BULL. AUSTRAL. MATH. SOC. 10A35, 14G20, 30D35, 30G05.
VOL. 29 (1984), 109-117.

P-ADIC METHODS IN THE STUDY OF TAYLOR COEFFICIENTS OF RATIONAL FUNCTIONS*

A. J. VAN DER POORTEN

I sketch the proof of the so-called Hadamard Quotient Theorem: If the Hadamard quotient of two rational functions is a Taylor series with integer coefficients (more generally: with coefficients in some finitely generated subring of a field) then it is a rational function.

1. Introduction

Let $\mathbb{K}$ be a field of characteristic zero, and r,s polynomials defined over $\mathbb{K}$ with $s(0) \neq 0$. A rational function is a quotient $r(X)/s(X)$ and we have a Taylor expansion

$$\frac{r(X)}{s(X)} = \sum_{h\geq 0} a_h X^h \quad .$$

We lose no generality in setting

$$s(X) = 1-s_1X - \dots - s_nX^n = \prod_{i=1}^{m} (1 - \alpha_i X)^{n(i)}$$

where the α_i are distinct elements of $\mathbb{K}$. It is then easy to see that

---

Received 12 September 1983.

* This is a lecture delivered at the Special Meeting of the Australian Mathematical Society "Celebration of the 80th Birthday of Kurt Mahler", Canberra, July 26, 1983.

---

we have

$$a_{h+n} = s_1 a_{h+n-1} + \dots + s_n a_h \quad ,$$

so (a_h) is a so-called *recurrence sequence* of order n, and, by expanding in partial fractions,

$$a_h = \sum_{i=1}^{m} A_i(h)\alpha_i^{\,h}$$

for polynomials A_i of degree respectively n_i-1. These assertions hold for integers $h \geq \max(0, \deg r - n+1)$. The various descriptions of (a_h) are equivalent.

2. p-adification

To study the sequence (a_h) it is convenient to have h a continuous parameter. Cassels [2] shows there are infinitely many rational primes p so that the field $\mathbb{K}$ may be embedded in the field Q_p of p-adic rationals whilst for each $\alpha = \alpha_i$

$$\alpha^{p-1} \equiv 1 (\mathrm{mod}\ p) \quad ,$$

equivalently:

$$\mathrm{ord}_p(\alpha^{p-1} - 1) \geq 1 \ .$$

Then

$$\log \alpha^{p-1} = \log(1 - (1-\alpha^{p-1}))$$

is well-defined p-adically, and $\alpha^{t(p-1)}$ is given by the power series

$$\exp(t \log \alpha^{p-1})$$

which converges for t with $\mathrm{ord}_p t > -1 + 1/p-1$. Thus a recurrence sequence (a_h) p-adifies to yield $p-1$ p-adic power series:

$$a_{p,r}(t) = a(t(p-1)+r) = \sum_{i=1}^{m} A_i(t(p-1)+r)\alpha_i^{\,r} exp(t \log \alpha_i^{\,p-1}) \ , \ 0 \leq r < p-1.$$

https://doi.org/10.1017/S0004972700021328 Published online by Cambridge University Press

It is now easy to prove the wonderful *Skolem-Mahler-Lech-Mahler Theorem: If* $\{h : a_h = 0\}$ *is infinite then it is a union of finitely many arithmetic progressions (and finitely many isolated points).* Indeed if the set is infinite then for some r the p-adic analytic function $a_{p,r}$ vanishes infinitely often on the compact set $\mathbb{Z}_p$. Hence $a_{p,r}$ vanishes identically, so $a(h(p-1)+r) = 0$ for h in $\mathbb{Z}$. We proceed similarly for each remaining $a_{p,r}$. It is interesting to notice that in the situation just described it follows from a theorem of Ritt that

$$\sin \frac{\pi(z-r)}{p-1} \,\Big|\, \sum A_i(z)\exp(z \log \alpha_i)$$

in the ring of exponential polynomials. Thus the Lech-Mahler theorem implies that an exponential polynomial with infinitely many integer zeros is sinful.

Some technical remarks. It can be shown by means of specialisation (see [5]) that here and in the sequel there is no loss of generality nor any introduced degeneracy in supposing $\mathbb{K}$ to be an algebraic number field of degree d, say, over Q. In that case the embedding into Q_p is successful for primes p of a set P satisfying

$$\prod_{\substack{p \leq x \\ p \in P}} p^{\frac{1}{p-1}} \geq Cx^{1/d} \quad \text{with } C > 0.$$

A major benefit of p-adification is obtained from the following fact: *If* $g(t) = \sum x_h t^h$ *converges for* $\operatorname{ord}_p t > -s$, *say, and* $\Delta g(i) =: g(i+1)-g(i)$ *then*

$$\underline{\lim}\, k^{-1} \operatorname{ord}_p \Delta^k g(0) \geq s + 1/p-1 .$$

Indeed we are given $\underline{\lim}\, h^{-1} \operatorname{ord}_p x_h \geq s$. But

$$\Delta^k f(t) = \sum_{h \geq k} x_h \Delta^k t^h \quad \text{and} \quad \operatorname{ord}_p \Delta^k t^h \Big|_{t=0} \approx k/p-1$$

https://doi.org/10.1017/S0004972700021328 Published online by Cambridge University Press

We use this basic result as follows: it is not terribly difficult to see that (a_h) *is a recurrence sequence if and only if its Hankel-Kronecker determinants*

$$K_h a := \left| a_{i+j} \right|_{0 \le i,j < h}$$

vanish for all sufficiently large h. But from elementary row and column operations one sees that

$$K_h a = \left| \Delta^k a_{\bar{o}(p-1)+r} \right|_{i+j=k(p-1)+r} \ .$$

So if $a_{t(p-1)+r}$ is given by p-adic power series converging beyond the p-adic unit disc we can show that $K_h a$ is divisible by a high power of p (that is, is of high p-adic order).

3. Hadamard division

If $\sum a_h X^h$, $\sum b_h X^h$ are rational then their 'child's product' $\sum (a_h b_h) X^h$ is again rational; for $(a_h), (b_h)$ are given by generalised power sums whence so is (c_h), $c_h = a_h b_h$. The product above is frequently spoken of as the *hadamard product* of the power series. We wish to consider the hadamard quotient of rational functions. Polya [4] showed that *if* $\sum h a_h X^h$ *is rational, and the* a_h *all are integers* (more generally, elements of a finitely generated subring R of $\mathbb{K}$) *then* $\sum a_h X^h$ *is rational.* Ultimately we have the theorem of Polya-Cantor [3] *: if* f *is a polynomial and* $\sum f(h) a_h X^h$ *is rational with the* a_h *all in* R*, then* $\sum a_h X^h$ *is rational.* The integrality condition is necessary: $\sum (h+1)^{-1} X^{h+1}$ is not rational, but it is the hadamard quotient of $\sum X^{h+1} = X(1-X)^{-1}$ *by* $\sum (h+1) X^{h+1} = X(1-X)^{-2}$.

We sketch a proof of the:

HADAMARD QUOTIENT THEOREM. *Suppose* $\sum c_h X^h$, $\sum b_h X^h$ *are Taylor expansions of functions rational over* $\mathbb{K}$ *and that there is a sequence*

(a_h') of elements of R so that $a_h' b_h = c_h$, $h \geq 0$. Then there is a rational function $\sum a_h X^h$ with $a_h b_h = c_h$, $h \geq 0$.

Proof. We p-adify and consider quotients

$$a(t(p-1)+r) = c(t(p-1)+r)/b(t(p-1)+r)$$

of p-adic exponential polynomials. If b is of order n then b has at most n zeros in the disc with $\text{ord}_p t > -1/n$. Hence for each $r : 0 \leq r < p-1$ there is a polynomial $f_{p,r}$ of degree at most n so that $f_{p,r}(t(p-1)+r)a(t(p-1)+r)$ converges for t with $\text{ord}_p t \geq -1/n$. The same holds for $f_p(t(p-1)+r)a(t(p-1)+r)$ if f_p is the lowest common multiple of the $f_{p,r}$; we note that f_p has degree at most $n(p-1)$.

Consider

$$K_H(f_p a) = \left| f_p(i+j)a(i+j) \right|_{0 \leq i,j < H} .$$

We have shown that

$$\underline{\lim}\, H^{-2} \text{ord}_p K_H(f_p a) \geq (\tfrac{1}{n} + \tfrac{1}{p-1})/p-1$$

so, say with H sufficiently large:

$$\text{ord}_p K_H (f_p a) > \frac{H^2}{n(p-1)} .$$

But to obtain this result we use only that

$$\text{ord}_p \Delta^k f_p(\overline{o}(p-1)+r)a(\overline{o}(p-1)+r) \geq k(\tfrac{1}{n} + \tfrac{1}{p-1})/p-1$$

with $k(p-1)+r \leq 2H$. Thus if we were to have truncated the coefficients of the f_p modulo

$$M(p;H) = p^{2H(\frac{1}{n} + \frac{1}{p-1})/(p-1)^2}$$

we would obtain the desired inequality for $\text{ord}_p K_H(f_p a)$.

However once coefficients are so truncated the f_p become elements of $\mathbb{Z}[X]$ with coefficients not exceeding $M(p;H)$. By the Chinese Remainder Theorem we may construct a polynomial f in $\mathbb{Z}[X]$ with coefficients not exceeding

$$M := M(H) = \prod_{p \in P} M(p;H)$$

so that f plays the role of f_p, each $p \in P$. The degree of f is at most

$$\max_{p \in P} n(p-1) .$$

To avoid the somewhat clumsy and naive notion of 'truncation' we can equivalently describe f as being so constructed as to satisfy

$$\|f - f_p\|_p \leq M(p;H)^{-1} ,$$

$p \in P$, thereby transforming our appeal to the Chinese Remainder Theorem to an appeal to the approximation theorem; here $\| \ \|_p$ is the valuation of the maximum of the coefficients.

As constructed, the polynomial f has coefficients that are far too large and degree that is uneconomically small. Fortunately the following is plain: if f_0 be any non-zero polynomial in $\mathbb{Z}[X]$ then the remarks above, to wit that

$$\text{ord}_p K_h(f\alpha) > h^2/n(p-1) , H_0 < h \leq H, p \in P$$

remain true with f replaced by $F = f_0 f$. Accordingly we now appeal to the box-principle to choose f_0 so as to obtain F with reasonably small coefficients and degree not too large. To see that we may replace f by F we need only recall that each f_p might have been replaced by a multiple of itself.

Select f_0 of degree $N = c_1 H^{\frac{1}{2}}(\log H)^{-\frac{1}{2}}$. Here and in the immediate sequel $c_0, c_1, \ldots$ denote positive constants and H is supposed large with respect to the prevailing parameters n and $p \in P$. Modulo M there are some M^N possibilities to choose f_0. We want $F = f_0 f$ to have coefficients no larger in absolute value than $M^{c_0/N}$, modulo M of course. Accordingly our 'boxes' each contain polynomials F with coefficients differing modulo M by no more than $M^{c_0/N}$. With c_0 appropriately large (not depending on H) there are fewer than M^N such boxes. Hence our construction succeeds and we have

$$\text{ord}_p\, K_h(Fa) > h^2/n(p-1) \qquad H_0 < h \leq H,\ p \in P$$

with F of degree $cH^{\frac{1}{2}}(\log H)^{-\frac{1}{2}}$ and with coefficients not exceeding $M^{c_0/N}$ in absolute value. A priori H_0 need only be large enough to validate the p-adic inequalities. It certainly suffices to set $H_0 = H^{\frac{1}{2}} \log H$.

We now need a suitable archimedean upper bound for the algebraic numbers $K_h(Fa)$.

Technical remark. The correct measure of the size of a sequence of algebraic numbers is provided by Bombieri [1] p. 37 in his discussion of G-functions. Since the a_h belong to a finitely generated subring R of K the sequence (a_h) has finite size ρ, say. For us it is convenient to define

$$\sigma_h(a) = \sum_v \max_{j\leq h} |a_j|_v$$

with the sum the appropriately normalised valuations v of $\mathbb{K}$. Then

$$\sigma(a) = \overline{\lim}_{h\to\infty} h^{-1} \log \sigma_h(a) = \log \rho \quad .$$

It then follows that

$$\overline{\lim}_{h\to\infty} h^{-2} \log \sigma_h(K(a)) = \log \rho \quad .$$

Then with the F chosen as above we obtain

$$\log \sigma_h\,(K(Fa)) < h^2 \log \rho + c_2 h\, H^{\frac{1}{2}} (\log H)^{\frac{1}{2}}$$

But for $H_0 < h \leq H$ and $p \in P$

$$\operatorname{ord}_p K_h(Fa) > h^2/n(p-1) .$$

Hence if $H_0 = H^{\frac{1}{2}} \log H$ then for $H_0 < h < H$ we have

$$h^{-2} \log \sigma_h(K(Fa)) < \log \rho + c_3(\log H)^{-\frac{1}{2}}$$

But by the product formula $K_h(Fa)$ vanishes if

$$\sum_p (\log p) \operatorname{ord}_p K_h(Fa) > d \log \sigma_h(K(Fa)) .$$

Indeed it is this formula that justifies the measure σ_h we have introduced above.

We can now return to the main argument. From the remarks above we see that $K_h(Fa) = 0$ for $H^{\frac{1}{2}} \log H < h < H$ if

$$\sum_{p \in P} \frac{\log p}{n(p-1)} > d \log \rho + dc_3(\log H)^{-\frac{1}{2}} .$$

We note that though c_3 depends on P it remains bounded if P grows, hence since the sum over $p \in P$ is unbounded as P grows we can certainly achieve the condition above for a suitably large choice of the set P.

The vanishing of $K_h(Fa)$ for $H^{\frac{1}{2}} \log H < h < H$ implies readily that there is a recurrence sequence (d_h) of order at most $H^{\frac{1}{2}} \log H$ so that

$$d_h = F(h)a_h = F(h)c_h/b_h$$

for $H^{\frac{1}{2}} \log H < h < H$. But the recurrence sequences $(b_h d_h)$ and $(F(h)c_h)$ then coincide over a range considerably greater than is their order. Hence they coincide for all h. It follows that F divides bd in the ring of exponential polynomials. By the Polya-Cantor lemma we lose no generality in assuming that b has no polynomial factor; for any such factor must also be a factor of c and so we may suppose it to have been removed. Hence F divides d in the ring of exponential polynomials, for the quotient satisfies the conditions of the Polya-Cantor lemma. Hence, as we wished to show, (a_h) is indeed a recurrence sequence.

To complete the proof we should deal with the case where some b_h vanish and with the general case where (a_h) is not defined over an algebraic number field. These technicalities seem inappropriate to this summary.

4. Concluding Remarks

The p-adic methods employed above were either introduced or flowered in the work of Kurt Mahler. It seems especially appropriate to describe a recent application of his ideas on this the occasion of his 80th birthday.

References

[1] E. Bombieri, "On G-functions", in H. Halberstam and C. Hooley (eds.) *Recent Progress in Analytic Number Theory* (Academic Press, 2, 1981, 1-67).

[2] J.W.S. Cassels, "An embedding theorem for fields", *Bull. Austral. Math. Soc.* 14 (1976), 193-198. Addendum, ibid. 14 (1976), 479-480.

[3] D.G. Cantor, "On arithmetic properties of the Taylor series of rational functions II", *Pacific J. Math.* 41 (1972), 329-334.

[4] G. Polya, "Arithmetische Eigenschaften der Reihenentwicklungen rationaler Functionen", *J. für die reine u. angew Math.* 151 (1920), 1-31.

[5] A.J. van der Poorten and H.P. Schlickewei, "The growth conditions for recurrence sequences", *Invent. Math.*, to appear.

School of Mathematics and Physics,
Macquarie University,
North Ryde,
New South Wales 2113,
Australia.

https://doi.org/10.1017/S0004972700021328 Published online by Cambridge University Press