Abstract. Extending work of Bell and of Bell, Ghioca, and Tucker, we prove that for a $p$-adic analytic self-map $f$ on a closed unit polydisk, if every coefficient of $f(x) - x$ has valuation greater than that of $p^{1/(p-1)}$, then the iterates of $f$ can be $p$-adically interpolated; i.e., there exists a function $(x,n)$ analytic in both $x$ and $n$ such that $g(x,n) = f^n(x)$ whenever $n \in \mathbb{Z}_{\geq 0}$.

Our proof will check directly that the Mahler series \cite{Mah58} interpolating the sequence

$x, f(x), f(f(x)), \ldots$

converges to an analytic function. This is the difference operator analogue of proving that a function $\phi$ is analytic by checking that its Taylor series converges to $\phi$. 

\section*{Acknowledgements}

This research was supported by National Science Foundation grant DMS-1069236. This article has been published in \textit{Bull. London Math. Soc.} \textbf{46} (2014), no. 3, 525–527.
Proof. Since \( f(x) \equiv x \pmod{p^c} \), we have \( h(f(x)) \equiv h(x) \pmod{p^c} \) for any \( h \in R[x]^d \) and (by taking limits) also for any \( h \in R(x)^d \). In other words, the linear operator \( \Delta \) defined by

\[
(\Delta h)(x) := h(f(x)) - h(x)
\]

maps \( R(x)^d \) into \( p^c R(x)^d \). In particular, \( m \) applications of \( \Delta \) to the identity function yields \( \Delta^m x \in p^{mc} R(x)^d \). On the other hand, \( |m!| \geq p^{-m/(p-1)} \). Thus the Mahler series

\[
g(x, n) := \sum_{m=0}^{\infty} \binom{n}{m} \Delta^m x = \sum_{m=0}^{\infty} n(n-1) \cdots (n-m+1) \frac{\Delta^m x}{m!}
\]

converges in \( R(x, n)^d \) with respect to \( || \cdot || \). Let \( I \) be the identity operator. If \( n \in \mathbb{Z}_{\geq 0} \), then

\[
g(x, n) = \sum_{m=0}^{n} \binom{n}{m} \Delta^m x = (\Delta + I)^n x = f^n(x).
\]

\( \square \)

Remark 2. The relation \( g(x, n+1) = f(g(x, n)) \) in \( R(x)^d \) holds for each \( n \) in the infinite set \( \mathbb{Z}_{\geq 0} \), so it is an identity in \( R(x)^d \).

Remark 3. The hypothesis on \( f \) holds for \( K = \mathbb{Q} \), if \( f(x) \equiv x \pmod{p} \) and \( p \geq 3 \); previously the conclusion was known only for \( p \geq 5 \) \cite{Bel08} \cite{BGT10, §3}. On the other hand, \( f(x) := -x \) is a counterexample for \( p = 2 \) \cite{Bel08, §3}. Similarly, the inequality on \( c \) in Theorem 1 is best possible for each \( p \) : consider \( f(x) := \zeta x \) where \( \zeta \) is a primitive \( p \)-th root of unity in \( \mathbb{C}_p \).

Remark 4. Let \( \mathfrak{m} \) be the maximal ideal of \( R \). Let \( k := R/\mathfrak{m} \). If \( f(x) \) mod \( \mathfrak{m} = x \), so that \( f(x) \equiv x \pmod{p^c} \) holds for some \( c > 0 \), then \( f^p(x) \equiv x \pmod{p^c} \) holds for a larger \( c \), and by iterating we find \( r \in \mathbb{Z}_{\geq 0} \) such that Theorem 1 applies to \( f^{p^r} \). More generally, if \( f(x) \) mod \( \mathfrak{m} = Ax \) for some \( A \in \text{GL}_d(k) \) of finite order, then there exists \( s \in \mathbb{Z}_{>0} \) such that \( f^s \) satisfies the hypothesis of Theorem 1. This finite order hypothesis is automatic if \( K \) is \( \mathbb{Q}_p \) or \( \mathbb{C}_p \) since then \( k \) is algebraic over \( \mathbb{F}_p \) and every element of \( \text{GL}_d(k) \) is of finite order. Cf. \cite{BGT10, §2.2].

Acknowledgements

We thank Joseph Silverman and Thomas J. Tucker for helpful suggestions.

References


DEPARTMENT OF MATHEMATICS, MASSACHUSETTS INSTITUTE OF TECHNOLOGY, CAMBRIDGE, MA 02139-4307, USA
E-mail address: poonen@math.mit.edu
URL: http://math.mit.edu/~poonen/