ISSN 2220-5438

Reprint from

Moscow Journal of Combinatorics and Number Theory

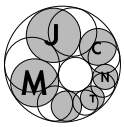
Volume 5 • Issue 1–2 2015

МФТИ

URSS

Moscow Journal of Combinatorics and Number Theory
Volume 5 • Issue 1–2 2015
URSS

Moscow Journal
of Combinatorics
and Number Theory
2015, vol. 5, iss. 1–2,
pp. 14–20



Estimating polynomials over $\mathbb{Z}_p$ at points from $\mathbb{C}_p$

Peter Bundschuh (Köln) and Vladimir G. Chirskii (Moscow)

Abstract: In the present note we establish a quantitative version of the algebraic independence over $\mathbb{Q}_p$ of elements from $\mathbb{C}_p$ given as certain p-adic series.

Keywords: algebraic independence, p-adic numbers

AMS Subject classification: 11J61, 11J85

Received: 15.04.2014; **revised:** 23.09.2014

1. Introduction

Let $\mathbb{Q}_p$ denote the field of p-adic numbers, and let $\mathbb{C}_p$ be the completion of the algebraic closure of $\mathbb{Q}_p$ with respect to the p-adic metric extended from $\mathbb{Q}_p$. Keeping our notation from [1–3], let $\mathbb{Z}_p := \{\beta \in \mathbb{Q}_p : |\beta|_p \leq 1\}$ be the ring of p-adic integers, and $U_p := \{\beta \in \mathbb{Q}_p : |\beta|_p = 1\}$ the unit group of $\mathbb{Q}_p$. As in our previous papers [2, 3], we consider here series of the shape

$$\alpha_i := \sum_{n=1}^{\infty} a_{n,i} p^{r_{n,i}} \qquad (i = 1, \ldots, m) \tag{1.1}$$

with all $a_{n,i} \in U_p$ and all m *exponent sequences* $(r_{n,i})_{n=1,2,\ldots} \in \mathbb{Q}_+^{\mathbb{N}}$ $(i = 1, \ldots, m)$ strictly increasing and unbounded; here $\mathbb{Q}_+ := \{r \in \mathbb{Q} : r > 0\}$.

Note that Lampert [5] used p-adic series of type (1.1) to answer two questions of Koblitz [4, p. 75] about the transcendence degrees of $\mathbb{C}_p$ over K, and of K over

$\mathbb{Q}_p$ for a certain intermediate field K of the extension $\mathbb{C}_p \mid \mathbb{Q}_p$. But whereas our $a_{n,i}$'s belong to U_p, Lampert's were certain roots of unity in $\mathbb{C}_p$.

The aim of our present note is to give a quantitative version of the algebraic independence over $\mathbb{Q}_p$ of elements $\alpha_1, \ldots, \alpha_m \in \mathbb{C}_p$ of type (1.1). For this, two hypotheses on the exponent sequences $(r_{n,i})$ are required, namely:

- For any $d \in \mathbb{N}$, there exists $N_1 = N_1(d) \in \mathbb{N}$ such that, for any rational integer $N \geq N_1$, one cannot have $\sum_{n=1}^{N} \sum_{i=1}^{m} D_{n,i} r_{n,i} \in \mathbb{Z}$ with all $D_{n,i} \in \mathbb{Z}$, $\sum_{n=1}^{N} \sum_{i=1}^{m} |D_{n,i}| \leq 2d$, and $\sum_{i=1}^{m} |D_{N,i}| > 0$.
- For any $(d, h) \in \mathbb{N}^2$, there exists $N_2 = N_2(d, h) \in \mathbb{N}$ such that

$$r_{N+1,i} > h + d r_{N,j} \tag{1.2}$$

holds for any $(i, j) \in \{1, \ldots, m\}^2$ as soon as $N \geq N_2$.

On denoting $r_n := \max\{r_{n,1}, \ldots, r_{n,m}\}$ for any $n \in \mathbb{N}$ we establish the following.

THEOREM 1. *If $\alpha_1, \ldots, \alpha_m \in \mathbb{C}_p$ from* (1.1) *satisfy the preceding hypotheses, then, for every $P \in \mathbb{Z}_p[x_1, \ldots, x_m] \setminus \{0\}$ with (total) $\deg P = d$ and all nonzero coefficients A having $\mathrm{ord}_p A \leq h$, the inequality*

$$|P(\alpha_1, \ldots, \alpha_m)|_p \geq p^{-h - d r_{N_0}} \tag{1.3}$$

holds with $N_0 := \max(N_1, N_2)$.

Remark 1.1. To assess the quality of the lower bound in (1.3) we give the following simple example. If r_1 is defined as above and $j \in \{1, \ldots, m\}$ satisfies $r_{1,j} = r_1$, then $P(x_1, \ldots, x_m) := p^h x_j^d$ has total degree d, only one non-zero coefficient A with $\mathrm{ord}_p A = h$ and satisfies

$$|P(\alpha_1, \ldots, \alpha_m)|_p = p^{-h - d r_1}.$$

Remark 1.2. In the case $d = 0$ of nonzero constant $P = A_0$, we have $|P|_p = |A_0|_p = p^{-\mathrm{ord}_p A_0} \geq p^{-h}$ without any further hypothesis. Thus, for the subsequent proof of our theorem, we may assume $d \in \mathbb{N}$.

In the last section, we will construct an example of m sequences $(r_{n,i})_n$ having all properties required above.

2. Auxiliary results

For the proof of the theorem, we need the following two auxiliary results the first of which being particularly simple.

LEMMA 1. *If $m \in \mathbb{N}$, if $R_1, \ldots, R_m \in \mathbb{Q}$ are distinct, and if all $B_1, \ldots, B_m \in \mathbb{C}_p$ have p-adic value* 1, *then*

$$|B_1 p^{R_1} + \ldots + B_m p^{R_m}|_p = p^{-\min\limits_i R_i}.$$

LEMMA 2. *If $\alpha_1, \ldots, \alpha_m$ and P satisfy the hypotheses of the theorem, and if $\alpha_{N,1}, \ldots, \alpha_{N,m}$ denote the Nth partial sums of $\alpha_1, \ldots, \alpha_m$, respectively, then the inequality*

$$|P(\alpha_{N,1}, \ldots, \alpha_{N,m})|_p \geq p^{-h-dr_N} \tag{2.1}$$

holds for any $N \geq N_1$, where r_N is defined before the theorem.

PROOF. As usual in algebra, we use the so-called *graded lexicographic order* of polynomials in m variables. This consists in comparing first the total degrees of the monomials, and then resolving the conflicts (that can occur only in case $m \geq 2$) by using the lexicographical order. This means that the monomial $x_1^{k_1} \ldots x_m^{k_m}$ precedes the monomial $x_1^{l_1} \ldots x_m^{l_m}$ if either $k_1 + \ldots + k_m > l_1 + \ldots + l_m$, or if $k_1 + \ldots + k_m = l_1 + \ldots + l_m$ and there is some $s \in \{0, \ldots, m-2\}$ such that $k_1 = l_1, \ldots, k_s = l_s, k_{s+1} > l_{s+1}$.

We now substitute $\alpha_{N,i}$ for x_i $(i = 1, \ldots, m)$. For any $k_i \in \mathbb{N}_0 := \mathbb{N} \cup \{0\}$, we obtain

$$\alpha_{N,i}^{k_i} = \Big(\sum_{n=1}^{N} a_{n,i} p^{r_{n,i}} \Big)^{k_i}$$

as a sum of terms of the shape

$$B p^{k_{N,i} r_{N,i} + \ldots + k_{1,i} r_{1,i}}$$

with $B \in \mathbb{Z}_p$ and $k_{N,i}, \ldots, k_{1,i} \in \mathbb{N}_0$ satisfying $k_{N,i} + \ldots + k_{1,i} = k_i$. Therefore, under the substitution $(x_1, \ldots, x_m) \mapsto (\alpha_{N,1}, \ldots, \alpha_{N,m})$, every monomial $x_1^{k_1} \ldots x_m^{k_m}$

gives a sum of terms of the form

$$Cp^{\sum\limits_{n=1}^{N}\sum\limits_{i=1}^{m} k_{n,i}r_{n,i}} \tag{2.2}$$

with $C \in \mathbb{Z}_p$ and $\sum\limits_{n=1}^{N} k_{n,i} = k_i \ \ (i = 1, \ldots, m)$. Thus, $P(\alpha_{N,1}, \ldots, \alpha_{N,m})$ turns out to be a sum of terms of the shape (2.2) with all $k_{n,i} \in \mathbb{N}_0$ and $\sum\limits_{n=1}^{N}\sum\limits_{i=1}^{m} k_{n,i} \leq d$.

Suppose that $Ax_1^{d_1} \cdots x_m^{d_m}$ with $A \in \mathbb{Z}_p \setminus \{0\}, d_1 + \ldots + d_m = d \in \mathbb{N}$ is the earliest term of P in the order we recalled above. On substituting $(x_1, \ldots, x_m) \mapsto \mapsto (\alpha_{N,1}, \ldots, \alpha_{N,m})$, this earliest term yields, among other terms, an expression

$$\widetilde{A}p^{\sum\limits_{i=1}^{m} d_i r_{N,i}} \tag{2.3}$$

with $\widetilde{A} \in \mathbb{Z}_p \setminus \{0\}$ satisfying $\widetilde{A}/A \in U_p$ (if we note that $\widetilde{A}/A$ is a product of $a_{n,i}$'s). This expression (2.3) cannot cancel out from $P(\alpha_{N,1}, \ldots, \alpha_{N,m})$. Indeed, all other summands resulting from the earliest term have the form (2.2) with $\sum\limits_{n=1}^{N} k_{n,i} = d_i$ for $i = 1, \ldots, m$. Every later (i. e., different from the earliest) monomial $x_1^{k_1} \cdots x_m^{k_m}$ leads, after our substitution, to terms of the shape (2.2).

If the term (2.3) would cancel out, in both cases we would obtain

$$\operatorname{ord}_p \widetilde{A} + \sum_{i=1}^{m} d_i r_{N,i} = \operatorname{ord}_p C + \sum_{n=1}^{N}\sum_{i=1}^{m} k_{n,i} r_{n,i}$$

implying

$$\sum_{i=1}^{m} D_{N,i} r_{N,i} + \sum_{n=1}^{N-1}\sum_{i=1}^{m} D_{n,i} r_{n,i} \in \mathbb{Z},$$

where, for $i = 1, \ldots, m$, we put $D_{N,i} := d_i - k_{N,i}$ and $D_{n,i} := -k_{n,i}$ $(n = 1, \ldots, N-1)$. But this contradicts the first hypothesis formulated before our theorem since

$$\sum_{n=1}^{N}\sum_{i=1}^{m} |D_{n,i}| \leq \sum_{i=1}^{m} d_i + \sum_{n=1}^{N}\sum_{i=1}^{m} k_{n,i} \leq 2d$$

and

$$\sum_{i=1}^{m} |D_{N,i}| = \sum_{i=1}^{m} |d_i - k_{N,i}| > 0.$$

Note here that the last sum vanishes if and only if $k_{N,i} = d_i$ for $i = 1, \dots, m$.

Since $\operatorname{ord}_p \widetilde{A} = \operatorname{ord}_p A \le h$, Lemma 1 combined with the fact that (2.3) cannot cancel out from $P(\alpha_{N,1}, \dots, \alpha_{N,m})$ leads to

$$|P(\alpha_{N,1}, \dots, \alpha_{N,m})|_p \ge p^{-\operatorname{ord}_p \widetilde{A} - \sum_{i=1}^{m} d_i r_{N,i}} \ge p^{-h-dr_N}$$

as asserted. □

3. Proof of theorem

To compare the p-adic value of $P(\alpha_1, \dots, \alpha_m)$ as appearing in our theorem to the one of $P(\alpha_{N,1}, \dots, \alpha_{N,m})$ in Lemma 2, we write

$$\begin{aligned} &P(\alpha_1, \dots, \alpha_m) - P(\alpha_{N,1}, \dots, \alpha_{N,m}) = \\ &= \sum_{i=1}^{m} \Big(P(\alpha_{N,1}, \dots, \alpha_{N,i-1}, \alpha_i, \dots, \alpha_m) - P(\alpha_{N,1}, \dots, \alpha_{N,i}, \alpha_{i+1}, \dots, \alpha_m) \Big). \end{aligned}$$

Since all α_i and $\alpha_{N,i}$ are in $\mathbb{C}_p$ and have p-adic values $p^{-r_{1,i}}$ (< 1), and since all coefficients of P are from $\mathbb{Z}_p$, we conclude that the typical difference entering in the preceding sum over i is p-adically bounded above by

$$|\alpha_i - \alpha_{N,i}|_p = p^{-r_{N+1,i}} < p^{-h-d \max\limits_{j} r_{N,j}},$$

the last inequality in virtue of our hypothesis (1.2) valid for $N \ge N_2$. Therefore we established

$$|P(\alpha_1, \dots, \alpha_m) - P(\alpha_{N,1}, \dots, \alpha_{N,m})|_p < p^{-h-dr_N},$$

and, by (2.1), we conclude from this

$$|P(\alpha_1, \dots, \alpha_m)|_p \ge p^{-h-dr_N}$$

for any $N \ge \max(N_1, N_2)$ as asserted. □

4. Example of exponent sequences

Here we exhibit m sequences $(r_{n,i})_n$ satisfying all conditions required above. To this purpose, let first $(M_{n,i})_n$ be m strictly increasing sequences of positive integers with

$$\lim_{n\to\infty} \frac{M_{n+1,j}}{M_{n,i}} = \infty \tag{4.1}$$

for any $(i,j) \in \{1,\dots,m\}^2$. Next, let $q_1,\dots,q_m$ be distinct prime numbers, and let $(s_{n,i})_n$ be m strictly increasing sequences of positive integers satisfying

$$\lim_{n\to\infty} (s_{n+1,i} - s_{n,i}) = \infty \quad (i = 1,\dots,m). \tag{4.2}$$

Then the sequences $(r_{n,i})_n$ with

$$r_{n,i} := M_{n,i} + q_i^{-s_{n,i}} \quad (i = 1,\dots,m;\ n = 1,2,\dots) \tag{4.3}$$

are exponent sequences.

Namely, for any $(d,h) \in \mathbb{N}^2$, we have

$$r_{n+1,i} > M_{n+1,i} > h + d(M_{n,j}+1) > h + dr_{n,j}$$

as soon as $n \ge N_2(d,h)$, the middle inequality being valid for n large enough, by (4.1). Moreover, by (4.3), we have

$$\sum_{n=1}^{N}\sum_{i=1}^{m} D_{n,i} r_{n,i} - \sum_{n=1}^{N}\sum_{i=1}^{m} D_{n,i} q_i^{-s_{n,i}} \in \mathbb{Z}. \tag{4.4}$$

Thus, it suffices to show that the second double sum here is not in $\mathbb{Z}$ for N large enough. By our assumption $\sum_{i=1}^{m} |D_{N,i}| > 0$, there exists, for any large N, some $i_0 \in \{1,\dots,m\}$ with $D_{N,i_0} \neq 0$. Writing q for q_{i_0} we clearly have

$$\Big| \sum_{n=1}^{N} \sum_{\substack{i=1 \\ i\neq i_0}}^{m} D_{n,i} q_i^{-s_{n,i}} \Big|_q \le 1, \tag{4.5}$$

and it remains to find a good lower bound for the q-adic value of $\sum_{n=1}^{N} D_{n,i_0} q^{-s_{n,i_0}}$.

First, we have $|\sum_{n<N} D_{n,i_0} q^{-s_{n,i_0}}|_q \le q^{s_{N-1,i_0}}$ and secondly, from the upper bound $\sum_{n=1}^{N}\sum_{i=1}^{m} |D_{n,i}| \le 2d$, we obtain $|D_{N,i_0}|_q \ge |D_{N,i_0}|^{-1} \ge 1/(2d)$. Both estimates together lead to

$$\Big|\sum_{n=1}^{N} D_{n,i_0} q^{-s_{n,i_0}}\Big|_q \ge q^{s_{N,i_0}}/(2d) \tag{4.6}$$

since $s_{N,i_0} - s_{N-1,i_0} > \log_q 2d$ for $N \ge N_1(d)$, by (4.2). Since the right-hand side of (4.6) exceeds 1 for large N, the same holds, by (4.5), for the second double sum in (4.4), whence this sum cannot belong to $\mathbb{Z}$.

Bibliography

1. ***P. Bundschuh, V. G. Chirskii***, *Algebraic independence of elements from $\mathbb{C}_p$ over $\mathbb{Q}_p$, I*, Arch. Math. (Basel) **79** (2002), 345–352.
2. ***P. Bundschuh, V. G. Chirskii***, *Algebraic independence of elements from $\mathbb{C}_p$ over $\mathbb{Q}_p$, II*, Acta Arith. **113** (2004), 309–326.
3. ***V. G. Chirskii***, *Values of analytic functions at points of $\mathbb{C}_p$*, Russ. J. Math. Phys. **20** (2013), 149–154.
4. ***N. Koblitz,*** *p-adic Numbers, p-adic Analysis, and Zeta-Functions*, 2nd ed., New York, Springer, 1984.
5. ***D. Lampert***, *Algebraic p-adic expansions*, J. Number Theory **23** (1986), 279–284.

PETER BUNDSCHUH

Mathematisches Institut
Universität zu Köln
Weyertal 86–90
50931 Köln, Germany
pb@math.uni-koeln.de

VLADIMIR G. CHIRSKII

Department of Mechanics and Mathematics
Moscow State University
119991 Moscow, Russia
vgchirskii@yandex.ru