*J. Austral. Math. Soc.* (*Series A*) **43** (1987), 314–327

# A NOTE ON THE HADAMARD $k$TH ROOT OF A RATIONAL FUNCTION

**ROBERT S. RUMELY and A. J. van der POORTEN**

(Received 12 December 1985; revised 30 September 1986)

Communicated by J. H. Loxton

**Abstract**

Suppose the sequence of Taylor coefficients of a rational function $f$ consists of $k$th powers of elements all belonging to some finitely generated extension field $F$ of $\mathbf{Q}$. Then it is a generalisation of a conjecture of Pisot that there is a rational function with Taylor coefficients term-by-term $k$th roots of those of $f$. The authors show that it suffices to prove the conjecture in the case that the field of definition is a number field and prove the conjecture in that case subject to the constraint that $f$ has a dominant pole, that is, that there is a valuation with respect to which $f$ has a unique pole either of maximal or of minimal absolute value.

1980 *Mathematics subject classification* (*Amer. Math. Soc.*): 10 A 35.

## 1. Introduction

Let $r$, $s$ be polynomials defined over $\mathbb{C}$ with $\deg r < \deg s = n$, and $s(0) \neq 0$. Consider the Taylor expansion

$$\frac{r(X)}{s(X)} = \sum_{h \geqslant 0} b_h X^h$$

The first author was supported in part by a Sloan Foundation and by NSF grant MCS 8201792. This work, and the first author's visit to Macquarie University which initiated the collaboration, was supported in part by ARGS grants B7915731 and B8215893.

and suppose that there is a sequence $(a'_h)$ of e lements of a finitely generated extension field $\mathbb{F}$ of $\mathbb{Q}$ so that $a'^k_h = b_h$, $h = 0, 1, 2, \ldots$, for some given positive integer $k$. Then it is (a generalisation of) a conjecture of Pisot, see [2], page 249 and also [3], [4], that there is a sequence $(a_h)$ so that $a_h^k = b_h$, $h = 0, 1, 2, \ldots$, and $\Sigma_{h \geqslant 0} a_h X^h$ is a rational function.

Without loss of generality we may set

$$s(X) = 1 - s_1 X - s_2 X^2 - \cdots - s_n X^n = \prod_{i=1}^{m} (1 - \beta_i X)^{n_i}$$

with the *roots* $\beta_i$ distinct non-zero complex numbers and the *multiplicities* $n_i$ positive integers. Except perhaps if $r(X)$, $s(X)$ have common factors, the $\beta_i$ are just the reciprocals of the poles of the given rational function. The $\beta_i$ are of course elements of some finitely generated extension field of $\mathbb{Q}$; by extending $\mathbb{F}$ if necessary we may suppose that the $\beta_i$ belong to $\mathbb{F}$.

We prove Pisot's conjecture in the following special case: $\mathbb{F}$ is a number field, and there is a valuation of $\mathbb{F}$ so that the given rational function has a unique pole either of maximal, or of minimal, absolute value with respect to that valuation. We also show that to prove Pisot's conjecture in general it suffices to deal with the algebraic case but without the dominant pole condition.

Our result generalises that of Pisot [8] in which the unique pole must be minimal, and of multiplicity one (and the given sequence of $k$th roots $(a'_h)$ is a sequence of rational integers); see also the remarks in [4]. Perelli and Zannier [7] show that the restriction on multiplicity may be removed, but they require the $\beta_i$ to be positive rational integers; so unique minimality becomes trivial. The allegation in [11] that Pisot's conjecture is accessible in general is quite unfounded. An example of Cantor [6] shows that our condition is restrictive.

## 2. Recurrence sequences and exponential polynomials

Though we speak of Hadamard operations on rational functions, that is of transformations $f$ taking a Taylor expansion $\Sigma b_h X^h$ to $\Sigma f(b_h) X^h$, our present problem concerns generalised power sums (or exponential polynomials). Briefly,

$$\frac{r(X)}{s(X)} = \sum_{h \geqslant 0} b_h X^h$$

implies

$$b_{h+n} = s_1 b_{h+n-1} + \cdots + s_n b_h, \qquad h = 0, 1, 2, \ldots,$$

https://doi.org/10.1017/S144678870002961X Published online by Cambridge University Press

so the sequence $(b_h)$ is a *recurrence sequence*. Plainly, if $E$ denotes the operator $E: f(h) \mapsto f(h+1)$ then the sequence $(b_n)$ is annihilated by the difference operator $\prod_{i=1}^{m}(E-\beta_i)^{n_i}$. It is easily verified that the kernel of this operator consists of generalised *power sums*

$$b_h =: b(h) = \sum_{i=1}^{m} B_i(h)\beta_i^h, \qquad h = 0, 1, 2, \ldots,$$

where the coefficients $B_i$ are polynomials of degree respectively at most $n_i - 1$, $(1 \leqslant i \leqslant m)$. Alternatively, a partial fraction expansion

$$\frac{r(X)}{s(X)} = \sum_{i=1}^{m} \sum_{j=1}^{n_i} \frac{r_{ij}}{(1-\beta_i X)^j} = \sum_{h \geqslant 0} \sum_{i} \sum_{j} r_{ij} \binom{h+j-1}{j-1} \beta_i^h X^h,$$

yields the same conclusion.

A power sum, or recurrence sequence, is just an exponential polynomial

$$b(t) = \sum_{i=1}^{m} B_i(t)\exp(t \log \beta_i)$$

with its domain restricted to the non-negative integers.

## 3. A conditional proof of the theorem

We shall prove the main result subject to the following special conditions:

(i) The given power sum

$$b_h = b(h) = \sum_{i=1}^{m} B_i \beta_i^h, \qquad h = 0, 1, 2, \ldots,$$

is defined over an algebraic number field $\mathbb{K}$, of degree $[\mathbb{K}:\mathbb{Q}]$ over $\mathbb{Q}$. That is: the roots $\beta_i$ and the coefficients $B_i$ are elements of $\mathbb{K}$. Moreover the power sum takes values that are $k$th powers of elements of $\mathbb{K}$; we write $b_h \in \mathbb{K}^k$.

(ii) The coefficients $B_i$ of the power sum are constants. Moreover, by extending $\mathbb{K}$, if necessary, we may suppose that the roots $\beta_i$ and the coefficients $B_i$ are in $\mathbb{K}^k$.

(iii) There is an absolute value, say $|\ |$, of $\mathbb{K}$ so that

$$|\beta_1| > |\beta_2| \geqslant \cdots \geqslant |\beta_m|.$$

PROPOSITION 1. *Given a recurrence sequence* $(b_h)$ *as described above, there is a recurrence sequence* $(a_h)$ *so that* $a_h^k = b_h$, $h = 0, 1, 2, \ldots$.

PROOF. Set $c_h = b_h / B_1 \beta_1^h$ and note that $(c_h)$ satisfies the conditions of the proposition.

https://doi.org/10.1017/S144678870002961X Published online by Cambridge University Press

Note that there is an $s \geqslant 1$ so that for all $l = 0, 1, 2, \ldots$

$$\left|\binom{1/k}{l}\right| \leqslant s^l$$

(with $s > 1$ only if the valuation $|\ |$ is nonarchimedean and $|k| < 1$). Write $c_h := 1 + r_h$, $h = 0, 1, 2, \ldots$, noting, that there is a $\delta > 0$ so that $\log s|r_h| < -h\delta$ for all sufficiently large $h$. We have

$$c_h^{1/k} = 1 + \binom{1/k}{1} r_h + \binom{1/k}{2} r_h^2 + \cdots + \binom{1/k}{n} r_h^n + R_h(h)$$

and

$$|R_n(h)| \leqslant \sum_{l=n+1}^{\infty} \left|\binom{1/k}{l} r_h^l\right| \leqslant \sum_{l=n+1}^{\infty} \left(s|r_h|\right)^l$$
$$= \left(s|r_h|\right)^{n+1} \frac{1}{1 - |r_h|},$$

so for $h$ and $n$ sufficiently large $\log|R_n(h)| < -hn\delta$. But

$$\left(\sum_{i=0}^{n} \binom{1/k}{i} r_h^i\right)$$

is a recurrence sequence because $(r_h)$ is a recurrence sequence. Say it is annihilated by the difference operator $F_n(E)$; of course this operator depends only on $n$, not on $h$. We have

$$F_n(E) c_h^{1/k} = F_n(E) R_n(h).$$

But $F_n(E)$ is a polynomial in $E$ defined over $\mathbb{K}$. Hence $F_n(E)c_h^{1/k}$ is an element of $\mathbb{K}$ for each $h = 0, 1, 2, \ldots$ . Now as $h \to \infty$

$$\limsup h^{-1} \log|F_n(E) R_n(h)| \leqslant -n\delta$$

while the height $\|F_n(E)c_h^{1/k}\|$ satisfies

$$\limsup h^{-1} \log\|F_n(E) c_h^{1/k}\| \leqslant A,$$

for some constant $A$ depending only on $k$ and the given sequence $(b_h)$.

Here, by definition, for a nonzero element $\lambda$ in a finite extension $L$ of $\mathbb{Q}$, one writes

$$\|\lambda\| = \exp\left\{([L:\mathbb{Q}])^{-1} \sum_v \max(0, \log|\lambda|_v)\right\}$$

with the sum taken over the normalised absolute values corresponding to all places of $L$ (see [5], pages 4–5, but note that we use $\|\ \|$ in place of $h(\ )$, that notation already being committed). Observe that it is consistent to set $\|0\| = 1$. By the hypothesis that $c_h^{1/k}$ is in $\mathbb{K}$ for every $h$ we can compute the heights of the

https://doi.org/10.1017/S144678870002961X Published online by Cambridge University Press

numbers $F_n(E)c_h^{1/k}$ using the places of $\mathbb{K}$. Now $F_n(E)$ is a fixed polynomial of degree $N$, say; while $c_h$ is a generalised power sum, so that in particular there are only finitely many places $v$ for which $|c_h|_v > 1$ for any $h$. Furthermore, at those places $\log|c_h|_v$ has at most linear growth in $h$. Thus we have at most geometric growth in $h$ for $\|c_h^{1/k}\|$ and hence for $\|F_n(E)c_h^{1/k}\|$ at these places. To summarise, there is a finite set $S$ of places of $\mathbb{K}$ and for each $v \in S$ a constant $A_v > 1$ such that for all large $h$

$$\left|F_n(E)c_h^{1/k}\right|_v \leqslant A_v^{h+N} \quad \text{if } v \in S; \qquad \left|F_n(E)c_h^{1/k}\right|_v \leqslant 1 \quad \text{if } v \notin S.$$

From this the existence of the constant $A$ is plain. By Liouville's inequality (the fundamental lemma of transcendence theory) [5], page 5, whereby $\lambda \in L$ either vanishes or

$$\operatorname{Log}|\lambda| > -[L:\mathbb{Q}]\operatorname{Log}\|\lambda\|,$$

we have either $F_n(E)c_h^{1/k} = 0$ for all sufficiently large integers $h$, or

$$-n\delta > -[\mathbb{K}:\mathbb{Q}]A.$$

But that inequality is false for large $n$. Hence $F_n(E)$ annihilates the sequence $(c_h^{1/k})$, so that sequence is a recurrence sequence, and then so is $((B_1\beta_1^h c_h)^{1/k})$ as alleged.

That this argument 'works' may seem mysterious. Liouville's inequality is just the generalisation to number fields of the observation that a rational integer of absolute value less than one vanishes. Otherwise, we are seeing the phenomenon instanced by

$$\begin{aligned}(1 + 2x + x^2)^{1/2} &= 1 + \tfrac{1}{2}(2x + x^2) - \tfrac{1}{8}(2x + x^2)^2 + \tfrac{1}{16}(2x + x^2)^3 - \cdots \\ &= 1 + x\end{aligned}$$

with the 'remainder' after any truncation of the expansion containing only high powers of $x$.

The rest of this note is dedicated to showing that the conditions we have placed on the sequence $(b_h)$ lose less generality than may appear.

## 4. Maxima to minima

PROPOSITION 2. *Suppose $(b_h)$ is a recurrence sequence such that, for all $h \geqslant 0$, $b_h$ is the kth power of an element in an algebraic number field $\mathbb{K}$. Then there is a finite extension $\mathbb{L}$ of $\mathbb{K}$ so that for each $h$ in $\mathbb{Z}$, $b(h) := b_h$ is the kth power of an element of $\mathbb{L}$. Thus $(b_{-h})$ is a recurrence sequence of kth powers of elements of $\mathbb{L}$.*

https://doi.org/10.1017/S144678870002961X Published online by Cambridge University Press

PROOF. Let $T$ be some finite set of primes of $\mathbb{K}$ including all archimedean primes, all primes at which a root $\beta_i$ of the power sum $b(h)$ is not a unit or a coefficient of a $B_i$ is non-integral, and all primes dividing $k$.

Denote by $\mathbb{K}_v$ the completion of $\mathbb{K}$ at the prime $v$. We claim that for $v \notin T$ we have $b(h) \in \mathbb{K}_v^k$ for all $h \in \mathbb{Z}$.

To see this set $q = \sharp\mathbb{F}_v$ where $\mathbb{F}_v$ is the residue class field of $\mathbb{K}$ at $v$, and denote by $\mathfrak{p}_v$ the prime ideal at $v$.

Fix $h \in \mathbb{Z}$, and suppose $\operatorname{ord}_v b(h) = s$: note $s \geqslant 0$, as $v \notin T$; thus $b(h) \equiv 0 \bmod \mathfrak{p}_v^s$. Let $l$ be an integer satisfying $l \equiv 0 \bmod q^{(2s+1)}(q-1)$. Then

$$B_i(h+l) \equiv B_i(h) \bmod \mathfrak{p}_v^{2s+1}, \qquad \beta_i^l \equiv 1 \bmod \mathfrak{p}_v^{2s+2} \qquad (1 \leqslant i \leqslant m).$$

Hence $b(h+l) \equiv b(h) \bmod \mathfrak{p}_v^{2s+1}$, so

$$\frac{b(h+l)}{b(h)} \equiv 1 \bmod \mathfrak{p}_v^{s+1}.$$

But $s+1 > 0$. So the quotient is certainly in $\mathbb{K}_v^k$. Moreover if $l > 0$ is sufficiently large then $h + l$ is non-negative so, by hypothesis $b(h+l) \in \mathbb{K}_v^k$. Hence $b(h) \in \mathbb{K}_v^k$ for all $h$ in $\mathbb{Z}$ as we alleged.

We are indebted to a referee for advising us that we might have argued as follows: For suitable subsequences, $h \mapsto b(l + hr)$ is a uniformly continuous function on $\mathbb{Z}_p$. As $\mathbb{K}_v^k$ is complete and $b(l+hr)$ is in $\mathbb{K}_v^k$ for all $h \in \mathbb{N}$, and $\mathbb{N}$ is dense in $\mathbb{Z}_p$, it follows that $b(l+hr)$ is in $\mathbb{K}_v^k$ for all $h$ in $\mathbb{Z}$.

We have this for all $v \notin T$. By the Grünwald-Wang Theorem as detailed in [1], pages 82–83, 93ff, in any event we have then

$$b(h) \in \mathbb{K}^k \cup \alpha_0 \mathbb{K}^k$$

with, at worst, $\alpha_0 \in \mathbb{K}^{k/2}$. Hence taking $\mathbb{L} = \mathbb{K}(\alpha_0^{1/2})$ allows us to conclude that $b(h) \in \mathbb{L}^k$ for all $h \in \mathbb{Z}$. Of course we lose no generality in presuming that in the first place we chose $\mathbb{K} = \mathbb{L}$.

The point of this result is that we may now apply Proposition 1 if the power sum $b(h)$ has a unique minimal root: $|\beta_1| < |\beta_2| \leqslant \cdots \leqslant |\beta_m|$, say. For then $b(-h)$ has a unique maximal root as is required by condition (iii) of the Proposition, and its other properties are retained.

## 5. Obtaining constant coefficients

PROPOSITION 3. *Suppose $b(h)$ is a generalised power sum taking values in $\mathbb{K}^k$. Then there are generalised power sums $u(h)$ and $\mathfrak{b}(h)$ taking values in $\mathbb{K}$, such that*

$$b(h) = u(h)^k \mathfrak{b}(h)$$

*and such that $\mathfrak{b}(h)$ has constant coefficients (and takes values in $\mathbb{K}^k$).*

https://doi.org/10.1017/S144678870002961X Published online by Cambridge University Press

PROOF. The gist of the argument below is that in a generalised power sum with polynomial coefficients, the coefficients may be shown to behave independently of the pure exponential terms. It is a generalisation of a proof of Perelli and Zannier [7], pages 13–15. It has been subsequently drawn to our attention that Proposition 3 was proved by J. P. Bézivin [3] by a different $p$-adic method.

We begin with an auxiliary computation. Recall that $b(h) = \sum B_i(h)\beta_i^h$; write

$$B_i^{(s)}(h) = \left(\frac{d}{dh}\right)^{(s)} B_i(h).$$

Let $\mathfrak{p} = \mathfrak{p}_v$ be a prime ideal not in $T$ (as in the previous section), such that the rational prime $p$ below $\mathfrak{p}$ is unramified in $\mathbb{K}$ and satisfies $p > k$. Let $q = \sharp F_v$ as before. Suppose $h$ is an integer for which $\mathfrak{p} | b(h)$. We claim that

$$\sum B_i^{(s)}(h)\beta_i^h \equiv 0 \bmod \mathfrak{p}; \qquad s = 0, 1, \ldots, k-1. \tag{1}$$

To show this, we introduce a new variable $t$ and, fixing $h$, consider the $p$-adic Taylor expansion

$$\begin{aligned} b(h + tp(q-1)) &= \sum B_i(h + tp(q-1))\beta_i^h \exp\left(tp \log \beta_i^{q-1}\right) \\ &= b(h) + \frac{tp}{1!}\left[(q-1)\sum B_i'(h)\beta_i^h + \sum B_i(h)\beta_i^h\left(\log \beta_i^{q-1}\right)\right] \\ &\quad + \frac{t^2p^2}{2!}\left[(q-1)^2\sum B_i''(h)\beta_i^h + 2(q-1)\sum B_i'(h)\beta_i^h\left(\log \beta_i^{q-1}\right)\right. \\ &\qquad \left. + \sum B_i(h)\beta_i^h\left(\log \beta_i^{q-1}\right)^2\right] \\ &\quad + \cdots \end{aligned}$$

which converges at least when $\operatorname{ord}_p(t) > -(1 - 1/p)$. For brevity, write

$$c_s(h) = \frac{1}{s!}\sum_{k=0}^{s}\binom{s}{k}(q-1)^{s-k}\sum_i B_i^{(s-k)}\sum_i B_i^{(s-k)}(h)\beta_i^h\left(\log \beta_i^{q-1}\right)^k$$

so

$$b(h + tp(q-1)) = c_0(h) + tpc_1(h) + \cdots + t^{k-1}p^{k-1}c_{k-1}(h) \mod \mathfrak{p}^k.$$

Our supposition $\mathfrak{p} \mid b(h)$ yields $c_0(h) \equiv 0 \bmod \mathfrak{p}$. Suppose we have already shown that, for some $s < k$.

$$c_j(h) \equiv 0 \bmod \mathfrak{p}^{s-j} \qquad (j = 0, 1, \ldots, s-1).$$

The hypothesis $b(h) \in \mathbb{K}^k$ means that in fact $\mathfrak{p}^k \mid b(h)$. Furthermore for $t \in \mathbb{Z}$

$$b(h + tp(q-1)) \equiv b(h) \bmod \mathfrak{p}$$

so similarly $\mathfrak{p}^k \mid b(h + tp(q-1))$. Setting

$$d_j(h) = c_j(h)p^{-(s-j)} \qquad (j = 0, \ldots, s),$$

we obtain

$$b(h + tp(q-1)) \equiv 0 \equiv \left(d_0(h) + td_1(h) + \cdots + t^s d_s(h)\right)p^s \mod \mathfrak{p}^{s+1}.$$

https://doi.org/10.1017/S144678870002961X Published online by Cambridge University Press

On the right we have a polynomial of degree $s < p$ in $t$, vanishing for all $t \bmod \mathfrak{p}$. Hence it vanishes identically mod $\mathfrak{p}$, and by induction we have

$$c_j(h) \equiv 0 \bmod \mathfrak{p}^{k-j} \qquad (j = 0, 1, \ldots, k-1). \tag{2}$$

Note that $\operatorname{ord}_{\mathfrak{p}}(\beta_i^{q-1} - 1) \geqslant 1$, so $\operatorname{ord}_{\mathfrak{p}}(\log \beta_i^{q-1}) \geqslant 1$, $(i = 1, \ldots, m)$. Hence, examining the formula defining $c_s(h)$, we see that (2) yields the claim (1).

Consider the subgroup of $\mathbb{K}^\times$ generated multiplicatively by the roots $\beta_1, \ldots, \beta_m$. By the structure theorem for finitely generated abelian groups, this is isomorphic to $\mathbf{Z}/d \times \mathbf{Z}^n$ for some $d$ and $n$. In order to prove the existence of the decomposition

$$b(h) = u(h)^k \mathfrak{b}(h)$$

it suffices to prove it separately on each arithmetic progression $h \equiv r \bmod d$. Thus, without loss of generality we can assume that $\langle \beta_1, \ldots, \beta_m \rangle$ is free. Let $\omega_1, \ldots, \omega_s$ be a set of independent generators.

In the sequel $h$ denotes, so to speak, a generic integer and the variable with which we mainly work is $t$. However, the proof involves a delicate interplay of viewing $h$ and $t$ alternately as variable and as constant. Taking $h$ as an indeterminate in $\mathbf{Z}$, let $E_h$ be the ring of all generalised power sums with coefficients in $\mathbb{K}$ and roots in the group generated by $\beta_1, \ldots, \beta_m$:

$$E_h = \mathbb{K}\left[h, \omega_1^h, \omega_1^{-h}, \omega_2^h, \omega_2^{-h}, \ldots, \omega_s^h, \omega_s^{-h}\right]$$

Especially, $b(h) \in E_h$. Since $\omega_1, \ldots, \omega_s$ are multiplicatively independent, and since the values of a generalised power sum completely determine its roots and its coefficients, the functions $h, \omega_1^h, \ldots, \omega_s^h$ are algebraically independent. Thus, $E_h$ is isomorphic to the localisation of a polynomial ring $\mathbb{K}[h, X_1, \ldots, X_s]$ with respect to the multiplicative set generated by $X_1, \ldots, X_s$. Now, any localisation of a unique factorisation domain is again such a domain. Thus, $E_h$ is a *UFD*. Let $G_h$ be its quotient field.

Our proof of the existence of the decomposition of $b(h)$ involves an obscured version of the well-known result that a polynomial (here in $G_h[t]$) taking $k$th power values, is the $k$th power of a polynomial. Consider the function

$$f_h(t) := \sum_{i=1}^{m} B_i(h - t)\beta_i^h$$

as a polynomial in $t$ with coefficients in $E_h$. We allege that each zero of $f_h(t)$ has multiplicity at least $k$.

Suppose $g_h(t)$ is an irreducible factor of $f_h(t)$ in $G_h[t]$. Clearing denominators, we lose no generality in assuming $g_h(t) \in E_h[t]$. Either $\{g_h(t)\}^k$ divides $f_h(t)$, or the set of polynomials $g_h, f_h, f_h', \ldots, f_h^{(k-1)}$ is relatively prime. In the latter case there is a linear combination over $G_h[t]$ of these polynomials summing to 1.

https://doi.org/10.1017/S144678870002961X Published online by Cambridge University Press

Again clearing denominators we obtain a linear combination over $E_h[t]$ summing to a nonzero constant $c_h \in E_h$:

$$c_h = x_h(t)g_h(t) + \sum_{s=0}^{k-1} y_{h,s}(t)f_h^{(s)}(t).$$

Now fix $h$, and note that elements of $E_h$, evaluated at $h$, belong to $\mathbb{K}$. Thus, for this $h$, we may regard $c_h$ as an element of $\mathbb{K}$ and the equation above as an identity of polynomials in $\mathbb{K}[t]$. There are only a finite number of primes of $\mathbb{K}$ at which some coefficient in the equation is non-integral. However, as $t$ runs through $\mathbb{Z}$, we have $\mathfrak{p} \mid g_h(t)$ for infinitely many distinct admissible $\mathfrak{p}$. Fix such a $\mathfrak{p}$ and $t$, taking $\mathfrak{p}$ so that all the coefficients are integral. Since $g_h \mid f_h$, also $\mathfrak{p} \mid f_h(t)$. We claim that $\mathfrak{p} \mid f_h^{(s)}(t)$ for $s = 0, 1, \ldots, k-1$. For any $s$,

$$\begin{aligned} f_h^{(s)}(t) &= (-1)^s \sum B_i^{(s)}(h-t)\beta_i^h \\ &\equiv (-1)^s \sum B_i^{(s)}(h + t(q-1))\beta_i^{h+t(q-1)} \mod \mathfrak{p}. \end{aligned}$$

For $s = 0$, this is $f_h(t) \equiv b(h + t(q-1)) \bmod \mathfrak{p}$, which shows that $\mathfrak{p} \mid b(h + t(q-1))$. Now applying (1) with $h$ replaced by $h + t(q-1)$ gives the claim.

It follows that $\mathfrak{p} \mid c_h$. Since this is true for infinitely many $\mathfrak{p}$, $c_h = 0$. We now again regard $h$ as a variable, and note that $c_h \in E_h$ is a generalised power sum whose value for each $h$ is 0. It is therefore the zero power sum, that is, $c_h = 0$ in $E_h$. This is a contradiction, and we conclude that $\{g_h(t)\}^k \mid f_h(t)$.

We complete our argument by descent on the degree in $t$ of the polynomial $f_h$. We note that the quotient

$$f_h(t)/\big(f_h(t), f_h'(t)\big)$$

(computed in $G_h(t)$) has distinct zeros. Hence its $k$th power divides $f_h(t)$. Clearing denominators, there are thus a polynomial $u_h(t) \in E_h[t]$ of positive degree, and an element $v_h \in E_h$, so that

$$v_h^k f_h(t) = \{u_h(t)\}^k \mathfrak{f}_h(t)$$

with $\mathfrak{f}_h(t) \in E_h[t]$ and $\mathfrak{f}_h$ of lower degree in $t$ then is $f_h$. But we may suppose $v_h = 1$. To see this recall that $E_h$ is a *UFD*, which implies that $E_h[t]$ is a *UFD* (Gauss' lemma). Hence if

$$\bar{v}_h = \big(v_h, u_h(t)\big), \qquad \bar{\bar{v}}_h = v_h/\bar{v}_h$$

where the *GCD* is computed in $E_h[t]$, it follows that $u_h(t)/\bar{v}_h$ and $\mathfrak{f}_h(t)/\bar{\bar{v}}_h^k$ belong to $E_h[t]$. Thus after an appropriate change of notation:

$$f_h(t) = \{u_h(t)\}^k \mathfrak{f}_h(t).$$

But $\mathfrak{f}_h(0)$ is a generalised power sum, being an element of $E_h$, and it takes values in $\mathbb{K}^k$ by its construction. Furthermore

$$f_h(t) = \sum B_i(h-t)\beta_i^h$$

https://doi.org/10.1017/S144678870002961X Published online by Cambridge University Press

actually has the form of a polynomial in $h - t$ with coefficients in the ring $\mathbb{K}[\omega_1^h, \omega_1^{-h}, \ldots, \omega_s^h, \omega_s^{-h}]$. Any factorisation must preserve this property. Indeed, let $R$ be any unique factorisation domain, and take an irreducible polynomial $g(x) \in R[x]$. If there were a factorisation

$$g(h - t) = \prod_{i=1}^{r} g_i(h, t)$$

in $R[h, t]$, then on setting $t = 0$ it would follow for some $i$, say $i = 1$, that $g_1(h, 0)$ was an associate of $g(h)$ and in particular its degree in $h$ would be the same as $\deg g$. Now on the left side, the maximum total degree of any monomial is $\deg g$. If any factor on the right side besides $g_1(h, t)$ were nonconstant, the right side would contain a monomial with total degree greater than $\deg g$. Since this is impossible, $g(h - t)$ must be irreducible.

Thus $\mathfrak{f}_h(t)$ is a polynomial in $h - t$ and bears the same relation to $\mathfrak{f}_h(0)$ as $f_h(t)$ bears to $f_h(0)$, other than being of lower degree in $t$. Arguing by descent on the degree in $t$ we obtain the proposition once we recall $b(h) = f_h(0)$ and set $u(h) = u_h(0)$, $\mathfrak{b}(h) = \mathfrak{f}_h(0)$.

REMARK. If the generalised power sum $b(h)$ has a unique maximal root, it need not be the case that $\mathfrak{b}(h)$ has one; some of its roots may differ from others by $d$th roots by unity which appear when $\mathfrak{b}(h)$ is assembled from its restrictions to the various subsequences $h \equiv r \bmod d$.

However, its restriction to each of these subsequences will have a unique maximal root. Indeed, supppose the group $\mathscr{B} = \langle \beta_1, \ldots, \beta_m \rangle$ is free, with generators $\omega_1, \ldots, \omega_s$ as above. Note that the proof above shows that all the roots of $u(h)$ and $\mathfrak{b}(h)$ belong to $W$. Use the isomorhism $W \cong \mathbb{Z}^n$ to place a lexicographic ordering on $W$, and observe that multiplication respects this ordering. Let $X$ be the set of roots of $u(h)$ which are maximal under the given absolute value, and $Y$ the set of roots of $\mathfrak{b}(h)$ which are maximal. Let $x_1$ be the largest element of $X$ under the lexicographic ordering, and $y_1$ the largest element of $Y$. Then there is a unique term in the product $u(h)^k \mathfrak{b}(h)$ which has root $x_1^k y_1$. Similarly if $x_2 \in X$ and $y_2 \in Y$ are smallest, there is a unique term with root $x_2^k y_2$. Unless $X$ and $Y$ are both one-element sets, these would be two distinct roots of $b(h)$ of maximal absolute value, contrary to the hypothesis.

## 6. Specialisation

We shall show that the hypothesis that the given power sum $b(h)$ takes values in $\mathbb{K}^k$, with $\mathbb{K}$ an algebraic number field, loses no generality. Indeed suppose that $b(h)$ takes values in $\mathbb{F}^k$, with $\mathbb{F}$ some arbitrary finitely generated extension of $\mathbb{Q}$. Denote by $\mathbf{x} = (x_1, \ldots, x_t)$ a transcendence basis for $\mathbb{F}$ over $\mathbb{Q}$. Then $\mathbb{F} = \mathbb{Q}(\mathbf{x})[y]$

https://doi.org/10.1017/S144678870002961X Published online by Cambridge University Press

with $y$ algebraic over $\mathbb{Q}(\mathbf{x})$, say with defining polynomial

$$H(Y;\mathbf{x}) = H_0(\mathbf{x})Y^d + H_1(\mathbf{x})Y^{d-1} + \cdots + H_d(\mathbf{x}),$$

where the $H_i(\mathbf{x})$ are elements of $\mathbb{Z}[\mathbf{x}]$. Each element $\phi \in \mathbb{F}$ has a representation

$$\phi = \frac{U_\phi(y;\mathbf{x})}{V_\phi(\mathbf{x})}$$

as a quotient of polynomials $U_\phi(y;\mathbf{x}) \in \mathbb{Z}[y;\mathbf{x}]$, $V_\phi(\mathbf{x}) \in \mathbb{Z}[\mathbf{x}]$. Let $\Gamma$ be a finite set of elements of $\mathbb{F}$ with the property that $\gamma \in \Gamma$ and $\gamma \neq 0$ implies $\gamma^{-1} \in \Gamma$. Given the power sum $b(h) = \sum_{i=1}^{m} B_i(h)\beta_i^h$ we lose no generality in supposing that its roots $\beta_i$ and the coefficients of the $B_i(h)$ belong to $\mathbb{F}$. We shall ask that the set $\Gamma$ contains these elements as well as, say, the coefficients and discriminant of $H(Y,\mathbf{x})$. Next set

$$V_\Gamma(\mathbf{x}) = \prod_{\gamma\in\Gamma} V_\gamma(\mathbf{x}).$$

Let $\mathbf{c} = (c_1,\ldots,c_t)$ be any $t$-tuple of rational integers so that

$$V_\Gamma(\mathbf{c}) \neq 0.$$

Note that it is easy to see by induction on $t$ that there are infinitely many such $t$-tuples. The set $\Gamma$ generates a subdomain of $\mathbb{F}$, and the map induced by

$$\mathbf{x} = (x_1,\ldots,x_t) \mapsto \mathbf{c} = (c_1,\ldots,c_t)$$

maps such a domain into an algebraic number field $\mathbb{K}$, of degree at most $d$ over $\mathbb{Q}$. We refer to the map just described as an $\Gamma$-specialisation of $\mathbb{F}$. Note that, in particular, $y$ is mapped to $y(\mathbf{c})$, a zero of the polynomial $H(Y;\mathbf{c})$.

Suppose that we have shown that, for appropriate finite sets $\Gamma$, every $\Gamma$-specialisation of $(b_h)$ is the $k$th power of some recurrence sequence. In [9] we detail the argument required to demonstrate that there are infinitely many $\Gamma$-specialisation of the sequence $(b_h)$ which, if they have a $k$th root $(a_h)$, say, which is a recurrence sequence, have such a $k$th root of order bounded in terms of the order of $(b_h)$ alone; (that is to say; independent of the specialisation). The argument below deals with the additional difficulty created by the fact that the sequence $(b_h^{1/k})$ of $k$th roots is not well defined.

Recall that $(a_h)$ is a recurrence sequence of order at most $N$ if and only if its sequence $(\Delta_h(a))$ of Kronecker-Hankel determinants

$$\Delta_h = \Delta_h(a) = |a_{i+j}|_{0\leqslant i,\,j\leqslant h}$$

has the property: $\Delta_h = 0$ for $h = N,\ N+1,\ldots$ (see, for example, [10], pages 5–7). As noted in [9], Section 5, we may suppose that the specialisations to which we refer below are such as to preserve the order of the given recurrence sequence $(b_h)$.

https://doi.org/10.1017/S144678870002961X Published online by Cambridge University Press

We propose to consider sets $\{\Delta_h : h = N,\ N+1, \ldots, N+M-1\}$ with $M$ to be chosen below. Because the $k$th roots $b_h^{1/k}$ are ill-defined, there being $k$ possibilities for each (or $b_h = 0$), we are led to consider $k^{2(N+M)-1}$ sets of $\Delta_h$, one for each set of choices of the $2(N+M)-1$ sequential $k$th roots involved. But even then there are just a finite number of $\Delta_h$ to be considered, namely at most $Mk^{2(N+M)-1}$ quantities. Thus we may, without loss of generality, suppose that all these quantities belonged to $\Gamma$ from the outset. This supposition has the consequence that if an admissible specialisation of a $\Delta_h$ vanishes then that $\Delta_h$ vanishes (for if $\Delta_h \neq 0$ then both $\Delta_h$ and $\Delta_h^{-1}$ are in $\Gamma$, so if $\Delta_h \neq 0$ its $\Gamma$-specialisations cannot vanish).

By hypothesis at least one of the sets $\{\Delta_h : h = N,\ N+1, \ldots, N+M-1\}$ vanishes for infinitely many admissible $\Gamma$-specialisations (where, by 'admissible' we refer to those specialisations identified in [9] and referred to above). Suppose that the set is that determined by the $k$th roots $\{a_h : h = 0, 1, \ldots, 2(N+M-1)\}$.

Our hypothesis entails that $\Delta_h = |a_{i+j}|_{0 \leqslant i,\, j \leqslant h} = 0$ for $h = N,\ N+1, \ldots, N+M-1$. A study of the Kronecker-Hankel criterion reveals that there then is a recurrence sequence $(\mathfrak{a}_h)$ of order $N_o \leqslant N$, essentially coinciding with $(a_n)$ in the sense that, at least, $\mathfrak{a}_h = a_h$ for $N - N_0 \leqslant h \leqslant N+M-1$. Thus we have a recurrence sequence $(\mathfrak{a}_h)$ with $\mathfrak{a}_h^k = b_h$ for $N - N_0 \leqslant h \leqslant N+M-1$.

Now consider the sequence $(\mathfrak{a}_h^k - b_h)$. It is a recurrence sequence, and it has order no greater than $N_0^k + n$. On the other hand, by the construction, the $M$ consecutive terms with $h = N,\ N+1, \ldots, N+M-1$ vanish. But it is easy to verify that a recurrence sequence of order less than $M$ with $M$ consecutive zero terms is identically zero. Thus, if we chose, as we may have, $M > N^k + n$, then $\mathfrak{a}_h^k = b_n$ for all $h = N - N_0,\ N - N_0 + 1, \ldots$. Hence there is no loss of generality in supposing that $\mathfrak{a}_h = a_h$ for all $h = 0, 1, 2, \ldots$ and then we have lifted our results in algebraic number fields back into arbitrary fields $\mathbb{F}$ of characteristic zero.

## 7. Summary

In this paper we have been dealing with the (Generalised Pisot $k$th root conjecture). *Let*

$$f(X) = \sum_{h \geqslant 0} b_h X^h$$

*be the Taylor series of a rational function defined over a field of characteristic zero, and suppose there is a sequence $(a'_h)$ of elements of a finitely generated extension field $\mathbb{F}$ of $\mathbb{Q}$ such that $a_h'^k = b_h$, $h = 0, 1, 2, 3, \ldots$, for some given positive integer $k$. Then there is a sequence $(a_h)$ with $a_h^k = b_h$, $h = 0, 1, 2, \ldots$, so that $\sum_{h>0} a_h X^h$ is a rational function.*

https://doi.org/10.1017/S144678870002961X Published online by Cambridge University Press

Let the distinct poles of $f(X)$ be $\beta_1^{-1}, \ldots, \beta_m^{-1}$. Combining the results we have obtained in the sections above we have the following theorems.

THEOREM 1. *Pisot's kth root conjecture is true if $f(X)$ is defined over a number field and there is some place of that number field at which $f(X)$ has a unique pole (of arbitrary multiplicity) of maximum, or of minimum absolute value.*

THEOREM 2. *Pisot's kth root conjecture is true for arbitrary rational functions if it is true for rational functions defined over a number field and with all poles of multiplicity* 1.

(Equivalently, in terms of recurrence sequences: *the conjecture is true if true for recurrence sequences with constant coefficients and with algebraic roots.*)

PROOF. There is a polynomial

$$s(X) = \prod_{i=1} (1 - \beta_i X)^{n_i} = 1 - s_1 X - \cdots - s_n X^n$$

so that $s(X)(\sum_{h \geqslant 0} b_h X^h)$ is a polynomial, implying that

$$b_{h+n} - (s_1 b_{h+n-1} + \cdots + s_n b_n) = 0$$

for $h = M, M+1, \ldots$ some $M \geqslant 0$. Plainly we lose no generality in subtracting a polynomial of degree $M-1$ from the given rational function and then multiplying by $X^{-M}$; so we may suppose $M = 0$. We are then in the situation discussed in Sections 3, 4 and 5.

Theorem 2 is a direct consequence of the arguments in Sections 5 and 6.

## 8. Remarks

Our constraint, whereby we require a unique minimal, or maximal pole seems unnatural. Nevertheless, the presence of a unique term, which is a $k$th power, is vital in Proposition 1 in order that we obtain a well-defined $k$th root. This suggests the following plan of attack so as to obtain an unconditional result. Suppose that

$$b(h) = \sum_{i=1}^{m} B_i(h) \beta_i^h$$

take values in $\mathbb{F}^k$. Then for any valuation $|\ |$ of $\mathbb{F}$, suppose $|\beta_i| = |\beta_2| = \cdots = |\beta_{m'}| > \cdots \geqslant |\beta_m|$ so that we have a set of maximal terms. It *seems* plain that the maximal subsum

$$\sum_{i=1}^{m'} B_i(h) \beta_i^h$$

https://doi.org/10.1017/S144678870002961X Published online by Cambridge University Press

is a $k$th power; that is, that it takes values in $\mathbb{F}_1^k$ (with $\mathbb{F}_1$ some finite extension of $\mathbb{F}$). We cannot show this. It does seem worth remarking that were we able to show that such a maximal subsum takes values in $\mathbb{F}_1^k$ then we could show it to be a $k$th power; in effect by descent on $m$.

We have also been unable to so generalise Proposition 1 as to deal with a maximal subsum of more than one term a priori known to be a $k$th power. These remarks suggest that a quite different line should be taken so as to attain an unconditional result.

On the other hand, we have shown that to prove the $k$th root conjecture it suffices to consider just the case of constant coefficients and just the 'algebraic case', where the data is provided over a number field. These simplifications may contribute to an eventual unconditional proof.

## References

[1] E. Artin and J. Tate, *Class field theory* (Harvard University).
[2] Benali Benzaghou, 'Algèbres de Hadamard', *Bull. Soc. Math. France* **98** (1970), 209–252.
[3] J.-P. Bézivin, 'Factorisation de suites récurrentes linéaires', *Groupe d'étude d'analyse ultramétrique* (*Amice-Barsky-Robba*) 1979–81 exposé 33, pp. 6–9 (Institut Henri Poincaré, Paris).
[4] J.-P. Bézivin, 'Factorisation de suites récurrentes linéaires et applications', *Bull. Soc. Math. France* **112** (1984), 365–376.
[5] E. Bombieri, 'On $G$-functions', *Recent progress in analytic number theory*, Vol. 2, edited by H. Halberstam and C. Hooley, pp. 1–67 (Academic Press, London, 1981).
[6] David G. Cantor, 'On arithmetic properties of the Taylor series of rational functions II', *Pacific J. Math.* **41** (1972), 329–334.
[7] A. Perelli and U. Zannier, 'Arithmetic properties of certain recurrence sequences', *J. Austral. Math. Soc.* (*Ser. A*) **37** (1984), 4–16.
[8] Charles Pisot, *Conférences donnees à l'Institut Fourier de Grenoble*, (1959).
[9] Robert S. Rumely and A. J. van der Poorten, 'Remarks on generalised power sums', *Bull. Austral. Math. Soc.*
[10] Raphael Salem, *Algebraic numbers and Fourier analysis*, (Heath, Boston, Mass., 1962).
[11] A. J. van der Poorten, 'Some problems of recurrent interest', *Colloq. Math. Soc. János Bolyai* **34** *Topics in classical number theory*, 1265–1294.

Department of Mathematics
University of Georgia
Athens, Georgia 30602
U.S.A.

School of Mathematics and Physics
Macquarie University
North Ryde, N.S.W. 2113
Australia