ACTA ARITHMETICA
XCI.3 (1999)

Continuous functions on compact subsets of local fields

by

MANJUL BHARGAVA and KIRAN S. KEDLAYA (Princeton, NJ)

A classical theorem of Mahler [4] states that every continuous function f from the p-adic ring $\mathbb{Z}_p$ to its quotient field $\mathbb{Q}_p$ (or to any finite extension of $\mathbb{Q}_p$) can be uniquely expressed in the form

$$f(x) = \sum_{n=0}^{\infty} c_n \binom{x}{n},$$

where the sequence c_n tends to 0 as $n \to \infty$. The purpose of this paper is to extend Mahler's theorem to continuous functions from any compact subset S of a local field K to K. Here by a *local field* we mean the fraction field of a complete discrete valuation ring R whose residue field $k = R/\pi R$ is finite.

Our theorem implies, in particular, that every continuous function from S to K can be uniformly approximated by polynomials. This generalization of Weierstrass's approximation theorem was first proved in the case $K = \mathbb{Q}_p$ by Dieudonné [3]. Mahler [4] made explicit Dieudonné's result in the case $S = \mathbb{Z}_p$ by giving a canonical polynomial interpolation series for the continuous functions from $\mathbb{Z}_p$ to $\mathbb{Q}_p$. Amice [1] later extended Mahler's theorem to continuous functions on certain "very well-distributed" subsets S of a local field K. The present work provides canonical polynomial interpolation series for all S and K, and thus constitutes a best possible generalization of Mahler's result in this context.

The main ingredient in our work is a generalization of the binomial polynomials $\binom{x}{n}$ introduced by the first author [2]. Their construction is as follows. Given a subset $S \subset K$, fix a π-*ordering* $\varLambda$ of S, which is a sequence $a_0, a_1, \ldots$ in which $a_n \in S$ is chosen to minimize the valuation of $(a_n - a_0) \cdots (a_n - a_{n-1})$. It is a fundamental lemma [2, Theorem 1] that the generalized factorial

$$n!_\varLambda = (a_n - a_0) \cdots (a_n - a_{n-1})$$

1991 *Mathematics Subject Classification*: 11S05, 11S80.

generates the same ideal for any choice of Λ. The nth *generalized binomial polynomial* is then defined as

$$\binom{x}{n}_{\Lambda} = \frac{(x-a_0)\cdots(x-a_{n-1})}{n!_{\Lambda}};$$

by construction, $\binom{x}{n}_{\Lambda}$ maps S into R for all $n \geq 0$. The usual binomial polynomials are of course recovered upon setting Λ to be the p-ordering $0, 1, 2, \ldots$ of the ring $R = \mathbb{Z}_p$.

Mahler's theorem implies that the ordinary binomial polynomials $\{\binom{x}{n}\}$ form a $\mathbb{Z}_p$-basis for the ring $\mathrm{Int}(\mathbb{Z}_p, \mathbb{Z}_p)$ of polynomials over $\mathbb{Q}_p$ mapping $\mathbb{Z}_p$ into $\mathbb{Z}_p$. This fundamental property of the usual binomial polynomials was first pointed out (with $\mathbb{Z}$ in place of $\mathbb{Z}_p$) by Pólya [5]. On the other hand, in [2] it was shown that, analogously, the generalized binomial polynomials $\{\binom{x}{n}_{\Lambda}\}$ form an R-basis for the ring $\mathrm{Int}(S, R)$ of polynomials over K mapping S into R. These results are what led us to conjecture, and subsequently prove, our extension of Mahler's theorem.

Our main result is

THEOREM 1. *Given any continuous map $f : S \to K$, there exists a unique sequence $\{c_n\}_{n=0}^{\infty}$ in K such that*

$$f(x) = \sum_{n=0}^{\infty} c_n \binom{x}{n}_{\Lambda} \tag{1}$$

for all $x \in S$. Moreover, $c_n \to 0$ as $n \to \infty$, so the series converges uniformly.

Note that the c_n for a given f may be computed recursively from the values of f at the a_i, by the formula

$$c_n = f(a_n) - \sum_{i=0}^{n-1} c_i \binom{a_n}{i}_{\Lambda}, \tag{2}$$

or directly (see [2, Theorem 6]) by the formula

$$c_n = \sum_{i=0}^{n} \Big(\prod_{j \neq i} \frac{a_n - a_j}{a_i - a_j} \Big) f(a_i). \tag{3}$$

We begin by proving Theorem 1 first for a special class of π-orderings. Given a π-ordering $\Lambda = \{a_i\}$ and a nonnegative integer n, we say that a_n is *old* $(\mathrm{mod}\, \pi^m)$ if $a_n \equiv a_j \pmod{\pi^m}$ for some $j < n$; otherwise, we say a_n is *new* $(\mathrm{mod}\, \pi^m)$. A π-ordering $\Lambda = \{a_i\}$ is *proper* if, for all k and m, a_k is chosen to be a new element $(\mathrm{mod}\, \pi^m)$ only when it is not possible to choose a_k to be old. Thus, for example, the p-ordering $0, 1, p, p^2+1, 2p$ is proper, whereas the p-ordering $0, 1, p, 2p, p^2+1$ is not.

If Λ is proper, we have the following weak analogue of Lucas's theorem for the generalized binomials $\binom{x}{n}_\Lambda$.

Lemma 1. *Assume $\Lambda = \{a_i\}$ is proper and that a_n is new* $\pmod{\pi^m}$. *Let $x, y \in S$, and suppose $x \equiv y \pmod{\pi^m}$. Then*

$$\binom{x}{n}_\Lambda \equiv \binom{y}{n}_\Lambda \pmod{\pi}.$$

Proof. If $x \not\equiv a_i \pmod{\pi^m}$ for all $i < n$, we have

$$\binom{y}{n}_\Lambda = \binom{x}{n}_\Lambda \prod_{j=0}^{n-1} \frac{y - a_j}{x - a_j} \equiv \binom{x}{n}_\Lambda \pmod{\pi},$$

since $y - a_j$ and $x - a_j$ have the same valuation and the same final nonzero π-adic digit.

On the other hand, suppose $x \equiv a_i \pmod{\pi^m}$ for some $i < n$. The fact that a new element a_n was chosen for the proper π-ordering Λ, instead of x, which would have been old modulo π^m, means that $(x - a_0) \cdots (x - a_{n-1})$ has strictly higher valuation than $(a_n - a_0) \cdots (a_n - a_{n-1})$. Hence we have

$$\binom{x}{n}_\Lambda \equiv 0 \pmod{\pi}.$$

Applying the same argument with y in place of x, we find

$$\binom{x}{n}_\Lambda \equiv \binom{y}{n}_\Lambda \equiv 0 \pmod{\pi},$$

and this completes the proof. ∎

From Lemma 1 we obtain

Corollary 1. *Assume the π-ordering Λ is proper, and let T be the set of n such that a_n is new* $\pmod{\pi^m}$. *If $h : S \to k$ is a function such that $h(x) = h(y)$ whenever $x \equiv y \pmod{\pi^m}$, then there exists a unique function $g : T \to k$ such that*

$$h(x) \equiv \sum_{n \in T} g(n) \binom{x}{n}_\Lambda \pmod{\pi} \quad \textit{for all } x \in S.$$

Proof. There are $|k|^{|T|}$ functions of each kind, and each h is represented by at most one g, since g can be recovered from h using the formula

$$g(i) = h(a_i) - \sum_{\substack{n \in T \\ n < i}} g(n) \binom{a_i}{n}_\Lambda. \tag{4}$$

Thus every h is represented by exactly one g. ∎

We may now give a proof of Theorem 1 in the case when Λ is proper.

Proof of Theorem 1 for a proper π-ordering Λ. Since S and its image under the continuous map f are both compact, each is contained in $\pi^m R$ for some m, and a suitable rescaling allows us to assume that S and $f(S)$ are both contained in R. If f admits a representation as in (1), then, as noted before, the c_n may be recovered from the values of f at the a_i using (2) or (3). Hence the sequence $\{c_n\}$ is unique if it exists. (Note that for this part of the argument we did not need that Λ is proper or that $c_n \to 0$.)

To prove existence of the desired null sequence under the assumption that Λ is proper, it suffices to exhibit a sequence c_n with finitely many nonzero terms such that

$$f(x) \equiv \sum_{n=0}^{\infty} c_n \binom{x}{n}_{\Lambda} \pmod{\pi},$$

since we can then apply the same reasoning to $\left[f(x) - \sum c_n \binom{x}{n}_{\Lambda}\right]/\pi$, and so on.

Let h be the composite of f with the projection of R onto k. Since h is continuous, the preimage of each element of k is a closed-open subset of S. It follows that h satisfies the condition of Corollary 1 for some m, in which case setting $c_n \equiv g(n) \pmod{\pi}$ for $n \in T$ and $c_n = 0$ otherwise furnishes the desired sequence. ∎

We may now deduce Theorem 1 for arbitrary π-orderings using a change-of-basis argument. In fact, we prove something even stronger.

THEOREM 2. *Let $\{P_i\}_{i=0}^{\infty}$ be any R-basis of the ring $\mathrm{Int}(S,R)$. Then for each continuous map $f : S \to K$, there exists a unique sequence $\{c_n\}$ in K with $c_n \to 0$ as $n \to \infty$ such that*

$$f(x) = \sum_{n=0}^{\infty} c_n P_n(x) \tag{5}$$

for all $x \in S$.

Note that the hypothesis of Theorem 2 is essentially the weakest possible, since the truth of the conclusion for given polynomials $\{P_i\}$ implies that they form (when appropriately scaled) an R-basis of $\mathrm{Int}(S,R)$. However, we must settle for a slightly weaker uniqueness statement in Theorem 2 than we had in Theorem 1; for as we shall see, if the polynomials P_i are not generalized binomial polynomials, and the condition $c_n \to 0$ is relaxed, then the representation (5) may not remain unique!

Proof (of Theorem 2). For Λ a proper π-ordering of S, we have already shown that there exists a unique sequence b_m such that

(6) $$f(x) = \sum_{m=0}^{\infty} b_m \binom{x}{m}_{\Lambda}$$

for all $x \in S$, and that $b_m \to 0$ as $n \to \infty$. Since both the P_i and the binomial polynomials form R-bases of $\mathrm{Int}(S, R)$, there exist transformations $T = (t_{mn})$ and $U = (u_{mn})$ over R such that

$$\binom{x}{m}_{\Lambda} = \sum_{n=0}^{\infty} t_{mn} P_n(x) \quad \text{and} \quad P_n(x) = \sum_{m=0}^{\infty} u_{nm} \binom{x}{m}_{\Lambda};$$

in particular, these summations each contain only finitely many nonzero terms. More precisely, there exist integers $N(m)$ and $M(n)$ such that $t_{mn} = 0$ for all $n \geq N(m)$ and $u_{nm} = 0$ for all $m \geq M(n)$.

Define c_n by the formula

$$c_n = \sum_{m=0}^{\infty} b_m t_{mn};$$

the series converges for every n since $t_{mn} \in R$ and $b_m \to 0$. Moreover, for any nonnegative integer i, there exists M such that π^i divides b_m for $m \geq M$, and there exists N such that $t_{1n} = \cdots = t_{Mn} = 0$ for $n \geq N$. Hence π^i divides c_n for $n \geq N$, and so $c_n \to 0$.

To demonstrate that

(7) $$\sum_{n=0}^{\infty} c_n P_n(x) = f(x),$$

it suffices to verify that the two sides of the equality agree modulo π^i for all nonnegative integers i. With notation as in the preceding paragraph, we have

$$\begin{aligned} f(x) = \sum_{m=0}^{\infty} b_m \binom{x}{m}_{\Lambda} &\equiv \sum_{m=0}^{M} b_m \sum_{n=0}^{\infty} t_{mn} P_n(x) \\ &= \sum_{m=0}^{M} \sum_{n=0}^{N} b_m t_{mn} P_n(x) \pmod{\pi^i}. \end{aligned}$$

On the other hand,

$$\begin{aligned} \sum_{n=0}^{\infty} c_n P_n(x) &\equiv \sum_{n=0}^{N} P_n(x) \sum_{m=0}^{\infty} b_m t_{mn} \\ &\equiv \sum_{n=0}^{N} \sum_{m=0}^{M} b_m t_{mn} P_n(x) \pmod{\pi^i}, \end{aligned}$$

and the desired congruence follows.

To show uniqueness, suppose that in addition to (5) we have

$$f(x) = \sum_{n=0}^{\infty} c'_n P_n(x) \tag{8}$$

for some sequence $\{c'_n\}$ with $c'_n \to 0$. Define the sequence $\{b'_m\}$ by

$$b'_m = \sum_{n=0}^{\infty} c'_n u_{nm}.$$

Then the same argument as before (with the transformation U in place of T) shows that the series

$$\sum_{n=0}^{\infty} b'_n \binom{x}{n}_{\Lambda}$$

converges uniformly to $f(x)$ on S. By Theorem 1, it follows that $b_n = b'_n$ for all n, and upon reapplying T, we obtain $c_n = c'_n$ for all n. This completes the proof of Theorem 2. ∎

As noted above, Theorem 2 includes the condition $c_n \to 0$ as a hypothesis rather than a conclusion. To illustrate why this occurs, we provide an example of a regular basis of $\mathrm{Int}(R, R)$ (an R-basis of $\mathrm{Int}(R, R)$ consisting of one polynomial of each degree) which admits a nontrivial representation of the identically zero function. In the case $R = \mathbb{F}_q[[t]]$, this resolves a question of Wagner [6, Section 4].

Let q be the cardinality of the residue field k, and choose a complete set of residues $a_0, \ldots, a_{q-1}$ modulo π such that $a_0 = 0$. We construct a π-ordering $\Lambda = \{a_i\}$ by the following rule: if $\sum_i c_i q^i$ is the base q expansion of n, then

$$a_n = \sum_i a_{c_i} \pi^i.$$

For m a nonnegative integer, let

$$Q_m(x) = \binom{x + a_{q^m - 1}}{q^{2m} - 1}_{\Lambda},$$

and define the regular basis $\{P_n(x)\}$ of $\mathrm{Int}(R, R)$ as follows:

$$P_n(x) = \begin{cases} Q_m(x) - Q_{m-1}(x) & \text{if } n = q^{2m} - 1 \text{ for some } m > 0, \\ \binom{x}{n}_{\Lambda} & \text{otherwise.} \end{cases}$$

Also, let $c_n = 1$ if $n = q^{2m} - 1$ for some $m \geq 0$ and $c_n = 0$ otherwise. We claim that the series $\sum_n c_n P_n(x)$ converges pointwise to 0 on R, even though the c_n are not all zero. Since

$$\sum_{n=0}^{N} c_n P_n(x) = Q_m(x) \qquad \text{for } q^{2m} - 1 \le N < q^{2(m+1)} - 1,$$

it is equivalent to show $Q_m(x)$ converges pointwise to 0 as $m \to \infty$.

We may assume $x \neq 0$, since $Q_m(0) = 0$ for all $m > 0$; in this case, $x \not\equiv 0 \pmod{\pi^l}$ for some l. Expanding the generalized binomial coefficient, we find

$$Q_m(x) = \prod_{i=0}^{q^{2m}-2} \frac{x + a_{q^m-1} - a_i}{a_{q^{2m}-1} - a_i}.$$

Note that if i and j are distinct nonnegative integers and s is the smallest integer such that $i \not\equiv j \pmod{q^s}$, then $a_i \not\equiv a_j \pmod{\pi^s}$. Hence the denominator in the above product runs through each nonzero residue class modulo π^{2m} exactly once, while the numerator runs through each residue class once except that of $x + a_{q^m-1} - a_{q^{2m}-1}$. For $m > l$, the latter fails to be divisible by π^l; it follows that for some π-adic integer r,

$$Q_m(x) = \frac{\pi^{2m} r}{x + a_{q^m-1} - a_{q^{2m}-1}} \equiv 0 \pmod{\pi^{2m-l+1}}.$$

In particular, $Q_m(x) \to 0$ as $m \to \infty$, as desired.

We conclude by briefly stating the implications of Theorem 1 for K-valued measures on S. Recall that a K-valued measure on S is a K-linear map μ from $C(S,K)$ to K, where $C(S,K)$ denotes the set of continuous functions from S to K. By convention, one writes $\mu(f)$ symbolically as $\int_S f\,d\mu$. With this notation, Theorem 1 immediately translates into the following characterization of measures on S.

THEOREM 3. *A K-valued measure μ on S is uniquely determined by the sequence $\mu_k = \int_S \binom{x}{k}_A d\mu$ of elements of K. Conversely, any bounded sequence $\{\mu_k\}$ in K determines a unique K-valued measure μ on S by the formula $\int_S f\,d\mu = \sum_{k=0}^{\infty} c_k \mu_k$, where $\{c_k\}$ is the sequence corresponding to f as in Theorem* 1.

References

[1] Y. Amice, *Interpolation p-adique*, Bull. Soc. Math. France 92 (1964), 117–180.

[2] M. Bhargava, *P-orderings and polynomial functions on arbitrary subsets of Dedekind rings*, J. Reine Angew. Math. 490 (1997), 101–127.

[3] J. Dieudonné, *Sur les fonctions continues p-adiques*, Bull. Sci. Math. 68 (1944), 79–95.

[4] K. Mahler, *An interpolation series for a continuous function of a p-adic variable*, J. Reine Angew. Math. 199 (1958), 23–34.

[5] G. Pólya, *Über ganzwertige ganze Funktionen*, Rend. Circ. Mat. Palermo 40 (1915), 1–16.

[6] C. Wagner, *Interpolation series for continuous functions on π-adic completions of* GF(q, x), Acta Arith. 17 (1971), 389–406.

Department of Mathematics
Princeton University
Princeton, NJ 08544, U.S.A.
E-mail: bhargava@math.harvard.edu
kedlaya@math.mit.edu

Received on 15.8.1997
and in revised form on 4.1.1999 (3218)