product of at most t pairwise distinct positive integers that are at most m. Also for any prime p, for any integer $t \geq 1$, and for any real number $r > 0$, he defines

$$C(p, t, r) = \max\left\{m \in \mathbb{Z}_{\geq 0} \,:\, mr - v_p(d_t(m)) \leq \max_{0 \leq i \leq t}\{ir - v_p(i!)\}\right\}.$$

In [7, Thm. 3] he proves that $D_{\mathrm{m}}(t, K) \leq C(p, t, 1/e)$. Next lemma shows that under the assumption $p > t + e$, we have $C(p, t, 1/e) = t$, therefore providing an alternative proof of Proposition 3.8.

Lemma 3.9. *Let p be a prime number and let t and e be positive integers. Assume that $p > t + e$. Then $C(p, t, 1/e) = t$.*

Proof. Observe that $d_t(t) = t!$, and then $C(p, t, 1/e) \geq t$ by definition. For the other inequality, we only have to show that for any $m > t$ and for any $i \leq t$, $m/e - v_p(d_t(m)) > i/e - v_p(i!)$ holds. By our assumption on p, we clearly have $v_p(i!) = 0$. Moreover, by considering the same three cases analyzed during the proof of Proposition 3.8, we have $m - i > ev_p(m!)$. This concludes the proof, since $v_p(m!) \geq v_p(d_t(m))$. $\qquad\square$

4. Lower bounds

Proof of Example 1.5. Note first that 1 is a double root, since $f(1) = f'(1) = 0$ and $f''(1) = (q-1)^2(1+q^{q-1})q^{q-1} \neq 0$. Also q is an approximate root of f, since

$$f(q) = q^{2(q-1)}\left(q^{(q-1)(q^{q-1}-1)} - 1\right) \quad \Rightarrow \quad v(f(q)) = 2(q-1)f_K$$

and also,

$$f'(q) = (q-1)(1+q^{q-1})q^{q-2}\left(q^{(q-1)q^{q-1}} - 1\right) \quad \Rightarrow \quad v(f'(q)) = (q-2)f_K.$$

Then $v(f(q)) > 2v(f'(q))$. Newton's method (Lemma 3.5) gives an exact root $r \in K$ of f such that $v(r-q) > v(f'(q)) = (q-2)f_K \geq f_K = v(q)$. This implies that $v(r) = v(q) = f_K$, and in particular $r \neq 1$. Note also that if $x \in K$ is a root of f and $\xi \in K$ is a $(q-1)$-root of the unity (i.e. $\xi^{q-1} = 1$), then $f(x\xi) = 0$, and similarly, if $f'(x) = 0$ then $f'(x\xi) = 0$. Since there are exactly $q-1$ different $(q-1)$-roots of unity $\xi_1, \ldots, \xi_{q-1} \in K$, the polynomial f has ξ_i as a double root and $r\xi_i$ as a simple root for $1 \leq i \leq q-1$. This gives at least $3(q-1)$ roots counted with multiplicities. $\qquad\square$

Proof of Theorem 1.6. Let A be the ring of integers of K and let $\mathfrak{M}$ be the maximal ideal of A. We proceed by induction in t, proving a much stronger statement: for any $t \geq 1$, there exists a polynomial f_t, such that

1. $f_t \in \mathbb{Z}_p[x]$,
2. f_t is monic and it has non-zero constant term,
3. f_t has $t+1$ terms,
4. f_t has all exponents divisible by $q-1$,
5. f_t has one simple root in $p^{t-1}(1+p\mathbb{Z}_p)$,
6. f_t has two simple roots in each $p^i(1+p\mathbb{Z}_p)$ for $0 \leq i < t-1$ if $t > 1$,
7. f_t has non-zero discriminant.

By multiplying each of the roots of f_t by the $(q-1)$-th roots of the unity in K, we obtain at least $(2t-1)(q-1)$ simple roots for f_t in K^*. Items 3, 5 and 6 imply that the polynomial f_t has a Newton polygon with exactly t segments (with slopes $0, -1, -2, \ldots, -t+1$), and therefore all its roots (even the ones in $\overline{K}$) have necessarily valuation $0, 1, \ldots, t-1$.

The polynomial $f_1 = x^{q-1} - 1$ proves the case $t = 1$. Now assume that $f_t = x^{\alpha_t} + a_{t-1}x^{\alpha_{t-1}} + \cdots + a_1 x^{\alpha_1} + a_0 \in \mathbb{Z}_p[x]$ satisfies Conditions 1-7. Since f_t is monic with coefficients in $\mathbb{Z}_p$, all its roots in K belong to A,

and in particular $f_t(1/p) \neq 0$. Furthermore $f_t(1/p) \in p^{-\alpha_t}(1 + p\mathbb{Z}_p)$, and therefore

$$\hat{f}_t(x) := \frac{f_t(x/p)}{f_t(1/p)} \;=\; \frac{p^{\alpha_t} f_t(x/p)}{p^{\alpha_t} f_t(1/p)} \;=\; u^{-1} h(x)$$

where

$$h(x) := x^{\alpha_t} + a_{t-1} p^{\alpha_t - \alpha_{t-1}} x^{\alpha_{t-1}} + \cdots + a_0 p^{\alpha_t} \;\in\; \mathbb{Z}_p[x], \qquad (3)$$
$$u := 1 + a_{t-1} p^{\alpha_t - \alpha_{t-1}} + \cdots + a_0 p^{\alpha_t} \;\in\; 1 + p\mathbb{Z}_p.$$

Therefore $\hat{f}_t(x) \in \mathbb{Z}_p[x]$ and we define

$$g_\alpha(x) := x^\alpha - \hat{f}_t(x) \in \mathbb{Z}_p[x]$$

for $\alpha > \alpha_t$. We show that, for suitable $\alpha > \alpha_t$ and $\varepsilon \in \mathbb{Z}_p$, the polynomial $f_{t+1}(x) = g_\alpha(x) + \varepsilon$ satisfies Conditions 1–7 for $t + 1$:

Since $\hat{f}_t(0) \neq 0$, then g_α satisfies Conditions 1–3 for any $\alpha > \alpha_t$. In addition $g_\alpha(1) = 0$ by construction.

We remark that since f_t and g_α are monic in $\mathbb{Z}_p[x]$, then all their roots in $\mathbb{Q}_p$ belong to $\mathbb{Z}_p$. Define $\gamma_t = \max\{v(f_t'(r)) : r \in \mathbb{Z}_p, \, f_t(r) = 0\}$. Note that $\gamma_t \neq \infty$ because f_t has non-zero discriminant.

Assume $\alpha \geq 2(\gamma_t + \alpha_t)$. We prove first that if $r_0 \in \mathbb{Z}_p$ is a root of f_t, then $p\,r_0$ is an approximate root of g_α, which induces a root $r \in \mathbb{Z}_p$ of g_α with $v(r) = v(r_0) + 1$:

The condition $f_t(r_0) = 0$ implies

$$g_\alpha(p\,r_0) = p^\alpha r_0^\alpha \quad \text{and} \quad g_\alpha'(p\,r_0) = \alpha p^{\alpha-1} r_0^{\alpha-1} - f_t'(r_0)/(p f_t(1/p)).$$

Since $v(\alpha p^{\alpha-1} r_0^{\alpha-1}) \geq \alpha - 1$ and $v(f_t'(r_0)/(p f_t(1/p))) \leq \gamma_t + \alpha_t - 1 < \alpha/2$, then $v(g_\alpha'(p\,r_0)) < \alpha/2 \leq v(g_\alpha(p\,r_0))/2$, Lemma 3.5 implies that $p\,r_0$ is an approximate root of g_α, corresponding to a root $r \in \mathbb{Z}_p$. Moreover, $v(r - p\,r_0) > \alpha/2$, which implies $v(r - p\,r_0) > \alpha_t \geq t \geq v(p\,r_0)$ by the observation after Conditions 1–7, and in particular $v(r) = v(p\,r_0) = v(r_0) + 1$. Therefore each root $r_0 \in p^i(1 + p\mathbb{Z}_p)$ for $0 \leq i \leq t - 1$ satisfying Conditions 5 or 6 of f_t induces a simple root $r \in p^{i+1}(1 + p\mathbb{Z}_p)$ of g_α. We still need to show these are all different.

Define $\gamma_t' = 1 + \max\{v(r_0 - r_0') : r_0, r_0' \in \mathbb{Z}_p, \, f_t(r_0) = f_t(r_0') = 0 \text{ and } r_0 \neq r_0'\}$ and assume that $\alpha \geq \max\{2(\gamma_t + \alpha_t), 2\gamma_t'\}$. Then two different roots $r_0 \neq r_0'$ of f_t in $\mathbb{Z}_p$ induce different roots $r \neq r'$ of g_α in $\mathbb{Z}_p$, since if $r = r'$ then

$$1 + v(r_0 - r_0') = v(p\,r_0 - p\,r_0') \geq \min\{v(r - p\,r_0), v(r' - p\,r_0')\} > \alpha/2 \geq \gamma_t',$$

21

in contradiction with the definition of γ'_t.

Therefore, we proved so far that for $\alpha > 2(\alpha_t + \gamma_t + \gamma'_t)$, g_α has at least one simple root in $p^t(1 + p\mathbb{Z}_p)$, two simple roots in each $p^i(1 + p\mathbb{Z}_p)$ for $1 \leq i < t$ and the root $1 \in 1 + p\mathbb{Z}_p$.

Our aim now is to produce an extra root. We construct such a root in $1 + p\mathbb{Z}_p$ but different from 1 following the following strategy. We start with a fixed r_0 congruent to 1 modulo p but not congruent to 1 modulo p^2, and show that we can guarantee the existence of some α such that the conditions of Lemma 3.5 are satisfied for r_0 and g_α. In order to achieve this, we construct a sequence of exponents $\alpha^{(i)}$ such that the order of r_0 as a root increases.

Fact 1 below shows that there exists r_0 with the required conditions such that $\big(v(g'_{\alpha^{(i)}}(r_0))\big)$ is bounded. Assuming this holds, we can pick a large enough $i \gg 1$ such that $g = g_{\alpha^{(i)}}$ satisfies Conditions 1–6 in our list for $t + 1$. Let $r_1, \ldots, r_{2t+1} \in \mathbb{Z}_p$ be the $2t + 1$ simple roots of g of Conditions 5 and 6 and set $C := 2 \max\{t, v(g'(r_j)), 1 \leq j \leq 2t + 1\}$.

We will define $f_{t+1}(x) := g(x) + \varepsilon$ for some $\varepsilon \in \mathbb{Z}_p$ so that f_{t+1} satisfies Conditons 1–7 for $t + 1$. By Lemma 3.5, if $v(\varepsilon) > C$, then $v(f_{t+1}(r_j)) = v(\varepsilon) > 2v(f'_{t+1}(r_j))$ for any j. Therefore the roots $r_1, \ldots, r_{2t+1}$ are approximate roots of f_{t+1}, with corresponding induced roots $\hat{r}_1, \ldots, \hat{r}_{2t+1} \in \mathbb{Z}_p$ that are all different and satisfy

$$v(\hat{r}_j - r_j) \geq v(\varepsilon) - v(f'_{t+1}(r_j)) > C/2 \geq t \geq v(r_j),$$

which implies $v(\hat{r}_j) = v(r_j)$. Also, if $v(\varepsilon) > v(g(0))$, then f_{t+1} has a non-zero constant term. Finally, the discriminant of f_{t+1} is a polynomial in ε of positive degree, and therefore vanishes at finitely many values of ε. We conclude by selecting ε with $v(\varepsilon) > \max\{C, v(g(0))\}$ such that f_{t+1} has non-zero discriminant. This polynomial f_{t+1} satisfies Conditions 1–7.

The rest of the proof focuses now on guaranteeing the existence of such an r_0 and such a sequence $(\alpha^{(i)})_i$. Let r_0 be any element of $1 + p\mathbb{Z}_p$ such that $r_0 \not\equiv 1 \pmod{p^2}$. Therefore $p^2 \nmid r_0^{p-1} - 1$ and $\hat{f}_t(r_0) \in 1 + p\mathbb{Z}_p$. Lemma 4.1 below implies there exists a sequence of integers $(\alpha^{(i)})_{i \geq 1}$ satisfying for all i:

- $\alpha^{(1)} \equiv 0 \pmod{\varphi(p)}$ and $\alpha^{(i+1)} \equiv \alpha^{(i)} \pmod{\varphi(p^i)}$,

- $r_0^{\alpha^{(i)}} \equiv \hat{f}_t(r_0) \pmod{p^i}$, i.e. $g_{\alpha^{(i)}}(r_0) \equiv 0 \pmod{p^i}$,

- $q - 1 \mid \alpha^{(i)}$ and $\alpha^{(i)} \geq 2(\alpha_t + \gamma_t + \gamma'_t)$.

Since $p^i \mid g_{\alpha^{(i)}}(r_0)$, then $v(g_{\alpha^{(i)}}(r_0)) \geq i$ for all $i \in \mathbb{N}$. By Fact 1 at the end of this proof, there exists some $r_0 \in 1 + p\mathbb{Z}_p$ with $p^2 \nmid r_0^{p-1} - 1$ such that

the sequence $\big(v(g'_{\alpha^{(i)}}(r_0))\big)_{i\geq 1}$ is bounded. Therefore, fixing $\alpha^{(i)}$ big enough, the hypotheses of Lemma 3.5 are satisfied, and r_0 is an approximate root of $g_{\alpha^{(i)}}$ inducing a root $r \in \mathbb{Z}_p$ with $v(r - r_0) > v(g'_{\alpha^{(i)}}(r_0))$.

Now for $i \geq 2$, since $r_0 \equiv 1 \pmod p$ and by Fact 2 below, $\alpha^{(i)} \equiv \alpha_t \pmod p$, we have

$$g'_{\alpha^{(i)}}(r_0) \equiv g'_{\alpha^{(i)}}(1) \equiv \alpha^{(i)} - \alpha_t \equiv 0 \pmod p, \quad \text{i.e.} \quad v\big(g'_{\alpha^{(i)}}(r_0)\big) \geq 1,$$

and therefore $v(r - r_0) > 1$, which implies $r = (r - r_0) + r_0 \in 1 + p\mathbb{Z}_p$ and $r \equiv r_0 \not\equiv 1 \pmod{p^2}$. In particular $r_0 \neq 1$ is a second simple root of $g_{\alpha^{(i)}}$ in $1 + p\mathbb{Z}_p$.

Fact 1. The sequence $\big(v(g'_{\alpha^{(i)}}(r_0))\big)_{i\geq 1}$ is bounded for some $r_0 \in 1 + p\mathbb{Z}_p$ such that $p^2 \nmid r_0^{p-1} - 1$.

Proof of Fact 1. Assume it is not for any r_0 satisfying the hypotheses, then we can extract a subsequence $(\beta_j)_{j\geq 1}$, where $\beta_j = \beta_j(r_0)$, of $(\alpha^{(i)})_{i\geq 1}$ with $\beta_1 \equiv 0 \pmod{\varphi(p)}$ such that for all j,

$$\beta_{j+1} \equiv \beta_j \pmod{\varphi(p^j)} , \quad r_0^{\beta_j} \equiv \hat{f}_t(r_0) \pmod{p^j}$$
$$\text{and} \quad v(g'_{\beta_j}(r_0)) \geq j, \quad \text{i.e.} \quad \beta_j r_0^{\beta_j - 1} \equiv \hat{f}'_t(r_0) \pmod{p^j}$$
$$\text{or equivalently } \beta_j r_0^{\beta_j} \equiv r_0\,\hat{f}'_t(r_0) \pmod{p^j}.$$

The sequence $(\beta_j)_{j\geq 1}$ has by construction a limit β in the set

$$\mathcal{E}_p = \varprojlim \mathbb{Z}/\varphi(p^n)\mathbb{Z} \approx \mathbb{Z}/(p-1)\mathbb{Z} \oplus \mathbb{Z}_p , \quad \beta \mapsto \big(\beta_1 = 0, (\beta_j)_{j\geq 2}\big)$$

of p-adic exponents, as defined in [2, Def. 2.1].

Thus, for all $r_0 \in 1 + p\mathbb{Z}_p$ such that $p^2 \nmid r_0^{p-1} - 1$ there exists $\beta := \beta(r_0) \in \mathcal{E}_p$ such that

$$r_0^\beta = \hat{f}_t(r_0) \quad \text{and} \quad \beta\hat{f}_t(r_0) = r_0\hat{f}'_t(r_0) \quad \text{in} \quad \mathbb{Z}_p$$

where the exponential of an element of $\mathbb{Z}_p^\times$ by an element of $\mathcal{E}_p$ is defined in [2, Prop. 2.2]. Our goal is to prove that if this is the case, then $\hat{f}_t$ needs to be a monomial, that is, $\hat{f}_t = ax^\gamma$ for some $a \in \mathbb{Q}_p$ and $\gamma \in \mathbb{N}$. But clearly $\hat{f}_t$ is not a monomial by construction, giving a contradiction. Therefore this would prove Fact 1.

Given such an r_0, let us define $r_N = r_0 + p^N$ for $N \geq 2$, which satisfies the same conditions, and denote $\beta := \beta(r_0)$ and $\beta_N := \beta(r_N)$. Then

$$\beta_N \hat{f}_t(r_N) = r_N \hat{f}'_t(r_N) \;\Rightarrow\; \beta_N \hat{f}_t(r_0) \equiv r_0 \hat{f}'_t(r_0) \pmod{p^N}$$
$$\Rightarrow\; \beta_N \equiv \beta \pmod{p^N}.$$

Therefore, since $p - 1 \mid \beta$ for any β, $\beta_N \equiv \beta \pmod{\varphi(p^{N+1})}$ and we can write

$$\beta_N = \beta + \varphi(p^{N+1})\,\delta \quad \text{for some} \quad \delta \in \mathbb{Z}_p.$$

Now, Taylor expanding $\hat{f}_t(r_0 + p^N)$ around r_0 up to order p^{2N} we obtain

$$(r_0 + p^N)^{\beta + \varphi(p^{N+1})\delta} = \hat{f}_t(r_0 + p^N) \implies$$
$$r_0^\beta (1 + p^N r_0^{-1})^\beta \left(r_0^{\varphi(p^{N+1})} (1 + p^N r_0^{-1})^{\varphi(p^{N+1})} \right)^\delta \equiv \hat{f}_t(r_0) + p^N \hat{f}_t'(r_0) \pmod{p^{2N}}.$$

We write $r_0 = 1 + p\,x_0$ and therefore, since

$$r_0^{\varphi(p^{N+1})} = (1 + p\,x_0)^{(p-1)p^N} = 1 + p^{N+1} u_N(r_0)$$

for some $u_N(r_0) \in \mathbb{Z}_p$, we get

$$\hat{f}_t(r_0)(1 + p^N r_0^{-1}\beta)(1 + p^{N+1} u_N(r_0)\,\delta) \equiv \hat{f}_t(r_0) + p^N \hat{f}_t'(r_0) \pmod{p^{2N}}.$$

Substracting $\hat{f}_t(r_0)$, multiplying by r_0 and dividing by p^N gives

$$\hat{f}_t(r_0)\,\beta + p\,r_0 u_N(r_0)\hat{f}_t(r_0)\,\delta \equiv r_0 \hat{f}_t'(r_0) \pmod{p^N},$$

i.e., since $\hat{f}_t(r_0)\,\beta = r_0\hat{f}_t'(r_0)$, we obtain $r_0\,u_N(r_0)\hat{f}_t(r_0)\,\delta \equiv 0 \pmod{p^{N-1}}$. Now we observe that

$$u_N(r_0) = (r_0^{\varphi(p^{N+1})} - 1)/p^{N+1} \equiv (r_0^{p-1} - 1)/p \not\equiv 0 \pmod{p},$$

and therefore since $r_0 \equiv 1 \pmod{p}$ and $\hat{f}_t(r_0) \equiv 1 \pmod{p}$, we conclude that $\delta \equiv 0 \pmod{p^{N-1}}$, i.e. $\beta_N \equiv \beta \pmod{p^{2N-1}}$. Going back to the identity $\beta_N \hat{f}_t(r_N) = r_N \hat{f}_t'(r_N)$ and Taylor expanding now around r_0 up to order p^{2N-1} we obtain

$$\beta\,\hat{f}_t(r_0) + p^N \beta\,\hat{f}_t'(r_0) \equiv (r_0 + p^N)\hat{f}_t'(r_0) + p^N\,r_0\,\hat{f}_t''(r_0) \pmod{p^{2N-1}},$$

which simplifies to

$$(\beta - 1)\,\hat{f}_t'(r_0) \equiv r_0\,\hat{f}_t''(r_0) \pmod{p^{N-1}}, \quad \forall\, N \geq 2,$$

and therefore $(\beta - 1)\hat{f}_t'(r_0) = r_0\hat{f}_t''(r_0)$ in $\mathbb{Z}_p$.

This last identity combined with $\beta\hat{f}_t(r_0) = r_0\hat{f}_t'(r_0)$ implies the following differential equation independent from β:

$$r_0\,\hat{f}_t''(r_0)\,\hat{f}_t(r_0) + \hat{f}_t(r_0)\,\hat{f}_t'(r_0) - r_0\hat{f}_t'(r_0)^2 = 0.$$

24

Since this identity holds for infinitely many $r_0 \in \mathbb{Z}_p$, it is a polynomial identity in $\mathbb{Q}_p[x]$ that can be rewritten as

$$\left(x\, \hat{f}_t'(x)/\hat{f}_t(x) \right)' = 0.$$

This means that $x\, \hat{f}_t'(x) = \gamma\, \hat{f}_t(x)$ for some $\gamma \in \mathbb{Q}_p$, and then if $\hat{f}_t \neq 0$, then $\gamma \in \mathbb{N}$ and $\hat{f}_t = ax^\gamma$ is a monomial. This proves Fact 1.

Fact 2. $\alpha^{(i)} \equiv \alpha_t \pmod{p}$ for all $i \geq 2$.

Proof of Fact 2. We note that, since $2 \leq q - 1 \mid \alpha_j$ for all j, Formula (3) implies that in $\mathbb{Z}_p[x]$,

$$h(x) \equiv x^{\alpha_t} \pmod{p^2} \quad \text{and} \quad u \equiv 1 \pmod{p^2} \implies u^{-1} \equiv 1 \pmod{p^2}.$$

Therefore

$$\hat{f}_t(x) \equiv x^{\alpha_t} \pmod{p^2}.$$

Thus writing $r_0 = 1 + p\, x_0$ with $x_0 \in \mathbb{Z}_p$ and $p \nmid x_0$ we get

$$\hat{f}_t(r_0) \equiv r_0^{\alpha_t} \equiv (1 + p\, x_0)^{\alpha_t} \equiv 1 + \alpha_t p\, x_0 \pmod{p^2}.$$

On the other hand, by construction, for any $i \geq 2$,

$$\hat{f}_t(r_0) \equiv r_0^{\alpha^{(i)}} \equiv (1 + p\, x_0)^{\alpha^{(i)}} \equiv 1 + \alpha^{(i)} p\, x_0 \pmod{p^2}.$$

This implies $\alpha^{(i)} \equiv \alpha_t \pmod{p}$ since $p \nmid x_0$, and proves Fact 2. $\qquad\square$

Lemma 4.1. *Let $y \equiv 1 \pmod{p}$ in $\mathbb{Z}_p[x]$ and let $r \in \mathbb{Z}_p$ be such that $r \equiv 1 \pmod{p}$ and $r \not\equiv 1 \pmod{p^2}$. Then, given $f, C \in \mathbb{N}$, there exists a sequence of natural numbers $(\alpha^{(i)})_{i \geq 1}$ satisfying that for all $i \in \mathbb{N}$,*

- $\alpha^{(1)} \equiv 0 \pmod{\varphi(p)}$ *and* $\alpha^{(i+1)} \equiv \alpha^{(i)} \pmod{\varphi(p^i)}$,

- $r^{\alpha^{(i)}} \equiv y \pmod{p^i}$,

- $p^f - 1 \mid \alpha^{(i)}$ *and* $\alpha^{(i)} \geq C$.

Proof. We apply [2, Proposition 3] to $g = r^\alpha$:
Since $r^0 \equiv y \pmod{p}$ and $r \not\equiv 1 \pmod{p^2}$ implies $r^{p-1} \not\equiv 1 \pmod{p^2}$, then there exists a sequence $0 =: \beta_1, \beta_2, \ldots$ such that $\beta_{i+1} \equiv \beta_i \pmod{\varphi(p^i)}$ and $r^{\beta_i} \equiv y \pmod{p^i}$ for all i.
Now we show that there exists $k_i \in \mathbb{N}$ such that $\alpha^{(i)} := \beta_i + k_i \varphi(p^i)$ satisfies

all the conditions. First we observe that under those conditions, since $r \not\equiv 0 \pmod{p}$, then

$$
\begin{aligned}
r^{\alpha^{(i+1)}} \equiv \ r^{\beta_{i+1}} \ \equiv \ y &\pmod{p^{i+1}} \\
\equiv \ r^{\beta_i} \ \equiv \ r^{\alpha^{(i)}} &\pmod{p^i}
\end{aligned}
$$

Therefore we only need to show that some k_i satisfies the last conditions. The congruence equation $\beta_i + k_i \varphi(p^i) \equiv 0 \pmod{(p^f - 1)}$ is equivalent, since $\beta_i \equiv 0 \pmod{(p-1)}$, to the equation

$$
k_i \, p^{i-1} \equiv -\beta_i/(p-1) \pmod{(1 + \cdots + p^{f-1})}
$$

which solutions exist and are equal to $k_{i,0} + k(1 + \cdots + p^{f-1})$ for all $k \in \mathbb{Z}$, where $k_{i,0}$ is a particular solution, since $\gcd(p^{i-1}, 1 + \cdots + p^{f-1}) = 1$. Clearly k can be chosen big enough so that $\alpha^{(i)} \geq C$. $\qquad\square$

Acknowledgements

References

[1] A.C. Aitken: *Determinants and Matrices.* Oliver and Boyd, Edinburgh, 1939. vii+135 pp.

[2] M. Avendaño, T. Krick, A. Pacetti: *Newton-Hensel interpolation lifting.* Foundations of Computational Mathematics, vol 6(1), pp. 81–120, 2006.

[3] M. Avendaño, A. Ibrahim: *Ultrametric root counting.* Houston Journal of Mathematics, to appear.

[4] J. Bochnak, M. Coste, M-F. Roy: *Real algebraic geometry.* Springer-Verlag, 1998.

[5] Y-M. Chen and H-C. Li: *Inductive Proofs on the Determinants of Generalized Vandermonde Matrices.* International Journal of Computational and Applied Mathematics, vol. 5(1), pp. 23–40, 2010.

[6] R.J. Evans, I.M. Isaacs: *Generalized Vandermonde determinants and roots of unity of prime order.* Proceedings of the American Mathematical Society, vol. 58(1), pp. 51–54, 1976.

[7] H.W. Lenstra: *On the factorization of lacunary polynomials.* Number Theory in Progress, vol. 1, pp. 277–291, 1999.

[8] D.A. Marcus: *Number Fields.* Universitex, Springer-Verlag, 1977.

[9] O.H. Mitchell: *Notes on determinants of powers.* Amer. J. Math., vol. 4, pp. 341–344, 1881.

[10] B. Poonen: *Zeros of sparse polynomials over local fields of characteristic p.* Math. Res. Lett., vol. 5(3), pp. 273–279, 1998.

[11] E. Weiss, *Algebraic Number Theory*, McGraw-Hill, 1963.