Mahler's theorem on continuous p-adic maps via generating functions

Noam D. Elkies

Fix a prime p. Let $a_0, a_1, a_2, \ldots$ be a sequence of p-adic numbers. By induction we may find $b_0, b_1, b_2, \ldots \in \mathbf{Q}_p$ such that

$$a_n = \sum_{i=0}^{\infty} \binom{n}{i} b_i.$$

(The sum is actually finite because $\binom{n}{i}$ vanishes once $i > n$.) If $b_i \to 0$ as $i \to \infty$ then the sum

$$A(x) := \sum_{i=0}^{\infty} \binom{x}{i} b_i \quad (x \in \mathbf{Z}_p)$$

is a uniform limit of polynomials and thus converges to a continuous function from $\mathbf{Z}_p$ to $\mathbf{Q}_p$ such that $A(n) = a_n$ for each $n = 0, 1, 2, \ldots$. Mahler proved that conversely if the function $n \mapsto a_n$ extends to a continuous function from $\mathbf{Z}_p$ to $\mathbf{Q}_p$ then $b_i \to 0$ in $\mathbf{Q}_p$ as $i \to \infty$. We give a direct and simple proof of this using generating functions.

Let $f(t)$, $g(u)$ be the formal power series

$$f(t) = \sum_{n=0}^{\infty} a_n t^n, \quad g(u) = \sum_{i=0}^{\infty} b_i u^i$$

in $\mathbf{Q}_p[[t]]$ and $\mathbf{Q}_p[[u]]$. We have

$$f(t) = \sum_{n=0}^{\infty} \sum_{i=0}^{n} \binom{n}{i} b_i t^n = \sum_{i=0}^{\infty} b_i \sum_{n=i}^{\infty} \binom{n}{i} t^n.$$

The inner sum is the Taylor series for $t^n/(1-t)^{n+1}$. Hence

$$f(t) = \frac{1}{1-t}\, g\Big(\frac{t}{1-t}\Big).$$

If $u = t/(1-t)$ then $t = u/(1+u)$. We can thus solve for g:

$$g(u) = \frac{1}{1+u}\, f\Big(\frac{u}{1+u}\Big).$$

We may now obtain the b_i explicitly in terms of the a_n by expanding each term $u^n/(1+u)^{n+1}$ in the sum defining $(1+u)^{-1} f(u/(1+u))$:

$$b_i = \sum_{m=0}^{i} (-1)^{m-i} \binom{i}{m} a_i.$$

But for our purposes it is more convenient to use the formula for the generating function $g(u)$.

Suppose now that there exists a continuous map $A : \mathbf{Z}_p \to \mathbf{Q}_p$ that extends the function $n \mapsto a_n$. Since $\mathbf{Z}_p$ is compact, the map is uniformly continuous.

Restricting A to $\{0,1,2,\ldots\}$ and unwinding the definition of uniform continuity in the p-adic metric, we conclude that for each integer k there exists an integer r such that $a_n - a_{n'}$ has p-adic valuation at least k for all positive integers n, n' such that $n \equiv n' \bmod p^r$. We shall show that this implies the existence of an integer $N(k)$ such that b_i is a multiple of p^k for all $i > N(k)$. (Specifically, we shall obtain $N(k) = (s+k+1)p^r$ where s is a nonnegative integer such that $p^s a_n \in \mathbf{Z}_p$ for all n.) Since k is arbitrary, this will verify that $b_i \to 0$.

Our assumption that $v_p(a_n - a_{n'}) \geq k$ when $v_p(n - n') \geq r$ means that

$$f(t) = \frac{P(t)}{1 - t^{p^r}} + p^k \alpha(t)$$

for some polynomial $P \in \mathbf{Q}_p[t]$ of degree less than p^r and some power series $\alpha \in \mathbf{Z}_p[[t]]$. (For instance, we may take $P(t) = \sum_{n=0}^{p^r-1} a_n t^n$ and $\alpha(t) = \sum_{n=p^r}^{\infty} p^{-k}(a_n - a_{n'})t^n$ where n' is the remainder of n when dividied by p^r.) Then

$$g(u) = \frac{1}{1+u} f\Big(\frac{u}{1+u}\Big) = \frac{Q(u)}{(1+u)^{p^r} - u^{p^r}} + \frac{p^k}{1+u}\,\alpha\Big(\frac{u}{1+u}\Big),$$

where

$$Q(u) = (1+u)^{p^r-1} P\Big(\frac{u}{1+u}\Big) \in \mathbf{Q}_p[u],$$

a polynomial of degree less than p^r, and the remainder $p^k\,\alpha(u/(1+u))\,/\,(1+u)$ is again a power series in $p^k \mathbf{Z}_p[[u]]$.

Now the key point is that the denominator $(1+u)^{p^r} - u^{p^r}$ of $g(u)$ is congruent to 1 mod p. (It is well known that $(X+Y)^p \equiv X^p + Y^p \bmod p$ in $\mathbf{Z}[X,Y]$; it follows by induction on r that $(X+Y)^{p^r} \equiv X^{p^r} + Y^{p^r} \bmod p$; now take $X = u$ and $Y = 1$.) That is,

$$(1+u)^{p^r} - u^{p^r} = 1 + pR(u)$$

for some polynomial R with coefficients in $\mathbf{Z}_p$ and degree $p^r - 1$. Therefore

$$\frac{Q(u)}{(1+u)^{p^r} - u^{p^r}} = Q(u)\big(1 + pR(u) + p^2R^2(u) + p^3R^3(u) + \cdots\big).$$

Let s be a nonnegative integer such that $p^s Q(u) \in \mathbf{Z}_p[u]$. Then

$$\frac{Q(u)}{(1+u)^{p^r} - u^{p^r}} = Q(u) \sum_{j=0}^{k+s-1} (pR(u))^j + \beta(u)$$

where

$$\beta(u) = Q(u) \sum_{j=k+s}^{\infty} (pR(u))^j \in p^k \mathbf{Z}_p[[u]]$$

while $Q(u) \sum_{j=0}^{k+s-1} (pR(u))^j$ is a polynomial, say of degree N_k. We have shown that $g(u)$ differs from this polynomial by a power series all of whose coefficients have p-adic valuation at least k. Thus $v_p(b_i) \geq k$ for all $i > N_k$. This establishes our claim and completes the proof of Mahler's theorem.